



Estratto del verbale della seduta del

Auszug aus dem Protokoll der Sitzung
vom

18.12.2024

DELIBERAZIONE N.

BESCHLUSS Nr.

240

Oggetto:

Betreff:

Approvazione del “Modello organizzativo privacy - (MOP)” della Regione Autonoma Trentino-Alto Adige/Südtirol

Genehmigung des Organisationsmodells für den Datenschutz der Autonomen Region Trentino-Südtirol

Arno Kompatscher	Presidente / Präsident	presente/anwesend
Giulia Zanotelli	Vice Presidente sostituta del Presidente / Vizepräsidentin-Stellvertreterin des Präsidenten	presente/anwesend
Franz Thomas Locher	Vice Presidente / Vizepräsident	presente/anwesend
Carlo Daldoss	Assessore / Assessor	presente/anwesend
Angelo Gennaccaro	Assessore / Assessor	presente/anwesend
Luca Guglielmi	Assessore / Assessor	presente/anwesend
Gabriele Morandell	Segretaria generale della Giunta regionale / Generalsekretärin der Regionalregierung	presente/anwesend

Su proposta del Presidente Arno
Kompatscher

Auf Vorschlag des Präsidenten Arno
Kompatscher

Segreteria generale

Generalsekretariat der Regionalregierung

Ufficio affari generali

Amt für allgemeine Angelegenheiten

In riferimento all'oggetto la Giunta regionale ha discusso e deliberato quanto segue:

Considerato che al fine di adempiere alle disposizioni previste dal Regolamento (UE) 2016/679 in materia di trattamento dei dati personali, risulta necessario adottare misure adeguate a garanzia della protezione dei dati personali trattati nell'ambito dell'attività dell'amministrazione regionale;

Visto il Decreto Legislativo n. 196/2003, come modificato dal Decreto Legislativo n. 101/2018, relativo al "Codice in materia di protezione dei dati personali";

Verificato che, ai sensi degli articoli 5, 24, 29 e 32 del Regolamento (UE) 2016/679 il Titolare del trattamento ha l'obbligo di adottare specifiche misure organizzative e di impartire istruzioni alle persone che sono autorizzate al trattamento dei dati personali e che ai sensi dell'art. 2-quaterdecies del decreto legislativo n. 196/2003 il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità;

Considerato che, in attuazione dell'articolo 5, paragrafo 2 del Regolamento (UE) 2016/679, il titolare del trattamento è responsabile del rispetto dei principi relativi al trattamento dei dati personali (indicati nel paragrafo 1) e deve essere in grado di dimostrare tale conformità.

Preso atto dell'impegno profuso dall'amministrazione regionale nell'adozione concreta di misure efficaci, in grado di garantire trasparenza, responsabilità e fiducia nel trattamento dei dati personali,

Die Regionalregierung hat über die oben genannte Angelegenheit beraten und Folgendes beschlossen:

In Anbetracht der Tatsache, dass zur Erfüllung der Bestimmungen laut der Verordnung (EU) 2016/679 betreffend die Verarbeitung personenbezogener Daten Maßnahmen zur Gewährleistung des Schutzes der im Rahmen der Tätigkeit der Regionalverwaltung verarbeiteten personenbezogenen Daten zu ergreifen sind;

Aufgrund des gesetzesvertretenden Dekrets Nr. 196/2003 „Datenschutzkodex“, geändert durch das gesetzesvertretende Dekret Nr. 101/2018;

Nach Feststellung der Tatsache, dass gemäß Art. 5, 24, 29 und 32 der Verordnung (EU) 2016/679 der Verantwortliche für die Datenverarbeitung verpflichtet ist, besondere organisatorische Maßnahmen zu treffen und den Personen, die zur Verarbeitung personenbezogener Daten befugt sind, Anweisungen zu erteilen, und dass laut Art. 2-quaterdecies des gesetzesvertretenden Dekrets Nr. 196/2003 der Verantwortliche oder der Auftragsverarbeiter in eigener Verantwortung und innerhalb seiner Organisationsstruktur vorsehen kann, dass bestimmte Aufgaben und Befugnisse im Zusammenhang mit der Verarbeitung personenbezogener Daten ausdrücklich bestimmten natürlichen Personen übertragen werden, die ihm unterstellt sind;

In Anbetracht der Tatsache, dass in Umsetzung des Art. 5 Abs. 2 der Verordnung (EU) 2016/679 der Verantwortliche für die Datenverarbeitung für die Einhaltung der (im Abs. 1 aufgelisteten) Grundsätze für die Verarbeitung personenbezogener Daten verantwortlich ist und deren Einhaltung nachweisen können muss;

Nach Kenntnisnahme der Bemühungen der Regionalverwaltung um das Ergreifen effektiver Maßnahmen zur Gewährleistung der Transparenz, des Verantwortungssinnes und des Vertrauens bei der Verarbeitung

attraverso la redazione e diffusione di circolari, procedure e prassi operative, destinate a tutte le strutture appartenenti all'amministrazione regionale.

Ritenuto necessario raccogliere tutta la documentazione elaborata in materia in un manuale operativo denominato "Modello Organizzativo Privacy – MOP" che raggruppa in maniera organica tutte le procedure adottate dall'amministrazione regionale in attuazione del principio di *accountability* sancito nel GDPR;

Visto il Decreto del Presidente della Regione Autonoma Trentino-Alto Adige/Südtirol del 7 dicembre 2022 n. 27 concernente la "Determinazione delle attribuzioni delle strutture organizzative regionali e delle loro articolazioni" ai sensi dell'art. 2, comma 1, della legge regionale 21 luglio 2000, n. 3";

Tutto quanto sopra premesso e considerato;

Ad unanimità di voti legalmente espressi,

delibera

1. di approvare il documento denominato "Modello Organizzativo Privacy - (MOP)" che unito al presente provvedimento ne forma parte integrante e sostanziale;
2. di incaricare la Segreteria generale – Ufficio affari generali alla diffusione a tutte le strutture organizzative della Regione Autonoma Trentino-Alto Adige/Südtirol, chiedendone l'osservanza da parte di tutti i dipendenti, collaboratori e soggetti che a vario titolo trattano dati personali per conto dell'amministrazione regionale;

personenbezogener Daten durch die Ausarbeitung und Verbreitung von Rundschreiben, Verfahren und Vorgehensweisen, die für alle Organisationsstrukturen der Regionalverwaltung bestimmt sind;

Nach Dafürhalten, sämtliche auf diesem Sachgebiet ausgearbeiteten Unterlagen in einem Handbuch („Organisationsmodell für den Datenschutz“) zu sammeln, das alle von der Regionalverwaltung in Umsetzung des in der DSGVO verankerten Grundsatzes der Rechenschaftspflicht angewandten Verfahren übersichtlich umfasst;

Aufgrund des Dekrets des Präsidenten der Autonomen Region Trentino-Südtirol vom 7. Dezember 2022, Nr. 27 „Festsetzung der Befugnisse der Organisationsstrukturen der Region und deren Gliederungen“ im Sinne des Art. 2 Abs. 1 des Regionalgesetzes vom 21. Juli 2000, Nr. 3;

All dies vorausgeschickt und berücksichtigt,

**beschließt
die Regionalregierung**

mit Einhelligkeit gesetzmäßig abgegebener Stimmen,

1. das Handbuch „Organisationsmodell für den Datenschutz“, das diesem Beschluss als ergänzender und wesentlicher Bestandteil beiliegt, zu genehmigen;
2. das Generalsekretariat – Amt für allgemeine Angelegenheiten mit der Übermittlung des genannten Handbuchs an sämtliche Organisationsstrukturen der Autonomen Region Trentino-Südtirol zu beauftragen, wobei alle Bediensteten, Mitarbeiter und Rechtssubjekte, die im Auftrag der Regionalverwaltung auf unterschiedliche Weise personenbezogene Daten verarbeiten, aufgefordert werden, es zu befolgen;

3. di prevedere revisione periodica del presente manuale per garantirne l'adeguamento all'evoluzione normativa e alle *best practises* in materia di protezione di dati personali.

3. die regelmäßige Revision des Handbuchs vorzusehen, um sicherzustellen, dass es mit der Entwicklung der Rechtsvorschriften und mit den bewährten Verfahren betreffend den Schutz personenbezogener Daten Schritt hält.

Letto, confermato e sottoscritto.

Gelesen, bestätigt und unterzeichnet

IL PRESIDENTE

LA SEGRETARIA GENERALE
DELLA GIUNTA REGIONALE

DER PRÄSIDENT

DIE GENERALSEKRETÄRIN DER
REGIONALREGIERUNG

Arno Kompatscher

firmato digitalmente / digital signiert

Gabriele Morandell

firmato digitalmente / digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Dokument in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

MODELLO ORGANIZZATIVO PRIVACY MOP

N. versione	Atto di approvazione	Principali modifiche	Validità/Cessazione
1		Prima redazione	



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

PRIMA PARTE MODELLO ORGANIZZATIVO PRIVACY SOMMARIO

1	INTRODUZIONE E CAMPO DI APPLICAZIONE.....	6
2	RIFERIMENTI NORMATIVI.....	6
3	DEFINIZIONI	7
4	DATO PERSONALE E TIPOLOGIE DI DATO PERSONALE	9
5	TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI.....	9
6	DATI IDONEI A RIVELARE LO STATO DI SALUTE	9
7	TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI.....	10
8	ATTIVITÀ, ORGANIZZAZIONE E SOGGETTI DIRETTAMENTE COINVOLTI.....	10
8.1	TITOLARE DEL TRATTAMENTO	10
8.2	CONTITOLARE DEL TRATTAMENTO.....	11
8.3	SOGGETTI AUTORIZZATI AL TRATTAMENTO	11
8.4	RESPONSABILI DEL TRATTAMENTO.....	12
8.5	AMMINISTRATORE DI SISTEMA.....	13
8.6	LA FIGURA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)	13
9	REGISTRO DI ATTIVITÀ DI TRATTAMENTO DEI DATI, BASE GIURIDICA E CONSENSO AL TRATTAMENTO DEI DATI.....	16
9.1	REGISTRO DEI TRATTAMENTI E TRATTAMENTI.....	16
9.2	DEFINIZIONE DI BASE GIURIDICA E CONSENSO AL TRATTAMENTO	16
10	TRATTAMENTO, COMUNICAZIONE E DIFFUSIONE DI DATI COMUNI.....	17
11	TRATTAMENTO, COMUNICAZIONE E DIFFUSIONE DI DATI PARTICOLARI.....	18
12	TRATTAMENTO, COMUNICAZIONE E DIFFUSIONE DI DATI GIUDIZIARI	18
13	MISURE MINIME DI SICUREZZA ICT	18
14	ARCHIVI CARTACEI E ACCESSO AGLI UFFICI.....	19
15	DATA BREACH.....	20
16	TRASFERIMENTI DI DATI A PAESI EXTRA UE.	20
16.1	TRASFERIMENTO DI DATI PERSONALI	20
17	VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA).....	21
18	UN APPROFONDIMENTO: LA CONSULTAZIONE DEL GARANTE SUGLI ATTI NORMATIVI DELLA REGIONE	22
19	INDICAZIONI IN MATERIA DI PUBBLICAZIONI SUL SITO INTERNET DELLA REGIONE E IN AMMINISTRAZIONE TRASPARENTE	22
20	MISURE DI SICUREZZA PER LO SVOLGIMENTO DI VIDEOCONFERENZE	24



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

21	INDICAZIONI IN MATERIA DI DIRITTO DI ACCESSO.....	24
22	FORMAZIONE ED INFORMAZIONE INTERNA.....	25
23	STRUMENTI PER IL MONITORAGGIO E CONTROLLO DELL'ACCOUNTABILITY DELLA REGIONE	25
24	RESPONSABILITÀ E SANZIONI	26



PARTE SECONDA MODELLO ORGANIZZATIVO PRIVACY ALLEGATI E DOCUMENTAZIONE PRIVACY A DISPOSIZIONE DEI COLLABORATORI

ALLEGATI

- 1) VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI SULLA VIDEOSORVEGLIANZA
- 2) VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI NEL TRATTAMENTO DI DATI PERSONALI, UFFICIO ISPETTIVO E SVILUPPO DEL PERSONALE
- 3) MODELLI DIVERSI:
 - 3.1 REGISTRI DEL TRATTAMENTO DEI DATI
 - 3.2 NOMINA DEL RESPONSABILE DELLA PROTEZIONE DATI
 - 3.3 NOMINA DEI RESPONSABILI DEL TRATTAMENTO DATI
 - 3.4 INFORMATIVA ESTESA E BREVE SULLA PRIVACY
- 4) PIANO PERIODICO DI VERIFICA DELLE MISURE ADOTTATE (generale per la struttura competente, particolare per ogni ufficio)
- 5) ELENCO DEI DOCUMENTI E DELLE CIRCOLARI IN MATERIA DI ADEMPIMENTO DI PRIVACY
 - 5.1 circolare n. 05/2023
 - 5.2 Circolare/Rundschreiben n. 12 -29/06/2023 - Esito audit dd. 05/06/2023 del RPD ed indicazioni in materia di privacy
 - 5.3 Circolare n. 29 del 2022 – Introduzione della segnatura permanente sui documenti repertoriati e protocollati in uscita
 - 5.4 Circolare del Consorzio dei Comuni Trentini del 2020 - Servizio privacy RPD – Approfondimento in merito alla figura del Titolare del trattamento e del Responsabile del trattamento alla luce di alcune nuove pronunce delle Autorità competenti (id. 11989712/2020)
 - 5.5 Circolare interna avente ad oggetto Oggetto: Aggiornamento del registro dei trattamenti e nomina dei soggetti autorizzati (incaricati) ai sensi dell'art. 4. par. 1, n. 10, in combinato disposto con l'art. 29 del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679. (Id: 15035688 / 2021)
 - 5.6 Circolare n. 11 del 2018 avente ad oggetto gestione delle istanze di accesso civico generalizzato, accesso civico (semplice), accesso documentale, tramite il sistema P.I.Tre. e registro degli accessi civici generalizzati
- 6) PUBBLICAZIONI SUL SITO: disposizioni in materia e suggerimenti tecnico operativi del servizio privacy RPD.
- 7) PROCEDURE WHISTLEBLOWING: indicazioni operative e valutazione di impatto del servizio.
- 8) NOMINA AMMINISTRATORE DI SISTEMA
- 9) DISCIPLINARE UTILIZZO STRUMENTI ELETTRONICI: Deliberazione della Giunta regionale n. 237 del 31.10.2019, avente



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

ad oggetto “Disciplinare per l'utilizzo dei dispositivi elettronici della Regione Autonoma Trentino-Alto Adige/Südtirol”

- 10) TRASFERIMENTO DI DATI ALL'ESTERO: approfondimento normative con circolare trasmessa dal servizio RPD dd. 16.10.2023;
- 11) INDICAZIONI PRIVACY PER UFFICI CENTRALI E UFFICI DEL GDP: circolare contenente ulteriori indicazioni in materia di privacy per gli uffici della sede centrale per gli uffici del Giudice di Pace, identificate da comunicazione dd. 05.09.2023 prot. N. 23924 e comunicazione dd. 06.10.2022 prot. N. 23830.
- 12) RIPARTIZIONE DELLE COMPETENZE: deliberazione della Giunta regionale n. 91 del 26.05.2021, avente ad oggetto “Determinazione delle competenze da riserva alla Giunta, alle Dirigenti ed ai Dirigenti, alle Direttrici ed ai Direttori degli Uffici”
- 13) CIRCOLARE DEL SULLA CONTITOLARITÀ DEL TRATTAMENTO DEI DATI PERSONALI
- 14) ALLEGATI N. 1 E N. 2 Sottosezione 2.3. Rischi corruttivi e trasparenza del PIAO 2024 – 2026
- 15) Trasparenza legge 13/1993 – L.R. 10/2014 e s.m. – Regolamento 16/11/2014 n. 7/L
- 16) Regolamento delle sedute di Giunta regionale
- 17) Circolare n. 17 del 24.08.2022 avente ad oggetto: “Disposizioni per la prestazione del lavoro in modalità agile”
- 18) Deliberazione della Giunta regionale n. 232 del 04/12/2024: “Sistema di tutela dei dati personali della Regione Autonoma Trentino-Alto Adige/Südtirol. Revisione e aggiornamento procedura data breach introdotta con deliberazione di Giunta regionale n. 193 del 3 settembre 2019”



INTRODUZIONE E CAMPO DI APPLICAZIONE

Il presente manuale operativo in materia di privacy è finalizzato a definire e raccogliere un insieme di procedure e buone pratiche per la corretta implementazione dei principi della privacy e la tutela dei dati personali sanciti dal GDPR, Regolamento Europeo 679/2016, e dal Codice della Privacy, dlgs 196/2003 così come modificato dal dlgs 101/2018. Il **Modello organizzativo privacy (MOP)** che si presenta, è composto da due parti:

- una prima parte “teorica”, ovvero descrittiva e riepilogativa dei principali elementi della normativa in materia di privacy, con qualche breve approfondimento;
- una seconda parte “pratica”, ovvero una raccolta di tutte le pratiche – regolamenti, procedure e circolari emesse nel tempo – in vigore ed applicati nell’amministrazione regionale

La corretta implementazione ed utilizzo delle procedure illustrate nella seconda parte del presente Manuale consente di rispondere nella maniera più efficace ed efficiente agli obblighi di legge previsti e a cui, in caso di sopralluogo da parte dell’autorità Garante, deve rispondere il Titolare del trattamento dei dati dell’amministrazione regionale.

I soggetti che trattano dati sono tenuti all’applicazione delle disposizioni in materia di privacy ogni qualvolta vengano eseguite azioni di raccolta, inserimento, cancellazione, modifica, elaborazione e custodia di informazioni relative a persone fisiche identificate o identificabili per finalità diverse da quelle strettamente private. Le procedure si applicano sia ai dati detenuti in formato cartaceo sia a quelli detenuti in formato digitale.

Il Manuale è approvato con deliberazione della Giunta regionale e viene periodicamente revisionato ed aggiornato (in particolar modo per la seconda parte) con le procedure via via adottate.

RIFERIMENTI NORMATIVI

Il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo ai sensi della Carta dei diritti fondamentali dell'Unione europea (art. 8). Oggi è tutelato, in particolare, dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). In ambito nazionale il diritto alla protezione dei dati personali è tutelato, dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), adeguato alle disposizioni del Regolamento (UE) 2016/679 tramite il Decreto legislativo 10 agosto 2018, n. 101. La sorveglianza della corretta applicazione delle disposizioni in materia di privacy è affidata ad un’autorità di controllo indipendente denominate “Garante per la protezione dei dati personali” la quale, tra gli altri compiti, adotta Provvedimenti e Linee guida. Si invita a consultare il sito istituzionale dell’autorità, raggiungibile tramite il link <https://www.garanteprivacy.it>, per ulteriori



approfondimenti.

DEFINIZIONI

Si riportano le definizioni maggiormente utilizzate come definite dall'art. 4 del GRPR:

- **«dato personale»:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
- **«trattamento»:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- **«limitazione di trattamento»:** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- **«profilazione»:** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
- **«pseudonimizzazione»:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
- **«archivio»:** qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
- **«titolare del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

- **«responsabile del trattamento»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **«destinatario»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- **«terzo»:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **«consenso dell'interessato»:** qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
- **«violazione dei dati personali»:** la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
- **«dati genetici»:** i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **«dati biometrici»:** i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **«dati relativi alla salute»:** i dati personali attinenti alla salute fisica o mentale di



una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

DATO PERSONALE E TIPOLOGIE DI DATO PERSONALE

Il Garante, definisce **dati personali** le informazioni che identificano o rendono identificabile, direttamente o indirettamente una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc...

Dal punto di vista della tipologia di informazione o del supporto usato, il concetto di dato personale comprende qualunque tipologia di informazione, che può essere disponibile in qualunque forma, alfabetica, numerica, grafica, fotografica o acustica, le informazioni registrate su carta e quelle conservate nella memoria di un computer attraverso un codice binario o in una videocassetta. In maniera aggiuntiva, sono stati via via qualificati dal Garante come dati personali:

- ✓ la registrazione della voce di un soggetto (ad es. le chiamate registrate dal 118);
- ✓ le immagini filmate da un impianto di videosorveglianza, nella misura in cui i singoli individui siano riconoscibili;
- ✓ l'indirizzo IP di posta elettronica;
- ✓ l'impronta digitale, ovvero un dato biometrico, che è dato personale in quanto identifica una persona (laddove i campioni di tessuto dai quali si estraggono i dati biometrici non sono di per sé dati personali, anche se le operazioni effettuate per estrarre tali informazioni biometriche configurano già un trattamento di dati personali).
- ✓ il numero di matricola, collegato ai dati personali di un collaboratore.

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

Le categorie particolari di dati personali, conosciuti con il nome di “sensibili” riguardano qualificazioni del soggetto nella sfera della razza, del pensiero, della salute e della vita sessuale. Precisamente, la legge definisce dati sensibili i dati personali idonei a rivelare: l'origine razziale ed etnica; le convinzioni religiose, filosofiche o di altro genere (ad es. morali in senso lato); le opinioni politiche; l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale. il Regolamento UE 2016/679 (articolo 9), ha incluso nella nozione anche i dati genetici, i dati biometrici e quelli relativi all'orientamento sessuale.

DATI IDONEI A RIVELARE LO STATO DI SALUTE

Si definiscono dati idonei a rivelare lo stato di salute, l'insieme delle informazioni tali da poter svelare, direttamente ma anche indirettamente, uno stato patologico o comunque uno stato di compromissione dello stato fisico, psichico e relazionale dell'individuo, anche pregresso o potenziale, ivi comprese le informazioni, anche meramente amministrative, connesse alla effettuazione di accertamenti sullo stato di



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

salute, nonché quelle relative a condizioni o situazioni che possano determinare uno stato in senso lato patologico o abbiano questo quale possibile presupposto.

Il Codice tutela i dati personali idonei a rivelare lo stato di salute dell'interessato. Il concetto di idoneità alla rivelazione dello stato di salute ricomprende le informazioni che permettono di avere un'idea, anche generale e comunque non necessariamente specifica, diretta come anche indiretta, delle condizioni di salute di un individuo.

Attenzione!!! Nell'amministrazione regionale possiamo, in particolar modo, trovare questa tipologia di dati nella gestione del fascicolo personale: è opportuno pertanto prestare attenzione al loro trattamento e soprattutto prestare attenzione alla divulgazione involontaria delle stesse (ad es. al telefono)

TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

I dati giudiziari (articolo 10 del Regolamento UE 2016/679) sono le tipologie di dati relativi a condanne penali e reati. Questa tipologia di dati possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Attenzione!!! Anche l'amministrazione regionale può trovarsi a trattare tali tipologie di dati in diverse situazioni, come ad esempio la gestione amministrativa di procedimenti penali a carico di dipendenti, oppure la gestione di certificazioni antimafia nell'ambito delle procedure di appalto. Per i dati giudiziari, si ricorda che sono previsti requisiti e modalità di trattamento analoghi a quelli per i dati sensibili, ovvero non possono essere comunicati a terzi, anche involontariamente.

ATTIVITÀ, ORGANIZZAZIONE E SOGGETTI DIRETTAMENTE COINVOLTI

TITOLARE DEL TRATTAMENTO

È all'amministrazione regionale, quale Titolare del trattamento, e non alle sue singole articolazioni organizzative e di responsabilità, che spetta il compito di operare le scelte di fondo sulle finalità, modalità, strumenti, inerenti al trattamento dei dati. Le finalità istituzionali perseguite dall'amministrazione regionale, che sono pertanto trasferite operativamente in carico ai responsabili interni (i/le Dirigenti/e e i/le Segretari/e particolari) del Trattamento dei dati, rendono legittimi i trattamenti da e per esso effettuati. La titolarità da parte dell'amministrazione regionale dei dati che essa tratta per le proprie finalità istituzionali, comporta tra l'altro che gli autorizzati al trattamento non possano farne uso per propri scopi personali, anche se in astratto legittimi (ad es. in ambito di contenzioso), senza autorizzazione. Inoltre al Titolare compete la nomina e l'individuazione dei soggetti autorizzati al trattamento impartendo loro le necessarie istruzioni per la corretta gestione e tutela dei dati



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

personali, ivi compresa la salvaguardia della loro integrità e sicurezza, e verificando periodicamente l'attività svolta rispetto alle istruzioni impartite.

Attenzione !!! Nell'amministrazione regionale le indicazioni sopra illustrate sono declinate ampiamente all'interno della deliberazione della Giunta regionale n. 193 del 03.09.2019.

CONTITOLARE DEL TRATTAMENTO

Per un determinato trattamento dati può essere configurata una situazione di contitolarità. Essa deve essere ricondotta ad una comunanza nella possibilità di determinare finalità e modalità del trattamento, derivante dalla compartecipazione finale agli interessi in vista dei quali il trattamento è predisposto. È una condizione che attualmente si trova spesso correlata a progetti di interesse interistituzionale o interaziendale. In questo caso si fa riferimento all'art. 26 del GDPR.

SOGGETTI AUTORIZZATI AL TRATTAMENTO

In seguito alla modificazioni di alcune parti del GDPR, le definizioni di "*responsabile interno*" e "*incaricato*" non sono più esplicitamente previste. L'art. 29 del GDPR menziona "*chiunque agisca sotto l'autorità del titolare o del responsabile (nota: quest'ultimo inteso come responsabile esterno all'amministrazione)*".

Il soggetto delegato dal Titolare a svolgere compiti specifici (che per chiarezza chiameremo come in passato Responsabile del trattamento) è colui che, in ragione delle proprie competenze, dell'incarico ricevuto e delle mansioni esercitate, sovrintende alle varie attività controllandone la corretta esecuzione ed esercitando un funzionale potere di iniziativa, anche svolgendo i compiti in materia di protezione dei dati personali funzionalmente correlati a quelle attività. Al Responsabile del trattamento si richiede di individuare in generale, in riferimento ai trattamenti di competenza ed in collaborazione attiva con il Titolare e con il Referente privacy, adeguate misure organizzative e gestionali. La responsabilità del trattamento è dunque in primo luogo una responsabilità di carattere organizzativo, diretta ad assicurare a tutti i soggetti interessati dei quali vengano trattati i dati, il diritto alla riservatezza ed alla protezione dei dati personali, attraverso:

- l'assegnazione di compiti e mansioni agli incaricati, che, qualora debbano essere effettuati con l'utilizzo di strumenti informatici, richiedono anche la definizione di una loro adeguata profilazione;
- la diramazione di istruzioni da seguire, anche di dettaglio rispetto a quelle individuate dal Titolare, ed una attività di verifica circa loro effettiva applicazione;

Attenzione!!! La deliberazione della Giunta regionale n. 193 del 03.09.2019 individua, quali Responsabili interni preposti al trattamento di dati personali per le materie e gli ambiti di rispettiva competenza, le/i singole/i Dirigenti delle strutture organizzative regionali e le/i Segretarie/i particolari dei componenti della Giunta



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

regionale. Inoltre, nomina il/la Segretario/a generale, in virtù delle proprie competenze, Referente privacy e responsabile della comunicazione dell'eventuale violazione di dati personali (data breach).

Le/i Dirigenti e le/i Segretari particolari nominano, a loro volta, i soggetti autorizzati al trattamento. Sono pertanto coloro che materialmente effettuano operazioni di trattamento di dati, attenendosi alle istruzioni impartite.

L'individuazione dei soggetti autorizzati deve essere effettuata quindi per iscritto ed individuare puntualmente l'ambito del trattamento consentito. L'ambito di trattamento consentito ai singoli soggetti autorizzati attraverso i sistemi informatici si traduce nella definizione di idonei profili di accesso ai sistemi (profili di autorizzazione), da individuarsi anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento, evitando così di incorrere nel rischio di eccesso di autorizzazioni non necessarie.

Attenzione!!! Nell'amministrazione regionale, è prassi consolidata provvedere ad attribuire ogni incarico e autorizzazione in maniera anticipata rispetta alla presa di servizio del collaboratore. La redazione della documentazione necessaria per l'attivazione di un nuovo profilo informatico, come per la chiusura e/o variazione dello stesso, avviene seguendo le indicazioni suggerite nel documento di prot. n. 23830/2022 ed intitolato "*Ulteriori disposizioni organizzative in materia di privacy*" ed allegato nella parte seconda del presente manuale.

RESPONSABILI DEL TRATTAMENTO

Il regolamento europeo all'art. 28 definisce il responsabile esterno del trattamento dati come la persona fisica o giuridica, autorità pubblica o organismo che effettua un trattamento per conto del Titolare del trattamento. In base al GDPR, invero, Responsabile e Titolare hanno compiti e doveri molto simili, ma non coincidenti.

La nomina del Responsabile di Trattamento è un atto obbligatorio quando si deve autorizzare un soggetto esterno a trattare i dati personali raccolti dal titolare del trattamento. Si ricorda che il Titolare è chi decide quali dati personali raccogliere e per quale motivo. Il **responsabile esterno del trattamento** quindi deve essere nominato per iscritto con un atto di nomina o deve essere nominato con contratto, cioè con un atto che vincola il responsabile del trattamento al titolare. Nell'ambito della materia di protezione dati, agire "per conto di" significa che il responsabile del trattamento non può effettuare trattamenti per proprie finalità: gli obiettivi da raggiungere e i mezzi da utilizzare devono essere sempre (e solo) stabiliti dal titolare del trattamento.

In questa sede risulta opportuno ricordare che la mancata nomina per iscritto del Responsabile esterno del trattamento dei dati, è motivo di sanzione da parte dell'autorità del Garante.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Inoltre, rientra tra gli obblighi del Titolare dei dati il controllo periodico del Responsabile esterno del trattamento dei dati da parte del Titolare. Il GDPR non prevede una cadenza specifica delle verifiche: il Titolare deve dimostrare periodicamente una verifica dell'adeguatezza o meno dell'incarico affidato al Responsabile esterno.

Attenzione!!! La deliberazione della Giunta regionale n. 193 del 03.09.2019, ai punti 5 e 6 del deliberato demanda proprio alle/ai singole/i Dirigenti l'aggiornamento della rilevazione delle fattispecie per le quali l'amministrazione regionale debba designare i responsabili esterni del trattamento ai sensi dell'art. 28 del GDPR. Conseguentemente è in capo alle/ai singole/i Dirigenti il perfezionamento del contratto/atto richiesto dal citato art. 28, con riguardo alle fattispecie dagli stessi individuate, nonché le modalità e i tempi di verifica dell'operato del Responsabile esterno del trattamento dei dati.

AMMINISTRATORE DI SISTEMA

La nozione di **amministratore di sistema** è estremamente ampia, e comprende anche attività non di esclusiva competenza di tecnici informatici (ad es. la mera gestione dei sistemi di autenticazione e di autorizzazione). All'amministratore di sistema sono affidati delicati compiti quali l'implementazione dei sistemi di sicurezza e la definizione di delle procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte degli utenti, la cura degli interventi di conservazione dei dati attraverso soluzioni di back up e la progettazione delle attività di supporto al disaster recovery. Di norma, secondo il Garante, l'amministratore di sistema è assunto quale figura professionale dedicata in senso lato alla gestione e alla manutenzione di impianti di elaborazione (compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza) con cui vengano effettuati trattamenti di dati personali, e nella misura in cui consentano di intervenire sui dati personali. Ne consegue che le funzioni che l'amministratore di sistema assolve implicano la capacità dello stesso di accedere in modo privilegiato alla totalità dei dati personali dell'amministrazione regionale.

L'individuazione, l'autorizzazione e il controllo dei soggetti idonei a svolgere le mansioni di amministratore di sistema sono fondamentali per la protezione dei dati personali di cui l'amministrazione regionale è depositaria. Ne consegue quindi che l'operato dell'amministratore di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali. Infine, quando un amministratore di sistema è nominato in outsourcing, cioè esterno all'azienda, questo deve essere considerato un responsabile del trattamento, e pertanto, in considerazione di ciò, il Titolare dovrà vincolare l'amministratore di sistema con un contratto scritto, contenente tutti i requisiti richiesti dall'art. 28 Reg. UE 216/679.

LA FIGURA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD)

In base all'articolo 37, paragrafo 7, del Regolamento UE 2016/679, è necessario che



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

i soggetti pubblici comunichino al Garante per la protezione dei dati personali il nominativo del Responsabile della Protezione dei dati (in inglese Data Protection Officer DPO),. Inoltre, si ricorda, infatti, che in base all'articolo 39, paragrafo 1, lettera e) del Regolamento, il Responsabile della Protezione dei Dati funge da punto di contatto fra il singolo ente o azienda e il Garante. L'RPD è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti. Egli può essere un dipendente del titolare del trattamento, qualora si rilevi adeguata figura professionale tra i propri collaboratori, o un soggetto esterno, dotato di specifiche competenze e requisiti professionali, che assolve i compiti in materia di privacy, in base a un contratto di servizio.

Attenzione!!! L'amministrazione regionale ha affidato, per il triennio 2025-2027, il servizio di RPD/DPO alla ditta Dream S.r.l. Si ricorda che è possibile sottoporre i quesiti in questa materia al referente, per il tramite dell'Ufficio affari generali.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

SCHEMA RIASSUNTIVO DELLE FIGURE

FIGURA PREVISTA DAL REGOLAMENTO UE 679/2016	ART. REG. UE 679/2016	FIGURA DI RIFERIMENTO NELL'AMMINISTRAZIONE REGIONALE
TITOLARE DEL TRATTAMENTO DEI DATI	ART. 4, PAR. 1, N.7	LA GIUNTA O IL PRESIDENTE QUALE LEGALE RAPPRESENTANTE
RESPONSABILE DEL TRATTAMENTO	ART. 4, PAR. 1 N. 8	DIRIGENTE DI RIPARTIZIONE / SEGRETARIO PARTICOLARE DELL'ASSESSORE
REFERENTE PRIVACY		SEGRETARIO GENERALE
AUTORIZZATI AL TRATTAMENTO	ART. 29 GDPR E ART. 2- QUATERDECIES DEL CODICE	DIPENDENTI DELL'ENTE
AMMINISTRATORE DI SISTEMA	ART. 28	ESTERNO
RPD / DPO	ART. 37	DREAM S.R.L.
RESPONSABILE ESTERNO TRATTAMENTO DATI	ART. 28	DI VOLTA IN VOLTA NOMINATO PER ISCRITTO
CONTITOLARI	ART. 26	INDIVIDUATO DI VOLTA IN VOLTA



REGISTRO DI ATTIVITÀ DI TRATTAMENTO DEI DATI, BASE GIURIDICA E CONSENSO AL TRATTAMENTO DEI DATI

REGISTRO DEI TRATTAMENTI E TRATTAMENTI

Il **Registro dei trattamenti** (articolo 30 del GDPR) è un documento di censimento e analisi dei trattamenti dei dati effettuati dal titolare o responsabile, o dai delegati. In quanto tale, il registro deve essere mantenuto costantemente aggiornato poiché il suo contenuto deve sempre corrispondere all'effettività dei trattamenti posti in essere. Non a caso il registro è anche il primo documento che viene sicuramente richiesto in caso di attività ispettiva da parte del Garante tramite nucleo speciale privacy della Guardia di Finanza.

DEFINIZIONE DI BASE GIURIDICA E CONSENSO AL TRATTAMENTO

Il GDPR prevede che ogni trattamento dei dati deve trovare fondamento in un'ideale **base giuridica**, ovvero ciò che autorizza legalmente il trattamento e che quindi allo stesso soddisfa il principio di liceità previsto dalla normativa. La scelta della base giuridica spetta al Titolare del Trattamento che deve prestare attenzione a scegliere quella più idonea ai propri obiettivi e deve essere indicata nell'informativa privacy. I fondamenti di liceità del trattamento di dati, ovvero della base giuridica del trattamento dei dati personali, sono indicati all'articolo 6 del GDPR. La base giuridica del trattamento dei dati deve essere sempre indicata nell'informativa privacy rivolta agli utenti (art. 13 e 14 del GDPR) e soprattutto deve essere sempre menzionata nel registro delle attività di trattamento dei dati.

Il GDPR, all'articolo 6, elenca le basi giuridiche del trattamento dei dati personali. Esse sono:

- il **consenso** dell'interessato;
- l'adempimento di **obblighi contrattuali** o **misure precontrattuali**;
- gli **obblighi di legge** cui è soggetto il titolare del trattamento;
- gli **interessi vitali** della **persona interessata** o di **terzi**;
- il **legittimo interesse prevalente del titolare** o di **terzi** cui i dati vengono comunicati;
- l'**interesse pubblico** o l'esercizio di **pubblici poteri**.

Attenzione!!!!: è base giuridica, per esempio, anche il bando di concorso emesso ed indicante le modalità di pubblicazione delle graduatorie. A tal fine si rimanda anche alla circolare esplicativa in tal senso rilasciata dal servizio RPD (parte seconda degli allegati)

Il **consenso** è definito dall'art. 4, 11) del GDPR 679/2016, come “qualsiasi



Regione Autonoma
Trentino-Alto Adige/Südtirol

Region Autonoma
Trentin-Südtirol

Autonome Region
Trentino-Südtirol

manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento”.

Il Titolare deve pertanto essere in grado di dimostrare che il consenso prestato dall'interessato è valido. Lo stesso è ritenuto valido se:

- all'interessato è stata resa l'informazione sul trattamento dei dati personali (articoli 13 o 14 del Regolamento, informative in materia di privacy);
- è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse. Il consenso deve essere sempre revocabile.

Infine bisogna prestare attenzione al fatto che la **richiesta di consenso** sia chiaramente distinguibile da altre richieste o dichiarazioni rivolte all'interessato (articolo 7.2). Per esempio all'interno della modulistica, non è ammesso il consenso tacito o presunto (presentando caselle già spuntate su un modulo). Quando il trattamento riguarda le “categorie particolari di dati personali” (articolo 9 GDPR) il consenso deve essere “esplicito”, lo stesso vale per il consenso a decisioni basate su trattamenti automatizzati (compresa la profilazione – articolo 22). Benché non espressamente previsto, ma a maggiore tutela del Titolare, qualora sia necessario dover procedere a richiedere il consenso per il trattamento dei dati, è necessario che si proceda nella forma scritta.

In linea generale il datore di lavoro pubblico – al pari di quello privato – può trattare i dati dei propri dipendenti anche in assenza del loro consenso, perché il trattamento per fini lavorativi ha come propria base giuridica quella prevista dall'art. 6, par. 1, lett. b (esecuzione di un contratto) e/o lett. c (adempimento di un obbligo legale del datore-titolare del trattamento) del GDPR.

TRATTAMENTO, COMUNICAZIONE E DIFFUSIONE DI DATI COMUNI

La base giuridica per il trattamento dei dati personali “comuni”, prevista dall'articolo 6, paragrafo 3, lettera b), del GDPR è costituita esclusivamente da una norma di legge o di regolamento o da atti amministrativi generali (art. 2-ter del Codice).

Il trattamento dei dati comincia dalla fase della raccolta delle informazioni e non si limita solamente alla sola fase di utilizzo, elaborazione o comunicazione/diffusione. Alla luce di ciò, l'informativa (art. 13 e 14 del GDPR), deve essere data prima della raccolta stessa dei dati e non al momento del loro utilizzo effettivo, ovvero durante le operazioni di trattamento.

Ogni trattamento di dati personali deve avvenire nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679. Il Regolamento (articolo 5, paragrafo 2) richiede al Titolare e ai suoi delegati di rispettare tutti questi principi e di essere “in grado di comprovare”. Questo è il principio detto di “responsabilizzazione” (o **accountability**) che viene poi esplicitato ulteriormente dall'articolo 24, paragrafo 1,



del Regolamento, dove si afferma che “il titolare mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento.”

TRATTAMENTO, COMUNICAZIONE E DIFFUSIONE DI DATI PARTICOLARI

Un ente pubblico può trattare solo i dati personali “particolari” detti anche “sensibili”, indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

La base giuridica per il trattamento di dati personali particolari di cui all'art. 9, paragrafo 1, del GDPR è costituita esclusivamente da una norma di legge o di regolamento o da atti amministrativi generali che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 2-sexies Codice).

TRATTAMENTO, COMUNICAZIONE E DIFFUSIONE DI DATI GIUDIZIARI

Il trattamento di dati relativi a condanne penali e reati è consentito se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati (art. 6 paragrafo 1 del GDPR e art. 2-octies del Codice).

Rientrano in questa tipologia ad esempio, la gestione amministrativa di procedimenti penali a carico di dipendenti, oppure la gestione delle certificazioni antimafia nell'ambito delle procedure di appalto.

MISURE MINIME DI SICUREZZA ICT

L'accesso al sistema informatico è consentito esclusivamente agli utenti abilitati, previa univoca identificazione e autenticazione. Gli utenti del sistema hanno autorizzazioni di accesso differenziate in base alle loro competenze e alle tipologie di operazioni stabilite dall'ufficio di appartenenza, al fine di evitare un eccesso di autorizzazioni in capo ad un unico utente.

A ogni utente sono assegnate:

- specifiche credenziali di accesso, cioè UserID (definita dall'amministrazione) e password (definita dall'utente)
- uno o più ruoli, ognuno dei quali ha specifiche funzioni e visibilità sui documenti e sui fascicoli, sulla base delle competenze e dei compiti istituzionali svolti.

L'accesso è effettuato sia dalla propria postazione di lavoro, che in modalità remota, mediante collegamento attraverso la rete VPN. Il/la Dirigente competente in materia di privacy individua le modalità organizzative per garantire un livello di sicurezza



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

adeguato al rischio in materia di protezione dei dati personali e fornisce a tutte le strutture le istruzioni operative, in conformità al Regolamento UE 679/2016. Sulla base di tali indicazioni i/le dirigenti autorizzano i propri collaboratori al trattamento dei dati e all'accesso ad uno di più ruoli nel sistema di gestione documentale, sulla base delle competenze e dei compiti istituzionali svolti.

Attenzione!!! Nell'amministrazione regionale, è stato adottato, e recentemente riproposto all'attenzione dei collaboratori, il "*Disciplinare utilizzo dispositivi elettronici*" (Deliberazione della Giunta regionale n. 237 del 31 ottobre 2019), strumento della amministrazione regionale implementato e ancora valido per contrastare il mal utilizzo della tecnologia informatica e mettere a disposizione di tutti gli utenti della rete regionale indicazioni circa il corretto utilizzo delle risorse informatiche e tecnologiche poste a loro disposizione. Inoltre si ricorda il ruolo sempre attivo svolto dall'ufficio informatica di supporto ai collaboratori e di collegamento con l'Amministratore di Sistema.

ARCHIVI CARTACEI E ACCESSO AGLI UFFICI

La protezione dei dati deve inoltre essere garantita mediante l'adozione di opportune misure fisiche di accesso e conservazione degli stessi, nonché di buone pratiche per tutti coloro che trattano i dati personali. Nella pratica questo significa che naturalmente l'accesso ai locali delle strutture dell'Amministrazione deve essere protetto da adeguati sistemi anti intrusione con l'eventuale utilizzo anche di allarmi e videosorveglianza. Tutti i documenti presenti all'interno degli uffici devono essere sempre correttamente riposti e conservati in maniera che venga garantito l'anonimato dei dati contenuti all'interno di essi, la conservazione dei documenti contenenti in particolare dati sensibili deve prevedere specifici e ulteriori meccanismi di protezione, quali ad esempio casseforti o armadietti dotati di chiave. I dipendenti e i collaboratori dell'Amministrazione sono responsabilizzati e sono tenuti non solo all'applicazione della normativa vigente ma anche a vigilare e controllare fattivamente il rispetto della protezione dei dati personali.

A tal fine, pare doveroso ricordare che il materiale cartaceo contenente dati personali utilizzato nel corso della propria attività lavorativa, non deve essere lasciato incustodito sulle scrivanie e, a fine lavoro, deve essere riposto in un luogo sicuro, possibilmente in armadi chiusi a chiave. Inoltre, è necessario prestare attenzione nello svolgimento delle normali quotidiane operazioni di lavoro, per evitare che documentazione contenente dati personali risulti facilmente visibile a persone terze o, comunque, ai non autorizzati al trattamento. In caso di trattamento di dati particolari (condizione di salute, dati giudiziari, ecc.), tutta la documentazione cartacea deve essere conservata in armadi/cassetti chiusi in caso di allontanamento, anche temporaneo, dalla postazione di lavoro.

Ricordiamo inoltre che la Regione dispone di un proprio archivio storico di deposito, situato in Trento, località Gardolo. La collocazione della documentazione, nonché la gestione dello scarto documentale è stata fatta sotto la guida della Soprintendenza. Allo scopo la Regione si è dotata di un manuale di gestione del protocollo.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Attenzione!!! Nell'amministrazione regionale i varchi sono controllati da delle telecamere appartenenti a un sistema di videosorveglianza. Per la particolarità dei dati trattati, la Regione ha svolto una valutazione di impatto dell'impianto di videosorveglianza, condivisa e valutata positivamente dal nostro RPD. "Traccia" di questo lavoro è rinvenibile nella cartellonistica esposta in prossimità delle telecamere.

DATA BREACH

I dati personali conservati, trasmessi o trattati dall'amministrazione regionale, possono essere soggetti, al pari di qualsiasi azienda private o pubblica amministrazione, al rischio di perdita, distruzione o diffusione indebita a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Sono eventi che possono mettere in serio pericolo la protezione dei dati degli interessati a cui si riferiscono i dati.

Il Garante ha introdotto, con il provvedimento *Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche* del 2 luglio 2015, l'obbligo di comunicare il verificarsi di violazioni dei dati o incidenti informatici (accessi abusivi, azione di *malware*), che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione, il cd. *Data Breach* (*breach* = *violazione*).

Anche l'amministrazione regionale, quale pubblica amministrazione, deve dunque comunicare al Garante, entro settantadue ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possano avere avuto un impatto significativo sui dati personali trattati.

La mancata comunicazione al Garante delle violazioni o degli incidenti informatici configura un illecito amministrativo sanzionato ai sensi dell'art. 162, comma 2-ter, del Codice.

Attenzione!!! È opportuno ricordare in questa sede, che la prima persona che deve essere allertata in caso di sospetta o conclamata violazione dei dati, è il Referente interno e l'amministratore di sistema. L'amministrazione regionale nel rispetto della normative in essere, ha redatto la procedura di Data Breach che la Regione ha adottato con deliberazione della Giunta regionale n. 232 del 4 dicembre 2024.

TRASFERIMENTI DI DATI A PAESI EXTRA UE.

TRASFERIMENTO DI DATI PERSONALI

Si definisce **trasferimento** di dati personali ogni mero spostamento anche temporaneo di informazioni, tanto all'interno che all'esterno dell'ambito di titolarità del trattamento (ad esempio da un server aziendale all'altro). Mentre viene definita **comunicazione** di dati la messa a disposizione a soggetti diversi dall'interessato, da parte del Titolare, dal responsabile o dagli incaricati.

Preso atto delle nozioni sopra declinate, deve intendersi come *trasferimento all'estero*



qualunque mero *spostamento* anche temporaneo di informazioni all'estero, compresa la loro momentanea collocazione su un server del Titolare situato all'esterno del territorio nazionale.

I principi che regolano il trasferimento transfrontaliero dei dati personali all'estero sono precisati dagli artt. 42-45 del Codice. In particolare il GDPR prevede che il trasferimento dei dati possa aver luogo solamente nei casi tassativamente previsti dall'art. 45 e seguenti dello stesso, ovvero in presenza di clausole contrattuali standard, di meccanismi di certificazione, di norme vincolanti di impresa o di codici di condotta. In particolar modo, fino a poco tempo fa, il trasferimento dei dati verso gli Stati Uniti seguiva il rigido protocollo delle clausole contrattuali standard. Nel corso del 2023, la Commissione Europea, ha adottato la decisione di adeguatezza sul quadro UE-USA per la protezione dei dati personali, la quale sancisce che gli Stati Uniti garantiscono un livello di protezione adeguato /comparabile a quello dell'UE per i dati personali trasferiti dall'UE alle imprese statunitensi nell'ambito del nuovo accordo quadro (Data Privacy Framework). I dati quindi possono essere trasferiti in maniera sicura verso le imprese statunitensi purchè aderenti all'accordo quadro, senza che quest'ultime debbano fornire ulteriori garanzie di protezione dei dati personali.

Attenzione!!! Nell'amministrazione regionale, in particolar modo all'interno del Registro delle attività di trattamento dei dati, va indicato (scegliendo nella colonna opportuna sì/no) se avviene o meno il trasferimento transfrontaliero dei dati trattati.

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

L'articolo 35 del Regolamento UE 2016/679, individua l'obbligatorietà della valutazione di impatto, prima di procedere al trattamento dei dati, ogni qual volta che un tipo di trattamento, qualora preveda in particolare l'uso di nuove tecnologie, e considerata la natura, l'oggetto, il contesto e le finalità del trattamento stesso, questo possa presentare un rischio elevato per i diritti e per le libertà delle persone fisiche. In questi casi quindi, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare una serie di trattamenti simili che presentano rischi analoghi.

È preferibile che la valutazione di impatto sia effettuata prima di procedere al trattamento dei dati stessi. Oltre a questa indicazione, si precisa che la DPIA è una procedura soggetta a un riesame continuo, in quanto i trattamenti tendono ad evolvere rapidamente e possono facilmente presentarsi nuovi elementi di vulnerabilità che impongono una revisione della stessa al fine di mantenere inalterato il livello di protezione dei dati al mutare delle condizioni nel tempo.

Attenzione!!! Nell'amministrazione regionale sono già state effettuate le valutazioni di impatto, in collaborazione con l'RPD, relativamente al trattamento dei dati in ambito



della videosorveglianza, del whistleblowing e allo svolgimento delle attività di trattamento dei dati dell'ufficio servizio ispettivo e di formazione.

UN APPROFONDIMENTO: LA CONSULTAZIONE DEL GARANTE SUGLI ATTI NORMATIVI DELLA REGIONE

Ai sensi dei commi 4 e 5 dell'articolo 36 del GDPR, la consultazione preventiva del Garante in sede di produzione di atti normativi o regolamentari, risulta essere un atto necessario ogni qualvolta gli stessi vanno a incidere sul trattamento di dati personali e ogni qualvolta che il titolare del trattamento ponga in essere un trattamento in esecuzione di un compito di interesse pubblico. Alla base di questa consultazione vi è innanzitutto una redazione della valutazione di impatto che, pur contemplando tutti gli aspetti di pericolo, lascia comunque aperto un rischio residuale difficile da minimizzare. In questa fase il Garante può prescrivere al titolare, a tutela del trattamento dei dati che coinvolge l'interessato, l'adozione di misure e accorgimenti a carico del titolare stesso del trattamento, mediante provvedimenti di carattere generale adottati d'ufficio.

Si evidenzia, quindi, che la consultazione con l'Autorità Garante nella fase di produzione normativa realizza l'applicazione del principio *privacy by design*.

INDICAZIONI IN MATERIA DI PUBBLICAZIONI SUL SITO INTERNET DELLA REGIONE E IN AMMINISTRAZIONE TRASPARENTE

La trasparenza online della pubblica amministrazione non è altro che la pubblicità di atti, documenti e dati appartenenti alla pubblica amministrazione attraverso il proprio sito internet. Scopo principale della trasparenza online è quello di diffondere forme di controllo riguardanti l'azione amministrativa, l'utilizzo delle risorse pubbliche e le modalità grazie alle quali la pubblica amministrazione raggiunge i propri obiettivi.

I dati, le informazioni e i documenti contenuti nella sezione del sito internet della Regione denominata "Amministrazione trasparente", sono pubblicati in conformità a quanto disposto dagli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni, ai sensi dell'articolo 1, comma 35 della legge 6 novembre 2012, n. 190 ("L. anticorruzione") come previsto dal decreto legislativo 14 marzo 2013 n. 33 successivamente modificato dal decreto legislativo 25 maggio 2016 n. 97. La sezione "Amministrazione trasparente" è strutturata secondo le previsioni di cui all'Allegato 1 della Delibera ANAC n. 1310 di data 28 dicembre 2016 ("Prime linee guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni contenute nel d.lgs. n. 33/2013 come modificato dal d.lgs. n. 97/2016"). Con legge regionale 29 ottobre 2014 n. 10 sono state emanate le disposizioni di adeguamento dell'ordinamento locale agli obblighi di pubblicità, trasparenza e diffusione di informazioni individuati dalla legge 6 novembre 2012, n. 190 e dal decreto legislativo 14 marzo 2013, n. 33. Con successiva L.R. 15 dicembre 2016 n. 16 gli obblighi di pubblicità, trasparenza e diffusione di informazioni sono stati adeguati alle novità introdotte dal citato decreto legislativo 25 maggio 2016, n. 97. Nell'amministrazione regionale la trasparenza è



disciplinata, oltre che dalle disposizioni sopra citate, anche dall'articolo 7-*quinquies* della legge regionale 21 luglio 2000, n. 3 e successive modifiche sulla base del quale la Giunta regionale provvede a rendere pubblici le deliberazioni, i decreti, le determinazioni dei dirigenti e comunque ogni altro atto amministrativo, fatto salvo quanto previsto dalla normativa vigente a tutela dei dati sensibili e giudiziari, per un periodo di cinque anni.

I principi e la disciplina di protezione dei dati personali nelle linee guida del Garante sono fondamentali e applicabili al processo di pubblicazione dei dati sul web per finalità di trasparenza. Inoltre, deve essere rispettato il principio di pertinenza e non eccedenza dei dati personali i quali, devono essere inclusi negli atti e nei documenti da pubblicare solo se realmente necessario. Tali dati devono essere proporzionati rispetto alla finalità di trasparenza perseguita.

La durata di pubblicazione degli atti pubblici è disciplinata dal decreto legislativo in materia di trasparenza e dalla legge regionale n. 3/2000 che stabilisce un limite di mantenimento di cinque anni per gli atti pubblicati on line, tranne per le seguenti eccezioni:

- per gli atti che producono ancora i loro effetti alla scadenza di cinque anni e che quindi devono rimanere pubblicati fino a quando non cessa la produzione degli effetti (informazioni su dirigenti e vertici della PA che vengono aggiornati e possono rimanere on line fino alla scadenza del loro contratto)
- i dati riguardanti i titolari di incarichi politici, dirigenti, consulenti e collaboratori (che devono rimanere pubblicati per i tre anni successive alla scadenza del contratto)
- i dati per i quali è previsto un termine diverso dalla normativa in materia di privacy.

Le pubblicazioni effettuate sul sito dell'amministrazione regionale, sono svolte al fine di garantire la massima trasparenza degli atti amministrativi regionali come sancito dall'articolo 7-*quinquies* della legge regionale 21 luglio 2000, n. 3 e successive modifiche. Ove necessario, i dati personali contenuti negli atti amministrativi sono resi anonimi per ragioni di tutela della riservatezza, secondo le indicazioni del Garante per la protezione dei dati personali. È riconosciuto a chiunque abbia interesse al procedimento il diritto di accesso agli atti amministrativi previsto dalla legge regionale 31 luglio 1993, n. 13.

Riteniamo in questa sede doveroso rilevare che l'amministrazione regionale adempie all'obbligo appena illustrato mediante la pubblicazione nella sezione amministrazione trasparente di quanto richiesto da normativa. I contenuti pubblicati, nonché i collaboratori responsabili della pubblicazione e del rispetto dei termini della stessa, sono contemplati nella sezione **ALLEGATO n. 1** Sottosezione 2.3. Rischi corruttivi e trasparenza del PIAO 2024 – 2026.

La deliberazione di Giunta regionale di approvazione del Piano integrato di attività e organizzazione della Regione Autonoma Trentino Alto-Adige/Südtirol per il triennio 2024-2026 è la n. 1 di data 30 gennaio 2024, che viene aggiornata annualmente.

Attenzione!!! Nell'amministrazione regionale il rispetto dei termini per le pubblicazioni obbligatorie per legge che devono essere pubblicate nell'area "Amministrazione Trasparente" del sito internet, è di competenza di ogni ufficio. Tutto



il materiale citato è disponibile alla pagina del sito dell'amministrazione regionale:
<https://www.regione.taa.it/Amministrazione-Trasparente/Altri-contenuti/Prevenzione-della-Corruzione/Piano-triennale-per-la-prevenzione-della-corruzione-e-per-la-trasparenza/Piano-integrato-di-attivita-e-organizzazione-PIAO-della-Regione-Autonomia-Trentino-Alto-Adige-Suedtiroel-per-il-triennio-2024-2026>

MISURE DI SICUREZZA PER LO SVOLGIMENTO DI VIDEOCONFERENZE

Proteggere la privacy durante le riunioni in videoconferenza è importante per garantire che le conversazioni rimangano riservate.

Nell'utilizzo del sistema di videoconferenza reso disponibile dall'amministrazione regionale, è necessario ricordare:

- se la riunione viene registrata da terzi, assicurarsi di sapere chi la registra, come verrà utilizzata la registrazione e dove sarà conservata. Richiedere il consenso dei partecipanti prima di avviare una registrazione, quando si è l'organizzatore;
- evitare le reti pubbliche non protette;
- Assicurarsi che la riunione sia protetta da una password e che il link sia condiviso solo con i partecipanti autorizzati.
- che i sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica, di dotarsi di cuffie con microfono (per esempio anche quelle del telefono cellulare); questo migliora sensibilmente la qualità del segnale audio;
- di spegnere il proprio microfono quando non utilizzato per evitare di introdurre rumori, brusii o interferenze;
- che nel caso ci si connetta dalla propria abitazione e non si disponga di una zona riservata è possibile utilizzare sfondi virtuali, o, se si preferisce, disattivare la videocamera testando preventivamente l'illuminazione;
- che nel caso in cui non si disponga di banda sufficiente a garantire un adeguato segnale audio- video è conveniente disattivare la videocamera;
- di scollegarsi sempre al termine della videoconferenza, la stessa stanza potrebbe essere utilizzata successivamente per altre riunioni.

INDICAZIONI IN MATERIA DI DIRITTO DI ACCESSO

La pubblicazione degli atti è svolta esclusivamente al fine di garantire la massima trasparenza degli atti amministrativi regionali (art. 7-quinquies della legge regionale 21 luglio 2000, n. 3 e successive modifiche). È riconosciuto a chiunque abbia interesse al procedimento il diritto di accesso agli atti amministrativi previsto dalla legge regionale 31 luglio 1993, n. 13, come modificata dalla legge regionale 23 ottobre 1998, n. 10 e dal relativo regolamento di esecuzione approvato con decreto del Presidente della Regione del 16 novembre 2004, n. 7/L, come modificato dal



decreto del Presidente della Regione del 20 novembre 2019, n. 83.

Anche in questo ambito, l'amministrazione regionale si attiene a quanto previsto e contenuto nella deliberazione n. 1 del 30 gennaio 2024 della Giunta regionale, di approvazione del Piano integrato di attività e organizzazione della Regione Autonoma Trentino Alto-Adige/Suedtiroil per il triennio 2024-2026. In questo caso specifico le indicazioni da seguire sono rintracciabili nell'**ALLEGATO n. 2** Sottosezione 2.3. Rischi corruttivi e trasparenza, contenente la Circolare n. 11 del 2018 prot. n. 18085 concernente "Gestione delle istanze di accesso civico generalizzato, accesso civico (semplice), accesso documentale, tramite sistema PITre e registro degli accessi civici generalizzati" e relativi Allegati.

FORMAZIONE ED INFORMAZIONE INTERNA

Nell'ottica di diffondere le conoscenze relative alla materia e fornire adeguate istruzioni a tutto il personale della Regione, vengono annualmente presi e declinati i seguenti impegni in ambito della formazione:

- garantire la formazione a tutti coloro che hanno il compito di supportare il Referente interno nella sua attività, al fine di agevolarne la conoscenza e lo svolgimento dei ruoli e delle attività previste dalla normativa
- realizzare progetti formativi specifici o eventi secondo le modalità ritenute più idonee, anche in accordo con il servizio RPD e con TSM – Trentino School of Management.

Le strutture e gli uffici dell'amministrazione regionale potranno quindi fare riferimento al servizio RPD, attraverso l'ufficio affari generali, per la proposta di quesiti, la richiesta di approfondimenti, anche previa condivisione con la sua struttura di supporto. Ulteriori attività di formazione / informazione saranno proposti in occasione di introduzione di nuovi significativi strumenti rispetto al trattamento di dati personali.

STRUMENTI PER IL MONITORAGGIO E CONTROLLO DELL'ACCOUNTABILITY DELLA REGIONE

Agli articoli 24 e 32 del GDPR rientrano, tra gli obblighi di accountability, l'implementazione di un sistema di monitoraggio, verifica e controllo del sistema privacy.

Nell'amministrazione regionale possiamo individuare diversi livelli di controllo:

- un primo livello di verifica, implementato all'interno degli uffici, attraverso le direttive impartite con le circolari di emanazione dirigenziale e l'utilizzo di procedure adeguate.
- un secondo livello di controllo (controllo di compliance) rientrante tra i servizi affidati al RPD, mediante audit che si svolgono a cadenza prestabilita.

A disposizione del RPD, in sede di audit, vengono messi i seguenti strumenti:

- registri delle attività di trattamento dei dati;
- registro del data breach, ovvero il registro che consente la registrazione e il tracciamento degli



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

eventi, degli incidenti e dei quasi incidenti (situazioni anomale o incidenti di sicurezza) nonché dei veri e propri data breach, a prescindere dal fatto che l'evento abbia dato origine alla notifica al Garante e/o alla comunicazione agli interessati di cui agli artt. 32 e 33.

Ulteriori documenti e dati necessari al fine del monitoraggio e controllo del sistema privacy che possono essere richiesti all'amministrazione regionale in sede di audit sono i seguenti:

- relazioni periodiche rese ai sensi dell'art. 28 del GDPR, al fine di rendicontare sul buon esito delle attività di trattamento svolte dal Responsabile esterno, secondo le istruzioni impartite.
- relazioni periodiche circa l'andamento delle attività di competenza degli amministratori di sistema;
- audit report e relazioni periodiche formalizzate dal RPD nel corso degli audit e verifiche di competenza.

La realizzazione di verifiche e audit al fine di verificare l'applicazione della normativa e delle istruzioni impartite è un compito affidato al servizio RPD il quale nello svolgimento delle attività è coadiuvato dall'Ufficio affari generali della Segreteria generale.

RESPONSABILITÀ E SANZIONI

La Pubblica Amministrazione (PA), come qualsiasi altro soggetto, è obbligata a rispettare il **GDPR** (Regolamento UE 2016/679) e il **Codice Privacy italiano** (D.Lgs. 196/2003, modificato dal D.Lgs. 101/2018).

Le violazioni alle disposizioni del GDPR e del Codice comportano sanzioni amministrative o sanzioni penali a seconda della gravità della violazione commessa.



DIFFUSIONE DEL MANUALE DELLE PROCEDURE PRIVACY

Il presente Manuale Operativo delle Procedure Privacy è a disposizione di chiunque, Titolare, Responsabile e Incaricato del trattamento dei dati personali. Le procedure in esso contenute devono essere conosciute dettagliatamente da parte di tutti i soggetti che entrino in contatto con i dati personali a qualsiasi titolo.

RIESAME DEL SISTEMA DI GESTIONE

Nell'ottica di miglioramento continuo, con un costante livello di attenzione al monitoraggio dell'efficacia delle misure tecniche e organizzative, il presente Manuale Operativo delle Procedure Privacy sarà oggetto di riesame in occasione di:

- emanazione di nuove disposizioni emanate dal Garante della protezione dei dati personali che abbiano un impatto sulla disciplina della protezione dei dati rilevante per l'amministrazione regionale;
- variazioni significative e sostanziali nelle competenze attribuite alle Ripartizioni;
- introduzione di nuovi significativi strumenti di gestione, rilevanti rispetto al trattamento dei dati personali;
- applicazioni di sanzioni da parte dell'Autorità giudiziaria ovvero del Garante nella materia di cui trattasi.

Il riesame è previsto con la collaborazione del RPD, e sottoposto alla Giunta regionale per l'assunzione delle eventuali decisioni necessarie a garantire la compliance e il miglioramento continuo.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

ORGANISATIONSMODELL FÜR DEN DATENSCHUTZ

Version Nr.	Genehmigungsakt	Wichtigste Änderungen	Gültigkeit/Ablauf
1		Erste Fassung	



ORGANISATIONSMODELL FÜR DEN DATENSCHUTZ – ERSTER TEIL INHALTSVERZEICHNIS

1	EINFÜHRUNG UND ANWENDUNGSBEREICH.....	6
2	BEZUGSBESTIMMUNGEN	6
3	BEGRIFFSBESTIMMUNGEN	7
4	PERSONENBEZOGENE DATEN UND ARTEN VON PERSONENBEZOGENEN DATEN	9
5	VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN	10
6	DATEN, DIE AUFSCHLUSS ÜBER DEN GESUNDHEITZUSTAND GEBEN KÖNNEN	10
7	VERARBEITUNG PERSONENBEZOGENER DATEN BETREFFEND STRAFRECHTLICHE VERURTEILUNGEN UND STRAFTATEN	11
8	TÄTIGKEITEN, ORGANISATION UND DIREKT BETEILIGTE RECHTSSUBJEKTE	11
8.1	VERANTWORTLICHER FÜR DIE DATENVERARBEITUNG	11
8.2	GEMEINSAM FÜR DIE VERARBEITUNG VERANTWORTLICHE	12
8.3	ZUR DATENVERARBEITUNG ERMÄCHTIGTE PERSONEN	12
8.4	AUFTRAGSVERARBEITER	13
8.5	SYSTEMADMINISTRATOR	14
8.6	DATENSCHUTZBEAUFTRAGTER (DSB)	15
9	VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN, RECHTSGRUNDLAGE UND EINWILLIGUNG ZUR VERARBEITUNG DER PERSONENBEZOGENEN DATEN	17
9.1	VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN UND VERARBEITUNGEN	17
9.2	DEFINITION DER RECHTSGRUNDLAGE UND EINWILLIGUNG ZUR VERARBEITUNG	17
10	VERARBEITUNG, OFFENLEGUNG UND VERBREITUNG „GEWÖHNLICHER“ PERSONENBEZOGENER DATEN	19
11	VERARBEITUNG, OFFENLEGUNG UND VERBREITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN	19
12	VERARBEITUNG, OFFENLEGUNG UND VERBREITUNG VON RICHTSDATEN	20
13	MINDESTMASSNAHMEN ZUR IT-SICHERHEIT	20
14	DATEISYSTEME IN PAPIERFORM UND ZUGANG ZU DEN ÄMTERN	21
15	DATA BREACH	22
16	ÜBERMITTLUNG VON DATEN AN NICHT-EU-LÄNDER	22
16.1	ÜBERMITTLUNG PERSONENBEZOGENER DATEN	22
17	DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)	23



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

18	ZUR VERTIEFUNG: KONSULTATION DER DATENSCHUTZBEHÖRDE HINSICHTLICH DER GESETZESAKTE DER REGION.....	24
19	HINWEISE BETREFFEND DIE VERÖFFENTLICHUNGEN AUF DER OFFIZIELLEN WEBSITE DER REGION UND IM BEREICH TRANSPARENTE VERWALTUNG	24
20	SICHERHEITSMASSNAHMEN FÜR DIE DURCHFÜHRUNG VON VIDEOKONFERENZEN.....	26
21	HINWEISE IN SACHEN RECHT AUF AKTENZUGANG	27
22	INTERNE WEITERBILDUNG UND INFORMATION	27
23	INSTRUMENTE FÜR DIE ÜBERWACHUNG UND ÜBERPRÜFUNG DER RECHENSCHAFTSPFLICHT DER REGION	28
24	HAFTUNG UND SANKTIONEN	28



ORGANISATIONSMODELL FÜR DEN DATENSCHUTZ – ZWEITER TEIL ANLAGEN UND UNTERLAGEN ZUM DATENSCHUTZ ZUR EINSICHTNAHME FÜR DIE BEDIENSTETEN

ANLAGEN

- 1) DATENSCHUTZ-FOLGENABSCHÄTZUNG IN BEZUG AUF DIE VIDEOÜBERWACHUNG
- 2) DATENSCHUTZ-FOLGENABSCHÄTZUNG IN BEZUG AUF DIE VERARBEITUNG PERSONENBEZOGENER DATEN, AMT FÜR PERSONALENTWICKLUNG UND INSPEKTIONSDIENST
- 3) VERSCHIEDENE VORLAGEN:
 - 3.1 VERZEICHNISSE DER DATENVERARBEITUNG
 - 3.2 ERNENNUNG DES DATENSCHUTZBEAUFTRAGTEN
 - 3.3 ERNENNUNG DER AUFTRAGSVERARBEITER
 - 3.4 AUSFÜHRLICHE UND KURZE DATENSCHUTZERKLÄRUNG
- 4) PLAN ZUR PERIODISCHEN ÜBERPRÜFUNG DER ERGRIFFENEN MASSNAHMEN (allgemein für die zuständige Organisationsstruktur, spezifisch für jedes Amt)
- 5) VERZEICHNIS DER UNTERLAGEN UND RUNDSCHREIBEN BETREFFEND VERPFLICHTUNGEN IN SACHEN DATENSCHUTZ
 - 5.1 Rundschreiben Nr. 5/2023
 - 5.2 Rundschreiben vom 29.6.2023, Nr. 12 - Ergebnisse des am 5. Juni 2023 vom DSB durchgeführten Audits und Anleitungen in Sachen Datenschutz
 - 5.3 Rundschreiben Nr. 29/2022 – Einführung der permanenten Signatur für registrierte und im Ausgangsprotokoll protokollierte Dokumente
 - 5.4 Rundschreiben des Trentiner Gemeindenverbands aus dem Jahr 2020 – Datenschutzdienst DSB – weiterführende Informationen zur Rolle des Verantwortlichen und des Auftragsverarbeiters angesichts einiger neuer Entscheidungen der zuständigen Behörden (ID 11989712/2020)
 - 5.5 Internes Rundschreiben betreffend die Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten und Ernennung der befugten Personen (Beauftragten) im Sinne des Art. 4 Abs. 1 Z. 10 in Verbindung mit Art. 29 der EU-Datenschutz-Grundverordnung Nr. 2016/679 (ID 15035688/2021).
 - 5.6 Rundschreiben Nr. 11/2018 betreffend die Abwicklung der Anträge auf allgemeinen Bürgerzugang, auf (einfachen) Bürgerzugang sowie auf Zugang zu den Verwaltungsunterlagen über das PiTre-System und das Register der allgemeinen Bürgerzugänge
- 6) VERÖFFENTLICHUNGEN AUF DER WEBSITE: Bestimmungen und technisch-organisatorische Empfehlungen des Datenschutzdienstes.
- 7) VERFAHREN ZUM WHISTLEBLOWING: Anleitungen und Überprüfung der Auswirkungen des Dienstes.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

- 8) ERNENNUNG DES SYSTEMADMINISTRATORS
- 9) ANWEISUNGEN FÜR DIE VERWENDUNG ELEKTRONISCHER GERÄTE: Beschluss der Regionalregierung vom 31.10.2019, Nr. 237 „Anweisungen für die Verwendung der elektronischen Geräte der Autonomen Region Trentino-Südtirol“
- 10) ÜBERTRAGUNG VON DATEN INS AUSLAND: Vom Datenschutzdienst am 16.10.2023 übermitteltes Rundschreiben mit weiterführenden Informationen zu den Gesetzesbestimmungen;
- 11) ANWEISUNGEN IN SACHEN DATENSCHUTZ FÜR DIE ZENTRALÄMTER UND FRIEDENSGERICHTE: Rundschreiben mit weiteren, in den Mitteilungen vom 5.9.2023, Prot.-Nr. 23924 und vom 6.10.2022, Prot.-Nr. 23830 enthaltenen Anweisungen in Sachen Datenschutz für die Zentralämter und die Friedensgerichte.
- 12) AUFTEILUNG DER ZUSTÄNDIGKEITEN: Beschluss der Regionalregierung vom 26.5.2021, Nr. 91 „Festlegung der der Regionalregierung, den Führungskräften und den Amtsdirektorinnen/Amtsdirektoren vorbehaltenen Zuständigkeiten“
- 13) RUNDSCHREIBEN DES TRENTINER GEMEINDENVERBANDS ÜBER DIE GEMEINSAME VERANTWORTUNG DER VERARBEITUNG PERSONENBEZOGENER DATEN
- 14) ANLAGEN NR. 1 UND NR. 2 Unterabschnitt 2.3. „Korruptionsrisiken und Transparenz“ des PIAO 2024-2026
- 15) RG Nr. 13/1993 – RG Nr. 10/2014 i.d.g.F. – Verordnung vom 16.11.2004, Nr. 7/L
- 16) Geschäftsordnung für die Sitzungen der Regionalregierung
- 17) Rundschreiben vom 24.8.2022, Nr. 17 „Bestimmungen für die Arbeit im agilen Modus“



EINFÜHRUNG UND ANWENDUNGSBEREICH

Dieses Handbuch in Sachen Datenschutz dient der Festlegung und Sammlung einer Reihe von Verfahren und bewährten Praktiken für die ordnungsgemäße Implementierung der in der DSGVO (Verordnung (EU) 2016/679) und im Datenschutzkodex (GvD Nr. 196/2003, geändert durch GvD Nr. 101/2018) enthaltenen Grundsätze des Datenschutzes und des Schutzes der personenbezogenen Daten. Dieses **Organisationsmodell für den Datenschutz** besteht aus zwei Teilen:

- Der erste „theoretische“ Teil enthält eine Beschreibung und Zusammenfassung der wichtigsten Elemente der Gesetzesbestimmungen in Sachen Datenschutz sowie einige kurze weiterführende Erklärungen
- Der zweite „praktische“ Teil umfasst eine Sammlung aller bei der Regionalverwaltung gültigen und angewandten Praktiken, die aus den im Laufe der Zeit erlassenen Verordnungen, Verfahren und Rundschreiben herrühren

Die ordnungsgemäße Implementierung und Anwendung der im zweiten Teil dieses Handbuchs dargelegten Verfahren ermöglicht eine möglichst wirksame und effiziente Erfüllung der gesetzlich festgelegten Verpflichtungen, über die der Verantwortliche für die Datenverarbeitung der Regionalverwaltung im Falle einer Kontrolle durch die Datenschutzbehörde Rechenschaft geben muss.

Die Personen, die Daten verarbeiten, sind zur Anwendung der Datenschutzbestimmungen verpflichtet, wenn Erhebung, Eingabe, Löschung, Änderung, Verarbeitung und Speicherung von Informationen über identifizierte oder identifizierbare natürliche Personen zu anderen als rein privaten Zwecken erfolgt. Die Verfahren werden sowohl auf Daten in Papierform als auch auf digital gespeicherte Daten angewandt.

Das Handbuch wird mit Beschluss der Regionalregierung genehmigt; es wird regelmäßig überprüft und (vor allem im zweiten Teil) mit den nach und nach neu eingeführten Verfahren aktualisiert.

BEZUGSBESTIMMUNGEN

Gemäß Art. 8 der Charta der Grundrechte der Europäischen Union hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Dieses Recht wird derzeit insbesondere durch die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) geschützt. Auf nationaler Ebene ist das Recht auf Schutz der personenbezogenen Daten durch den „Datenschutzkodex“ (gesetzesvertretendes Dekret vom 30. Juni 2003, Nr. 196) geregelt, der den Bestimmungen der Verordnung (EU) 2016/679 mit dem



gesetzesvertretenden Dekret vom 10. August 2018, Nr. 101 angepasst wurde. Die Aufsicht über die ordnungsgemäße Anwendung der Datenschutzbestimmungen führt eine unabhängige Datenschutzbehörde, die unter anderem für den Erlass von Maßnahmen und Richtlinien zuständig ist. Weitere Informationen können über die offizielle Website der Datenschutzbehörde unter dem Link <https://www.garanteprivacy.it> eingesehen werden.

BEGRIFFSBESTIMMUNGEN

Im Folgenden wird die Definition der gebräuchlichsten Begriffe gemäß Art. 4 der DSGVO angeführt:

- **„personenbezogene Daten“** alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
- **„Verarbeitung“** jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;
- **„Einschränkung der Verarbeitung“** die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
- **„Profiling“** jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;
- **„Pseudonymisierung“** die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher



Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

- **„Dateisystem“** jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;
- **„Verantwortlicher“** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;
- **„Auftragsverarbeiter“** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
- **„Empfänger“** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;
- **„Dritter“** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;
- **„Einwilligung“** der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;



- „**Verletzung des Schutzes personenbezogener Daten**“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
- „**genetische Daten**“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;
- „**biometrische Daten**“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
- „**Gesundheitsdaten**“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

PERSONENBEZOGENE DATEN UND ARTEN VON PERSONENBEZOGENEN DATEN

Die Datenschutzbehörde definiert als **personenbezogene Daten** alle Informationen, die eine natürliche Person direkt oder indirekt identifizieren oder identifizierbar machen und Auskunft über ihre Merkmale, ihre Gewohnheiten, ihren Lebensstil, ihre persönlichen Beziehungen, ihren Gesundheitszustand, ihre wirtschaftliche Lage usw. geben.

Unter dem Gesichtspunkt der Art von Information oder des verwendeten Datenträgers umfasst der Begriff der personenbezogenen Daten jede Art von Information, die in beliebiger Form vorliegen kann, sei es in alphabetischer, numerischer, grafischer, fotografischer oder akustischer Form, auf Papier aufgezeichnete Informationen und Informationen, die im Speicher eines Computers mittels eines binären Codes oder auf einem Videoband gespeichert sind. In der Folge wurden von der Datenschutzbehörde ebenfalls die folgenden Daten als personenbezogene Daten definiert:

- ✓ die Stimmaufnahme einer Person (z. B. aufgezeichnete Anrufe beim Notruf);
- ✓ Bilder, die von einem Videoüberwachungssystem aufgenommen wurden, sofern die einzelnen Personen erkennbar sind;
- ✓ IP-Adresse von E-Mails;
- ✓ Fingerabdrücke, d. h. biometrische Daten, die zu den personenbezogenen Daten



gezählt werden, da sie eine Person identifizieren (wohingegen Gewebeproben, aus denen biometrische Daten gewonnen werden, nicht *per se* personenbezogene Daten sind, auch wenn die zur Gewinnung dieser biometrischen Informationen durchgeführten Vorgänge bereits eine Verarbeitung personenbezogener Daten darstellen);

- ✓ die mit den personenbezogenen Daten eines Mitarbeiters verbundene Matrikelnummer.

VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

Die besonderen Kategorien personenbezogener Daten, die auch als „sensible Daten“ bezeichnet werden, betreffen Merkmale der betroffenen Person in den Bereichen Ethnie, Denken, Gesundheit und Sexualleben. Im Detail bezeichnet das Gesetz als sensible Daten die personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, religiöse oder weltanschauliche oder sonstige (z. B. im weitesten Sinne moralische) Überzeugungen, politische Meinungen, die Mitgliedschaft bei Parteien, Gewerkschaften, Verbänden oder Organisationen mit religiösem, philosophischem, politischem oder gewerkschaftlichem Charakter hervorgehen. Die Verordnung (EU) 2016/679 schließt auch genetische Daten, biometrische Daten und Daten zur sexuellen Orientierung einer Person mit in die Definition ein (Art. 9).

DATEN, DIE AUFSCHLUSS ÜBER DEN GESUNDHEITZUSTAND GEBEN KÖNNEN

Als Daten, die Aufschluss über den Gesundheitszustand geben können, gelten alle Informationen, die direkt, aber auch indirekt einen Krankheitszustand oder auf jeden Fall einen – auch früheren oder potenziellen – Zustand der Beeinträchtigung des körperlichen, geistigen und emotionalen Befindens der Person offenbaren können, einschließlich der – auch nur verwaltungstechnischen – Informationen betreffend die Durchführung von Gesundheitskontrollen sowie Bedingungen oder Situationen, die zu einem Krankheitszustand im weitesten Sinne führen könnten oder dies als mögliche Voraussetzung haben.

Im Datenschutzkodex ist der Schutz der personenbezogenen Daten festgelegt, die Aufschluss über den Gesundheitszustand der betroffenen Person geben können. Als Daten, die Aufschluss über den Gesundheitszustand geben können, gelten jene Informationen, die einen direkten oder indirekten, auch allgemeinen und nicht unbedingt spezifischen Eindruck vom Gesundheitszustand einer Person vermitteln.

Hinweis: Bei der Regionalverwaltung findet man diese Art von Daten insbesondere bei der Führung des Personalfaszikels weshalb es ratsam ist, bei ihrer Verarbeitung besonders sorgfältig vorzugehen und darauf zu achten, dass sie nicht unbeabsichtigt weitergegeben werden (z. B. am Telefon).



VERARBEITUNG PERSONENBEZOGENER DATEN BETREFFEND STRAFRECHTLICHE VERURTEILUNGEN UND STRAFTATEN

Gerichtsdaten (Art. 10 der Verordnung (EU) 679/2016) sind Daten, die sich auf strafrechtliche Verurteilungen und Straftaten beziehen. Diese Art von Daten kann über das Vorliegen bestimmter strafregisterpflichtiger gerichtlicher Verfügungen und Maßnahmen (zum Beispiel rechtskräftige strafrechtliche Verurteilungen, bedingte Entlassung, Aufenthaltsverbot oder -gebot, haftersetzende Maßnahmen) oder über die Eigenschaft einer Person als Angeklagter oder als Beschuldigter Aufschluss geben.

Hinweis: Auch die Regionalverwaltung muss unter Umständen diese Art von Daten verarbeiten, zum Beispiel bei der verwaltungsmäßigen Abwicklung von Strafverfahren gegen Bedienstete oder bei der Verwaltung der Anti-Mafia-Bescheinigungen im Rahmen von Vergabeverfahren. Es wird darauf hingewiesen, dass für Gerichtsdaten ähnliche Voraussetzungen und Verarbeitungsmodalitäten bestehen wie für sensible Daten, d. h. sie dürfen nicht – auch nicht unabsichtlich – an Dritte weitergegeben werden.

TÄTIGKEITEN, ORGANISATION UND DIREKT BETEILIGTE RECHTSSUBJEKTE

VERANTWORTLICHER FÜR DIE DATENVERARBEITUNG

Es ist Aufgabe der Regionalverwaltung als Verantwortliche für die Datenverarbeitung – und nicht der einzelnen Organisationsstrukturen mit ihren jeweiligen Verantwortungsebenen –, die grundlegenden Entscheidungen in Bezug auf Zwecke, Modalitäten und Mittel der Datenverarbeitung zu treffen. Die von der Regionalverwaltung verfolgten institutionellen Ziele, deren operative Umsetzung auf die internen Auftragsverarbeiter (die Führungskräfte und persönlichen Referenten/Referentinnen) übertragen wird, legitimieren die von ihr und für sie durchgeführte Verarbeitung. Die Verantwortung der Regionalverwaltung für die für ihre institutionellen Ziele verarbeiteten Daten bedeutet unter anderem, dass die zur Datenverarbeitung ermächtigten Personen diese ohne ausdrückliche Ermächtigung nicht zu privaten, wenn auch theoretisch rechtmäßigen Zwecken (z. B. in einem Rechtsstreit) verwenden dürfen. Der Verantwortliche ist außerdem für die Bestimmung und Ernennung der zur Datenverarbeitung ermächtigten Personen zuständig und hat diesen die notwendigen Anweisungen für die ordnungsgemäße Verwaltung und den Schutz der personenbezogenen Daten, einschließlich des Schutzes ihrer Vollständigkeit und Sicherheit, zu erteilen sowie die durchgeführte Tätigkeit im Hinblick auf die erteilten Anweisungen regelmäßig zu überprüfen.

Hinweis: Bei der Regionalverwaltung sind die oben genannten Anweisungen im Detail im Beschluss der Regionalregierung vom 3.9.2019, Nr. 193 dargelegt.



GEMEINSAM FÜR DIE VERARBEITUNG VERANTWORTLICHE

Bei einer bestimmten Datenverarbeitung kann es zu einer gemeinsamen Verantwortlichkeit kommen. Diese muss auf eine gemeinsame Möglichkeit, Zwecke und Modalitäten der Datenverarbeitung festzulegen, zurückgeführt werden, die sich aus der abschließenden gemeinsamen Beteiligung an den Interessen im Hinblick auf die Verarbeitung ergibt. Diese Bedingung liegt derzeit häufig in Zusammenhang mit Projekten von interinstitutionellem oder betriebsübergreifendem Belang vor. In diesem Fall wird Bezug auf den Art. 26 der DSGVO genommen.

ZUR DATENVERARBEITUNG ERMÄCHTIGTE PERSONEN

Infolge der Änderung einiger Teile der DSGVO sind die Bezeichnungen „*interner Auftragsverarbeiter*“ und „*Beauftragter*“ nicht mehr ausdrücklich vorgesehen. In Art. 29 wird „*jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person*“ erwähnt (der Auftragsverarbeiter wird hier als verwaltungsfremde Person aufgefasst). Die vom Verantwortlichen mit der Durchführung spezifischer Aufgaben beauftragte Person (die wir aus Gründen der Klarheit weiterhin als Auftragsverarbeiter bezeichnen), ist die Person, die aufgrund ihrer Zuständigkeiten, des erhaltenen Auftrags und der ausgeübten Aufgaben die Oberaufsicht über die verschiedenen Tätigkeiten führt, deren ordnungsgemäße Ausführung kontrolliert und eine funktionale Weisungsbefugnis ausübt, wobei sie auch die mit diesen Tätigkeiten funktionell verbundenen Aufgaben zum Schutz personenbezogener Daten wahrnimmt. Der Auftragsverarbeiter ist grundsätzlich verpflichtet, in aktiver Zusammenarbeit mit dem Verantwortlichen und dem Datenschutzreferenten geeignete organisatorische und verwaltungstechnische Maßnahmen in Bezug auf die Verarbeitungen, für die er zuständig ist, festzulegen. Die Auftragsverarbeitung ist daher in erster Linie eine organisatorische Verantwortung, die darauf abzielt, allen Personen, deren Daten verarbeitet werden, das Recht auf die Vertraulichkeit und den Schutz personenbezogener Daten zu garantieren, und zwar durch:

- die Zuweisung von Aufgaben und Funktionen an die Beauftragten, die, wenn sie mit Hilfe von EDV-Geräten durchgeführt werden sollen, auch deren entsprechende Profilierung erfordern;
- die Erteilung von Anweisungen, die eventuell detaillierter als die von dem Verantwortlichen festgelegten sein können, und die Überprüfung ihrer effektiven Anwendung;

Hinweis: Im Beschluss der Regionalregierung vom 3.9.2019, Nr. 193 werden als interne Auftragsverarbeiter, die der Verarbeitung personenbezogener Daten im Rahmen der in ihre Zuständigkeit fallenden Sachgebiete und Bereiche vorstehen, die einzelnen Führungskräfte der regionalen Organisationsstrukturen und die persönlichen Referenten und Referentinnen der Mitglieder der Regionalregierung bestimmt. Der Generalsekretär / Die Generalsekretärin wird außerdem aufgrund seiner/ihrer Befugnisse als Datenschutzreferent und als Verantwortlicher für die Meldung eventueller Verletzungen des Schutzes personenbezogener Daten (Data Breach) ernannt.



Die Führungskräfte und persönlichen Referenten/Referentinnen ernennen wiederum die zur Datenverarbeitung ermächtigten Personen. Es sind demnach diejenigen, die konkret unter Einhaltung der erteilten Anweisungen Datenverarbeitungsvorgänge durchführen.

Die zur Datenverarbeitung ermächtigten Personen sind schriftlich zu bestimmen und der Verarbeitungsbereich muss genau festgelegt sein. Der Verarbeitungsbereich, in dem die einzelnen zur Datenverarbeitung ermächtigten Personen mit Hilfe von Computersystemen Datenverarbeitungsvorgänge durchführen dürfen, ist durch die Festlegung geeigneter Zugriffsprofile (Berechtigungsprofile) vor Beginn der Verarbeitung abzugrenzen, damit der Zugriff nur auf die Daten beschränkt wird, die für die Durchführung der Verarbeitungsvorgänge erforderlich sind, wodurch die Gefahr einer übermäßigen Anzahl unnötiger Berechtigungen vermieden wird.

Hinweis: Bei der Regionalverwaltung ist es üblich, jeden Auftrag und jede Berechtigung vor dem Dienstantritt des Bediensteten zuzuweisen. Die Erstellung der für die Aktivierung eines neuen IT-Profiles sowie für dessen Schließung und/oder Änderung erforderlichen Dokumentation erfolgt gemäß den Anweisungen im Dokument Prot.-Nr. 23830/2022 „*Weitere organisatorische Bestimmungen in Sachen Datenschutz*“, das dem zweiten Teil dieses Handbuchs beigelegt ist.

AUFTRAGSVERARBEITER

Im Art. 28 der EU-Verordnung wird der externe Auftragsverarbeiter als eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die im Auftrag des Verantwortlichen eine Datenverarbeitung vornimmt, definiert. Laut DSGVO haben Verantwortlicher und Auftragsverarbeiter sehr ähnliche, aber nicht gleiche Aufgaben und Pflichten.

Die Ernennung des Auftragsverarbeiters ist vorgeschrieben, wenn ein externes Rechtssubjekt die Befugnis erhält, die vom Verantwortlichen für die Datenverarbeitung gesammelten personenbezogenen Daten zu verarbeiten. Es wird darauf hingewiesen, dass die Entscheidung, welche personenbezogenen Daten aus welchem Grund gesammelt werden, bei dem Verantwortlichen liegt. **Der externe Auftragsverarbeiter** muss schriftlich mit Ernennungsakt oder mit Vertrag – d. h. mit einem Akt, der den Auftragsverarbeiter an den Verantwortlichen bindet – ernannt werden. Auf dem Sachgebiet des Datenschutzes bedeutet der Begriff „im Auftrag des Verantwortlichen“, dass der Auftragsverarbeiter keine Verarbeitungen zu eigenen Zwecken vornehmen darf: Die zu erreichenden Ziele und die zu verwendenden Mittel müssen immer (und dürfen nur) vom Verantwortlichen festgelegt werden.

An dieser Stelle ist darauf hinzuweisen, dass die fehlende schriftliche Ernennung des externen Auftragsverarbeiters eine Sanktion durch die Datenschutzbehörde nach sich zieht.

Außerdem gehört es zu den Pflichten des Verantwortlichen, den externen



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Auftragsverarbeiter regelmäßig zu kontrollieren. In der DSGVO ist kein bestimmter Zeitplan für die Kontrollen vorgesehen – der Verantwortliche muss in regelmäßigen Abständen eine Überprüfung bezüglich der Angemessenheit des dem externen Auftragsverarbeiter erteilten Auftrags vornehmen und nachweisen.

Hinweis: Unter Z. 5 und 6 des Beschlusses der Regionalregierung vom 3.9.2019, Nr. 193 werden die einzelnen Führungskräfte beauftragt, die Sachverhalte zu aktualisieren, für die die Autonome Region Trentino-Südtirol externe Auftragsverarbeiter im Sinne des Art. 28 der Verordnung namhaft machen muss. Folglich sind die einzelnen Führungskräfte dafür zuständig, mit Bezug auf die von ihnen bestimmten Sachverhalte sowie die Modalitäten und den Zeitplan für die Überprüfung der Arbeit des externen Auftragsverarbeiters den gemäß Art. 28 erforderlichen Vertrag/Akt auszuarbeiten und abzuschließen.

SYSTEMADMINISTRATOR

Der Begriff des **Systemadministrators** ist sehr weit gefasst und umfasst auch Tätigkeiten, die nicht in der alleinigen Verantwortung des IT-Personals liegen (z. B. die reine Verwaltung von Authentifizierungs- und Autorisierungssystemen). Der Systemadministrator ist mit heiklen Aufgaben betraut, wie z. B. der Implementierung von Sicherheitssystemen, der Festlegung von Verfahren zur Netzauthentifizierung und zur Autorisierung des Datenzugriffs für Benutzer, der Pflege der Datensicherung durch Back-up-Lösungen und der Konzeption von Maßnahmen zur Unterstützung beim Disaster Recovery. In der Regel ist der Systemadministrator gemäß der Datenschutzbehörde eine Fachkraft, die sich im weitesten Sinne mit dem Betrieb und der Wartung von Datenverarbeitungssystemen (einschließlich Datenbankverwaltungssystemen, komplexer Softwaresysteme, lokaler Netze und Sicherheitseinrichtungen) beschäftigt, mit denen personenbezogene Daten verarbeitet werden. Daraus folgt, dass die vom Systemadministrator ausgeübten Funktionen einen bevorrechtigten Zugang zu allen personenbezogenen Daten der Regionalverwaltung voraussetzen.

Die Bestimmung, Ermächtigung und Kontrolle von Personen, die geeignet sind, die Aufgaben eines Systemadministrators zu erfüllen, sind von grundlegender Bedeutung für den Schutz der personenbezogenen Daten, die von der Regionalverwaltung aufbewahrt werden. Daraus folgt, dass die Arbeit des Systemadministrators jährlich vom Verantwortlichen für die Datenverarbeitung überprüft werden muss, um die Einhaltung der technischen, organisatorischen und sicherheitstechnischen Maßnahmen zu kontrollieren, die für die Verarbeitung personenbezogener Daten eingeführt wurden. Wird ein Systemadministrator auf Outsourcing-Basis, d. h. außerhalb des Betriebs, ernannt, so ist er als Auftragsverarbeiter zu betrachten, und daher muss der Verantwortliche für die Datenverarbeitung den Systemadministrator mit einem schriftlichen Vertrag binden, der alle Anforderungen von Artikel 28 der Verordnung (EU) 2016/679 erfüllt.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

DATENSCHUTZBEAUFTRAGTER (DSB)

Auf der Grundlage des Art. 37 Abs. 7 der Verordnung (EU) 2016/679 müssen Rechtssubjekte des öffentlichen Rechts der Datenschutzbehörde den Namen des Datenschutzbeauftragten (auf Englisch: Data Protection Officer – DPO) mitteilen. Der Datenschutzbeauftragte fungiert nämlich gemäß Art. 39 Abs. 1 Buchst. e) der Verordnung als Kontaktstelle zwischen der Körperschaften bzw. dem Betrieb und der Datenschutzbehörde. Der DSB wird aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit, den Auftrag wahrzunehmen, ernannt. Dabei kann es sich um einen Mitarbeiter des Verantwortlichen handeln, wenn sich unter dessen Mitarbeitern ein geeigneter Fachmann findet, oder um ein externes Rechtssubjekt mit spezifischen beruflichen Fähigkeiten und Anforderungen, das auf der Grundlage eines Dienstleistungsvertrags Aufgaben im Bereich des Datenschutzes wahrnimmt.

Hinweis: Die Regionalverwaltung hat den Dienst des DSB/DPO für das Jahr 2024 dem Trentiner Gemeindenverband anvertraut. Es wird darauf hingewiesen, dass über das Amt für allgemeine Angelegenheiten der zuständigen Kontaktstelle des Trentiner Gemeindenverbands Fragen in Sachen Datenschutz gerichtet werden können.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

ÜBERSICHT ÜBER DIE AM DATENSCHUTZ BETEILIGTEN FUNKTIONSTRÄGER

IN DER VERORDNUNG (EU) 2016/679 FESTGELEGTE FUNKTIONEN	ART. VERORDNUNG (EU) 2016/679	FUNKTIONSTRÄGER BEI DER REGIONALVERWALTUNG
VERANTWORTLICHER FÜR DIE DATENVERARBEITUNG	ART. 4 ABS. 1 Z. 7	DIE REGIONALREGIERUNG ODER DER PRÄSIDENT ALS GESETZLICHER VERTRETER
AUFTRAGSVERARBEITER	ART. 4 ABS. 1 Z. 8	FÜHRUNGSKRÄFTE / PERSÖNLICHE REFERENTEN DER MITGLIEDER DER REGIONALREGIERUNG
DATENSCHUTZREFERENT		GENERALSEKRETÄR
ZUR DATENVERARBEITUNG ERMÄCHTIGTE PERSONEN	ART. 29 DSGVO UND ART. 2- QUATERDECIES DES DATENSCHUTZKODE X	BEDIENSTETE DER KÖRPERSCHAFT
SYSTEMADMINISTRATOR	ART. 28	EXTERN
DSB/DPO	ART. 37	DREAM S.R.L.
EXTERNER AUFTRAGSVERARBEITER	ART. 28	JEWELLS SCHRIFTLICH ERNANNT
GEMEINSAM VERANTWORTLICHE	ART. 26	VON MAL ZU MAL BESTIMMT



VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN, RECHTSGRUNDLAGE UND EINWILLIGUNG ZUR VERARBEITUNG DER PERSONENBEZOGENEN DATEN

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN UND VERARBEITUNGEN

Das **Verzeichnis der Verarbeitungstätigkeiten** (Art. 30 DSGVO) ist ein Dokument, in dem die vom Verantwortlichen oder Auftragsverarbeiter oder von den Beauftragten durchgeführten Datenverarbeitungen erfasst und analysiert werden. Das Verzeichnis muss daher ständig aktualisiert werden, da sein Inhalt stets den tatsächlich durchgeführten Verarbeitungen entsprechen muss. So ist das Verzeichnis auch das erste Dokument, das im Falle einer Inspektion der Datenschutzbehörde durch die Spezialeinheit für Datenschutz der Guardia di Finanza eingesehen wird.

DEFINITION DER RECHTSGRUNDLAGE UND EINWILLIGUNG ZUR VERARBEITUNG

Laut DSGVO muss jede Datenverarbeitung auf einer angemessenen **Rechtsgrundlage** beruhen, die die Verarbeitung rechtlich zulässt, so dass diese dem in den Rechtsvorschriften verankerten Grundsatz der Rechtmäßigkeit entspricht. Die Wahl der Rechtsgrundlage obliegt dem Verantwortlichen für die Datenverarbeitung, der darauf achten muss, die für seine Ziele am besten geeignete zu wählen; die Rechtsgrundlage muss in der Datenschutzerklärung angegeben werden. Die Grundlagen der Rechtmäßigkeit der Datenverarbeitung bzw. die Rechtsgrundlage der Verarbeitung personenbezogener Daten sind im Art. 6 der DSGVO festgelegt. Die Rechtsgrundlage für die Datenverarbeitung muss immer in der Datenschutzerklärung an die Nutzer (Art. 13 und 14 DSGVO) angegeben werden und muss vor allem immer im Verzeichnis der Verarbeitungstätigkeiten angeführt werden.

Im Art. 6 der DSGVO sind die folgenden Rechtsgrundlagen der Verarbeitung personenbezogener Daten angeführt:

- die **Einwilligung** der betroffenen Person
- die Erfüllung **vertraglicher Verpflichtungen** oder die Durchführung **vorvertraglicher Maßnahmen**
- die **gesetzlich vorgesehenen Pflichten**, denen der Verantwortliche für die Datenverarbeitung unterliegt;
- die **lebenswichtigen Interessen** der **betroffenen Person** oder **Dritter**;
- das **vorrangige berechnete Interesse des Verantwortlichen** oder **Dritter**, denen die Daten offengelegt werden;
- **öffentliches Interesse** oder Ausübung **öffentlicher Gewalt**.



Hinweis: Auch die Wettbewerbsausschreibung, in der die Modalitäten für die Veröffentlichung der Rangordnung angegeben sind, gelten beispielsweise als Rechtsgrundlage. Diesbezüglich wird auch auf das vom DSB übermittelte erläuternde Rundschreiben verwiesen (zweiter Teil der Anlagen).

Die Einwilligung wird im Art. 4 Z. 11) der DSGVO 679/2016 folgendermaßen definiert: *„jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“.*

Der Verantwortliche muss somit nachweisen können, dass die von der betroffenen Person erteilte Einwilligung gültig ist. Diese kann unter folgenden Voraussetzungen als gültig betrachtet werden:

- Der betroffenen Person wurde Auskunft über die Verarbeitung der personenbezogenen Daten erteilt (Art. 13 oder 14 der Verordnung, Datenschutzerklärungen);
- Sie wurde von der betroffenen Person freiwillig, unmissverständlich und – wenn die Verarbeitung zu mehreren Zwecken erfolgt – für jeden einzelnen dieser Zwecke erteilt. Die Einwilligung muss jederzeit widerrufbar sein.

Schließlich muss außerdem darauf geachtet werden, dass das Ersuchen um Einwilligung von anderen an die betroffene Person gerichteten Ansuchen oder Erklärungen klar zu unterscheiden ist (Art. 7.2). So ist beispielsweise auf den Vordrucken eine stillschweigende oder mutmaßliche Einwilligung (durch bereits angekreuzte Kästchen) nicht zulässig. Wenn die Verarbeitung besondere Kategorien personenbezogener Daten betrifft (Art. 9 DSGVO), muss die Einwilligung „ausdrücklich“ erfolgen, dasselbe gilt für die auf einer automatisierten Verarbeitung beruhenden Entscheidungen (einschließlich Profiling – Art. 22). Auch wenn dies nicht ausdrücklich vorgesehen ist, muss zum besseren Schutz des Verantwortlichen die eventuell erforderliche Einwilligung zur Datenverarbeitung schriftlich eingeholt werden.

Grundsätzlich kann der öffentliche – ebenso wie der private – Arbeitgeber die Daten seiner Angestellten auch ohne deren Einwilligung verarbeiten, da die rechtliche Grundlage für die Datenverarbeitung zu Arbeitszwecken im Art. 6 Abs. 1 Buchst. b) (Erfüllung eines Vertrags) und/oder Buchst. c) (Erfüllung einer rechtlichen Verpflichtung) der DSGVO festgelegt ist.



VERARBEITUNG, OFFENLEGUNG UND VERBREITUNG „GEWÖHNLICHER“ PERSONENBEZOGENER DATEN

Als Rechtsgrundlage für die Verarbeitung „gewöhnlicher“ personenbezogener Daten gemäß Art. 6 Abs. 3 Buchst. b) der DSGVO gelten ausschließlich Gesetzesbestimmungen, Verordnungsbestimmungen oder allgemeine Verwaltungsakte (Art. 2-ter des Datenschutzkodex).

Die Datenverarbeitung beginnt mit der Phase der Datenerhebung und ist nicht auf die Verwendung, Verarbeitung oder Offenlegung/Verbreitung beschränkt. Demzufolge muss die im Art. 13 und 14 der DSGVO vorgesehene Information bereits vor der Erhebung der Daten und nicht erst zum Zeitpunkt von deren tatsächlicher Verwendung, d. h. während der Verarbeitungsvorgänge, erfolgen.

Jede Verarbeitung personenbezogener Daten muss unter Einhaltung der im Art. 5 der Verordnung (EU) 2016/679 festgelegten Grundsätze erfolgen. Laut Art. 5 Abs. 2 der Verordnung müssen der Verantwortliche und seine Vertreter diese Grundsätze einhalten und ihre Einhaltung „nachweisen können“. Dieser sogenannte „Grundsatz der Rechenschaftspflicht“ (**accountability**) wird im Art. 24 Abs. 1 der Verordnung genauer definiert: „Der Verantwortliche setzt [...] geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“.

VERARBEITUNG, OFFENLEGUNG UND VERBREITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

Eine öffentliche Körperschaft kann nur jene personenbezogenen Daten „besonderer Kategorie“ – auch als sensible Daten bezeichnet – verarbeiten, die für die Ausübung institutioneller Tätigkeiten unentbehrlich sind, und wenn diese nicht von Fall zu Fall durch die Verarbeitung anonymer Daten oder personenbezogener Daten anderer Art erfüllt werden können.

Als Rechtsgrundlage für die Verarbeitung besonderer Kategorien personenbezogener Daten laut Art. 9 Abs. 1 der DSGVO gelten ausschließlich Gesetzesbestimmungen, Verordnungsbestimmungen oder allgemeine Verwaltungsakte, in denen die Arten von Daten, die verarbeitet werden dürfen, die ausführbaren Verarbeitungsvorgänge, der Grund des relevanten öffentlichen Interesses sowie gezielte angemessene Maßnahmen zum Schutze der Grundrechte und der Interessen der betroffenen Person genau angegeben sind (Art. 2-sexies des Datenschutzkodex).



VERARBEITUNG, OFFENLEGUNG UND VERBREITUNG VON GERICHTSDATEN

Die Verarbeitung von Daten betreffend strafrechtliche Verurteilungen und Straftaten ist nur zulässig, wenn dies aufgrund einer Gesetzesbestimmung oder, in den gesetzlich vorgesehenen Fällen, einer Ordnungsbestimmung erlaubt ist, die angemessene Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht (Art. 6 Abs. 1 der DSGVO und Art. 2-*octies* des Datenschutzkodex). Diese Art von Daten umfasst zum Beispiel die verwaltungsmäßige Abwicklung von Strafverfahren gegen Bedienstete oder die Verwaltung der Anti-Mafia-Bescheinigungen im Rahmen von Vergabeverfahren.

MINDESTMASSNAHMEN ZUR IT-SICHERHEIT

Der Zugang zum IT-System ist ausschließlich den ermächtigten Benutzern nach eindeutiger Identifizierung und Authentifizierung gestattet. Die Nutzer des Systems verfügen über differenzierte Zugriffsberechtigungen entsprechend ihren Zuständigkeiten und den von ihrem Amt festgelegten Arten von Vorgängen, um ein Übermaß an Berechtigungen in den Händen eines einzigen Nutzers zu vermeiden. Jeder Benutzer erhält:

- eigene Authentifizierungsdaten, d. h. User-ID (von der Verwaltung festgelegt) und Passwort (vom Benutzer festgelegt)
- eine oder mehrere Rollen, von denen jede mit spezifischen Funktionen und Einsichtsberechtigungen in Dokumente und Faszikel, je nach den ausgeübten Zuständigkeiten und institutionellen Aufgaben, verbunden ist.

Der Zugriff erfolgt sowohl vom eigenen Arbeitsplatz aus oder im Remote-Modus über eine VPN-Verbindung. Die für Datenschutz zuständige Führungskraft legt die Organisationsabläufe fest, um ein dem Risiko im Bereich des Datenschutzes angemessenes Sicherheitsniveau zu gewährleisten, und erteilt allen Organisationsstrukturen die operativen Anweisungen gemäß Verordnung (EU) 2016/679. Auf der Grundlage dieser Anweisungen ermächtigen die Führungskräfte ihre Mitarbeiter zur Verarbeitung der Daten und – je nach den ausgeübten Zuständigkeiten und institutionellen Aufgaben – zum Zugang zu einer oder mehreren Rollen innerhalb des Dokumentenverwaltungssystems.

Hinweis: Bei der Regionalverwaltung wurden „Anweisungen für die Verwendung der elektronischen Geräte“ (Beschluss der Regionalregierung vom 31. Oktober 2019, Nr. 237) erlassen und vor Kurzem den Bediensteten erneut zur Kenntnisnahme unterbreitet. Sie sind ein bewährtes und weiterhin gültiges Instrument der Regionalverwaltung zur Bekämpfung des Missbrauchs der Informationstechnologie und geben allen Nutzern des regionalen Netzwerks Hinweise zur korrekten Verwendung der ihnen zur Verfügung gestellten IT- und technologischen Ressourcen. Darüber hinaus ist die stets aktive Rolle des Amts für Informatik und Digitalisierung bei der Unterstützung der Bediensteten und der Zusammenarbeit mit



dem Systemadministrator zu erwähnen.

DATEISYSTEME IN PAPIERFORM UND ZUGANG ZU DEN ÄMTERN

Der Datenschutz muss auch durch geeignete materielle Maßnahmen hinsichtlich Datenzugang und Datenspeicherung sowie durch die Anwendung bewährter Verfahren seitens aller Personen, die personenbezogene Daten verarbeiten, gewährleistet werden. In der Praxis bedeutet dies, dass der Zugang zu den Räumlichkeiten der Verwaltung natürlich durch geeignete Systeme zur Verhinderung von Einbrüchen geschützt werden muss, gegebenenfalls auch durch Alarmanlagen und Videoüberwachung. Alle Dokumente in den Büros müssen stets ordnungsgemäß abgelegt und so aufbewahrt werden, dass die Anonymität der darin enthaltenen Daten gewährleistet ist; insbesondere müssen für die Aufbewahrung von Dokumenten, die sensible Daten enthalten, besondere und zusätzliche Sicherheitsmaßnahmen vorgesehen werden, wie Tresore oder Schränke mit Schlüsseln. Die Bediensteten und Mitarbeiter der Verwaltung unterliegen der Rechenschaftspflicht und müssen nicht die geltenden Vorschriften anwenden, sondern auch die Einhaltung des Schutzes der personenbezogenen Daten konkret überwachen und überprüfen.

In diesem Zusammenhang ist daran zu erinnern, dass Papiermaterial mit personenbezogenen Daten, das im Rahmen der Arbeitstätigkeit verwendet wird, nicht unbeaufsichtigt auf den Schreibtischen liegen darf und nach Arbeitsende an einem sicheren Ort, nach Möglichkeit in einem verschlossenen Schrank, aufbewahrt werden muss. Darüber hinaus ist während des normalen täglichen Arbeitsablaufs darauf zu achten, dass Dokumente, die personenbezogene Daten enthalten, nicht ohne weiteres für Dritte oder jedenfalls für Personen, die nicht zur Verarbeitung befugt sind, einsehbar sind. Im Falle der Verarbeitung besonderer Daten (Gesundheitszustand, Gerichtsdaten usw.) müssen alle Papierunterlagen in verschlossenen Schränken/Schubladen aufbewahrt werden, falls man sich, auch nur vorübergehend, vom Arbeitsplatz entfernt. Es wird außerdem darauf hingewiesen, dass die Region über ein eigenes historisches Archiv und Zwischenarchiv in Gardolo (Trient) verfügt. Die Unterbringung der Dokumentation sowie die Aussonderung und Entsorgung veralteter Materialien erfolgten unter der Leitung der „Soprintendenza archivistica“. Hierzu hat die Region ein Handbuch des Dokumentenverwaltungssystems erstellt.

Hinweis: Bei der Regionalverwaltung werden Eingänge und Einfahrten durch ein Videoüberwachungssystem kontrolliert. Aufgrund der besonderen Art der verarbeiteten Daten hat die Region eine Datenschutz-Folgenabschätzung zum Einsatz des Videoüberwachungssystems durchgeführt, die von unserem DSB befürwortet und positiv beurteilt wurde. „Hinweise“ auf diese Arbeit finden sich auf den neben den Kameras angebrachten Schildern.



DATA BREACH

Die von der Regionalverwaltung aufbewahrten, übermittelten oder verarbeiteten personenbezogenen Daten können – genauso wie bei privaten Unternehmen oder anderen öffentlichen Verwaltungen – der Gefahr des Verlustes, der Zerstörung oder der unzulässigen Verbreitung infolge von Cyberangriffen, unbefugtem Zugriff, Unfällen oder Zwischenfällen wie Bränden oder anderen Katastrophen ausgesetzt sein. Diese Ereignisse können den Datenschutz der betroffenen Personen ernsthaft gefährden.

Die Datenschutzbehörde hat mit der Maßnahme *Sicherheitsvorkehrungen und Modalitäten für den Austausch von personenbezogenen Daten zwischen öffentlichen Verwaltungen* vom 2. Juli 2015 die Pflicht vorgesehen, Datenschutzverletzungen oder IT-Zwischenfälle (unbefugte Zugriffe, *Malware*-Vorfälle) zu melden, die, auch wenn sie keine direkte Auswirkungen auf die Daten haben, diese dennoch der Gefahr einer Datenschutzverletzung (= *Data Breach*) aussetzen können.

Auch die Regionalverwaltung muss demnach als öffentliche Verwaltung sämtliche Datenschutzverletzungen oder IT-Zwischenfälle, die beachtliche Auswirkungen auf die verarbeiteten personenbezogenen Daten haben könnten, innerhalb von zweiundsiebzig Stunden nach deren Bekanntwerden der Datenschutzbehörde melden.

Das Versäumnis, die Datenschutzbehörde über Datenschutzverletzungen oder IT-Zwischenfälle zu benachrichtigen, stellt eine Ordnungswidrigkeit dar, die gemäß Art. 162 Abs. 2 Buchst. b) des Datenschutzkodex sanktioniert wird.

Hinweis: Es ist an dieser Stelle darauf hinzuweisen, dass die ersten im Falle einer vermuteten oder bestätigten Datenschutzverletzung zu benachrichtigenden Personen der interne Datenschutzreferent und der Systemadministrator sind. Die Regionalverwaltung hat unter Beachtung der geltenden Bestimmungen das bei *Data Breach* anzuwendende Verfahren erarbeitet, das die Regionalregierung mit Beschluss vom 4. Dezember 2024, Nr. 232 genehmigt hat.

ÜBERMITTLUNG VON DATEN AN NICHT-EU-LÄNDER

ÜBERMITTLUNG PERSONENBEZOGENER DATEN

Als **Übermittlung** personenbezogener Daten gilt jede auch nur vorübergehende Weitergabe von Informationen innerhalb oder außerhalb des Bereichs, in dem die Verarbeitung stattfindet (z. B. von einem Betriebsserver zu einem anderen), während die **Offenlegung** von Daten als die Zurverfügungstellung von Daten an andere Personen als die betroffene Person durch den Verantwortlichen für die Datenverarbeitung, den Auftragsverarbeiter oder die beauftragten Personen definiert wird.

In Anbetracht der oben genannten Begriffe ist jede auch nur vorübergehende



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Weitergabe von Informationen ins Ausland, einschließlich ihrer vorübergehenden Speicherung auf einem Server des Verantwortlichen für die Datenverarbeitung, der sich außerhalb des nationalen Hoheitsgebiets befindet, als *Übermittlung ins Ausland* zu verstehen.

Die Übermittlung personenbezogener Daten ins Ausland ist in den Art. 42-45 der Verordnung (EU) 2016/679 geregelt. Insbesondere sieht die DSGVO vor, dass die Übermittlung von Daten nur in den ausdrücklich im Art. 45 ff. der Verordnung festgelegten Fällen erfolgen darf, d. h. bei Vorliegen von Standardvertragsklauseln, Zertifizierungsmechanismen, verbindlichen internen Datenschutzvorschriften oder Verhaltensregeln. Vor allem die Übermittlung von Daten in die Vereinigten Staaten erfolgte bis vor kurzem nach dem strengen Protokoll der Standardvertragsklauseln. 2023 hat die Europäische Kommission den Angemessenheitsbeschluss zum Datenschutzrahmen EU-USA angenommen, in dem festgelegt ist, dass die Vereinigten Staaten ein angemessenes und mit dem der EU vergleichbares Datenschutzniveau für die aus der EU an die amerikanischen Unternehmen im Rahmen der neuen Vereinbarung (Data Privacy Framework) übermittelten Daten gewährleisten. Die personenbezogenen Daten können demnach an die der Rahmenvereinbarung beigetretenen Unternehmen in den Vereinigten Staaten übermittelt werden, ohne dass zusätzliche Datenschutzgarantien geleistet werden müssen.

Hinweis: Bei der Regionalverwaltung ist im Verzeichnis der Verarbeitungstätigkeiten durch Ankreuzen von „ja“ bzw. „nein“ in der entsprechenden Spalte anzugeben, ob eine Übermittlung der verarbeiteten Daten ins Ausland erfolgt.

DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)

Laut Art. 35 der Verordnung (EU) 2016/679 muss der Verantwortliche für die Datenverarbeitung vorab eine Abschätzung der Folgen immer dann durchführen, wenn die Art der Verarbeitung, insbesondere bei Verwendung neuer Technologien und aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben kann. In diesen Fällen führt der Verantwortliche für die Datenverarbeitung demnach eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. In einer einzigen Folgenabschätzung können mehrere ähnliche Verarbeitungen untersucht werden, die ähnliche Risiken aufweisen.

Die Folgenabschätzung sollte möglichst vor der eigentlichen Datenverarbeitung vorgenommen werden. Neben dieser Vorgabe ist darauf hinzuweisen, dass das Verfahren der Datenschutz-Folgenabschätzung einer ständigen Überprüfung unterliegen muss, da sich die Verarbeitungsvorgänge in der Regel rasch weiterentwickeln und leicht neue Elemente der Gefährdung auftreten können, die eine Überarbeitung des Verfahrens erforderlich machen, um das Datenschutzniveau zu wahren, wenn sich die Bedingungen im Laufe der Zeit



ändern.

Hinweis: Bei der Regionalverwaltung wurden bereits in Zusammenarbeit mit dem DSB die Folgenabschätzungen in Bezug auf die Datenverarbeitung in Zusammenhang mit der Videoüberwachung, dem Whistleblowing und der Durchführung von Datenverarbeitungstätigkeiten des Amts für Personalentwicklung und Inspektionsdienst vorgenommen.

ZUR VERTIEFUNG: KONSULTATION DER DATENSCHUTZBEHÖRDE HINSICHTLICH DER GESETZESAKTE DER REGION

Im Sinne von Art. 36 Abs. 4 und 5 der DSGVO ist die vorherige Konsultation der Datenschutzbehörde im Falle der Ausarbeitung von Gesetzesbestimmungen oder Verordnungen immer dann erforderlich, wenn die Bestimmungen Auswirkungen auf die Verarbeitung personenbezogener Daten haben bzw. wenn der Verantwortliche eine Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe vornimmt. Grundlage für diese Konsultation ist in erster Linie eine Folgenabschätzung, die zwar alle Gefahrenaspekte abdeckt, aber ein schwer zu minimierendes Restrisiko offen lässt. In dieser Phase kann die Datenschutzbehörde den Verantwortlichen auffordern, zum Schutz der Daten der betroffenen Person für entsprechende Maßnahmen und Vorkehrungen zu sorgen, die in Form von Maßnahmen allgemeinen Charakters von Amts wegen getroffen werden.

Es wird dementsprechend darauf hingewiesen, dass durch die Konsultation der Datenschutzbehörde in der Phase der Ausarbeitung der Rechtsvorschriften der Grundsatz „*Privacy by Design*“ zur Anwendung kommt.

HINWEISE BETREFFEND DIE VERÖFFENTLICHUNGEN AUF DER OFFIZIELLEN WEBSITE DER REGION UND IM BEREICH TRANSPARENTE VERWALTUNG

Die Online-Transparenz der öffentlichen Verwaltung ist nichts anderes als die Veröffentlichung von Akten, Dokumenten und Daten der öffentlichen Verwaltung auf ihrer Website. Der Hauptzweck der Online-Transparenz besteht darin, Formen der Kontrolle über das Verwaltungshandeln, die Verwendung der öffentlichen Mittel und die Art und Weise, wie die öffentliche Verwaltung ihre Ziele erreicht, zu fördern.

Die Veröffentlichung der Daten, Informationen und Dokumente im Bereich „Transparente Verwaltung“ auf der offiziellen Website der Region erfolgt in



Beachtung der Veröffentlichungs-, Transparenz- und Informationspflichten der öffentlichen Verwaltungen im Sinne des Art. 1 Abs. 35 des Gesetzes vom 6. November 2012, Nr. 190 („Anti-Korruptionsgesetz“) gemäß Gesetzesdekret vom 14. März 2013, Nr. 33, geändert durch das Gesetzesdekret vom 25. Mai 2016, Nr. 97. Der Bereich „Transparente Verwaltung“ ist gemäß den Vorgaben laut Anlage 1 des ANAC-Beschlusses vom 28. Dezember 2016, Nr. 1310 „Erste Richtlinien mit Hinweisen zur Erfüllung der Veröffentlichungs-, Transparenz- und Informationspflichten gemäß GvD Nr. 33/2013, geändert durch GvD Nr. 97/2016“ gegliedert. Mit Regionalgesetz vom 29. Oktober 2014, Nr. 10 wurden die Bestimmungen zur Anpassung der Rechtsordnung der Region an die Veröffentlichungs-, Transparenz- und Informationspflichten gemäß Gesetz vom 6. November 2012, Nr. 190 und gesetzesvertretendem Dekret vom 14. März 2013, Nr. 33 erlassen. Mit RG vom 15. Dezember 2016, Nr. 16 wurden diese Pflichten den durch das gesetzesvertretende Dekret vom 25. Mai 2016, Nr. 97 eingeführten Neuerungen angepasst. Bei der Regionalverwaltung ist die Transparenz neben den genannten Bestimmungen auch durch Art. 7-*quinquies* des Regionalgesetzes vom 21. Juli 2000, Nr. 3 i.d.g.F. geregelt, laut dem die Regionalregierung Beschlüsse, Dekrete, Entscheidungen der Führungskräfte und jeden anderen Verwaltungsakt – unbeschadet der geltenden Gesetzesbestimmungen zum Schutz von sensiblen und Gerichtsdaten – veröffentlicht und für die Dauer von fünf Jahren zugänglich hält.

Die in den Richtlinien der Datenschutzbehörde enthaltenen Grundsätze und Bestimmungen zum Schutz personenbezogener Daten sind grundlegend und auch auf den Prozess der Datenveröffentlichung im Internet zu Zwecken der Transparenz anzuwenden. Darüber hinaus müssen die Grundsätze der Erheblichkeit und der Minimierung personenbezogener Daten beachtet werden, die nur dann in die zu veröffentlichenden Akte und Dokumente aufgenommen werden dürfen, wenn dies wirklich erforderlich ist. Diese Daten müssen in einem angemessenen Verhältnis zu dem verfolgten Zweck der Transparenz stehen.

Die Dauer der Veröffentlichung öffentlicher Akte ist durch das gesetzesvertretende Dekret in Sachen Transparenz und durch das Regionalgesetz Nr. 3/2000 geregelt, in dem festgelegt ist, dass die online veröffentlichten Akte für höchstens fünf Jahre zugänglich sein müssen, wobei folgende Ausnahmen gelten:

- Akte, die nach Ablauf der fünf Jahre weiterhin ihre Wirkungen erzeugen und folglich solange veröffentlicht werden müssen, bis die Wirkungen erlöschen (Informationen zu Führungskräften und Inhabern von Spitzenpositionen bei der öffentlichen Verwaltung, die aktualisiert werden und bis zum Ablauf ihres Vertrags online bleiben können)
- Daten betreffend die Inhaber politischer Ämter, Führungskräfte, Berater und Mitarbeiter (die nach Ablauf des Vertrags weitere drei Jahre zugänglich bleiben müssen)
- Daten, für die in Datenschutzbestimmungen eine andere Frist festgelegt ist.

Die Veröffentlichungen auf der offiziellen Website der Region erfolgen zur Gewährleistung der höchstmöglichen Transparenz der Verwaltungsakte, wie es im Art. 7-*quinquies* des Regionalgesetzes vom 21. Juli 2000, Nr. 3 i.d.g.F. festgelegt ist. Die in den Verwaltungsakten enthaltenen personenbezogenen Daten werden, sofern erforderlich, gemäß den Anweisungen der Datenschutzbehörde aus Gründen des Schutzes der Vertraulichkeit anonymisiert. Jeder, der ein Interesse am Verfahren hat, hat das Recht auf Zugang zu den Verwaltungsunterlagen gemäß Regionalgesetz



vom 31. Juli 1993, Nr. 13.

An dieser Stelle ist darauf hinzuweisen, dass die Regionalverwaltung der dargelegten Pflicht durch die Veröffentlichung aller gesetzlich vorgeschriebenen Akte und Informationen im Bereich „Transparente Verwaltung“ nachkommt. Die veröffentlichten Inhalte sowie die für die Veröffentlichung und die Einhaltung der Veröffentlichungsfristen verantwortlichen Bediensteten können in der **ANLAGE Nr. 1** Unterabschnitt 2.3 „Korruptionsrisiken und Transparenz“ des PIAO 2024-2026 eingesehen werden.

Mit Beschluss der Regionalregierung vom 30. Jänner 2024, Nr. 1 wurde der jährlich aktualisierte Integrierte Tätigkeits- und Organisationsplan (PIAO) der Autonomen Region Trentino-Südtirol für den Dreijahreszeitraum 2024-2026 genehmigt.

Hinweis: Bei der Regionalverwaltung ist jedes einzelne Amt für die Einhaltung der Fristen für die Veröffentlichung im Bereich „Transparente Verwaltung“ der offiziellen Website der Region selbst zuständig. Das gesamte oben genannte Material kann auf der Website der Region unter folgendem Link eingesehen werden:

<https://www.region.tnst.it/Transparente-Verwaltung/Sonstige-Inhalte/Korruptionsvorbeugung/Dreijahresplan-fuer-die-Korruptionsvorbeugung-und-die-Transparenz/Integrierter-Taetigkeits-und-Organisationsplan-PIAO-der-Autonomen-Region-Trentino-Suedtirol-fuer-den-Dreijahreszeitraum-2024-2026>

SICHERHEITSMASSNAHMEN FÜR DIE DURCHFÜHRUNG VON VIDEOKONFERENZEN

Der Schutz der Privatsphäre bei Videokonferenzen ist wichtig, um sicherzustellen, dass die Gespräche vertraulich bleiben.

Bei der Nutzung des von der Regionalverwaltung zur Verfügung gestellten Videokonferenzsystems ist Folgendes zu beachten:

- Wenn die Sitzung von Dritten aufgezeichnet wird, muss man sich vergewissern, wer sie aufzeichnet, wie die Aufzeichnung verwendet wird und wo die Aufzeichnung gespeichert wird. Wenn man der Organisator ist, ist die Zustimmung der Teilnehmenden einzuholen, bevor eine Aufzeichnung gestartet wird;
- Ungeschützte, öffentliche Netze sollten nicht verwendet werden;
- Es ist sicherzustellen, dass die Besprechung durch ein Passwort geschützt ist und dass der Link nur für berechtigte Teilnehmende freigegeben wird;
- Videokonferenzsysteme sind Arbeitsmittel, die als Alternative zu Präsenzsitzungen oder zu Telefongesprächen verwendet werden können und für die ein Headset mit Mikrofon (z. B. auch mit dem eines Mobiltelefons) zu benutzen ist; dadurch verbessert sich die Qualität des Audiosignals erheblich;
- Das eigene Mikrofon ist auszuschalten, wenn es nicht verwendet wird, um das Auftreten von Rauschen oder Störungen zu vermeiden;
- Wird die Verbindung von zu Hause aus hergestellt und steht kein abgesonderter Raum zur Verfügung, so kann ein virtueller Hintergrund verwendet oder die Videokamera nach Testen der Beleuchtung ausgeschaltet werden;



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

- Steht keine ausreichende Bandbreite zur Verfügung, um ein adäquates Audio- und Videosignal zu gewährleisten, ist es sinnvoll, die Videokamera auszuschalten;
- Am Ende der Videokonferenz ist immer die Verbindung zu unterbrechen, da derselbe Raum später für andere Sitzungen genutzt werden könnte.

HINWEISE IN SACHEN RECHT AUF AKTENZUGANG

Die Veröffentlichung der Akte erfolgt ausschließlich zur Gewährleistung der höchstmöglichen Transparenz der Verwaltungsakte (Art. 7-*quinquies* des Regionalgesetzes vom 21. Juli 2000, Nr. 3 i.d.g.F.). Jeder, der ein Interesse am Verfahren hat, hat das Recht auf Zugang zu den Verwaltungsunterlagen gemäß dem Regionalgesetz vom 31. Juli 1993, Nr. 13, geändert durch das Regionalgesetz vom 23. Oktober 1998, Nr. 10, und der entsprechenden mit Dekret des Präsidenten der Region vom 16. November 2004, Nr. 7/L genehmigten und durch Dekret des Präsidenten der Region vom 20. November 2019, Nr. 83 geänderten Durchführungsverordnung.

Auch in diesem Bereich hält sich die Regionalverwaltung an die im Beschluss der Regionalregierung vom 30. Jänner 2024, Nr. 1 zur Genehmigung des Integrierten Tätigkeits- und Organisationsplans (PIAO) der Autonomen Region Trentino-Südtirol für den Dreijahreszeitraum 2024-2026 enthaltenen Bestimmungen. Für diesen spezifischen Sachverhalt sind die zu befolgenden Anweisungen in der **ANLAGE Nr. 2** Unterabschnitt 2.3 – Korruptionsrisiken und Transparenz angeführt, die das Rundschreiben Nr. 11/2018 Prot.-Nr. 18085 betreffend „Abwicklung der Anträge auf allgemeinen Bürgerzugang, auf (einfachen) Bürgerzugang sowie auf Zugang zu den Verwaltungsunterlagen über das P.I.Tre.-System und Register der allgemeinen Bürgerzugänge“ und die diesbezüglichen Anlagen enthält.

INTERNE WEITERBILDUNG UND INFORMATION

Um das Wissen zu diesem Thema zu verbreiten und das gesamte Personal der Region entsprechend zu unterweisen, werden jährlich folgende Verpflichtungen im Bereich der Personalschulung eingegangen und umgesetzt:

- Gewährleistung von Schulungen für alle Personen, die den internen Datenschutzreferenten bei seiner Tätigkeit unterstützen, um ihnen die Kenntnis und Ausführung der in den Vorschriften vorgesehenen Aufgaben und Tätigkeiten zu erleichtern
- Durchführung spezifischer Schulungsprojekte oder -veranstaltungen entsprechend den am besten geeigneten Modalitäten, auch in Absprache mit dem DSB und Trentino School of Management (TSM).

Die Organisationsstrukturen und Ämter der Regionalverwaltung können sich über das Amt für allgemeine Angelegenheiten an den Datenschutzbeauftragten wenden, um Fragen zu stellen oder weitere Informationen anzufordern, nachdem sie sich mit den Mitarbeitern seiner Unterstützungsstruktur ausgetauscht haben. Weitere Schulungs-/Informationsmaßnahmen werden anlässlich der Einführung neuer wichtiger



Instrumente in Bezug auf die Verarbeitung personenbezogener Daten vorgeschlagen.

INSTRUMENTE FÜR DIE ÜBERWACHUNG UND ÜBERPRÜFUNG DER RECHENSCHAFTSPFLICHT DER REGION

Gemäß Art. 24 und 32 der DSGVO gehört zu den Pflichten in Zusammenhang mit der Rechenschaftspflicht die Implementierung eines Überwachungs-, Überprüfungs- und Kontrollmechanismus für das Datenschutzsystem.

Bei der Regionalverwaltung sind verschiedene Kontrollebenen vorhanden:

- eine erste Überprüfungsebene, die in den einzelnen Ämtern durch die in den Rundschreiben der Führungskräfte enthaltenen Anweisungen und die Anwendung geeigneter Verfahren umgesetzt wird;
- eine zweite Überprüfungsebene (Compliance-Kontrolle), die zu den Diensten des DSB gehört und durch regelmäßig durchgeführte Audits umgesetzt wird.

Dem DSB werden zur Durchführung der Audits folgende Instrumente zur Verfügung gestellt:

- Das Verzeichnis der Verarbeitungstätigkeiten;
- Das Verzeichnis der Datenschutzverletzungen, d. h. das Verzeichnis, in dem Ereignisse, Zwischenfälle, Beinahe-Zwischenfälle (anormale Situationen oder Sicherheitsvorfälle) sowie die tatsächlichen Datenschutzverletzungen einzutragen sind, unabhängig davon, ob der Fall gemäß Art. 32 und 33 der Datenschutzbehörde gemeldet und/oder die betroffenen Personen benachrichtigt wurden.

Folgende weitere zur Überwachung und Kontrolle des Datenschutzsystems erforderliche Dokumente und Daten können in Zusammenhang mit den Audits bei der Regionalverwaltung angefordert werden:

- regelmäßige Berichte gemäß Art. 28 der DSGVO über den ordnungsgemäßen Abschluss der vom externen Auftragsverarbeiter gemäß den erteilten Anweisungen durchgeführten Verarbeitungstätigkeiten;
- regelmäßige Berichte über die Durchführung der Tätigkeiten, die in die Zuständigkeit der Systemadministratoren fallen;
- Audit-Berichte und regelmäßige Berichte, die der DSB bei Audits und Überprüfungen in seinem Zuständigkeitsbereich formell erstellt.

Die Durchführung von Kontrollen und Audits zur Überprüfung der Anwendung der geltenden Bestimmungen und der erteilten Anweisungen ist eine Aufgabe des Datenschutzbeauftragten, der dabei vom Amt für allgemeine Angelegenheiten des Generalsekretariats unterstützt wird.

HAFTUNG UND SANKTIONEN

Die öffentliche Verwaltung ist wie jedes andere Rechtssubjekt verpflichtet, die **DSGV** (Verordnung (EU) 2016/679) und den **italienischen Datenschutzkodex** (GvD Nr. 196/2003, geändert durch GvD Nr. 101/2018) einzuhalten.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Verstöße gegen die Bestimmungen der DSGVO und des Kodex führen je nach Schwere des Verstoßes zu Verwaltungsstrafen oder strafrechtlichen Folgen.



BEREITSTELLUNG DES HANDBUCHS DER DATENSCHUTZVERFAHREN

Dieses Handbuch der Datenschutzverfahren steht allen Bediensteten, dem Verantwortlichen, dem Auftragsverarbeiter und den mit der Verarbeitung personenbezogener Daten beauftragten Personen zur Verfügung. Die darin enthaltenen Verfahren müssen allen Personen, die in irgendeiner Funktion mit personenbezogenen Daten in Berührung kommen, im Detail bekannt sein.

ÜBERPRÜFUNG DES DATENSCHUTZSYSTEMS

Im Hinblick auf eine kontinuierliche Verbesserung, bei der die Wirksamkeit der technischen und organisatorischen Maßnahmen stets im Mittelpunkt steht, wird dieses Handbuch der Datenschutzverfahren bei folgenden Gelegenheiten überprüft:

- neue von der Datenschutzbehörde erlassene Bestimmungen, die sich auf die für die Regionalverwaltung relevanten Datenschutzvorschriften auswirken;
- wesentliche und bedeutende Änderungen der den Abteilungen zugewiesenen Befugnisse;
- Einführung neuer, für die Verarbeitung personenbezogener Daten relevanter Verwaltungsinstrumente;
- Verhängung von Sanktionen durch die Gerichtsbehörde oder die Datenschutzbehörde in diesem Sachbereich.

Die Überprüfung erfolgt in Zusammenarbeit mit dem DSB und das Ergebnis wird der Regionalregierung unterbreitet, die die eventuell erforderlichen Beschlüsse fasst, um die Einhaltung der Vorschriften und eine kontinuierliche Verbesserung zu gewährleisten



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Segreteria generale
Ufficio affari generali
☎ 0461 201323
@ affgen@regione.taa.it
pec: affgen@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come
metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files
allegati alla medesima.

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

TRATTAMENTO VIDEOSORVEGLIANZA

(art. 35 Regolamento europeo 679/2016)



1. Descrizione sistematica del trattamento

- Attività di trattamento: Il sistema di videosorveglianza in essere opera raccogliendo, registrando e conservando immagini, per un tempo massimo pari a 72 ore dalla data di registrazione, configurando così un trattamento di dati personali (art. 4, comma 1, lett b.) del Codice). È infatti considerato dato personale qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione.
- Finalità:
 - ✓ Protezione della proprietà pubblica, in particolar modo degli spazi antistanti la Regione e dello spazio adibito a parcheggio del personale dipendente¹;
 - ✓ Acquisizione di prove, da fornire alle Autorità pubbliche in caso di richiesta motivata di accesso alle registrazioni, nel quadro delle competenze ad essi attribuite per legge e al fine di produrre un atteggiamento collaborativo nei confronti delle Autorità pubbliche richiedenti.
- Tipologia di dati trattati: vengono trattati esclusivamente immagini, pertanto solamente questa tipologia di dati personali rientra nelle finalità sopra elencate.
- Modalità: l'attività di videosorveglianza viene effettuata in relazione anche l'area di ripresa, la quale deve essere dimensionata al fine di non eccedere con il trattamento dei dati. Vengono pertanto formalmente incaricati i dipendenti dei Servizi generali dedicati al servizio di portierato per la visione delle immagini. L'estrapolazione invece delle immagini è effettuata da personale dipendente della Regione, autorizzato mediante specifica lettera di incarico.
- Categorie di interessati: sono interessati al trattamento dei dati i seguenti soggetti:
 - ✓ soggetti con rapporti funzionali o di dipendenza dall'Ente
 - ✓ cittadini e utenti
- Categorie di destinatari: sono destinatari del trattamento dei dati i seguenti soggetti:
 - ✓ persone autorizzate alla visione ed estrapolazione dei dati;
 - ✓ altre pubbliche amministrazioni, che nelle modalità e nei tempi previsti ne facciano richiesta.
- Contesto: il contesto operativo a cui viene applicato il presente schema sintetico di trattamento dei dati, riguarda essenzialmente l'area circostante il palazzo della Regione, a Trento in via Gazzoletti n. 2, destinata al monitoraggio visivo degli ingressi e delle uscite dagli uffici della Regione, all'attività di videosorveglianza dei varchi nonché del parcheggio riservato ai dipendenti della Regione (la telecamera dedicata alla sorveglianza di questo spazio, effettua ogni due minuti circa, una rotazione su se stessa pari a 360°, cambiando così con cadenza regolare l'area di registrazione).

¹ La telecamera dedicata alla sorveglianza del parcheggio della Regione, effettua ogni due minuti circa una rotazione su se stessa di 360°.



Estratto del verbale della seduta del 4 dicembre 2024

DELIBERAZIONE N. 233

Oggetto:

Valutazione di impatto della Regione Autonoma Trentino-Alto Adige/Südtirol sulla protezione dei dati relativa al Servizio ispettivo e di formazione, incardinato presso la Segreteria generale dell'amministrazione regionale

Arno Kompatscher	Presidente	presente
Giulia Zanotelli	Vice Presidente sostituta del Presidente	presente
Franz Thomas Locher	Vice Presidente	presente
Carlo Daldoss	Assessore	presente
Angelo Gennaccaro	Assessore	presente
Luca Guglielmi	Assessore	presente
Gabriele Morandell	Segretaria generale della Giunta regionale	presente

Su proposta del Presidente Arno Kompatscher

Segreteria generale

Ufficio affari generali

In riferimento all'oggetto la Giunta regionale ha discusso e deliberato quanto segue:

Premesso che:

- la valutazione di impatto sulla protezione dei dati, di seguito in sigla DPIA, è una procedura intesa a descrivere un trattamento, a valutarne la necessità e la proporzionalità nonché a valutarne i rischi per i diritti e libertà delle persone fisiche, allo scopo di determinare le misure per affrontarli, gestirli e se possibile eliminarli o comunque ridurli al minimo;
- la DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il Titolare non soltanto a rispettare le prescrizioni del Regolamento (UE) n. 2016/679 ma anche ad attestare di aver adottato misure idonee a garantire tali prescrizioni;
- ai sensi dell'art. 5, par. 2, del Regolamento (UE) n. 2016/679, la Regione Autonoma Trentino-Alto Adige/Südtirol, quale Titolare del trattamento, è competente per il rispetto delle disposizioni relative alla protezione delle persone fisiche a riguardo del trattamento dei dati personali ed in grado di provarlo secondo il principio della "responsabilizzazione";
- ai sensi dell'art. 35 del Regolamento (UE) n. 2016/679, il Titolare del trattamento effettua una valutazione dell'impatto quando un tipo di trattamento, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi;
- le attività di trattamento poste in essere dall'Ufficio sviluppo del personale e servizio ispettivo della Regione Autonoma Trentino-Alto Adige/Südtirol presentano un rischio elevato in ragione della particolare delicatezza delle informazioni trattate, nonché degli elevati rischi, in termini di possibili effetti lesivi dei diritti e delle libertà dei dipendenti, quali interessati cui si riferiscono i dati personali oggetto dei trattamenti;
- il Titolare del trattamento ha sottoposto le attività di trattamento sopramenzionate a valutazione d'impatto.

Rilevato che il Responsabile Protezione dei Dati (d'ora in poi, RPD) con nota n. 29628 di data 08/11/2024 ha dichiarato di aver ricevuto copiosa documentazione amministrativa interna attestante le modalità di svolgimento dell'attività di trattamento, nonché delle misure di sicurezza attivate, e che il Titolare del trattamento dei dati dell'amministrazione regionale:

- ha individuato la base giuridica legittimante l'attività di trattamento;
- ha descritto i trattamenti posti in essere per l'attività oggetto della DPIA;
- ha valutato la necessità e proporzionalità dei trattamenti in relazione alle finalità dichiarate;
- ha condotto la valutazione dei rischi per i diritti e le libertà degli interessati, ipotizzando gli eventi/violazioni di dati e le minacce specifiche ritenute pertinenti nelle attività di trattamento in esame. Nello specifico, il Titolare ha valutato quale potesse essere l'impatto dell'evento sui diritti dell'interessato, nonché la probabilità del suo accadimento;

- ha riscontrato un primo esito di livello medio-basso dell'analisi del rischio, fatta eccezione per nr. 3 minacce che hanno riscontrato un livello di rischio medio alto/rilevante;
- ha individuato alcune misure in grado di attenuare i livelli di rischio medio-alti rilevati e, per ciascuna di queste, ha individuato i soggetti preposti alla loro implementazione;
- ha condotto una seconda analisi del rischio misurando la bontà delle misure di mitigazione del rischio ed ha ottenuto un livello di rischio medio-basso di rischio generale per i diritti e le libertà degli interessati;
- ha riscontrato le richieste di integrazione formulate dell'RPD con e-mail dd. 20/06/2023, 26/10/2023, 28/02/2024 e, da ultimo, per le vie brevi, in data 28/08/2024;
- ha fornito la documentazione a corredo delle analisi condotte.

Preso atto che alla luce delle azioni intraprese dall'amministrazione regionale l'RPD, con la nota sopracitata, ha espresso parere favorevole alla DPIA trasmessa, condizionato tuttavia all'osservanza di ulteriori indicazioni e suggerimenti, che vanno a migliorare e completare la valutazione di impatto svolta. In particolare viene richiesto:

- di integrare l'informativa completa, con particolare riferimento all'art. 14 e alla base giuridica legittimante;
- di verificare con tutti i fornitori nominati all'interno della DPIA che le misure di sicurezza siano adeguate ed aggiornate, al fine di garantire la tutela dei dati personali in linea con l'art. 32 del GDPR.

Dato atto inoltre che l'amministrazione regionale provvede ad adeguarsi alle indicazioni prescritte.

Considerato altresì che la DPIA rappresenta una misura di *accountability* e in quanto tale è necessario condurla nuovamente sulle medesime attività di trattamento se:

- vi è una variazione delle caratteristiche delle attività di trattamento (modalità del trattamento o modifiche impattanti sugli aspetti della sicurezza fisica, tecnica, organizzativa o informatica)
- se l'attività di trattamento riguarda dati particolari che, per loro natura, richiedono una maggiore tutela e cura;
- in ogni caso, periodicamente, alla modifica delle condizioni generali interne alla struttura organizzativa dell'amministrazione regionale.

Ad unanimità di voti legalmente espressi,

delibera

- di approvare la valutazione di impatto della Regione autonoma Trentino-Alto Adige/Südtirol condotta sull'attività di trattamento relativa alle attività poste in essere dall'Ufficio sviluppo del personale e servizio ispettivo, corredata della relativa documentazione, come registrata nel protocollo dell'amministrazione regionale all'ID n. 28574699.

Letto, confermato e sottoscritto.

IL PRESIDENTE

Arno Kompatscher
firmato digitalmente

LA SEGRETARIA GENERALE
DELLA GIUNTA REGIONALE

Gabriele Morandell
firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

	Regione Autonoma Trentino-Alto Adige Registro delle attività di trattamento Art. 30 Regolamento (UE) 2016/679 Responsabile protezione dati

[illegible]

e/Südtirol - Ripartizione _____
 ento (aggiornato al _____)
 ento UE n. 679/2016
 ne dati: _____

[illegible]



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Struttura

Ufficio _____

Tel: 0461 20

e-mail: _____@regione.taa.it

pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Gentile Signore / Gentile Signora

Oggetto: Autorizzazione al trattamento dei dati

Il _____

ai sensi dell'art. 29 GDPR (Reg. n. 2016/679), dell'art. 2-quaterdecies del Codice della privacy (D.Lgs. 196 del 2003) come novellato dal D.Lgs. 10 agosto 2018, n. 101 e della deliberazione della Giunta regionale 3 settembre 2019, n. 193

autorizza

al trattamento dei dati personali e di categorie particolari di dati, indicati nel Registro dei trattamenti, ex art. 9 del GDPR effettuato con l'utilizzo di strumenti cartacei, informatici e telematici, il seguente soggetto incardinato e preposto presso l'Ufficio _____:

Il soggetto autorizzato è tenuto a rispettare rigorosamente i principi GDPR e la normativa di settore, nonché ad attenersi alle circolari, policy in materia di sicurezza informatica, istruzioni impartite dal Titolare o da suo delegato.

Il soggetto autorizzato è tenuto a seguire le seguenti istruzioni organizzative e tecniche:

- trattare i dati personali in modo lecito e secondo correttezza;
- accedere solo ai dati strettamente necessari all'esercizio delle proprie funzioni;
- raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi;
- verificare che siano esatti e, se necessario, aggiornarli;
- verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- comunicare o trasferire all'estero i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- ove necessario, prima di iniziare il trattamento di dati personali, consegnare/trasmettere il documento definito Informativa e raccogliere il Consenso al trattamento;
- informare prontamente il Dirigente di ogni circostanza idonea a determinare pericolo di dispersione o

utilizzazione non autorizzata dei dati stessi;

- informare prontamente il Dirigente qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite dal Dirigente o dal Titolare;
- seguire le attività di formazioni organizzate dalla Regione Autonoma Trentino-Alto Adige/Südtirol per gli autorizzati al trattamento dei dati;
- accedere, per esigenze di servizio, esclusivamente alle banche dati informatiche o cartacee della propria Struttura o Ufficio a cui è stato autorizzato dal Dirigente;
- mantenere riservate le proprie credenziali di autenticazione;
- in presenza di dati particolari (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) e giudiziari (es. condanne penali) effettuare i trattamenti strettamente necessari ed eventualmente inseriti in regolamenti, procedure e/o disciplinari;
- effettuare i trattamenti sulla base di ogni ulteriore disciplinare o regolamento che il presente Ente emetterà in materia di privacy;

Specificazioni relative ad accessi particolari:

- il soggetto è autorizzato ad accedere a banche dati online, in particolare:

-
-
-

Il soggetto è autorizzato ad accedere alle cartelle ed agli applicativi come da documentazione sottoscritta e depositata presso l'amministrazione.

Il soggetto è altresì autorizzato ad utilizzare tutti i software, programmi, applicativi accessibili (programmi elaborazione testi, dati ecc...), installati per finalità d'ufficio, dall'Ufficio Informatica e digitalizzazione sul PC, al quale egli ha accesso.

La presente nomina di Autorizzato al trattamento dei dati personali può essere revocata in qualsiasi momento.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa Amministrazione, per trasferimento ad altra Amministrazione o cessazione del rapporto di lavoro.

Successivamente a tale data, il soggetto destinatario della presente lettera non è più autorizzato ad effettuare alcun tipo di trattamento di dati per conto dell' Amministrazione.

In presenza di eventuali sanzioni legate a specifiche inosservanze il Titolare ed il Responsabile del trattamento si riservano di agire secondo le norme vigenti.

Si rappresenta che la conoscenza dei dati personali da parte di un Autorizzato, nell'ambito dei trattamenti assegnati al suo Servizio/Ufficio, non è considerata comunicazione di dati personali.

Il presente atto sostituisce le eventuali nomine al trattamento dei dati personali precedenti.

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Il/La sottoscritto/a _____ dichiara di aver ricevuto la presente nomina ad Autorizzato al trattamento dei dati personali e si impegna a seguirne e rispettarne il contenuto

Data,

firma dell'autorizzato al trattamento



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Ripartizione _____

Ufficio

☎ 0461 20 _____

@ _____@regione.taa.it

pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Oggetto: _____ (indicare il nominativo del responsabile
"esterno")
Nomina a responsabile del trattamento dei dati per il servizio
_____ (indicare servizio affidato) ai sensi dell'art. 28
del Regolamento UE 2016/679
Allegato parte integrante del contratto _____ (indicare i riferimenti – n.
prot. o repertorio - del contratto/provvedimento di adesione all'offerta
economica/contratto relativo all'ordine MePat n..dd. ..)

premesse che

- ai sensi dell'art. 4 del Reg. UE n. 679/2016, per trattamento dei dati personali si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
- secondo la definizione di cui all'art. 4 del Reg. UE n. 679/2016, responsabile esterno del trattamento dei dati personali è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento";
- ai sensi dell'art. 29 del Reg. UE n. 679/2016, "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento";
- Il paragrafo 1 dell'art. 28 del Regolamento UE 2016/679 prevede che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".
- Il paragrafo 3 dell'art. 28 del Regolamento UE 2016/679 prevede che "i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento".



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

- La Regione Autonoma Trentino-Alto Adige/Südtirol per e nello svolgimento delle proprie funzioni istituzionali si avvale delle attività e dei servizi di altri soggetti, che per svolgerli trattano dati personali per conto dello stesso.
- In data _____ tra _____ la Regione Autonoma Trentino-Alto Adige/Südtirol e _____ (indicare il nominativo del responsabile "esterno"), è stato stipulato il contratto riferimento _____ (indicare i riferimenti del contratto) avente ad oggetto il servizio di _____ (indicare servizio affidato).
- Per lo svolgimento di tale attività e/o servizio, _____ (indicare il nominativo del responsabile "esterno") tratta dati personali di cui è titolare l'Ente.
- Visto il Codice degli Enti Locali della Regione autonoma Trentino Alto-Adige approvato con Legge regionale 3 maggio 2018 n. 2.
- Visto lo Statuto.

pertanto

IL DELEGATO AL TRATTAMENTO DEI DATI (giusta deliberazione della Giunta regionale n. 193/2019)

NOMINA

_____ (indicare il nominativo del responsabile "esterno")

quale RESPONSABILE DEL TRATTAMENTO

per il servizio di _____ (indicare servizio affidato),

effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi

a decorrere dal _____ e fino alla cessazione del contratto.

_____ (indicare il nominativo del responsabile "esterno"), in qualità di Responsabile del trattamento dei dati, ha il compito e la responsabilità di adempiere a tutto quanto necessario per il rispetto delle disposizioni della normativa vigente in materia e di osservare scrupolosamente quanto in essa previsto nonché le istruzioni impartite dal Titolare.

Il Responsabile è autorizzato a trattare per conto dell'Ente i dati personali necessari per fornire il servizio di cui è affidatario in virtù del contratto in oggetto, di cui il presente atto è parte integrante, che prevede:

1. Indicare l'elenco delle attività affidate
2.

NOMINA A SUBRESPONSABILE

Per l'erogazione delle attività affidate e dei relativi trattamenti di dati personali, il Responsabile (*scegliere una delle due opzioni*)

a. non è legittimato a ricorrere a un altro responsabile senza previa specifica autorizzazione scritta.

La richiesta deve indicare le specifiche attività di trattamento affidate all'altro responsabile.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

b. è autorizzato ad affidare a un altro responsabile specifiche attività di trattamento, fornendo l'elenco degli eventuali subresponsabili entro 10 giorni dalla sottoscrizione della presente nomina.

Il Responsabile del trattamento deve informare il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento; il titolare del trattamento può opporsi a tali modifiche.

Si ricorda che, se il responsabile ricorre ad un subresponsabile per l'esecuzione di specifiche attività di trattamento per conto del titolare, il responsabile deve nominare il subresponsabile con contratto o altro atto giuridico, prescrivendo gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento UE 2016/679.

Di seguito le prescrizioni e le condizioni da seguire per il corretto e lecito trattamento dei dati, effettuato in virtù del ruolo di Responsabile del trattamento:

TRATTAMENTO

Finalità del trattamento è l'espletamento del servizio di _____, reso all'Ente secondo le regole di esecuzione delle prestazioni dettate nel contratto d'appalto, nonché negli allegati - già costituenti documentazione di gara – che ne sono parte integrante e sostanziale.

I dati personali sono trattati dal Titolare per l'esecuzione di un compito di interesse pubblico e per lo svolgimento di funzioni istituzionali dell'Ente.

Categorie di dati trattati: _____ (indicare la/e categoria/e di dati come da registro dei trattamenti).

Categorie di interessati: _____ (indicare la/e categoria/e di interessati come da registro dei trattamenti).

Banche dati utilizzate dal Responsabile: _____ (il nominativo della banca dati o del software e la relativa localizzazione).

Localizzazione della banca dati: _____ (indicare se la banca dati è situata in un Paese dell'Unione Europea, oppure in un Paese extra-europeo; se sì, quale).

Se i dati contenuti nelle banche dati vengono trasferiti in Paesi extraeuropei, il Responsabile deve offrire garanzie adeguate e verificare che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi, ai sensi dell'art. 46 GDPR, oppure sulla base di una decisione di adeguatezza della Commissione Europea.

Natura del trattamento: il trattamento è svolto sia in forma automatizzata che in forma non automatizzata (es. manuale, cartacea).

Durata: il trattamento può essere svolto fino al termine della durata contrattuale o, se anteriore, fino alla cessazione di efficacia del contratto, con possibilità di proroga automatica in caso di rinnovo contrattuale alle medesime condizioni.

Trasmissione e cancellazione: _____ (indicare un lasso temporale) prima della data di cessazione del contratto, a richiesta del Titolare, il Responsabile deve restituire tutti i dati personali, trattati per ed in relazione al servizio svolto.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Alla data di cessazione del contratto, il Responsabile deve cancellare e trasmettere tutti gli ulteriori dati personali trattati nel periodo tra la trasmissione dei dati di cui sopra e la data di cessazione del contratto.

Una volta eseguita la cancellazione dei dati, il Responsabile deve comunicare al Titolare il suo effettivo avvenimento senza ingiustificato ritardo.

I dati personali devono essere restituiti, se ed in quanto possibile, in formato aperto e strutturato (es. xlsx, csv, ...), salvo che il diritto dell'Unione o il diritto nazionale ne prescrivano la conservazione.

La mancata trasmissione dei dati personali nei termini sopra indicati o la mancata trasmissione dei dati personali nel formato sopra indicato costituisce grave inadempimento contrattuale.

OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

Il Titolare attesta che i dati trasmessi al Responsabile sono stati raccolti nel rispetto di quanto previsto dal Regolamento europeo 679/2016, dal D. Lgs. 196/2003 e dalla normativa vigente in materia.

OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

Istruzioni

Il Responsabile ha l'obbligo di osservare le istruzioni che sono e saranno impartite dal Titolare con il presente atto e con comunicazioni successive in materia di trattamento dei dati personali.

Il Responsabile ha l'obbligo di osservare la normativa speciale in materia di trattamento dei dati relativa al servizio oggetto del contratto.

Incaricati al trattamento

Il Responsabile ha l'obbligo di individuare, secondo idonee modalità, i soggetti incaricati al trattamento che agiscono sotto la sua autorità.

Il Responsabile ha l'obbligo di impartire le disposizioni organizzative e operative e fornire ai soggetti autorizzati le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, eseguendo gli opportuni controlli.

Misure di sicurezza

Il Responsabile si impegna ad attuare, in via autonoma, le misure di sicurezza tecniche e organizzative più adeguate a garantire un livello di tutela dei dati adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato in esecuzione del Contratto.

Le misure che il Responsabile osserva nella esecuzione del trattamento sono indicate nell'Appendice A, parte integrante della presente nomina, nonché eventualmente in un documento allegato alla presente e redatto a cura del responsabile in cui vengono descritti i mezzi adottati per garantire la riservatezza, integrità, disponibilità, resilienza dei sistemi e servizi di trattamento, controlli periodici per testare, analizzare e valutare regolarmente l'efficacia delle misure tecniche, misure di tipo organizzativo o quanto altro applicabile.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Il Responsabile provvede affinché vengano rigorosamente adottate tutte le misure idonee a garantire la disponibilità, l'integrità e la riservatezza dei dati; vale a dire misure che permettano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati raccolti e di modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.

Il Responsabile verifica periodicamente lo stato di applicazione del D.lgs. 30 giugno 2003 n. 196 e del Regolamento Europeo 2016/679, nonché la corretta applicazione, il buon funzionamento dei sistemi e, ai sensi dell'art. 32 del GDPR, delle misure adottate per la tutela dei dati personali e la conformità alle indicazioni dell'Autorità Garante e del Titolare.

I dati personali, trattati in esecuzione del contratto, devono essere tenuti separati rispetto a quelli eventualmente trattati per conto di altre terze parti applicando una segregazione fisica e logica, ove possibile.

Il Responsabile garantisce la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali che esuli dalle attività previste nel Contratto.

Il Responsabile ha l'obbligo di provvedere alla formazione e tenuta del registro delle attività di trattamento svolte per conto del Titolare, se previsto dall'art. 30 del Regolamento UE 2016/679.

Il Responsabile ha l'obbligo di designare un Responsabile della protezione dei dati, se previsto dall'art. 37 del Regolamento UE 2016/679 e di comunicarne il nominativo e riferimento al Titolare entro 10 giorni dalla nomina.

Il Responsabile ha l'obbligo di adottare tutte le misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 Regolamento UE 2016/679.

Il Responsabile ha l'obbligo di garantire il rispetto delle misure e degli accorgimenti relativi alle attribuzioni degli Amministratori di sistema.

Il Responsabile si impegna a supportare il titolare nella predisposizione e aggiornamento della valutazione di impatto del trattamento sui diritti e sulle libertà delle persone.

Trasferimento dati extra UE

Se i dati contenuti nelle banche dati vengono trasferiti in Paesi extraeuropei o se ci si avvale di un sub responsabile che trasferisce i dati in Paesi extraeuropei, il Responsabile deve verificare che il Paese extraeuropeo sia destinatario di una decisione di adeguatezza della Commissione Europea oppure, in mancanza, il Responsabile deve offrire garanzie adeguate e verificare che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi ai sensi dell'art. 46 GDPR.

In quest'ultimo caso, il Responsabile del trattamento deve verificare, caso per caso, in collaborazione con il sub responsabile che trasferisce i dati, se la legge o la prassi del Paese terzo incidono sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento.

Il Responsabile dovrà, se necessario, attuare misure supplementari che andranno identificate, caso per caso, conformemente alle raccomandazioni adottate dall'European Data Protection Board (raccomandazioni 01/2020; raccomandazioni 02/2020) e ne dovrà fornire puntuale rendicontazione nei termini del paragrafo Controlli e ispezioni.



Assistenza

- esercizio dei diritti dell'interessato

Il Responsabile ha l'obbligo di prestare la propria collaborazione al Titolare nella predisposizione, ai sensi degli artt. 13 e 14 Regolamento UE 2016/679, dell'informativa agli interessati, della modulistica e delle altre forme idonee di informazione, inerenti al proprio servizio.

Il Responsabile ha l'obbligo di assistere il Titolare del trattamento con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo dello stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento UE 2016/679.

Il Responsabile ha l'obbligo di prestare la propria collaborazione per consentire al Titolare di rispondere in modo esaustivo e tempestivo alle richieste e prescrizioni delle Autorità di controllo e dell'Autorità Giudiziaria.

- misure di sicurezza

Il Responsabile ha l'obbligo di assistere il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 Regolamento UE 2016/679, tenendo conto della natura del trattamento e delle informazioni a disposizione.

Il Responsabile del trattamento notifica al Titolare del trattamento ogni violazione di dati a carattere personale, tempestivamente, senza ingiustificato ritardo, dopo esserne venuto a conoscenza. Tale notifica è accompagnata da ogni documentazione utile per permettere al Titolare del trattamento, se necessario, di notificare la violazione all'autorità di controllo competente.

Spetta solo al Titolare decidere di non effettuare la notifica all'Autorità di controllo competente, in presenza di semplice incidente che non ha comportato perdita, distruzione, diffusione o modifica dei dati e/o, nonostante la violazione dei dati personali, sia improbabile che essa comporti un rischio per i diritti e le libertà degli Interessati. Il Responsabile del trattamento provvederà a fornire al Titolare del trattamento tutte le informazioni di propria competenza al fine di consentire a quest'ultimo di effettuare tale valutazione.

Previo accordo con il Titolare del trattamento, il Responsabile del trattamento comunica, in nome e per conto del Titolare del trattamento, la violazione di dati a carattere personale alla persona interessata al più presto, qualora, in base alla valutazione del Titolare, tale violazione sia suscettibile di generare un rischio elevato per i diritti e le libertà di una persona fisica.

- informazioni accountability (responsabilizzazione)

Il Responsabile ha l'obbligo di mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento UE 2016/679 e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto dallo stesso incaricato.

Il Responsabile ha l'obbligo di informare il Titolare del trattamento di ogni comunicazione o attività di controllo o ispettiva dell'Autorità di controllo.

Controlli e ispezioni



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Il Responsabile ha l'obbligo di fornire, su richiesta del Titolare del trattamento, una relazione sull'attività di trattamento svolta e sulle misure tecniche e organizzative di sicurezza adottate.

Il Responsabile ha l'obbligo di permettere al Titolare del trattamento di porre in essere controlli periodici finalizzati ad accertare l'adeguatezza delle misure di sicurezza, l'osservanza delle istruzioni impartite e in generale il rispetto della normativa in materia. Queste verifiche possono essere condotte mediante preavviso scritto di minimo 7 giorni lavorativi.

Il Titolare garantisce che:

- i controlli, le ispezioni e le verifiche di cui al paragrafo che precede avranno luogo durante il normale orario di lavoro e senza ostacolare l'attività del Responsabile e di altri clienti del Responsabile;
- tutte le informazioni ottenute o generate dal Titolare o dal/i proprio/i auditor in relazione a tali controlli, ispezioni e verifiche saranno mantenute strettamente confidenziali (salvo richieste da parte delle Autorità di controllo o, se altrimenti richiesto, dalla legge applicabile);
- conviene che il costo di siffatti controlli, verifiche o ispezioni, sarà a proprio carico, a meno che dai predetti accertamenti, controlli o ispezioni non risultino inadempimenti e/o violazioni del Responsabile agli obblighi su di lui incombenti.

Manleve

Il Responsabile s'impegna a risarcire, manlevare e tenere indenne il Titolare per qualsiasi danno, pretesa, risarcimento, sanzione e/o pregiudizio che possa derivargli dalla mancata osservanza degli obblighi di cui al presente atto, delle istruzioni impartite e della normativa vigente.

Il Responsabile è altresì responsabile per ogni pregiudizio cagionato al Titolare da parte degli eventuali subresponsabili da lui nominati.

Il presente atto è parte integrante del contratto di appalto in oggetto, cui accede.

Luogo e data _____

IL RESPONSABILE

**IL DIRIGENTE DELLA
RIPARTIZIONE _____**

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).



APPENDICE A - ATTO DI NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO DI DATI PERSONALI

1. Controlli: il Responsabile implementa le misure appropriate finalizzate al raggiungimento di quanto segue:

- negare l'accesso ai soggetti non autorizzati rispetto ad ogni dispositivo utilizzato per le attività di trattamento di dati personali (*controllo di accesso ai dispositivi*);
- evitare la lettura, copia, alterazione, rimozione non autorizzate di dati personali (*controllo dei supporti*);
- evitare accessi, modifiche o cancellazioni di dati personali conservati (*controllo della conservazione*);
- evitare l'uso di sistemi di trattamento dati automatizzato da parte di soggetti non autorizzati (*controllo delle utenze*);
- limitare l'accesso ai dati personali ai soli soggetti autorizzati a trattarli nei limiti temporali e sostanziali della propria autorizzazione (*controllo di accesso ai dati*);
- verificare i canali di comunicazione dei dati;
- permettere la verifica dell'identità dei soggetti che hanno inserito i dati in sistemi di trattamento automatizzato e della data e ora dell'inserimento (*controllo degli input*);
- evitare la lettura, copiatura, alterazione o cancellazione di dati personali durante il trasferimento degli stessi o durante il trasporto dei supporti fisici (*controllo del trasferimento*);
- in caso di interruzione del servizio, permettere il ripristino dei sistemi installati al fine di effettuare le operazioni di trattamento dati (*controllo sulle procedure di 'recovery'*);
- in caso di 'data breach' adottare un piano teso a ripristinare la piena funzionalità dei sistemi, nonché limitare sostanzialmente gli effetti negativi dell'evento di sicurezza;
- assicurare che le funzioni e i sistemi utilizzati per trattare i dati personali siano in funzione, che eventuali errori o criticità vengano inseriti in appositi report e che i sistemi siano protetti dal danneggiamento dei dati in seguito a malfunzionamenti dei sistemi stessi.

2. Personale: il Responsabile adotterà misure idonee ad assicurare che nessun soggetto tratti i dati a meno che lo stesso:

- sia competente e qualificato ad effettuare le specifiche mansioni assegnate;
- sia stato autorizzato dal Responsabile;
- sia stato specificamente istruito dal Responsabile circa i requisiti rilevanti al fine di rispettare gli obblighi del Contratto, in particolare con riguardo alla limitazione delle finalità del trattamento.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

3. *Controllo delle copie*: il Responsabile non dovrà effettuare copie dei dati personali all'infuori di quelle strettamente necessarie per dar corso agli obblighi contrattuali e di legge.

4. *Politiche di back up*: i back up vengono effettuati con cadenza giornaliera e salvati su server ubicati in luogo diverso dalla sede aziendale. L'accesso al server è protetto da controllo degli accessi fisici e informativi.

5. *Controllo degli accessi informatici*: l'accesso ai data base informatici per interventi di manutenzione ordinaria, straordinaria e verifiche di back up, è limitato solo agli utenti autorizzati.

6. *Controllo sulle intrusioni*: i sistemi utilizzati a fini di trattamento dei dati personali saranno soggetti al monitoraggio di eventuali attività intrusive non autorizzate, per mezzo di dispositivi riconosciuti in linea agli standard di settore.

7. *Gestione degli incidenti*: ai dati personali conservati si applicano le policy e le procedure in materia di gestione degli incidenti di sicurezza. Il Responsabile informerà senza ritardo il Titolare di ogni incidente di sicurezza, sospettato o effettivo, avente ad oggetto l'integrità dei dati personali.

8. *Sicurezza Fisica*: ogni area in cui sono conservati i dati personali è soggetta a controlli di sicurezza fisica degli accessi.

9. *Crittografia*: in caso di trasferimenti di dati personali saranno utilizzati meccanismi di crittografia in linea con gli standard di settore generalmente accettati.

10. *Accesso software*: la sicurezza dei file è gestita da sistemi di sicurezza standard in forma delle liste di controllo di accesso.

11. *Misure di Sicurezza informatiche*: la rete aziendale è protetta da Firewall, antivirus e anti - rootkit. Le work station sono protette da password personale, minimo 8 caratteri alfanumerica con variazione ogni 3 mesi.

12. *Privacy by design e Privacy by default*: Il Responsabile dichiara di essere costantemente impegnato per la configurazione delle soluzioni applicative oggetto di fornitura affinché siano rispettati i principi sanciti dall'art. 25 GDPR, mettendo in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, che contemplano protocolli crittografati per la trasmissione dei dati e dei servizi SaaS, tecniche sicure per la protezione delle banche dati, criteri di autenticazione e procedure di gestione delle credenziali adeguati (password con criteri di complessità, scadenza periodica, blocco utente dopo n. tentativi di accesso falliti, reset delle password), funzionalità di attivazione dei log degli accessi e dell'attività degli utenti, procedure per facilitare l'esercizio dei diritti di oblio/cancellazione dei dati e della portabilità degli stessi.

13. *Modifiche e aggiornamenti dei sistemi*: il Responsabile dovrà aggiornare e mantenere le misure di sicurezza durante l'intera durata delle prestazioni dedotte nel Contratto. A tali fini, potranno essere aggiunti o modificati controlli di sicurezza, procedure, policy e caratteristiche dei sistemi. Il Responsabile dovrà fornire un livello di sicurezza che non sia mai sostanzialmente inferiore rispetto a quello fornito *ab initio* del rapporto contrattuale.

INFORMATIVA BREVE DA INSERIRE IN CALCE ALLA MODULISTICA DELL'ENTE, PRIMA DELLA FIRMA

Si informa che ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 e del D. Lgs. 196/2003, i dati personali sono raccolti dal Servizio/Ufficio __ad es. Segreteria__ in esecuzione di un compito o di una funzione di interesse pubblico. I dati sono oggetto di comunicazione e diffusione nei soli casi previsti dalla legge.

Titolare del trattamento è l'Ente (e-mail ____, sito internet ____), Responsabile della Protezione dei Dati è il Consorzio dei Comuni Trentini (e-mail servizioRPD@comunitrentini.it, sito internet www.comunitrentini.it). L'informativa completa è a disposizione presso gli uffici comunali e alla voce "privacy" del sito istituzionale <https://www.regione.taa.it/Privacy>.

Lei può esercitare il diritto di accesso e gli altri diritti di cui agli artt. 15 e seguenti del Regolamento UE 2016/679.

AVVISO DI RISERVATEZZA DA INSERIRE IN CALCE ALLE CASELLE DI POSTA ELETTRONICA ISTITUZIONALE

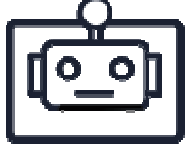
I dati contenuti nella presente e-mail sono raccolti e trattati nel rispetto del Regolamento UE 2016/679 (GDPR). Gli interessati possono rivolgersi in qualsiasi momento al Titolare del trattamento, Regione Autonoma Trentino-Alto Adige/Südtirol, per esercitare i diritti previsti dal GDPR. I dati di contatto del Responsabile Protezione dei Dati e del Titolare oltre che l'informativa completa sono disponibili al link <https://www.regione.taa.it/Privacy> sotto la voce "Privacy".

Si precisa inoltre che le informazioni contenute nel presente messaggio, e negli eventuali allegati, sono riservate e per uso esclusivo del destinatario. In caso di ricezione dello stesso per errore, siete pregati di informare immediatamente il mittente e di cancellarlo dal vostro archivio in conformità con quanto disposto dall'art. 17 del GDPR. Ogni trattamento della presente e-mail che non sia quello del destinatario reale è inteso come non autorizzato dal mittente. Inoltre, in quanto non destinatari reali, vi informiamo che il mittente si oppone alla copia, alla diffusione e alla rivelazione anche parziale dei dati in esso contenuti alle persone non autorizzate dal medesimo, in virtù di quanto disposto dall'art. 21 del GDPR.

Informativa sui trattamenti di dati personali effettuati per la gestione del servizio _____
(indicare l'attività di trattamento o il gruppo di trattamenti omogenei a cui l'informativa si riferisce)

La informiamo che il Regolamento UE 2016/679 (GDPR) e il Decreto legislativo 196/2003 hanno ad oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali. Gli artt. 13 e 14 del GDPR prevedono che il soggetto i cui dati vengono trattati (Lei, in qualità di interessato) venga debitamente informato sul trattamento medesimo.

TITOLARE/ CONTITOLARE	TITOLARE/CONTITOLARE DEL TRATTAMENTO
 Chi decide le modalità e le finalità del trattamento? La Regione Trentino-Alto Adige/Südtirol, in qualità di titolare/contitolare del trattamento, decide le modalità e le finalità del trattamento.	Ente Regione Autonoma Trentino Alto Adige / Südtirol con sede a Trento, in via Gazzoletti n. 2 • e-mail _____@regione.taa.it • sito internet www.regione.taa.it • pec _____@pec.regione.taa.it
RPD	RESPONSABILE PER LA PROTEZIONE DATI
 Chi è il RPD? Il Responsabile per la protezione dei dati (RPD) è il soggetto individuato dal titolare del trattamento che svolge funzioni di supporto e controllo, sull'applicazione del Regolamento UE.	Consorzio dei Comuni Trentini, con sede a Trento, in via Torre Verde n. 23 • e-mail servizioRPD@comunitrentini.it • sito internet www.comunitrentini.it
DATI	CATEGORIE DI DATI PERSONALI TRATTATI
 Quali dati raccogliamo? Raccogliamo diverse categorie di dati personali, a seconda della finalità del trattamento.	• dati identificativi semplici (es. nome, cognome, data di nascita, telefono, e-mail/pec, username, password, indirizzo IP, ...) • categorie particolari di dati (es. salute, origine razziale o etnica; opinioni politiche; convinzioni religiose o filosofiche; appartenenza sindacale; dati biometrici, ...) • dati di localizzazione (es. coordinate gps, ...) • dati giudiziari (es. condanne penali, reati, misure di sicurezza, ...) • dati di profilazione (es. preferenze, interessi che portano a decisioni automatizzate, ...)
FONTE	FONTE DEI DATI

 Dove sono stati raccolti i dati? I dati possono essere raccolti direttamente presso l'interessato, oppure presso enti terzi che ne hanno fatto comunicazione al titolare del trattamento.	☐ sono stati raccolti presso _____ (indicare altri eventuali soggetti che hanno raccolto e comunicato i dati all'Ente. Ad es. soggetti pubblici e/o privati; altre Pubbliche Amministrazioni e/o Autorità giudiziaria; altri Enti quali contitolari del trattamento). ☐ sono stati raccolti presso l'interessato (lei medesimo).
SCOPO	FINALITÀ DEL TRATTAMENTO
 A che scopo trattiamo i Suoi dati? Il trattamento dei Suoi dati è realizzato per diverse finalità.	I dati personali vengono raccolti e trattati per le seguenti attività: _____ (inserire le attività di trattamento indicate nel Registro dei trattamenti). Inoltre, i dati personali possono essere trattati per finalità diverse da quelle per le quali sono stati raccolti, garantendo in ogni caso la compatibilità con i fini istituzionali.
CONDIZIONI	BASE GIURIDICA DEL TRATTAMENTO
 Quale condizione rende lecito il trattamento? Il trattamento, per essere lecito, deve essere fondato su un'adeguata base giuridica.	I dati sono trattati per l'esecuzione di un compito o di una funzione di interesse pubblico. In particolare, quanto alle norme che regolano l'attività amministrativa, si vedano: • L.R. n. 02/2018 e ss. mm. (Codice Enti Locali) • D.lgs. 14 marzo 2013, n. 33 e Legge Regionale T.A.A. 29 ottobre 2014 n. 10, in materia di trasparenza amministrativa; • D.lgs. 7 marzo 2005, n. 82 e ss. mm. - Codice dell'amministrazione digitale; • Legge provinciale 30 novembre 1992, n. 23, che disciplina i principi per la democratizzazione, la semplificazione e la partecipazione all'azione amministrativa provinciale e degli enti locali e norme in materia di procedimento amministrativo; • ... Quanto alle specifiche disposizioni di legge, di regolamento o di atti amministrativi generali che regolano le attività di trattamento svolte nell'ambito del servizio in oggetto, si vedano: • _____ (specificare altre eventuali norme di riferimento)
MODALITÀ	MODALITÀ DEL TRATTAMENTO
 I Suoi dati sono al sicuro? Nel trattare i Suoi dati adottiamo specifiche misure di sicurezza per prevenire la perdita, gli usi illeciti o non corretti e gli	I dati sono trattati con strumenti informatici o manuali e tramite procedure adeguate a garantirne la sicurezza e la riservatezza. Il trattamento è effettuato, esclusivamente per le finalità sopra indicate, da personale specificamente autorizzato in relazione ai compiti e alle mansioni assegnate e nel rispetto del segreto professionale e del segreto di ufficio. Abbiamo adottato specifiche misure di sicurezza per prevenire la perdita dei dati personali, usi illeciti o non corretti ed accessi non autorizzati.

accessi non autorizzati ai tuoi dati personali.	È esclusa l'esistenza di un processo decisionale automatizzato, compresa la profilazione.
CONSERVAZIONE	PERIODO DI CONSERVAZIONE DEI DATI
 Per quanto tempo conserviamo i Suoi dati? Conserviamo i Suoi dati per un periodo di tempo che varia in base alle finalità del trattamento.	Il periodo di conservazione dei dati è determinato sulla base della vigente normativa in materia di conservazione della documentazione e degli archivi della pubblica amministrazione, e potrà protrarsi, nell'osservanza di tali disposizioni, anche a tempo indeterminato. I dati, nel rispetto delle misure a tutela dei Suoi diritti e delle Sue libertà, possono essere trattati anche a fini statistici.
DESTINATARI	A CHI POSSONO ESSERE COMUNICATI
 A chi potremmo trasmettere i Suoi dati? Per le finalità del trattamento indicate in questa Informativa potremmo trasmettere alcuni Suoi dati a soggetti esterni che agiscono come titolari e/o responsabili del trattamento.	I dati possono essere trattati da soggetti esterni operanti in qualità di titolari quali, ad esempio, Autorità ed organi di vigilanza e controllo e, in generale, soggetti, anche privati, legittimati a richiedere i dati, Pubbliche Autorità che ne facciano espressa richiesta per finalità amministrative o istituzionali (<i>indicare altri eventuali soggetti a cui i dati vengono comunicati</i>). Per le finalità indicate, i dati possono essere trattati da soggetti terzi (fornitori, consulenti, prestatori d'opera), nominati quali responsabili del trattamento ex art. 28 del GDPR. I dati sono oggetto di diffusione nei soli casi ammessi dalla legge (la pubblicazione su internet equivale a diffusione): - ad es. pubblicazioni in amministrazione trasparente; - ad es. pubblicazioni su albo telematico; - ad es. altre pubblicazioni – internet/bollettino cartaceo.
AUTORIZZATI	CHI PUÒ TRATTARE I DATI
 Chi sono i soggetti autorizzati a trattare i Suoi dati? I Suoi dati potranno essere trattati dai dipendenti e collaboratori dell'Ente.	I dati possono essere conosciuti da personale specificamente autorizzato in relazione ai compiti e alle mansioni assegnate.
TRASFERIMENTO	TRASFERIMENTO DEI DATI IN PAESI EXTRA UE
 I Suoi dati potranno essere trasferiti all'estero in Paesi fuori dall'Unione Europea? I Suoi dati potrebbero essere trasferiti in Paesi extra-europei. In caso di trasferimento di dati	I dati <i>sono/non sono</i> oggetto di trasferimento delle banche dati fuori dall'Unione Europea (<i>verificare il luogo di localizzazione dei server fisici o in cloud in cui avviene la conservazione dei dati</i>). In caso di trasferimento i dati sono soggetti alle seguenti garanzie adeguate: • decisione di adeguatezza della Commissione Europea • clausole contrattuali standard • meccanismi di certificazione • codici di condotta

all'estero Le garantiamo il rispetto dei requisiti di legge per il trasferimento.	
OBBLIGATORIETÀ	OBBLIGATORIETÀ DEL CONFERIMENTO DEI DATI
 Perché è necessario il conferimento dei Suoi dati? Per alcune finalità del trattamento è necessario che Lei conferisca i Suoi dati, senza i quali non potremo fornirLe i nostri servizi. Per altre, Lei è libero di non conferire i Suoi dati; in tal caso, il servizio ulteriore non sarà erogato.	Il conferimento dei dati ha natura: ☐ obbligatoria. Non fornire i dati comporta non osservare obblighi di legge e/o impedire che l'Ente possa espletare le proprie funzioni istituzionali e/o erogare il servizio. ☐ facoltativa.
DIRITTI	I DIRITTI DELL'INTERESSATO
 Quali sono i Suoi diritti? Può esercitare i diritti che Le sono riconosciuti dal Regolamento Europeo. Ad esempio, può chiedere al titolare l'accesso ai dati che la riguardano, la loro cancellazione, rettifica, integrazione, nonché la limitazione del trattamento. Può inoltre proporre reclamo all'Autorità di controllo competente.	I diritti dell'interessato sono: – richiedere la conferma dell'esistenza o meno dei dati che lo riguardano; – ottenere la loro comunicazione in forma intelligibile; – richiedere di conoscere le finalità e modalità del trattamento; – ottenere la rettifica, l'eventuale cancellazione, la limitazione o la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge; – aggiornare, correggere o integrare i dati che lo riguardano; – opporsi, per motivi legittimi, al trattamento dei dati; – di proporre reclamo al Garante per la protezione dei dati personali (https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/4535524).

MODIFICHE E AGGIORNAMENTI: la presente informativa può essere soggetta a modifiche e/o integrazioni.

Versione di data _____

MODELLO ORGANIZZATIVO DI PROTEZIONE DEI DATI - check list di controllo generale

Responsabile protezione dati:

Referente interno: il Segretario generale

ADEMPIMENTI	ART. RGDP	DOCUMENTI DA PRODURRE	AZIONI	sì no
Mappa trattamenti	30	Registro trattamenti	Compilare il registro trattamenti: in caso di assunzioni, cessazioni, variazioni di incarico Tenere aggiornato il registro trattamenti	
Sistemi IT	28, 32	Nomina amministratore di sistema	Nomina amministratore di sistema e gestione del rapporto: programmazione relazione periodica	
sicurezza	32	Documento valutazione/analisi dei rischi	Compilare il documento valutazione dei rischi	
			Tenere aggiornato il documento valutazione dei rischi;	
			Esecuzione misure tecniche inserite nel documento	
			Esecuzione misure organizzative inserite nel documento	
			Controllo su misure tecniche eseguite	
	35	Documento di Valutazione di impatto privacy (Vip)	Controllo su misure organizzative eseguite	
			Verificare casi di obbligo di compilazione	
			Chiedere parere DPO/RPD	
			Compilare il documento VIP	
			Tenere aggiornato il documento VIP	
	36	Consultazione preventiva	Esecuzione misure tecniche inserite nel documento	
			Esecuzione misure organizzative inserite nel documento	
			Controllo su misure tecniche eseguite	
			Controllo su misure organizzative eseguite	
	33, 34	Procedura data breach	Verificare obbligo di richiesta al Garante	
			Compilare la richiesta di parere	
			Esecuzione prescrizioni segnalate dal Garante	
			Controllo su prescrizioni eseguite	
			Individuazione figura responsabile: Referente interno - Segretario generale e/o suoi sostituti	
Contitolari	26	Accordo con contitolari	Redazione procedura data breach e sua diffusione all'interno dell'ente Esecuzione misure tecniche e organizzative inserite nel protocollo Aggiornamento protocollo data breach Compilare il registro della violazione dei dati Tenere aggiornato il registro della violazione dei dati Formazione continua in materia di data breach verifica casi contitolarità, Stesura e sottoscrizione accordo di contitolarità Esecuzione misure organizzative e tecniche previste dall'accordo	
Nomina responsabili esterni	28	Contratto di responsabile esterno	Mappatura della esternalizzazione dei trattamenti; Compilazione e sottoscrizione dei contratti con responsabili esterni; Esecuzione misure normative previste nei contratti Esecuzione misure tecniche e organizzative previste nei contratti Programmazione controlli nei confronti del responsabile esterno: relazione periodica esecuzione controlli nei confronti del responsabile esterno stesura modifiche e sottoscrizione clausole aggiuntive/sostitutive	
Nomina sub-responsabili esterni	28	Contratto con sub-responsabili	Mappatura della sub-esternalizzazione dei trattamenti Stesura di apposite clausole nei contratti con responsabili esterni Pianificazione ed esecuzione di procedure selettive previste nelle clausole contrattuali Pianificazione ed esecuzione di controlli per il tramite del responsabile esterno	
Nomina "designati interni"	5	Atto di nomina e disciplinare	Mappatura delle nomine esistenti (ex resp. Trattam. Interni) e verifica del mantenimento di centri apicali interni Stesura nuovi atti di nomina: delibera di ripartizione delle competenze Eventuale integrazione atti di nomina precedenti al RGPD	
Nomina autorizzati	29	Nomina dipendenti e collaboratori	Attività rimandata ad ogni Ripartizione di competenza	
Formazione autorizzati	39	Corsi per gli autorizzati	Corsi base per autorizzati al trattamento: parte di competenza dell'ufficio preposto	
RPD/DPO	37, 38, 39	Nomina RPD/DPO	Salvo individuazione tra le professionalità all'interno della Regione, individuazione dell'organizzazione esterna a cui affidare l'incarico	
			Individuazioni delle motivazioni ai sensi della normativa in materia di contratti e appalti	
			Stesura del decreto di affidamento e sottoscrizione contratto	
			Comunicazione al Garante di avvenuta nomina/cessazione del RPD/DPO, eventuali variazioni del Referente del DPO	
			Esecuzione misure previste nel contratto	
Trasferimenti dati estero - Extra UE	44-50	condizione di liceità	Istituzione di punto di contatto del RPD/DPO con interessati: informazione ai collaboratori del DPO e delle modalità per contattarlo	
			Verifica del rispetto delle condizioni per il trasferimento dei dati extra UE	
			Applicazione contratto Data privacy Framework (accordo quadro in materia di trasferimento dei dati)	
			Stesura documenti/contratti in base alla condizione di liceità applicabile	
Altri adempimenti documentali: mantenere aggiornate e aderenti alla normativa vigente le seguenti policy già in uso (attraverso prassi consolidate)			Esecuzione cautele imposte dal Garante o dal contratto o dalle altre condizioni di liceità	
			sito web e social: condizioni di utilizzo servizi	
			sito web: cookie policy	
			siti web: policy servizi di analytics	
			Predisposizione e aggiornamento periodico delle informative: aggiornamento normativo	
			policy consegna dispositivi e utilizzo dotazioni informatiche: verificarne sempre l'attualità	
			policy BYOD: non viene effettuato	
			regolamento dismissione dispositivi	
			regolamento videosorveglianza -mantenere aggiornato	
			regolamento scarto documenti (durata conservazione dati) - manuale di gestione documentale	
			policy relativa a pubblicazioni su Amministrazione Trasparente	
			policy gestione dei diritti degli interessati (coordinamento con disciplina di accesso documentale, civico, ecc.)	

MODELLO ORGANIZZATIVO DI PROTEZIONE DEI DATI - check list di controllo da attivare all'interno degli uffici				
Responsabile protezione dati:				
Referente interno: il Segretario generale - Delegato al trattamento dei dati: Il/La Dirigente di Ripartizione				
ADEMPIMENTI	ART. RGDP	DOCUMENTI DA PRODURRE	AZIONI	si no
Mappatura dei trattamenti dei dati				
Mappa trattamenti	30	Registro trattamenti	Ci sono state variazioni di attività nell'attività amministrativa dell'ufficio?	
			Sono state annotate nel Registro dei trattamenti?	
			Sono stati introdotti nuovi software nell'attività amministrativa dell'Ufficio ?	
			Ci sono nuovi trattamenti che implicano l'annotazione di nuove attività nel Registro?	
			Ci sono state assunzioni, cessazioni, variazioni di incarico?	
			E' stato puntualmente aggiornato il Registro delle attività di Trattaemnto dei dati?	
Nomina amministratori di sistema e gestione del rapporto				
Nomina amministratore di sistema	28	Nomina amministratore di sistema	E' prevista per questo semestre la scadenza del contratto di amministratore di sistema?	
			Se sì, sono state controllate le clausole del contratto che siano aderenti alla realtà attuale?	
			E' stata programmata la redazione della relazione periodica da parte dell'Amministratore di sistema?	
			E' stata richiesta? E' pervenuta? E' stata archiviata opportunamente?	
Individuazione e gestione delle aree di rischio nel trattamento di dati personali				
Valutazione dell'impatto del trattamento dati sulle libertà di terzi	32/35	Documento di valutazione/analisi dei rischi	Sono individuate all'interno di tutti i processi dell'ufficio dei trattamenti di dati per cui è necessario la valutazione di impatto?	
			E' stato consultato l'RPD (attraverso ufficio affari generali) per la verifica dell'opportunità di effettuare una valutazione di impatto?	
			Attraverso la matrice del rischio, sono state individuate le minacce possibili, in accordo anche con l'ufficio informatica?	
			Sono state individuate le diverse possibili soluzioni alle minacce individuate, in accordo anche con l'ufficio informatica?	
			Se già presente, viene nei casi previsti aggiornato?	
			Le misure tecniche previste nel documento, sono rispettate? Sono ancora attuali?	
			Le misure organizzative previste nel documento, sono rispettate? Sono ancora attuali?	
			Vengono periodicamente verificate sia le misure tecniche che organizzative?	
Procedura di data breach: applicazione in ogni ufficio				
Monitoraggio della procedura - segnalazione dell'evento	33,34	Procedura data breach	Tutti i collaboratori sanno dove è salvata la procedura di data breach?	
			I collaboratori hanno compreso il concetto di data breach e delle modalità e tempistiche di segnalazione?	
			I collaboratori sanno come devono comportarsi in caso di data breach? Sono stati edotti delle misure tecniche e organizzative inserite nella procedura?	
Accordi di contitolarità				
Accordo di contitolarità, punto di contatto, trattamento congiunto di dati	26	Accordo di contitolarità	E' ricorrente il caso di contitolarità di dati?	
			E' stato chiarito il perimetro di azione di ogni parte coinvolta per il trattamento e la gestione dei dati?	
			E' stato individuato il punto di contatto a cui fare riferimento per ogni questione?	
			Sono state individuate, anche in forma riassuntiva, le attività di trattamento svolte in contitolarità?	
			Tra le diverse parti sono state suddivisi i compiti e i ruoli?	
			E' stato redatto e sottoscritto dalle parti il contratto di contitolarità?	
Contratto di responsabile esterno e contratto contratto con i sub responsabili				
Responsabile e sub responsabile esterno	28	Contratto di responsabile esterno e con sub responsabili	E' ricorrente il caso di trattamento di dati da parte di un responsabile esterno?	
			sono stati mappati tutti i trattamenti che sono trattati da un Responsabile esterno?	
			Sono stati redatti per iscritto i contratti con i responsabili esterni?	
			Sono state concordate con ufficio informatica le misure minime di sicurezza da attuare?	
			E' stato scadenziato il controllo nei confronti del responsabile esterno, fissando un termine entro cui far pervenire le relazioni da parte del Responsabile esterno?	
			sono stati effettuati i controlli sull'operato del responsabile esterno affinché sia possibile confermare/rinnovare/cambiare il responsabile esterno del trattamento dei dati?	
			Stesura di apposite clausole nei contratti con responsabili esterni	
			Sono stati previsti e mappati eventuali trattamenti sub-esternalizzati?	
			Pianificazione ed esecuzione di procedure selettive previste nelle clausole contrattuali	
			Controlli e gestione del Registro delle attività di trattamento dei dati	
Controlli ulteriori sul Registro delle attività di trattamento dei dati	29	Registro delle attività di trattamento dei dati	Sono state mappati i database ed i software che sono in uso all'interno dell'ufficio?	
			E' stato compilato il Registro per il trattamento dei dati? Vi è esatta corrispondenza tra lettera di incarico e Registro dei trattamenti?	
			E' stata programmata per tempo la richiesta delle abilitazioni informatiche attraverso Profili Informatici?	
			In caso di variazioni di profilo e/o cessazioni, è stato aggiornato il Registro delle attività di trattamento dei dati?	
			In caso di cessazione del collaboratore, sono stati disabilitati i profili informatici?	

ok 19/08/2024



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Segreteria generale
Generalsekretariat
Ufficio affari generali
Amt für allgemeine Angelegenheiten
☎ 0461 201323
@ affgen@regione.taa.it
pec: affgen@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Protokollnummer und Registrierungsdatum sind dem Dokument als Metadaten zugeordnet (Dekret des Präsidenten des Ministerrates vom 3.12.2013, Art. 20). Gegenstand der zertifizierten E-Mail bzw. beigefügte Dateien überprüfen.

Al Capo dell'Ufficio di Gabinetto del
Presidente della Regione

Alla Vicesegretaria generale

Alle Dirigenti delle ripartizioni

Alle Direttrici e ai Direttori degli uffici centrali

Alle Sostitute Direttrici e ai Sostituti Direttori
degli uffici centrali

Alle Segretarie e ai Segretari particolari dei
componenti della Giunta regionale

e, p.c.

Alle collaboratrici e ai collaboratori

An den Kabinettschef des Präsidenten der
Region

An die Vizegeneralsekretärin

An die Leiterinnen der Abteilungen

An die Direktorinnen und Direktoren der
Zentralämter

An die Stellvertretenden der Direktorinnen
und Direktoren der Zentralämter

An die persönlichen Referenten der
Mitglieder der Regionalregierung

u.z.K.

An die Bediensteten

CIRCOLARE/RUNDSCHREIBEN

Oggetto:

**Indicazioni per la formazione dell'ordine
del giorno delle sedute della Giunta
regionale e per la predisposizione delle
proposte di deliberazione.**

In seguito al ripetersi di alcune criticità, in
sede di formazione dell'ordine del giorno
delle sedute della Giunta regionale, ritengo
opportuno richiamare nuovamente alla
vostra attenzione alcuni aspetti fondamentali
della procedura.

Betreff:

**Anweisungen für die Erstellung der
Tagesordnung der Sitzungen der
Regionalregierung sowie der
Beschlussfassungsvorschläge**

Da wiederholt Schwierigkeiten bei der
Erstellung der Tagesordnung der Sitzungen
der Regionalregierung auftreten, wird
hiermit erneut auf einige grundlegende
Verfahrensaspekte verwiesen.

È ricorrente, ad esempio, che gli uffici anticipino via e-mail, all'Ufficio affari generali, l'oggetto della proposta di deliberazione caricando il documento in Pi.Tre. in ritardo rispetto ai tempi previsti dal regolamento interno per la stesura e trasmissione dell'OdG.

Ciò comporta che la trasmissione di tali proposte ai componenti della Giunta regionale avvenga dopo l'invio dell'OdG, in tempi troppo ravvicinati alla seduta. Questo può implicare, per gli stessi, una non adeguata preparazione sull'argomento.

L'ordine del giorno ha un'importanza sostanziale perché delimita gli argomenti sui quali la Giunta è chiamata a decidere. La sua funzione è quella di consentire ai componenti dell'organo collegiale di intervenire alla seduta adeguatamente preparati sugli argomenti che saranno oggetto di discussione.

La modalità di svolgimento delle sedute, la convocazione e la formazione dell'ordine del giorno, sono disciplinati dal regolamento interno delle sedute della Giunta regionale emanato con decreto del Presidente della Regione 6 novembre 2020, n. 49.

Con la presente circolare, colgo anche l'occasione per ricordare altri aspetti relativi alla predisposizione delle proposte e alla formazione delle deliberazioni, che ritengo possano costituire un valido supporto agli uffici.

1. Trasmissione delle deliberazioni e dei promemoria per la redazione dell'ordine del giorno

Le proposte di deliberazione, complete dei visti amministrativi e degli eventuali visti contabili, devono pervenire all'Ufficio affari generali tramite l'applicativo Pi.Tre., almeno 4 giorni lavorativi prima della seduta di Giunta, affinché la bozza dell'OdG possa essere, per tempo, esaminata attentamente dal Presidente della Regione prima della formale sottoscrizione.

Pertanto:

- se la seduta si tiene di mercoledì, le proposte di deliberazione devono essere

Die Regionalämter pflegen des Öfteren dem Amt für allgemeine Angelegenheiten den Gegenstand von Beschlussfassungsvorschlägen im Voraus per E-Mail mitzuteilen, das Dokument selbst jedoch nicht innerhalb der laut Geschäftsordnung für die Sitzungen der Regionalregierung vorgesehenen Frist im Pi.Tre.-System hochzuladen.

Infolgedessen können diese Beschlussfassungsvorschläge den Mitgliedern der Regionalregierung erst nach der Tagesordnung und nur kurz vor der Sitzung übermittelt werden, weshalb ihnen eventuell nicht ausreichend Zeit für eine angemessene Vorbereitung über das Thema bleibt.

Die Tagesordnung ist von größter Bedeutung, da sie die Themen abgrenzt, über die die Regionalregierung befinden muss, so dass deren Mitglieder sich mit Sachkenntnis an der Diskussion über die anstehenden Themen beteiligen können.

Die Einzelheiten betreffend die Abwicklung der Sitzungen, deren Einberufung und die Erstellung der Tagesordnung werden durch die mit Dekret des Präsidenten der Region vom 6. November 2020, Nr. 49 erlassene Geschäftsordnung für die Sitzungen der Regionalregierung geregelt.

Darüber hinaus möchte ich in diesem Rundschreiben auf andere Aspekte hinsichtlich der Erstellung der Beschlussfassungsvorschläge und der Bearbeitung der Beschlüsse hinweisen, die sich für die Regionalämter als nützlich erweisen können.

1. Übermittlung der Beschlüsse und der Promemoria für die Erstellung der Tagesordnung

Die mit den Sichtvermerken über die administrative Ordnungsmäßigkeit und eventuell mit jenen über die buchhalterische Ordnungsmäßigkeit versehenen Beschlussfassungsvorschläge müssen dem Amt für allgemeine Angelegenheiten über das Pi.Tre.-System mindestens 4 Werktage vor der Sitzung der Regionalregierung übermittelt werden, damit der Tagesordnungsentwurf vom Präsidenten der Region eingehend geprüft und anschließend formal unterzeichnet werden kann.

- Findet die Sitzung mittwochs statt, so sind die Beschlussfassungsvorschläge

trasmesse entro il giovedì precedente;

- se la seduta si tiene di martedì, il termine per la trasmissione delle proposte di deliberazione è il mercoledì precedente;
- se la seduta si tiene di giovedì, il termine per la trasmissione delle proposte di deliberazione è il venerdì precedente.

Ricordo che la presente tempistica si trova esposta anche in calce al calendario delle sedute di Giunta regionale relativo all'anno in corso, già trasmesso alle strutture e agli uffici. Anche i promemoria per la Giunta (PM), vanno trasmessi all'Ufficio affari generali in forma di documenti non protocollati (NP) con la medesima tempistica attraverso l'applicativo Pi.Tre., completi di firma digitale della/del Dirigente e d'intesa con il referente politico competente per materia, allegando anche la versione in formato *word*.

2.Importanza del visto amministrativo e del visto contabile

Attraverso evidenze informatiche vengono acquisiti i visti amministrativi della/del Direttrice/Direttore e della/del Dirigente, nonché i visti di natura contabile.

Con i visti amministrativi viene attestata la regolarità tecnica e quindi la legittimità delle proposte di deliberazione sottoposte all'esame della Giunta, secondo quanto previsto dall'art. 22 della legge regionale 9 novembre 1983, n. 15 e succ. mod.⁽¹⁾.

Il controllo di regolarità contabile e la procedura per l'accertamento di entrate e

bis spätestens donnerstags der vorhergehenden Woche zu übermitteln;

- findet die Sitzung dienstags statt, so sind die Beschlussfassungsvorschläge bis spätestens mittwochs der vorhergehenden Woche zu übermitteln;
- findet die Sitzung donnerstags statt, so sind die Beschlussfassungsvorschläge bis spätestens freitags der vorhergehenden Woche zu übermitteln;

Dieser Zeitplan wurde bereits zusammen mit dem Sitzungskalender der Regionalregierung für das laufende Jahr den Organisationsstrukturen und den Regionalämtern mitgeteilt. Auch die Promemoria für die Regionalregierung sind gemäß dem obigen Zeitplan dem Amt für allgemeine Angelegenheiten in Form von nicht protokollierten Dokumenten über das Pi.Tre.-System – von der Leiterin/dem Leiter der Abteilung digital signiert und im Einvernehmen mit dem zuständigen Mitglied der Regionalregierung – zusammen mit einer Fassung des Dokuments im Word-Format zu übermitteln.

2.Die Bedeutung des Sichtvermerks über die administrative bzw. über die buchhalterische Ordnungsmäßigkeit

Die Sichtvermerke der Amtsdirektorin/des Amtsdirektors und der Abteilungsleiterin/des Abteilungsleiters über die administrative Ordnungsmäßigkeit sowie jene über die buchhalterische Ordnungsmäßigkeit werden digital eingeholt.

Gemäß Art. 22 des Regionalgesetzes vom 9. November 1983, Nr. 15 i.d.g.F.⁽¹⁾ wird anhand der Sichtvermerke über die administrative Ordnungsmäßigkeit die verwaltungstechnische Ordnungsmäßigkeit und demnach die Rechtmäßigkeit der der Regionalregierung unterbreiteten Beschlussfassungsvorschläge bestätigt.

Die Überprüfung der buchhalterischen Ordnungsmäßigkeit sowie das Verfahren für

¹ Art. 22 (Responsabilità dei dirigenti e dei direttori di Ufficio).

1. Nell'ambito delle rispettive attribuzioni, i dirigenti di Ripartizione, i direttori di Ufficio e gli altri funzionari preposti alle strutture previste dal presente titolo, rispondono per gli atti amministrativi alla cui emanazione abbiano collaborato, nonché per l'omissione di attività o di atti ai quali siano per legge tenuti.

2. La disposizione di cui al precedente comma non esclude la responsabilità del personale assegnato alle Ripartizioni o agli Uffici per gli atti da esso compiuti o per l'omissione di attività o di atti ai quali sia tenuto nell'ambito dei compiti rispettivamente assegnati. A tale fine ogni atto deve recare l'indicazione del suo estensore.

¹ Art. 22 (Verantwortung der Dirigenten und der Amtsleiter)

(1) Im Rahmen der jeweiligen Aufgabenbereiche sind die Dirigenten, die Amtsleiter und die Beamten, die den in diesem Titel vorgesehenen Organisationseinheiten vorstehen, für die Verwaltungsakte, an denen sie mitgewirkt haben, sowie für die Unterlassung von Amtshandlungen verantwortlich, zu denen sie kraft Gesetz verpflichtet sind

(2) Die Bestimmung nach dem vorstehenden Absatz schließt die Verantwortung des den Abteilungen oder den Ämtern zugeteilten Personals für die von diesem durchgeführten oder unterlassenen Amtshandlungen oder die ihm im Rahmen der jeweils zugeteilten Aufgaben zustehen, nicht aus. Zu diesem Zweck muss in jedem Verwaltungsakt der Name des Verfassers angegeben sein.

l'assunzione di impegni sono regolati dall'art. 34 della legge regionale 15 luglio 2009, n. 3 e succ. mod.. Segnalo, in particolare, il comma 8-*bis* che prevede la registrazione contabile della proposta di deliberazione prima dell'inserimento nell'ordine del giorno della Giunta.

Attualmente la procedura informatizzata non impedisce ai collaboratori e alle collaboratrici di sostituirsi alle/ai Dirigenti e alle/ai Direttrici/Direttori nell'apposizione dei visti. Tuttavia, anche alla luce della rilevanza che il sistema dei controlli può assumere in un giudizio di responsabilità amministrativo-contabile, ribadisco che il rilascio dei visti è di esclusiva competenza di Dirigenti e Direttrici/Direttori. In assenza dei titolari degli uffici, o in accordo con loro, il visto sarà rilasciato dai sostituti individuati a tale scopo. Le indicazioni operative inerenti alla procedura per la gestione delle deliberazioni, tra le quali la modalità di apposizione dei visti, sono sempre consultabili attraverso la *directory*: M:\Comune\P.I.Tre\ Decreti e Delibere ODL - Manuale operativo.

3.Apposizione dei visti: rispetto dei tempi tecnici e monitoraggio dello stato di avanzamento della proposta di deliberazione

Chiedo gentilmente di voler prestare attenzione ai tempi tecnici necessari all'apposizione dei visti da parte delle/dei Direttrici/Direttori e delle/dei Dirigenti, in particolare per le proposte che necessitano anche del visto da parte dell'Ufficio bilancio e controllo contabile.

In tale ultimo caso, è necessario che la proposta di deliberazione, con i visti delle/dei Direttrici/Direttori e delle/dei Dirigenti della struttura proponente, venga trasmessa all'Ufficio bilancio e controllo contabile almeno 7 giorni lavorativi prima della seduta di Giunta.

Ricordo che solamente quando è concluso

die Einnahmenfeststellungen und die Ausgabenverpflichtungen sind im Art. 34 des Regionalgesetzes vom 15. Juli 2009, Nr. 3 i.d.g.F. geregelt. Ich mache insbesondere auf den Abs. 8-*bis* aufmerksam, laut dem der Beschlussfassungsvorschlag in der Regel vor seiner Aufnahme in die Tagesordnung der Sitzung der Regionalregierung buchhalterisch registriert werden muss.

Derzeit erlaubt das Anwendungsprogramm den Mitarbeitenden, an Stelle der Abteilungsleiterinnen/Abteilungsleiter bzw. der Amtsdirektorinnen/Amtsdirektoren genannte Sichtvermerke anzubringen. Angesichts der Relevanz des Kontrollsystems im Rahmen eines eventuellen Verfahrens wegen Amts- und Rechnungshaftung wird nachdrücklich darauf hingewiesen, dass das Anbringen von Sichtvermerken ausschließlich unter die Zuständigkeit der Abteilungsleiterinnen/Abteilungsleiter und der Amtsdirektorinnen/Amtsdirektoren fällt. Bei deren Abwesenheit oder im Einvernehmen mit denselben kann der Sichtvermerk von den eigens dafür bestimmten Stellvertretenden angebracht werden. Die Verfahrensanweisungen für die Bearbeitung der Beschlüsse einschließlich der Vorgehensweise für das Anbringen der Sichtvermerke können stets unter M:\Comune\P.I.Tre\ Decreti e Delibere ODL - Manuale operativo nachgelesen werden.

3.Anbringen der Sichtvermerke: Einhaltung der Bearbeitungszeiten und Überprüfung des Bearbeitungsstands des Beschlussfassungsvorschlags

Die für das Anbringen der Sichtvermerke seitens der Amtsdirektorinnen/Amtsdirektoren sowie der Abteilungsleiterinnen/Abteilungsleiter erforderlichen Bearbeitungszeiten sind unbedingt zu berücksichtigen, insbesondere wenn es um Beschlussfassungsvorschläge geht, die auch den Sichtvermerk des Amtes für Haushalt und Buchhaltungskontrolle erfordern.

Im letzteren Fall ist der Beschlussfassungsvorschlag samt den Sichtvermerken der Amtsdirektorin/des Amtsdirektors und der Leiterin/des Leiters der einbringenden Abteilung mindestens 7 Werktage vor der Sitzung der Regionalregierung dem Amt für Haushalt und Buchhaltungskontrolle zu übermitteln.

Es sei an dieser Stelle daran erinnert, dass

l'iter dei visti (Direttrice/Direttore, Dirigente e, ove necessario, visto contabile) la procedura informatica trasmette in automatico le proposte di deliberazione all'Ufficio affari generali, per l'inserimento nell'OdG.

Le collaboratrici e i collaboratori dell'ufficio proponente sono invitati a tenere costantemente monitorato lo stato di avanzamento della proposta di deliberazione, affinché la medesima possa pervenire, nei tempi prestabiliti, all'Ufficio affari generali per l'inserimento nell'OdG.

4. Proposte di deliberazione con testo bilingue

Di norma, le proposte di deliberazione redatte nella doppia lingua vanno inserite nell'applicativo Pi.Tre. già complete di traduzione, in modo tale che i necessari visti vengano apposti al testo definitivo in formato bilingue. Pertanto, è necessario che gli uffici proponenti informino con congruo anticipo l'Ufficio traduzioni al fine di consentire allo stesso la programmazione delle proprie attività, in ragione dell'impegno e della tempistica richiesti per la traduzione dei testi, soprattutto se voluminosi o di carattere non routinario, considerato che in prossimità delle sedute di Giunta all'Ufficio confluiscono richieste da tutte le strutture regionali. In caso di deliberazioni o allegati con contenuti particolarmente tecnici è comunque auspicabile un coinvolgimento dell'Ufficio traduzioni già nella fase di stesura delle relative bozze.

Per le proposte di deliberazione che rivestono carattere d'urgenza o di particolare complessità, è eccezionalmente possibile avviare l'iter in Pi.Tre. con il testo redatto nella sola lingua italiana. In tal caso, si chiede di dare adeguata comunicazione scritta all'Ufficio affari generali mediante e-mail all'indirizzo dedicato riportato al successivo punto 12. Nel momento in cui la proposta di deliberazione sarà tradotta, la collaboratrice o il collaboratore dell'ufficio proponente caricherà una nuova versione nell'applicativo Pi.Tre., indicando, nelle note di versione, che trattasi del documento tradotto. Ne va poi data comunicazione all'Ufficio affari generali.

das Anwendungsprogramm dem Amt für allgemeine Angelegenheiten die Beschlussfassungsvorschläge zwecks Erstellung der Tagesordnung erst übermittelt, wenn der Vorgang der anzubringenden Sichtvermerke (Amtsleiterin/Amtsleiter, Abteilungsleiterin/Abteilungsleiter und eventueller Sichtvermerk über die buchhalterische Ordnungsmäßigkeit) abgeschlossen ist.

Die Bediensteten des den Beschlussfassungsvorschlag einbringenden Amtes müssen dessen Bearbeitungsstand regelmäßig überprüfen, damit er fristgerecht beim Amt für allgemeine Angelegenheiten zwecks Erstellung der Tagesordnung eingehen kann.

4. Beschlussfassungsvorschläge mit zweisprachigem Wortlaut

In der Regel sind die zweisprachig zu verfassenden Beschlussfassungsvorschläge samt Übersetzung in das Pi.Tre.-System einzugeben, so dass die erforderlichen Sichtvermerke am endgültigen zweisprachigen Dokument angebracht werden. Demnach muss das den Beschlussfassungsvorschlag einbringende Amt das Übersetzungsamt mit angemessener Vorlaufzeit kontaktieren, damit dieses seine Tätigkeit je nach dem für die Übersetzung der Texte erforderlichen Zeitaufwand planen kann; dies gilt insbesondere, wenn es sich um umfangreiche oder unübliche Texte handelt, da das Amt für Übersetzungen kurz vor den Sitzungen der Regionalregierung Anfragen von allen Organisationsstrukturen der Region erhält. Bei Beschlüssen oder Anlagen besonders fachlichen Inhalts ist es in jedem Fall angebracht, das Amt für Übersetzungen bereits zum Zeitpunkt der Ausarbeitung der diesbezüglichen Entwürfe einzubeziehen.

Bei dringenden oder besonders komplexen Beschlussfassungsvorschlägen kann der Vorgang im Pi.Tre.-System ausnahmsweise mit dem nur in italienischer Sprache verfassten Text begonnen werden. In diesem Fall ist das Amt für allgemeine Angelegenheiten mittels E-Mail an die spezifische unter Z. 12 angeführte Adresse darüber zu informieren. Sobald der Beschlussfassungsvorschlag übersetzt ist, muss das den Vorschlag einbringende Amt eine neue Fassung in das Pi.Tre.-System hochladen und unter den entsprechenden Anmerkungen angeben, dass es sich um das übersetzte Dokument handelt.

Anschließend ist das Amt für allgemeine Angelegenheiten darüber in Kenntnis zu setzen.

5.Caso eccezionale: anticipazione dell'oggetto della proposta di deliberazione e iscrizione provvisoria all'OdG

Qualora si presentasse l'urgente e imprevista necessità di predisporre un provvedimento a ridosso della seduta di Giunta, chiedo al collega e alle colleghe Dirigenti di comunicare direttamente al sottoscritto, via e-mail, l'oggetto di tali proposte, con la motivazione a base dell'urgenza.

Non verrà dunque dato corso alle richieste di inserimento nell'OdG di proposte pervenute da soggetti diversi dai Dirigenti preposti alle strutture organizzative.

6.Gestione delle versioni nell'applicativo Pi.Tre.

6.1 Procedura ordinaria

Il gestionale Pi.Tre. permette di acquisire ulteriori versioni della stessa proposta di deliberazione nel caso in cui si renda necessario apportare al documento modifiche o correzioni.

Questa possibilità può essere utilizzata dall'ufficio proponente nei seguenti casi:

- a) prima dei visti della/del Direttrice/Direttore e della/del Dirigente (nello stato "Bozza");
- b) in seguito al recepimento, da parte dell'ufficio proponente ed in accordo con il/la Dirigente/Direttore del medesimo, delle osservazioni formulate dall'Ufficio bilancio nell'esercizio del controllo contabile. In tal caso, il nuovo documento, in formato *word*, verrà vistato dalla/dal Direttrice/Direttore e dalla/dal Dirigente, utilizzando l'apposita icona (*nota: è necessario aprire il documento per attivare l'icona*):



5.Ausnahmefall: Vorankündigung des Gegenstands des Beschlussfassungsvorschlags und vorläufige Aufnahme in die Tagesordnung

Bei besonderer Dringlichkeit und unvorhersehbarer Notwendigkeit, einen Beschluss kurz vor der Sitzung der Regionalregierung zu erstellen, werden die zuständigen Abteilungsleiterinnen/Abteilungsleiter ersucht, den Gegenstand des entsprechenden Beschlussfassungsvorschlags samt der Begründung für die Dringlichkeit direkt dem Unterfertigten per E-Mail mitzuteilen.

Beschlussfassungsvorschläge, deren Aufnahme in die Tagesordnung von anderen Personen als der Leiterin/dem Leiter der zuständigen Abteilung beantragt wird, werden demnach nicht berücksichtigt.

6.Handhabung der Fassungen im Pi.Tre.-System

6.1 Ordentliche Vorgangsweise

Das Pi.Tre-System erlaubt das Hochladen weiterer Fassungen desselben Beschlussfassungsvorschlags, sofern dieser geändert oder berichtigt werden muss.

Das den Beschlussfassungsvorschlag einbringende Amt kann in nachstehenden Fällen von dieser Möglichkeit Gebrauch machen:

- a) vor Anbringen des Sichtvermerks der Amtsdirektorin/des Amtsdirektors und der Abteilungsleiterin/des Abteilungsleiters (im Status „Bozza“);
- b) nachdem das einbringende Amt im Einvernehmen mit der Amtsdirektorin/dem Amtsdirektor bzw. mit der Abteilungsleiterin/dem Abteilungsleiter den vom Amt für Haushalt im Zuge der Buchhaltungskontrolle vorgebrachten Bemerkungen Rechnung getragen hat. In diesem Fall wird das neue Dokument im Word-Format von der Amtsdirektorin/dem Amtsdirektor und der Abteilungsleiterin/dem Abteilungsleiter durch das nachstehende Symbol mit dem Sichtvermerk versehen (*Anm.: Das Dokument muss geöffnet sein, um das Symbol zu aktivieren*):



In entrambi i casi sopra delineati, con l'apposizione del visto della/del Dirigente oppure mediante la vidimazione contabile, la procedura informatica trasmette in automatico all'Ufficio affari generali il documento definitivo che verrà inoltrato ai componenti della Giunta come allegato all'OdG.

Al fine di attribuire certezza all'atto amministrativo viene riportato, nell'OdG e nel verbale della seduta di Giunta, in corrispondenza dell'oggetto della deliberazione, il numero dell'ID di Pi.Tre. e il numero dell'unica o dell'ultima versione.

Pertanto, è di tutta evidenza, che non devono essere inserite in Pi.Tre. nuove versioni dopo il visto Dirigente oppure, ove previsto, dopo il visto contabile.

6.2 Gestione dei casi eccezionali

Nel caso, straordinario e motivato, in cui l'Ufficio proponente debba inserire nel gestionale un'ulteriore versione, dopo la conclusione dell'*iter* dei visti, e in accordo con la/il Dirigente, ne darà tempestiva comunicazione scritta all'Ufficio affari generali e, ove previsto, anche all'Ufficio bilancio e controllo contabile. Come già specificato al punto 4, è necessario indicare il motivo nelle note di versione.

Si fa presente che, in assenza di comunicazione, la nuova versione potrebbe non essere presa in considerazione.

7. Gestione e formalizzazione degli allegati al provvedimento che formano parte integrante e sostanziale

Gli allegati che costituiscono parte integrante e sostanziale delle deliberazioni vanno gestiti, nel gestionale Pi.Tre., secondo una delle seguenti modalità:

- a) la proposta di deliberazione è formata da un unico documento in formato *word* che comprende l'atto deliberativo e il testo dell'allegato o degli allegati. Nel

In beiden Fällen wird das endgültige Dokument nach Anbringen des Sichtvermerks seitens der Abteilungsleiterin/des Abteilungsleiters bzw. des Sichtvermerks über die buchhalterische Ordnungsmäßigkeit automatisch vom Anwendungsprogramm dem Amt für allgemeine Angelegenheiten übermittelt und den Mitgliedern der Regionalregierung im Anhang zur Tagesordnung weitergeleitet.

Um die Rechtssicherheit des Verwaltungsakts zu gewährleisten, werden in der Tagesordnung und in der Niederschrift der Sitzung der Regionalregierung neben jedem Beschlussgegenstand die Pi.Tre.-Identifikationsnummer sowie die Nummer der einzigen bzw. der letzten Fassung angeführt.

Daraus folgt offensichtlich, dass nach dem Anbringen des Sichtvermerks durch die Abteilungsleiterin/den Abteilungsleiter und – sofern vorgesehen – des Sichtvermerks über die buchhalterische Ordnungsmäßigkeit keine neuen Fassungen im Pi.Tre.-System hochgeladen werden dürfen.

6.2 Vorgangsweise in Ausnahmefällen

Muss das den Beschlussfassungsvorschlag einbringende Amt in einem begründeten Ausnahmefall nach dem Anbringen der Sichtvermerke und im Einvernehmen mit der Abteilungsleiterin/dem Abteilungsleiter eine weitere Fassung hochladen, so ist dies umgehend dem Amt für allgemeine Angelegenheiten und – sofern vorgesehen – dem Amt für Haushalt und Buchhaltungskontrolle schriftlich mitzuteilen. Wie bereits unter Z. 4 erklärt, ist dies unter den Anmerkungen entsprechend zu begründen. Es wird darauf aufmerksam gemacht, dass in Ermangelung einer solchen Mitteilung die neue Fassung eventuell nicht berücksichtigt werden könnte.

7. Handhabung und Formalisierung der Anlagen, die der Maßnahme als ergänzender und wesentlicher Bestandteil beiliegen

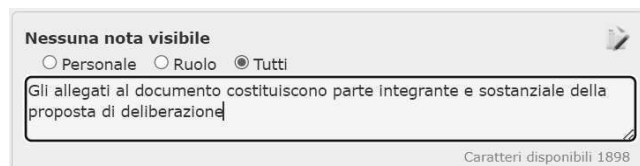
Bei Anlagen, die den Beschlüssen als ergänzender und wesentlicher Bestandteil beiliegen, ist im Pi.Tre.-Anwendungsprogramm wie folgt vorzugehen:

- a) Besteht der Beschlussfassungsvorschlag aus einem einzigen Dokument im Word-Format, das den Beschluss und die Anlage bzw. Anlagen umfasst,

gestionale Pi.Tre. il *file* viene acquisito come documento principale, al pari delle proposte di deliberazione che non hanno allegati. Questa modalità va utilizzata per l'approvazione di regolamenti, schemi di contratto, convenzioni, accordi tra enti, ecc.

- b) la proposta di deliberazione è formata da un documento *word* costituito dall'atto deliberativo e da uno o più allegati in formato *pdf*. In questo caso la proposta di deliberazione va acquisita in Pi.Tre. come documento principale e il *file pdf* come "allegato". Questa modalità va utilizzata solamente quando l'allegato parte integrante e sostanziale è costituito da tabelle, tabulati provenienti da gestionali o da documenti di altri enti.

L'Ufficio affari generali deve essere messo al corrente, mediante nota in Pi.Tre., che l'allegato costituisce parte integrante e sostanziale della deliberazione al fine di allegarlo all'OdG unitamente alla relativa deliberazione. A tal fine, andrà utilizzato il campo di seguito indicato e l'inserimento della nota andrà confermato attraverso la funzione "Salva":



Questo è indispensabile perché, la sezione "allegati", viene utilizzata anche per gestire documentazione che non costituisce parte integrante e sostanziale del provvedimento (es. versione con *omissis*).

Sarà cura dell'Ufficio affari generali, unire materialmente l'allegato al corrispondente provvedimento, dopo l'approvazione da parte della Giunta regionale.

Ritengo opportuno precisare che, per i provvedimenti aventi ad oggetto l'approvazione di schemi di convenzione / contratti / accordo tra enti o di atto analogo, nel dispositivo va indicato il soggetto a cui compete la sottoscrizione del medesimo. Va inoltre indicata la struttura, che di norma corrisponde alla struttura proponente, competente all'adozione di tutti gli atti

so ist die Datei als Hauptdokument im Pi.Tre.-System hochzuladen, so wie es für Beschlussfassungsvorschläge ohne Anlagen der Fall ist. Diese Vorgangsweise gilt für die Genehmigung von Verordnungen, Vertragsentwürfen usw.

- b) Besteht der Beschlussfassungsvorschlag aus einem Beschluss im Word-Format und einer oder mehreren Anlagen im PDF-Format, so sind der Beschluss als Hauptdokument und die PDF-Dateien als Anlagen im Pi.Tre.-System hochzuladen. Diese Vorgangsweise gilt ausschließlich, wenn die als ergänzender und wesentlicher Bestandteil beiliegende Anlage aus Tabellen – auch aus anderen Anwendungsprogrammen – oder aus Dokumenten anderer Körperschaften besteht.

Das Amt für allgemeine Angelegenheiten ist über eine entsprechende Anmerkung im Pi.Tre.-System davon in Kenntnis zu setzen, dass die Anlage ergänzender und wesentlicher Bestandteil des Beschlusses ist, damit sie zusammen mit dem Beschluss selbst in die Tagesordnung aufgenommen wird. Hierfür ist das nachstehende Feld zu verwenden, wobei die Eingabe durch die Funktion „Salva“ zu bestätigen ist.

Diese Vorgangsweise ist unerlässlich, da der Bereich „allegati“ auch für andere Unterlagen verwendet wird, die nicht ergänzender und wesentlicher Bestandteil der Maßnahme sind. (z. B. für Fassungen mit anonymisierten Stellen).

Nach der Genehmigung seitens der Regionalregierung wird das Amt für allgemeine Angelegenheiten dafür Sorge tragen, dass die Anlage mit dem entsprechenden Beschluss konkret zusammengefügt wird.

Es sei an dieser Stelle darauf hingewiesen, dass bei Maßnahmen betreffend die Genehmigung der Entwürfe von Vereinbarungen/Verträgen/Abkommen zwischen Körperschaften oder vergleichbaren Akten im beschließenden Teil stets das für die Unterzeichnung zuständige Rechtssubjekt angegeben werden muss. Des Weiteren ist die Organisationsstruktur

d'esecuzione del provvedimento. Tra questi rientra anche la formalizzazione della convenzione / contratto / accordo tra enti o di atto analogo, mediante la tempestiva raccolta delle firme delle parti e l'immediato inserimento dell'atto nel repertorio del gestionale Pi.Tre denominato *"Registro di raccolta dei contratti"*, per la conservazione.

8.Deliberazioni approvate dalla Giunta con modificazioni

In caso di approvazione della deliberazione con modificazioni da parte della Giunta regionale, ne viene data tempestiva comunicazione alla/al Dirigente della struttura proponente affinché provveda a formulare un nuovo testo che recepisca la modifica approvata. Se la modifica ha riflessi contabili ne viene informato anche l'Ufficio bilancio e controllo contabile. L'Ufficio interessato, dopo aver modificato il testo e ottenuto l'eventuale benestare dell'Ufficio bilancio, ed effettuate le eventuali modifiche anche nel testo tradotto, inserirà il documento in Pi.Tre., in formato *word*, aggiungendo una nuova versione al documento originario.

Anche in tal caso, il nuovo documento, in formato *word*, verrà vistato dalla/dal Direttrice/Direttore e dalla/dal Dirigente, utilizzando l'apposita icona (*nota: è necessario aprire il documento per attivare l'icona*):



Dopo l'apposizione del/dei visto/i, l'ufficio proponente comunicherà tempestivamente all'Ufficio affari generali e comunque entro la medesima giornata, via e-mail, l'avvenuto inserimento della nuova ed ultima versione.

9.Numerazione e sottoscrizione delle deliberazioni

L'apposizione del numero e della data della deliberazione, nonché l'eventuale indicazione

anzugeben (in der Regel handelt es sich hierbei um die einbringende Abteilung), die für den Erlass sämtlicher zur Umsetzung der Maßnahme erforderlichen Akte zuständig ist. Unter diese Akte fällt auch die Formalisierung der Vereinbarung/des Vertrags/des Abkommens zwischen Körperschaften bzw. des vergleichbaren Aktes, durch Einholen der Unterschriften der Parteien und die umgehende Eintragung des Aktes in das entsprechende Pi.Tre.-Register *„Registro di raccolta dei contratti“* zum Zweck seiner Aufbewahrung.

8.Von der Regionalregierung mit Änderungen genehmigte Beschlüsse

Genehmigt die Regionalregierung den Beschluss mit Änderungen, so wird die Leiterin / der Leiter der einbringenden Abteilung umgehend davon in Kenntnis gesetzt, damit ein neuer Wortlaut mit den genehmigten Änderungen ausgearbeitet wird. Sollten die Änderungen Auswirkungen auf die Buchhaltung haben, ist auch das Amt für Haushalt und Buchhaltungskontrolle zu informieren. Nach der Änderung des Wortlauts und der eventuellen Zustimmung des Amtes für Haushalt sowie der eventuellen Änderung des übersetzten Wortlauts muss das betreffende Amt das Dokument im Wort-Format als zusätzliche Fassung zum ursprünglichen Dokument im Pi.Tre.-System hochladen.

Auch in diesem Fall wird das neue Dokument im Word-Format von der Amtsdirektorin/dem Amtsdirektor und der Abteilungsleiterin/dem Abteilungsleiter durch das nachstehende Symbol mit dem Sichtvermerk versehen (*Anm.: Das Dokument muss geöffnet sein, um das Symbol zu aktivieren*):



Nach Anbringen des Sichtvermerks/der Sichtvermerke muss das einbringende Amt umgehend und in jedem Fall noch am selben Tag das Amt für allgemeine Angelegenheiten per E-Mail davon in Kenntnis setzen, dass die neue und letzte Fassung hochgeladen wurde.

9.Nummerierung und Unterzeichnung der Beschlüsse

Das Amt für allgemeine Angelegenheiten versieht nach der Sitzung der

dei componenti assenti, è effettuata dall'Ufficio affari generali successivamente alla seduta di Giunta. Per tale ragione il testo della proposta di deliberazione va acquisito nel gestionale Pi.Tre. esclusivamente come *file* in formato *word*.

Raccomando di seguire scrupolosamente le indicazioni esposte nei punti precedenti per permettere all'Ufficio affari generali di sottoporre alla firma del Presidente e del Segretario generale la versione definitiva e corretta della deliberazione approvata dalla Giunta.

10. Privacy

Le disposizioni in materia di protezione dei dati personali di cui al Regolamento (UE) n. 2016/679, al decreto legislativo n. 196/2003 e succ. mod., e alle Linee guida emanate dal Garante (*Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati - Allegato alla deliberazione n. 243 del 15 maggio 2014*), sanciscono il divieto assoluto di diffusione dei dati idonei a rivelare lo stato di salute e la vita sessuale delle persone.

Le medesime disposizioni stabiliscono altresì che i soggetti pubblici non possono rendere intelligibili i dati personali (nome e cognome, data e luogo di nascita, sesso, indirizzo e codice fiscale) non necessari e non pertinenti con le finalità della pubblicazione. Specificano, inoltre, che per anonimizzare un documento occorre oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possono consentire l'identificazione anche a posteriori.

Premesso quanto sopra, ove l'Ufficio proponente rilevi la necessità anonimizzare dati e informazioni nel testo del provvedimento, opererà nel seguente modo:

- creazione contestuale di un nuovo documento in formato word nel quale i dati personali e le informazioni sono sostituiti dalla dicitura "...omissis...";
- caricamento del nuovo documento in

Regionalregierung den Beschluss mit Nummer und Datum sowie mit der Angabe der abwesenden Mitglieder. Aus diesem Grund darf der Beschlussfassungsvorschlag ausschließlich im Word-Format im Pi.Tre. Anwendungsprogramm hochgeladen werden.

Die oben genannte Vorgangsweise ist genauestens zu befolgen, damit das Amt für allgemeine Angelegenheiten dem Präsidenten und dem Generalsekretär die endgültige und korrekte Fassung des von der Regionalregierung genehmigten Beschlusses zur Unterschrift vorlegen kann.

10. Datenschutz

Gemäß den Bestimmungen zum Schutz personenbezogener Daten laut Verordnung (EU) 2016/679 und GvD Nr. 196/2003 i.d.g.F. sowie den von der Datenschutzbehörde herausgegebenen Leitlinien (*Leitlinien für die Verarbeitung von auch in Verwaltungsakten und Dokumenten enthalten personenbezogenen Daten, die von öffentlichen Einrichtungen und anderen Verpflichteten zum Zwecke der Bekanntmachung und Transparenz im Internet durchgeführt wird – Anlage zum Beschluss vom 15. Mai 2014, Nr. 243*) ist die Verbreitung von Daten, die Aufschluss über die Gesundheit und das Sexualleben von Personen geben, strengstens verboten.

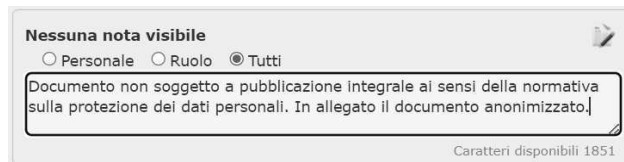
Laut denselben Bestimmungen dürfen öffentliche Einrichtungen auch keine personenbezogenen Daten (Vor- und Nachname, Geburtsdatum und -ort, Geschlecht, Anschrift und Steuernummer) weitergeben, die für den Zweck der Veröffentlichung nicht erheblich und nicht erforderlich sind. Darüber hinaus müssen zur Anonymisierung eines Dokuments der Name und die anderen Informationen, die sich auf die betroffene Person beziehen und seine Identifizierung auch im Nachhinein ermöglichen könnten, vollständig verborgen werden.

Dies vorausgeschickt muss das einbringende Amt – falls die Notwendigkeit besteht, Daten und Informationen im Wortlaut des Beschlusses zu anonymisieren

- gleichzeitig ein neues Dokument im Word-Format erstellen, in dem die personenbezogenen Daten und Informationen durch Einsetzen von „omissis“ im italienischen Text und „(...)“ im deutschen Text ersetzt wurden;
- das neue Dokument im Word-Format als

Pi.Tre., in formato *word*, come “allegato” del documento principale.

L'Ufficio affari generali deve essere messo al corrente, mediante nota in Pi.Tre., che il documento originale non andrà pubblicato sul sito internet ma andrà sostituito da un documento anonimizzato. A tal fine, andrà utilizzato il campo di seguito indicato e l'inserimento della nota andrà confermato attraverso la funzione “Salva”:



Come è noto, con deliberazione della Giunta regionale n. 193 di data 3 settembre 2019 le/i Dirigenti delle singole strutture sono stati individuati quali responsabili interni preposti al trattamento dei dati personali. Pertanto spetta alle/ai Dirigenti operare una valutazione sul contenuto degli atti ai fini della pubblicazione, da effettuare alla luce dei principi e delle specifiche disposizioni di cui al Regolamento (EU) n. 679/2016, nonché degli orientamenti assunti dall'Autorità Garante per la protezione dei dati personali.

11. Veste grafica dei provvedimenti

Gli atti amministrativi, tra i quali anche le deliberazioni della Giunta, sono soggetti a pubblicazione sul sito internet istituzionale e hanno quindi ampia visibilità sull'esterno. Anche per tale ragione va rispettata la modulistica aggiornata e messa a disposizione nella cartella di rete M:\Comune\AFFARI GENERALI - MODELLI senza introdurre adattamenti o personalizzazioni.

12. E-mail dedicata

Tutte le comunicazioni inerenti alla redazione dell'OdG e alla gestione delle proposte di deliberazione, vanno inviate esclusivamente sulla e-mail dedicata delibere@regione.taa.it. È opportuno, quindi, non trasmettere comunicazioni rilevanti alla casella di posta elettronica personale dei collaboratori dell'Ufficio affari generali.

Anlage zum Hauptdokument im Pi:-Tre.-System hochladen.

Das Amt für allgemeine Angelegenheiten ist über eine entsprechende Anmerkung im Pi.Tre.-System davon in Kenntnis zu setzen, dass das Originaldokument nicht auf der Website veröffentlicht werden darf, sondern durch ein anonymisiertes Dokument ersetzt wird. Hierfür ist das nachstehende Feld zu verwenden, wobei die Eingabe durch die Funktion „Salva“ zu bestätigen ist.

Bekanntlich wurden die Leiterinnen und Leiter der einzelnen Organisationsstrukturen mit Beschluss der Regionalregierung vom 3. September 2019, Nr. 193 als interne Auftragsverarbeiter bestimmt. Daher obliegt es den Abteilungsleiterinnen und Abteilungsleitern, den Inhalt der Maßnahmen im Hinblick auf ihre Veröffentlichung unter Berücksichtigung der Grundsätze und spezifischen Bestimmungen der Verordnung (EU) 679/2016 sowie der von der Datenschutzbehörde herausgegebenen Leitlinien zu überprüfen.

11. Grafische Gestaltung der Maßnahmen

Die Beschlüsse der Regionalregierung müssen als Verwaltungsakt auf der offiziellen Website veröffentlicht werden, wo sie für die Allgemeinheit einsehbar sind. Aus diesem Grund sind unbedingt die aktualisierten Vorlagen zu verwenden, die im Ordner M:\Comune\AFFARI GENERALI – MODELLI zur Verfügung stehen, welche in keiner Weise angepasst oder geändert werden dürfen.

12. Spezifische E-Mail-Adresse

Sämtliche Mitteilungen betreffend die Tagesordnung und die Handhabung der Beschlussfassungsvorschläge sind ausschließlich an die spezifische E-Mail-Adresse delibere@regione.taa.it zu richten. Demnach sind wichtige Mitteilungen nie an die persönliche E-Mail-Adresse der Bediensteten des Amtes für allgemeine Angelegenheiten zu senden.

Fiducioso della vostra collaborazione, vi segnalo che il personale dell'Ufficio affari generali rimane a disposizione per ulteriori chiarimenti.

Cordiali saluti.

Ich danke Ihnen für Ihre Zusammenarbeit. Die Bediensteten des Amtes für allgemeine Angelegenheiten stehen gerne für nähere Auskünfte zur Verfügung.

Mit freundlichen Grüßen

**IL SEGRETARIO GENERALE/
DER GENERALSEKRETÄR**

Michael Mayr
firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Schreiben in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (Art. 3-bis des GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

MM/RG/MB/NC/DM



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Segreteria generale
Generalsekretariat
Ufficio affari generali
Amt für allgemeine Angelegenheiten
☎ 0461 201323
@ affgen@regione.taa.it
pec: affgen@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Protokollnummer und Registrierungsdatum sind dem Dokument als Metadaten zugeordnet (Dekret des Präsidenten des Ministerrates vom 3.12.2013, Art. 20). Gegenstand der zertifizierten E-Mail bzw. beigefügte Dateien überprüfen.

CIRCOLARE/RUNDSCHREIBEN

**Oggetto: Esito audit dd. 05/06/2023 del
Consorzio dei Comuni ed indicazioni in
materia di privacy**

**Betreff: Ergebnisse des am 5. Juni 2023
vom Gemeindenverband durchgeführten
Audit und Hinweise in Sachen
Datenschutz**

Gentili collaboratrici e collaboratori,

Werte Mitarbeiterinnen und Mitarbeiter,

a seguito dell'audit dd. 05 giugno con il Consorzio dei Comuni Trentini, volto a verificare la corretta applicazione della normativa in materia di privacy da parte della Regione, riteniamo doveroso darvi riscontro della valutazione. Non sono state evidenziate difformità rilevanti nell'applicazione della materia. Il materiale oggetto di indagine sarà in un secondo momento richiesto dal CCT: si richiede quindi la Vostra massima collaborazione nel fornire in tempi rapidi la documentazione richiesta (seguirà successiva comunicazione).

am 5. Juni 2023 hat der Gemeindenverband der Provinz Trient im Rahmen eines Audit die korrekte Anwendung der Datenschutzbestimmungen seitens der Regionalverwaltung überprüft, wobei keine relevanten Verletzungen der einschlägigen Bestimmungen festgestellt wurden. Die überprüften Unterlagen werden später vom technischen Beratungsgremium angefordert, weshalb Ihre volle Unterstützung bei der umgehenden Bereitstellung der angeforderten Dokumente gefragt ist (es wird ein Schreiben folgen).

Il CCT ha chiesto, ai presenti, di portare nuovamente all'attenzione dei collaboratori, alcuni fondamentali concetti in materia di privacy, che sono:

Das technische Beratungsgremium ersucht darum, die Mitarbeiterinnen und Mitarbeiter erneut auf einige wichtige Grundsätze in Sachen Datenschutz hinzuweisen, und zwar:

- **Dato personale:** è definito dato personale qualunque dato che può o potrebbe essere riferito, in connessione o in combinazione con altre informazioni o dati, tanto nel contesto attuale di trattamento come anche in contesti diversi ed anche futuri ma comunque prevedibili, ad una persona fisica

- Als **personenbezogene Daten** gelten all jene, die sowohl bei einer laufenden Verarbeitung als auch in anderen – eventuell auch zukünftigen, aber in jedem Fall vorhersehbaren – Kontexten in Verbindung oder in Kombination mit anderen Informationen oder Daten einer bestimmten



Regione Autonoma Trentino-Alto Adige/Südtirol

Region Autonoma Trentin-Südtirol

Autonome Region Trentino-Südtirol

identificata o comunque distinguibile dalle altre. Rientrano nella tipologia di dati personali: il nome, la ragione sociale di un'azienda, un numero di identificazione, dati relativi all'ubicazione, un identificativo online (e-mail) e recapiti telefonici. I dati personali pertanto consentono di identificare in maniera **diretta il soggetto** (ad esempio: nome e cognome, i dati anagrafici), mentre le immagini, ecc. e i dati permettono invece l'identificazione in maniera **indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa). Si ponga in particolar modo attenzione al fatto che anche il semplice conferimento di nome e cognome in forma verbale (ad esempio l'identificazione del visitatore da parte del servizio di portineria) rappresenta un trattamento di dati personali, che deve essere inserito nel registro delle attività di trattamento dei dati. Nel contempo deve anche essere esposta l'informativa (art. 13 GDPR).

- **Trattamento di dati personali:** è definito trattamento di dati personali un insieme coerente e coordinato di operazioni sui dati personali - organizzati o meno in una o più banche di dati – effettuato da parte di responsabili ed incaricati a ciò specificamente legittimati, funzionale ad una data attività del titolare e preordinato a soddisfare una più ampia, finalità, anche di rilevante interesse pubblico, che si caratterizza per le tipologie di dati trattati, le procedure (informatizzate o manuali) utilizzate ed il flusso informativo in cui si struttura.

- la figura del **RPD** (Responsabile della Protezione dei Dati Personali oppure, nella versione inglese, **DPO** – Data Protection Officer).

oder in jedem Fall von anderen unterscheidbaren natürlichen Person zugeordnet werden können. Zur Kategorie der personenbezogener Daten zählen: Name, Bezeichnung eines Unternehmens, Kennnummer, Standortdaten, Online-Kennung (E-Mail) und Telefonnummern. Personenbezogene Daten ermöglichen nämlich eine **direkte** Identifizierung der **Person** (z. B. Vor- und Zuname, Personalien); Bilder u. Ä. und Daten wie beispielsweise eine Kennnummer (Steuernummer, IP-Adresse, Kfz-Kennzeichen) erlauben hingegen eine **indirekte** Identifizierung. Diesbezüglich wird insbesondere darauf aufmerksam gemacht, dass auch eine einfache mündliche Auskunft über Vor- und Zuname (z. B. die Identifizierung eines Besuchers von Seiten des Pfortnerdienstes) als Verarbeitung personenbezogener Daten zählt, die im Verzeichnis der Verarbeitungstätigkeiten zu vermerken ist. Gleichzeitig ist auch die Datenschutzerklärung auszuhängen (Art. 13 DSGVO).

- **Verarbeitung personenbezogener Daten:** Als Verarbeitung personenbezogener Daten wird eine kohärente und koordinierte Gesamtheit von Vorgängen mit personenbezogenen Daten bezeichnet, die - unabhängig davon, ob sie in einer oder mehreren Datenbanken gespeichert sind - von eigens dazu befugten Auftragsverarbeitern und beauftragten Mitarbeitern durchgeführt werden, die für eine bestimmte Tätigkeit des für die Verarbeitung Verantwortlichen zweckdienlich sind und einem umfassenderen Zweck dienen, der auch von erheblichem öffentlichem Interesse sein kann, und die durch die Art der verarbeiteten Daten, die (digitalen oder manuellen) Verfahren und den Informationsfluss, in den sie eingebunden sind, gekennzeichnet sind.

- der **DSB** (Datenschutzbeauftragte) bzw. in englischer Sprache **DPO** (Data Protection Officer).



Si evidenzia che, in base all'articolo 39, paragrafo 1, lettera e) del Regolamento, il Responsabile della Protezione dei Dati funge da punto di contatto fra il singolo ente e il Garante. Il responsabile della protezione dei dati (RPD) è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti. Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi. Il RPD/DPO deve eseguire i seguenti compiti:

- sorvegliare l'osservanza del regolamento;
- supportare il titolare in ogni attività connessa al trattamento dei dati personali anche con riguardo alla tenuta di un registro dell'attività di trattamento;
- supportare nella valutazione d'impatto sulla protezione dei dati;
- informare e sensibilizzare il titolare o il responsabile nonché i dipendenti riguardo agli obblighi del regolamento;
- cooperare con le autorità di controllo e fungere da punto di contatto.

La Regione ha incaricato per il biennio 2022-2023 il Consorzio dei Comuni Trentini al servizio di RPD, come previsto dall'art. 39 del GDPR. Ogni ufficio può ricorrere al supporto del RPD/DPO per risolvere i propri dubbi, quesiti in materia di privacy. Al fine di armonizzare le richieste, l'accesso al servizio deve essere fatto per il tramite dell'Ufficio affari generali.

Gemäß Art. 39 Abs. 1 Buchst. e) der Verordnung ist der Datenschutzbeauftragte das Bindeglied zwischen den einzelnen Körperschaften und der Datenschutzbehörde. Der Datenschutzbeauftragte (DSB) wird aufgrund seiner beruflichen Eignung, insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und seiner Datenschutzpraxis sowie seiner Fähigkeit, den Auftrag wahrzunehmen, ernannt. Der Datenschutzbeauftragte kann ein Bediensteter des Verantwortlichen für die Datenverarbeitung oder des Auftragsverarbeiters sein oder aber aufgrund eines Dienstvertrags den Auftrag wahrnehmen. Dem DSB/DPO obliegen nachstehende Aufgaben:

- die Überprüfung der Beachtung der Verordnung;
- die Unterstützung des Verantwortlichen bei allen Tätigkeiten in Zusammenhang mit der Verarbeitung personenbezogener Daten auch hinsichtlich der Führung des Verzeichnisses der Verarbeitungstätigkeiten;
- der Beistand bei der Datenschutz-Folgenabschätzung;
- die Information und Sensibilisierung des Verantwortlichen und des Auftragsverarbeiters sowie der Bediensteten über die in der Verordnung enthaltenen Pflichten;
- die Zusammenarbeit mit den Aufsichtsbehörden, wobei er als Bindeglied fungiert.

Die Region hat den Gemeindenverband der Provinz Trient für den Zweijahreszeitraum 2022-2023 als DSB gemäß Art. 39 der DSGVO beauftragt. Jedes Amt kann sich an den DSB/DPO wenden, um Zweifel in Fragen des Datenschutzes auszuräumen. Im Sinne der Vereinheitlichung der diesbezüglichen Anträge ist der Dienst über das Amt für allgemeine Angelegenheiten zu kontaktieren.



- Procedura di **Data Breach**. I dati personali conservati, trasmessi o trattati dalla Regione, possono essere soggetti, al pari di qualsiasi azienda private o pubblica amministrazione, al rischio di perdita, distruzione o diffusione indebita a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi, come incendi o altre calamità. Sono eventi che possono mettere in serio pericolo la privacy degli interessati a cui si riferiscono i dati. Il Garante ha introdotto l'obbligo di comunicare il verificarsi di violazioni dei dati o incidenti informatici (accessi abusivi, azione di *malware*), che, pur non avendo un impatto diretto su di essi, possano comunque esporli a rischi di violazione, è appunto il cd. *Data Breach* (*breach* = *violazione*). Anche la Regione, quale pubblica amministrazione, deve dunque comunicare al Garante, entro settantadue ore dalla conoscenza del fatto (art. 33 del GDPR), tutte le violazioni dei dati o gli incidenti informatici che possano avere avuto un impatto significativo sui dati personali trattati. Ricordiamo in questa sede che non ci si deve limitare al concetto di *Data Breach* nel senso strettamente informatico (ovvero come incursione nel sistema informatico della Regione), ma anche nelle seguenti ipotesi:

- Pubblicazione non autorizzata di dati sensibili. Un esempio di *Data Breach* può verificarsi nel caso in cui una persona accede all'archivio per poi fare delle copie e pubblicare i dati rendendoli pubblici;
- Perdita di documenti cartacei. Il *Data Breach*, in questo caso accidentale, può essere l'abbandonare in o luoghi non protetti o diversi dalla propria postazione lavorativa, documenti cartacei contenenti dati personali.
- Calamità naturali. Anche in caso di

- **Data-Breach-Verfahren**. Die von der Region aufbewahrten, übermittelten oder verarbeiteten personenbezogenen Daten können – genauso wie bei privaten Unternehmen oder anderen öffentlichen Verwaltungen – der Gefahr des Verlustes, der Zerstörung oder der unzulässigen Verbreitung infolge von Cyberangriffen, unbefugtem Zugriff, Unfällen oder Zwischenfällen wie Bränden oder anderen Katastrophen ausgesetzt sein. Diese Ereignisse können die Privatsphäre der Personen, auf die sich die Daten beziehen, ernsthaft gefährden. Die Datenschutzbehörde hat die Pflicht vorgesehen, Datenschutzverletzungen oder IT-Zwischenfälle (unbefugte Zugriffe, *Malware*-Vorfälle) zu melden, die, auch wenn sie keine direkte Auswirkungen auf die Daten haben, diese dennoch der Gefahr einer Datenschutzverletzung (= *Data Breach*) aussetzen können. Auch die Region muss als öffentliche Verwaltung sämtliche Datenschutzverletzungen oder IT-Zwischenfälle, die beachtliche Auswirkungen auf die verarbeiteten personenbezogenen Daten haben könnten, innerhalb von zweiundsiebzig Stunden nach Bekanntwerden derselben der Datenschutzbehörde melden (Art. 33 der DSGVO). Es sei an dieser Stelle daran erinnert, dass der Begriff *Data Breach* nicht nur im IT-Bereich (d. h. bei Eindringen in das IT-Netz der Region), sondern auch für nachstehende Fälle gilt:

- Unerlaubte Veröffentlichung sensibler Daten: Es handelt sich beispielsweise um ein *Data Breach*, wenn eine Person auf das Archiv zugreift, Daten kopiert und diese dann veröffentlicht.
- Verlust von Dokumenten in Papierform: Ein *Data Breach* kann darin bestehen, dass Papierdokumente, die personenbezogene Daten enthalten, versehentlich an einem ungeschützten Ort und nicht am eigenen Arbeitsplatz liegen gelassen werden.
- Naturkatastrophen: Auch wenn sich ein



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

terremoto, i documenti cartacei sensibili possono andare persi e distrutti.

Erdbeben ereignet, können Papierdokumente, die sensible Daten enthalten, verloren gehen oder zerstört werden.

L'attivazione della procedura di *Data Breach* è effettuata dal Segretario generale. La segnalazione dell'episodio di *Data Breach* deve essere fatta tempestivamente (entro 72 ore, vedi deliberazione della Giunta regionale n. 193 del 03/09/2019) all'Ufficio affari generali e al Segretario generale.

Das Verfahren im Fall einer Datenschutzverletzung wird vom Generalsekretär eingeleitet. Das Ereignis einer Datenschutzverletzung ist umgehend (laut Beschluss der Regionalregierung vom 3. September 2019, Nr. 193 innerhalb von 72 Stunden) dem Amt für allgemeine Angelegenheiten und dem Generalsekretär zu melden.

Infine, facciamo presente che la documentazione di lavoro, contenente dati sensibili, al termine della giornata lavorativa, oppure in previsione di assenze dall'ufficio, non deve essere lasciata incustodita sulla scrivania. È buona prassi infatti, riporre il materiale contenente dati sensibili in cassetti o armadi chiusi a chiave.

Schließlich wird darauf hingewiesen, dass Arbeitsunterlagen, die sensible Daten enthalten, am Ende des Arbeitstages oder im Vorfeld einer Abwesenheit vom Büro nicht unbeaufsichtigt auf dem Schreibtisch liegen gelassen werden dürfen. Tatsächlich sollten Unterlagen mit sensiblen Daten stets in verschlossenen Schubladen oder Schränken aufbewahrt werden.

Fiducioso della vostra collaborazione, cordiali saluti.

Im Vertrauen auf Ihre Zusammenarbeit verbleibe ich mit freundlichen Grüßen.

**IL SEGRETARIO GENERALE/
DER GENERALSEKRETÄR**

Michael Mayr
firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Schreiben in Papierform übermittelt wird, stellt es die für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (Art. 3-bis des GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

MM/RG/MB



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Segreteria generale
Ufficio affari generali
Generalsekretariat
Amt für allgemeine Angelegenheiten
☎ 0461 201030
@ affgen@regione.taa.it
pec: affgen@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Protokollnummer und Registrierungsdatum sind dem Dokument als Metadaten zugeordnet (Dekret des Präsidenten des Ministerrates vom 3.12.2013, Art. 20). Gegenstand der zertifizierten E-Mail bzw. beigefügte Dateien überprüfen.

Al Capo dell'Ufficio di Gabinetto del Presidente della Regione	An den Kabinettschef des Präsidenten der Region
Alla Vicesegretaria generale	An die Vizegeneralsekretärin
Alle Dirigenti delle ripartizioni	An die Leiterinnen der Abteilungen
Alle Segretarie e ai Segretari particolari dei componenti della Giunta	An die persönlichen Referentinnen und Referenten der Mitglieder der Regionalregierung
Alle Direttrici e ai Direttori degli uffici centrali	An die Direktorinnen und Direktoren der Zentralämter
Alle Sostitute Direttrici e ai Sostituti Direttori degli uffici centrali	An die Stellvertreterinnen und Stellvertreter der Direktorinnen und Direktoren der Zentralämter

CIRCOLARE/RUNDSCHREIBEN

Oggetto:
Introduzione della segnatura permanente sui documenti repertoriati e protocollati in uscita

A far data da lunedì 12 dicembre p.v. nel sistema di gestione documentale "Pi.Tre." verrà progressivamente introdotta la segnatura permanente sui documenti repertoriati e protocollati in uscita, aventi file principale in formato .pdf (eventualmente sottoscritti con una o più firme Pades).

Betreff:
Einführung der permanenten Signatur für registrierte und im Ausgangsprotokoll protokollierte Dokumente

Ab Montag, dem 12. Dezember 2022 wird im Rahmen des Dokumentenverwaltungssystems „P.I.Tre.“ schrittweise die permanente Signatur für registrierte und im Ausgangsprotokoll protokollierte Dokumente mit Hauptdatei im PDF-Format (eventuell versehen mit einer oder mehreren Unterschriften im Pades-Format) eingeführt.

Limitatamente a tali tipologie, la segnatura di protocollo e di repertorio verrà apposta sui documenti prodotti dall'Amministrazione regionale. Infatti, il sistema di gestione documentale apporrà **in alto a sinistra** la segnatura permanente, dalla quale risulteranno la **data**, nonché il **numero di repertoriazione o protocollazione** attribuito dal sistema.

Dal punto di vista grafico, la segnatura permanente non sarà più di colore rosso e in carattere „courier new“ ma si presenterà come di seguito:

7-27/10/2022 13:48 - Ordine di liquidazione

La segnatura permanente è realizzata mediante una firma digitale in formato Pades, il cui **certificato di firma è intestato alla Regione**. Tale segnatura viene apposta sul documento in maniera automatica durante la repertoriazione o la protocollazione in uscita di documenti.

Con riferimento ai **documenti repertoriati** (ad es. decreti, ordini di liquidazione, atti gestionali e atti di gestione del personale), il nuovo sistema avrà il pregio di consentire di scaricare da „Pi.Tre.“ un duplicato informatico degli stessi, comprensivo di tipologia e numerazione, senza però far venir meno la validità della firma digitale.

Per quanto riguarda invece i **protocolli in uscita**, la funzionalità consentirà di far risultare la data e la segnatura di protocollo direttamente sul documento principale. Ad oggi, infatti, in caso di invio di una nota attraverso „Pi.Tre.“, tali riferimenti non risultano in calce al documento ma sono ricavabili dall'oggetto del messaggio di posta elettronica certificata, dal relativo testo e dall'allegato denominato „*segnatura.xml*“.

Al fine di consentire l'apposizione della segnatura permanente su tutti i documenti repertoriati e protocollati in uscita, gli uffici dell'Amministrazione regionale provvederanno ad **utilizzare la firma digitale in formato Pades** (estensione .pdf, con elemento grafico o meno) per sottoscrivere tutti i documenti.

Die Protokoll- und Registersignatur werden ausschließlich auf diese Kategorie von Dokumenten, die von der Regionalverwaltung erstellt wurden, vermerkt. Das Dokumentenverwaltungssystem platziert nämlich die permanente Signatur, die das **Datum** und die vom System zugeteilte **Register- oder Protokollnummer** enthält, in die **linke obere Ecke**.

Was den grafischen Aspekt anbelangt, wird die permanente Signatur nicht mehr rot und in der Schriftart „courier new“ sein, sondern wie folgt erscheinen:

Die permanente Signatur wird mittels einer digitalen Signatur im Pades-Format erstellt, deren **Signaturzertifikat auf den Namen der Region** lautet, und wird automatisch auf den registrierten oder im Ausgang protokollierten Dokumenten vermerkt.

Was die **registrierten Dokumente** (z. B. Dekrete, Liquidierungsanweisungen, Gebärungsakte und Personalverwaltungsakte) anbelangt, hat das neue System den Vorteil, dass ein elektronisches Duplikat dieser Dokumente, einschließlich Kategorie und Nummer, vom „P.I.Tre.-System“ heruntergeladen werden kann, ohne dass die digitale Signatur ungültig wird.

Was das **Ausgangsprotokoll** betrifft, werden dank dieser Funktion das Datum und die Protokollsignatur direkt auf dem Hauptdokument aufscheinen. Derzeit werden diese Daten bei der Übermittlung von Dokumenten über das „P.I.Tre.-System“ nicht auf denselben vermerkt, sondern gehen aus dem Betreff der zertifizierten E-Mail (PEC), dem Wortlaut der E-Mail und dem Anhang mit der Bezeichnung „segnatura.xml“ hervor.

Um die permanente Signatur auf allen registrierten und im Ausgangsprotokoll protokollierten Dokumenten zu ermöglichen, werden die Ämter der Regionalverwaltung sämtliche Dokumente mit der **digitalen Signatur im Pades-Format** (Erweiterung .pdf, mit oder ohne grafisches Element) unterzeichnen.

A tale indicazione di carattere generale si sottraggono le deliberazioni della Giunta regionale e i documenti che - per esigenze rappresentate dai destinatari oppure per ragioni tecniche - richiedono l'utilizzo della firma digitale in formato *Cades* (estensione .p7m).

Ulteriori informazioni sono disponibili nella scheda tecnica redatta dall'Ufficio informatica e digitalizzazione, che fornisce le indicazioni operative per l'utilizzo della segnatura permanente.

Cordiali saluti.

IL SEGRETARIO GENERALE /
DER GENERALSEKRETÄR

Michael Mayr
firmato digitalmente/digital signiert

Von dieser allgemeinen Anweisung ausgenommen sind die Beschlüsse der Regionalregierung sowie die Dokumente, die aufgrund der Bedürfnisse der Empfänger oder aus technischen Gründen die digitale Signatur im Cades-Format (Erweiterung .p7m) erfordern.

Nähere Informationen können der vom Amt für Informatik und Digitalisierung verfassten technischen Übersicht entnommen werden, in der die Handhabung der permanenten Signatur erläutert wird.

Mit freundlichen Grüßen

LA RESPONSABILE PER LA TRANSIZIONE AL
DIGITALE /
DIE VERANTWORTLICHE FÜR DEN
DIGITALEN WANDEL

Antonella Chiusole
firmato digitalmente/ digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Schreiben in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

MM/RG/NC

Allegato/Anlage: scheda tecnica/technische Übersicht



CIRCOLARE/RUNDSCHREIBEN

Oggetto: indicazioni per la distruzione di documenti riportanti dati personali, sensibili, giudiziari o documenti con contenuto a carattere riservato.

Betreff: Hinweise zur Vernichtung von Dokumenten, die personenbezogene, sensible, gerichtliche oder vertrauliche Daten enthalten

Alle Segreterie del Presidente e degli Assessori

An das Sekretariat des Präsidenten
und an die Sekretariate
der Mitglieder der Regionalregierung

Alle Dirigenti e ai Dirigenti di Ripartizione e Strutture equiparate

An die Leiterinnen und Leiter der Abteilungen
und der gleichgestellten
Organisationsstrukturen

Alle Direttrici e ai Direttori degli Uffici

An die Amtsdirektorinnen und Amtsdirektoren

Al personale regionale

An das Personal der Region

Il Regolamento europeo di data 27/04/2016, n. 2016/679/UE (d'ora in poi GDPR) agli artt. 23-25, pone con forza l'accento sulla "responsabilizzazione" (accountability) di titolari e responsabili, ossia sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Die Europäische Verordnung vom 27.04.2016, Nr. 2016/679/EU (in der Folge: DSGVO) betont in den Artikeln 23-25 nachdrücklich die „Rechenschaftspflicht“ der für die Datenverarbeitung Verantwortlichen und der Auftragsverarbeiter, d. h. dass diese ein proaktives Handeln und den konkreten Erlass von Maßnahmen zur Anwendung der Verordnung gewährleisten müssen.

Nello specifico, l'art. 25 del GDPR richiede un'analisi preventiva e un impegno applicativo da parte dei titolari che deve sostanziarsi in una serie di attività specifiche e dimostrabili (data protection by default and by design) finalizzate a ridurre il rischio inerente al trattamento dei dati, inteso quest'ultimo come rischio di impatti negativi sulle libertà e sui diritti degli interessati.

Insbesondere sieht Art. 25 der DSGVO vor, dass die für die Verarbeitung Verantwortlichen eine vorherige Analyse vornehmen und sich konkret darum bemühen müssen, eine Reihe spezifischer und nachweisbarer Maßnahmen zu ergreifen (Datenschutz by Default und by Design), die darauf abzielen, das mit der Datenverarbeitung verbundene Risiko zu verringern, wobei unter letzterem das Risiko negativer Auswirkungen auf die Freiheiten und Rechte der betroffenen Personen zu verstehen ist.

Tra i rischi relativi alla sicurezza del trattamento va tenuta in debita considerazione la violazione della riservatezza del dato, che può avvenire nel momento in cui il documento

Unter den Risiken im Zusammenhang mit der Sicherheit der Verarbeitung ist zu berücksichtigen, dass die Vertraulichkeit der Daten verletzt werden kann, wenn das

non è più di interesse e viene cestinato.

Al fine di prevenire tale rischio, sono stati acquistati, per la sede regionale, degli apparecchi distruggi documenti che frammentano la carta all'elevato livello di sicurezza P5. Nello specifico, dovranno essere distrutti con questa modalità i documenti che contengono dati personali, dati sensibili, dati giudiziari oppure, generalmente, i documenti che contengono informazioni riservate.

In allegato alla presente si riportano l'ubicazione degli apparecchi e le istruzioni per il loro uso. Si invita a non spostare gli apparecchi in quanto sono così registrati nel gestionale del patrimonio regionale.

Si coglie, inoltre, l'occasione per ricordare che la violazione della riservatezza del dato può avvenire anche attraverso il ritiro non tempestivo dei documenti inviati alle stampanti. Per ridurre tale rischio si segnala che le stampanti multifunzione hanno la possibilità di impostare un pin e, quindi, di attivare la stampa solo dopo che il titolare ha inserito tale codice.

Cordiali saluti.

Dokument nicht mehr von Interesse ist und vernichtet wird.

Um diesem Risiko vorzubeugen, wurden für das Amtsgebäude der Region Aktenvernichter angekauft, die Papier entsprechend der hohen Sicherheitsstufe P5 zerkleinern. Insbesondere Dokumente, die personenbezogene, sensible oder gerichtliche Daten bzw. Dokumente mit vertraulichen Informationen im Allgemeinen müssen auf diese Weise vernichtet werden.

Im Anhang sind die Standorte der Aktenvernichter und ihre Gebrauchsanweisung aufgeführt. Die Geräte dürfen nicht verstellt werden, da sie am jeweiligen Standort in den Vermögensverzeichnissen der Region eingetragen sind.

Bei dieser Gelegenheit wird darauf hingewiesen, dass das Datengeheimnis auch verletzt werden kann, wenn die an die Drucker gesendeten Dokumente nicht rechtzeitig abgeholt werden. Um dieses Risiko zu verringern, besteht bei Multifunktionsdruckern die Möglichkeit, einen PIN-Code zu erstellen und somit den Druck erst dann zu aktivieren, wenn der Anwender diesen Code eingegeben hat.

Mit freundlichen Grüßen.

IL SEGRETARIO GENERALE/
DER GENERALSEKRETÄR

Michael Mayr

firmato digitalmente / digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Dokument in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

MM/RG

UBICAZIONE APPARECCHI DISTRUGGI DOCUMENTI	STANDORTE DER AKTENVERNICHTER

UBICAZIONE PRECISA DEL CESPITE	GENAUER STANDORT DES VERMÖGENSWERTS	N. ETICHETTA APPLICATA ETIKETTEN-NUMMER
corridoio 1. piano lato nord altezza stanza 131	Korridor 1. Stock, Nordseite, bei Raum 131	865365
corridoio 1. piano lato sud altezza stanza 110	Korridor 1. Stock, Südseite, bei Raum 110	865362
corridoio 2. piano lato sud altezza stanza 213	Korridor 2. Stock, Südseite, bei Raum 213	865366
2. piano Presidenza	2. Stock, Präsidium	865360
corridoio 3. piano lato sud altezza stanza 314	Korridor 3. Stock, Südseite, bei Raum 314	865367
corridoio 3. piano lato nord altezza stanza 336	Korridor 3. Stock, Nordseite, bei Raum 336	865361
corridoio 4. piano lato sud altezza stanza 402	Korridor 4. Stock, Südseite, bei Raum 402	865368
corridoio 4. piano lato nord altezza stanza 434	Korridor 4. Stock, Nordseite, bei Raum 434	865364
4. piano Vicepresidenza	4. Stock, Sekretariat des Vizepräsidenten	865363



Instruction Manual

Optimum AutoFeed+ 45X
Optimum AutoFeed+ 50X
Optimum AutoFeed+ 90X
Optimum AutoFeed+ 100X
Optimum AutoFeed+ 100M
Optimum AutoFeed+ 130X
Optimum AutoFeed+ 130M
Optimum AutoFeed+ 140X
Optimum AutoFeed+ 150X
Optimum AutoFeed+ 150M
Optimum AutoFeed+ 225X
Optimum AutoFeed+ 225M
Optimum AutoFeed+ 300X
Optimum AutoFeed+ 300M
Optimum AutoFeed+ 600X
Optimum AutoFeed+ 600M
Optimum AutoFeed+ 750X
Optimum AutoFeed+ 750M



start here
starten sie hier
démarez ici
iniziare qui
empieza aquí
comece aqui
begin hier
start her

start her
börja här
aloita tästä
alusta siit
sāc šeit
pradėti čia
rozpocznij tutaj
починай тут

начинать здесь
мұнда бастаңыз
začňte zde
tu začnite
kezdés itt
începe aici
Ξεκινήστε εδώ
buradan başlayın
أبدأ هنا



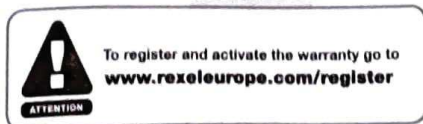
Optimum AutoFeed+ 45X
 Optimum AutoFeed+ 50X
 Optimum AutoFeed+ 90X
 Optimum AutoFeed+ 100X
 Optimum AutoFeed+ 100M
 Optimum AutoFeed+ 130X
 Optimum AutoFeed+ 130M
 Optimum AutoFeed+ 140X
 Optimum AutoFeed+ 150X
 Optimum AutoFeed+ 150M
 Optimum AutoFeed+ 225X
 Optimum AutoFeed+ 225M
 Optimum AutoFeed+ 300X
 Optimum AutoFeed+ 300M
 Optimum AutoFeed+ 600X
 Optimum AutoFeed+ 600M
 Optimum AutoFeed+ 750X
 Optimum AutoFeed+ 750M

Specifications

Model Rexel	Sheets Auto	Cut Level	Sheets Manual	Bin size	Amperage
Optimum AutoFeed+ 45X	45	P4	6	20	0.8
Optimum AutoFeed+ 50X	50	P4	6	20	0.8
Optimum AutoFeed+ 90X	90	P4	8	34	1.2
Optimum AutoFeed+ 100X	100	P4	8	34	1.2
Optimum AutoFeed+ 100M	100	P5	6	34	1.2
Optimum AutoFeed+ 130X	130	P4	8	44	1.2
Optimum AutoFeed+ 130M	130	P5	6	44	1.2
Optimum AutoFeed+ 140X	140	P4	8	44	1.2
Optimum AutoFeed+ 150X	150	P4	8	44	1.2
Optimum AutoFeed+ 150M	150	P5	6	44	1.2
Optimum AutoFeed+ 225X	225	P4	10	60	1.6
Optimum AutoFeed+ 225M	225	P5	8	60	1.6
Optimum AutoFeed+ 300X	300	P4	10	60	1.6
Optimum AutoFeed+ 300M	300	P5	8	60	1.6
Optimum AutoFeed+ 600X	600	P4	15	110	1.8
Optimum AutoFeed+ 600M	600	P5	10	110	1.8
Optimum AutoFeed+ 750X	750	P4	20	140	2.8
Optimum AutoFeed+ 750M	750	P5	15	140	2.8

EN 4
 DE 8
 FR 12
 IT 16
 ES 20
 PT 24
 NL 28
 DA 32
 NO 36
 SV 40
 FI 44
 ET 48
 LV 52
 LT 56
 PL 60
 UK 64
 RU 68
 KK 72
 CS 76
 SK 80
 HU 84
 RO 88
 GR 92
 TR 96
 AR 100

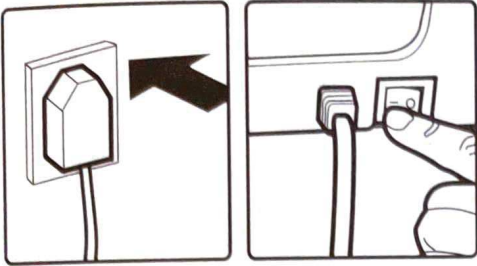
220-240V~ 50Hz



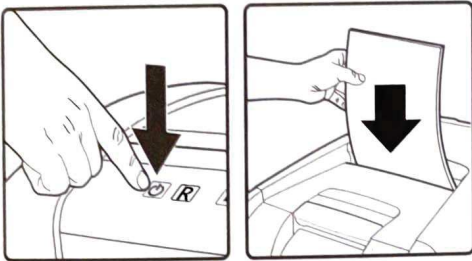
For service addresses, go to www.rexeleurope.com/en-gb/services/service-centres/

Operation

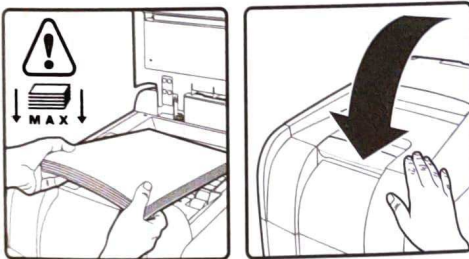
Switching machine on



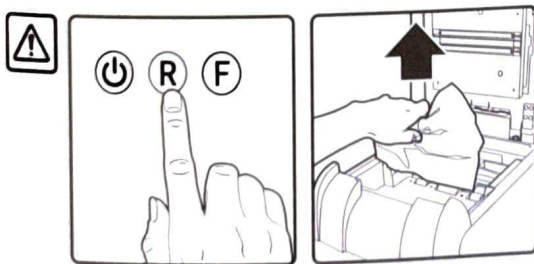
Manual shredding



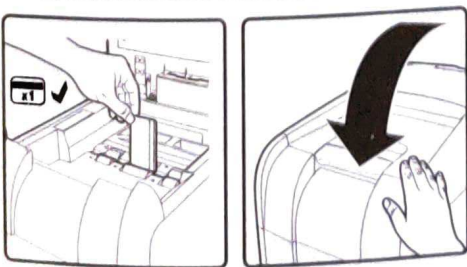
Auto-shredding



Removing jam



Credit card shredding





Leggere e conservare queste importanti avvertenze di sicurezza.



Per visionare il testo completo delle istruzioni per l'uso, i dati di contatto per l'assistenza tecnica, consigli e suggerimenti e la guida alla risoluzione dei problemi, visitare il sito www.rexeurope.com/support oppure www.leitz.com



Il seguente simbolo riportato sul prodotto segnala la possibilità di subire gravi lesioni, anche mortali, in caso di apertura della macchina.



NON APRIRE.



ATTENZIONE: Non toccare i coltelli di taglio. Fare attenzione a bordi taglienti.



ATTENZIONE: Pericolo generato da parti mobili. Tenere lontane le mani dai rulli durante il funzionamento.

- Leggere tutte le istruzioni e avvertenze di sicurezza. Il produttore non è responsabile in caso di danni materiali o lesioni personali dovuti all'incorretto uso del distruggidocumenti o alla mancata osservanza delle avvertenze di sicurezza. In tale evenienza, la garanzia sarà invalidata.
- Utilizzare la macchina esclusivamente per le funzioni per cui è stata progettata.
- L'unità deve essere collegata solo a una tensione di alimentazione corrispondente alle specifiche elettriche riportate sulla macchina.
- L'unità deve essere collegata a una presa elettrica posta nelle sue vicinanze e facilmente accessibile.
- Non collegare l'unità a un adattatore multiplo o utilizzare una prolunga.
- Non tentare di effettuare personalmente interventi di manutenzione o riparazione.
- Qualora si desidera riciclare la carta, separarla dai frammenti delle carte di credito.
- Non usare la macchina con il cavo di alimentazione o la spina danneggiati.
- Quando si sposta il distruggidocumenti fare attenzione a evitare superfici irregolari.
- La macchina è stata progettata solamente per l'uso in locali interni. Non utilizzare il distruggidocumenti in ambienti esterni.
- Tenere il dispositivo lontano dall'umidità.
- Prestare sempre la massima attenzione e cautela durante l'uso della macchina. Non utilizzare dispositivi elettrici in caso di mancanza di concentrazione o di consapevolezza oppure sotto l'influenza di droghe, alcol o farmaci. Quando si utilizzano dispositivi elettrici, anche un solo istante di disattenzione può causare gravi infortuni e lesioni.
- Non tentare di aprire o modificare il distruggidocumenti o di effettuare interventi di manutenzione o riparazioni. Evitare di far cadere, forare o rompere il distruggidocumenti o di esporlo a pressioni elevate.
- Non è consentito effettuare alterazioni alla macchina o apportarvi modifiche tecniche.
- Prima dell'uso, assicurarsi che l'unità e il cavo (e, se del caso, l'adattatore) non presentino danni. In caso di danni visibili, un forte odore o un eccessivo surriscaldamento dei componenti, scollegare immediatamente tutti i componenti e interrompere l'uso del distruggidocumenti.
- Il distruggidocumenti va scollegato dalla fonte di alimentazione quando non se ne prevede l'uso per un periodo di tempo prolungato.
- Non usare detergenti o lubrificanti spray in quanto possono produrre fiammate.
- Non bypassare mai il dispositivo di interblocco (assolutamente vietato e pericoloso, in particolare quando l'unità è collegata a una fonte di alimentazione).
- Non appoggiarsi allo sportello del distruggidocumenti in quanto è possibile danneggiarlo e non sarà coperto dalla garanzia.
- La mancata osservanza di queste istruzioni potrebbe causare danni/lesioni e invaliderà la garanzia.

Simboli di avvertimento



Simboli di avvertimento



Tenere lontano catenine e braccialetti



Tenere lontano cravatte e abiti larghi



Tenere lontano capelli lunghi



Non infilare le mani nell'imboccatura



Questa macchina non è destinata all'utilizzo da parte di bambini



Non utilizzare bombolette spray. Non usare detergenti o lubrificanti spray in quanto possono produrre fiammate.



Capacità di taglio



Niente CD



Niente punti extra-lunghi di oltre 26 mm



Avvertenza: parti mobili

Simboli di avvertimento nel comparto di alimentazione automatica



Indicazione numero max. di fogli



Avvertenza: niente punti extra-lunghi di oltre 26 mm



Avvertenza: non oltre 25 fogli pinzati insieme



Avvertenza: niente documenti rilegati



Avvertenza: non sono consentiti fogli multipli ripiegati



Avvertenza: niente graffette di oltre 32 mm



Avvertenza: niente fogli di plastica



Avvertenza: niente buste chiuse con corrispondenza all'interno



Avvertenza: niente riviste



Avvertenza: niente carta o cartoncino di oltre 200 gm²

Icona	Tipo	Modelli	Tasti/indicatori e intervento
	Tasti di comando	Tutti i modelli	Tasto avviamento automatico e modalità standby (unica pressione)
			Tasto reverse manuale (mantener premuto)
			Tasto funzionamento in avanti manuale (mantener premuto)
	Indicatore di pronto macchina		
	Indicatore di surriscaldamento (far raffreddare il distruggidocumenti)		
	Indicatori di stato		Indicatore di sovraccarico / Indicatore di inceppamento (ridurre il numero di fogli / eliminare l'inceppamento)
			Indicatore di cestino pieno (aprire lo sportello e svuotare il cestino. 45X - sollevare la testa del distruggidocumenti e svuotare il cestino)
			Indicatore di sportello aperto o di testa del distruggidocumenti rimossa (chiudere bene lo sportello o rimettere la testa del distruggidocumenti)
	Tasti per bloccare lo sportello di caricamento		300 fogli od oltre
		Blocco dello sportello di caricamento - combinazione di sicurezza, tasto 1	
		Blocco dello sportello di caricamento - combinazione di sicurezza, tasto 2	
		Blocco dello sportello di caricamento - combinazione di sicurezza, tasto 3	
		Blocco dello sportello di caricamento - combinazione di sicurezza, tasto 4	

5. Il dispositivo inizierà a distruggere automaticamente i documenti SOLO dopo la chiusura dello sportello di caricamento.

Se rimangono ancora dei fogli nel comparto di alimentazione automatica dopo il primo tentativo, aprire e chiudere di nuovo lo sportello di caricamento.

Attenzione: se necessario è ora possibile bloccare lo sportello di caricamento inserendo un codice a 4 cifre (vedere la sezione Blocco dello sportello di caricamento della carta).

6. Se i fogli da distruggere sono pochi, usare l'imboccatura di alimentazione manuale, a condizione che il comparto di alimentazione automatica sia vuoto.
7. Inserire i fogli da distruggere nell'imboccatura di alimentazione manuale. Il distruggidocumenti rileverà la presenza dei fogli e verrà avviato automaticamente.
8. Se lasciato nella modalità di funzionamento automatico per più di 2 minuti senza essere utilizzato, il distruggidocumenti ritornerà automaticamente alla modalità Sleep per risparmiare corrente.
9. Il distruggidocumenti si "sveglierà" automaticamente dalla modalità Sleep quando vengono inseriti i fogli nell'imboccatura di alimentazione o viene aperto lo sportello di caricamento della carta. Non è necessario premere il tasto di avviamento automatico

Blocco dello sportello di caricamento della carta

Per garantire maggiore sicurezza, lo sportello di caricamento della carta può essere bloccato durante la distruzione di documenti riservati.

Per bloccare il distruggidocumenti:

1. inserire i documenti nel comparto di alimentazione automatica e chiudere lo sportello di caricamento della carta;
2. inserire un codice a 4 cifre a scelta. RICORDARE IL CODICE USATO!

Lo sportello di caricamento del distruggidocumenti si sblocca automaticamente quando:

- viene nuovamente inserito il codice a 4 cifre;
- l'operazione di distruzione è stata completata;
- il distruggidocumenti è inattivo per 30 minuti (ma nel comparto di alimentazione automatica rimangono dei documenti).

Cestino pieno

Il distruggidocumenti non funziona se il cestino è pieno e il simbolo di cestino pieno è illuminato.

In questo caso è necessario svuotare il cestino.

- Estrarre lentamente il cestino da svuotare..
- Inserire nuovamente il cestino vuoto e premere il tasto di avviamento automatico per riprendere l'operazione di distruzione.

Nel modello 45X, la testa del distruggidocumenti si solleva dal cestino qualora il cestino sia pieno. Tale sollevamento della testa arresterà l'operazione di distruzione della carta. Rimuovere la testa, svuotare il cestino e rimettere la testa assicurando che sia stata posizionata correttamente (non al contrario).

Le macchine da 600 o 750 fogli possono essere utilizzate con sacchetti di plastica (2020175B)

Funzionamento

1. Estrarre il distruggidocumenti dalla confezione.
2. Collegare il distruggidocumenti alla rete di alimentazione.
3. Controllare che il tasto di accensione/spegnimento sul retro dell'unità sia nella posizione "ON" (acceso). Si illuminerà il simbolo blu di standby
4. Per caricare il distruggidocumenti, sollevare semplicemente l'impugnatura dello sportello di caricamento per aprire lo sportello e inserire i documenti. Se necessario è possibile portare manualmente l'apertura dello sportello fino a 90°. Inserire i fogli nel comparto di alimentazione automatica assicurandosi di non superare ogni volta il numero massimo consentito. Non inserire i fogli oltre il livello "MAX" in quanto ciò potrebbe danneggiare il distruggidocumenti.

Supporti che il dispositivo è in grado di distruggere

Optimum AutoFeed È in grado di distruggere i tipi di documenti elencati di seguito.



- Documenti pinzati. Punto posizionato a non più di 25 mm dall'angolo.
- Punti 26/6 e 24/6 o più piccoli.
- Fogli di piccole dimensioni caricati in posizione centrale.



- Fogli formato A3 piegati a metà, max. 2 fogli.
- 300 fogli.
- Fogli da 80 gm²
 - A4 - 210mm x 297mm
 - A5 - 148mm x 210mm
 - A3 foglio singolo piegato a metà per creare formato A4.



- Documenti con graffetta. Graffetta posizionata a non più di 25 mm dall'angolo (modello 300M: SOLO attraverso l'imboccatura di alimentazione manuale).
- Graffette piccole/medie (spessore massimo filo metallico = 0,9 mm).
- Carta > 80/100 gm² (SOLO attraverso l'imboccatura di alimentazione manuale).

Optimum AutoFeed È in grado di distruggere (attraverso l'imboccatura di alimentazione manuale) i tipi di documenti elencati di seguito.



Carta spessa o cartoncino.
<200gsm



Carta lucida o foglio
stampato su entrambi i lati.



Fogli multipli ripiegati
(ad esempio fogli formato
A3 piegati a metà).

Supporti NON ACCETTATI:



Punti extra-lunghi. Verificare che
la lunghezza della gamba del
punto non sia superiore a 6mm.



Graffetta di grandi dimensioni.
Verificare che la lunghezza
della graffetta non sia
superiore a 32mm.



Fogli e buste di plastica,
documenti plastificati,
cartelline in plastica.



Molle fermafogli Bulldog



Documenti rilegati



Riviste o altri
documenti rilegati con
più punti o graffette.



Etichette adesive



Non utilizzare
bombolette spray



No Oil, solo fogli di olio



CD e DVD

Surriscaldamento

Se viene utilizzato ininterrottamente senza alcuna pausa, il distruggidocumenti potrebbe surriscaldarsi e, in questo caso, l'indicatore di raffreddamento  lampeggerà in rosso. Si prega di lasciar raffreddare il distruggidocumenti. Quando il distruggidocumenti sarà di nuovo pronto per essere usato, l'indicatore di surriscaldamento / raffreddamento si spegnerà. Se il distruggidocumenti deve raffreddarsi durante il ciclo di distruzione della carta, non è richiesto alcun intervento. Il distruggidocumenti inizierà automaticamente a distruggere i fogli una volta raffreddatosi. Durante questa fase di raffreddamento, occorre solo controllare che i fogli siano stati caricati nel comparto di alimentazione automatica e che il cestino sia vuoto.

Lubrificazione del distruggidocumenti

Per lubrificare il distruggidocumenti utilizzare solo fogli di lubrificazione Rexel (2101948 & 2101949). ACCO Brands declina qualsiasi responsabilità per la prestazione o la sicurezza del prodotto qualora vengano utilizzati altri tipi di lubrificante su qualsiasi parte di questo distruggidocumenti. Rexel consiglia di utilizzare un foglio di lubrificazione dopo tre svuotamenti del cestino (e ogni tre svuotamenti dopo questo). Inserire il foglio di lubrificazione nell'imboccatura di alimentazione manuale e NON nel comparto di alimentazione automatica. L'inserimento di un foglio di lubrificazione nel comparto di alimentazione automatica causa la contaminazione dei rulli impedendo il funzionamento del meccanismo di alimentazione automatica. Se i rulli si sporcano, seguire le istruzioni per la manutenzione.

Manutenzione

Nel corso del tempo sui rulli del meccanismo di alimentazione automatica può accumularsi sporco. Pulirli con un panno asciutto per mantenere inalterate le prestazioni del prodotto.

Sul sensore a infrarossi per l'avviamento automatico, situato nell'imboccatura di alimentazione della carta, può a volte accumularsi uno strato di polvere di carta che causa il funzionamento della macchina anche quando non è stato inserito alcun foglio. Spegnerne il distruggidocumenti azionando l'interruttore posto sul retro della macchina e pulire con cura il sensore usando un batuffolo di cotone.

Macchine riparabili

(per 300 fogli e oltre)

Per questi dispositivi raccomandiamo che vengano effettuati interventi di manutenzione ogni 6-12 mesi da parte di un tecnico Rexel – consultare il sito www.rexeleurope.com/support per eventuali richieste di informazioni sui contratti di manutenzione.

Rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

- Al termine della loro vita utile, i prodotti acquistati verranno considerati rifiuti di apparecchiature elettriche ed elettroniche (RAEE) ed è pertanto importante prendere atto di quanto di seguito riportato.
- I RAEE non devono essere smaltiti come rifiuti urbani misti ma vanno raccolti separatamente in modo tale da essere smontati per consentire il riciclaggio, riutilizzo e recupero (come carburante ai fini del recupero di energia nella produzione di energia elettrica) dei relativi componenti e materiali.
- Punti pubblici di raccolta sono stati predisposti dalle amministrazioni comunali per la raccolta gratuita dei RAEE.
- I RAEE vanno smaltiti presso il centro di raccolta più vicino all'abitazione o all'ufficio dell'utente.
- Qualora si incontrino difficoltà nel trovare un centro di raccolta abilitato al ricevimento dei RAEE, il rivenditore al dettaglio presso cui si è acquistato il prodotto dovrebbe accettare tali rifiuti.
- Nel caso in cui l'utente non si sia più in contatto con il proprio rivenditore, è possibile rivolgersi ad ACCO per ottenere informazioni a riguardo.
- Il riciclaggio dei RAEE è volto a proteggere l'ambiente e la salute umana, salvaguardare le materie prime, migliorare lo sviluppo sostenibile e garantire un migliore approvvigionamento di materie prime nel territorio dell'Unione europea. Tali obiettivi potranno essere conseguiti recuperando materie prime secondarie di valore e riducendo il volume dei rifiuti da smaltire. I consumatori possono contribuire al raggiungimento di questi obiettivi provvedendo a smaltire i propri RAEE presso gli appositi centri di raccolta.
- Sui prodotti acquistati è riportato il simbolo RAEE (cassonetto barrato). Tale simbolo indica che i RAEE non vanno smaltiti come rifiuti urbani misti.

Garanzia

- Il funzionamento di questa macchina è garantito per due anni dalla data di acquisto, subordinatamente a uso normale. Durante il periodo di garanzia, ACCO Brands Europe provvederà, a propria discrezione, a riparare o sostituire gratuitamente la macchina difettosa. Difetti risultanti dall'uso improprio o dall'uso per scopi diversi da quelli per cui il prodotto è stato concepito non sono coperti dalla garanzia.
- Sarà necessario fornire una prova della data di acquisto. Riparazioni o modifiche effettuate da persone non autorizzate da Acco Brands Europe invalideranno la garanzia. ACCO Brands Europe si propone di assicurare che i propri prodotti funzionino in conformità alle caratteristiche tecniche indicate. La presente garanzia non pregiudica alcun diritto riconosciuto ai consumatori dalla normativa nazionale vigente in materia di vendita di beni.
- La presente garanzia non è pertinente per i clienti australiani - vedere i dettagli relativi alla garanzia riportati a pagina 104.



Consorzio dei
Comuni Trentini

Trento, 9 luglio 2021
GF/fd/lb

Ai segretari
Ai Referenti privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE/PEC

OGGETTO: Servizio privacy RPD - Garante privacy: no al controllo indiscriminato della navigazione in internet dei lavoratori - L'Autorità sanziona il comune di Bolzano per 84mila euro – necessità del disciplinare dell'uso di internet e della compiuta informativa ai dipendenti – valutazione di impatto privacy

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto.
Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.
Cordiali saluti.

Il Direttore Generale
dott. Marco Riccadonna

Il Presidente
dott. Paride Giannone



Si dà conto e si segnala di porre particolare attenzione alla tematica oggetto di un recentissimo provvedimento del Garante per la protezione dei dati personali che ha sanzionato il Comune di Bolzano a causa di un sistema di monitoraggio della navigazione in internet dei dipendenti non conforme al Regolamento europeo 679/2016 e all'art. 4 dello Statuto dei lavoratori nonché per la mancanza di una conforme informazione ai dipendenti stessi.

Per il Garante non è possibile monitorare la navigazione internet dei lavoratori in modo indiscriminato. Indipendentemente da specifici accordi sindacali, le eventuali attività di controllo devono comunque essere sempre svolte nel rispetto dello Statuto dei lavoratori e della normativa sulla privacy.

È quanto affermato dal Garante per la protezione dei dati personali nel provvedimento sanzionatorio del 13 maggio 2021 nei confronti del Comune di Bolzano, avviato sulla base del reclamo presentato da un dipendente che, nel corso di un procedimento disciplinare, aveva "scoperto" che il sistema di monitoraggio della navigazione in internet implementato dal Comune prevedeva e consentiva un controllo costante e massivo degli accessi dei dipendenti. Il Comune, che inizialmente gli aveva contestato la consultazione di Facebook e Youtube durante l'orario di lavoro, ha archiviato il procedimento per l'inattendibilità dei dati di navigazione raccolti.

Dagli accertamenti del Garante è emerso che il Comune impiegava, da circa dieci anni, un sistema di controllo e filtraggio della navigazione internet dei dipendenti, con la conservazione dei dati per un mese e la creazione di apposita reportistica, per finalità di sicurezza della rete. Sebbene il datore di lavoro avesse stipulato un accordo con le organizzazioni sindacali, come richiesto dalla disciplina di settore, il Garante ha evidenziato che tale trattamento di dati deve comunque rispettare anche i principi di protezione dei dati previsti dal GDPR.

Il sistema, implementato dal Comune, **senza aver adeguatamente informato i dipendenti**, consentiva invece operazioni di trattamento non necessarie e sproporzionate rispetto alla finalità di protezione e sicurezza della rete interna, **effettuando una raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web visitati dai singoli dipendenti**.

Nel provvedimento l'Autorità ha rimarcato che l'esigenza di ridurre il rischio di usi impropri della navigazione in Internet non può portare al completo annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro, anche nei casi in cui il dipendente utilizzi i servizi di rete messi a disposizione del datore di lavoro.

Il Garante, tenendo conto della piena collaborazione del Comune, ha disposto una sanzione di 84.000 euro per l'illecito trattamento dei dati del personale. Il Comune dovrà anche adottare misure tecniche e organizzative per anonimizzare il dato relativo alla postazione di lavoro dei dipendenti, cancellare i dati personali presenti nei log di navigazione web registrati, nonché aggiornare le procedure interne individuate e inserite nell'accordo sindacale.

Data la rilevanza della tematica si analizzano di seguito alcuni elementi chiave della vicenda per porre l'attenzione su aspetti di cui è necessario che **tutti gli enti verifichino lo stato dell'arte e le attuali modalità implementative eventualmente conformandole con urgenza** al rispetto della normativa in materia di trattamento dei dati personali.



Principio di liceità correttezza e trasparenza del trattamento dei dati relativi alla navigazione in Internet dei dipendenti: l'informativa agli interessati

Nel rispetto del principio di "liceità, correttezza e trasparenza", il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12 del Regolamento).

Il Comune ha adottato fin dal 2000 un sistema che consentiva il tracciamento generalizzato (ed ex ante) degli accessi ad Internet da parte dei dipendenti e la memorizzazione, per trenta giorni, di informazioni di natura personale ("giorno, ora, nome utente, PC utilizzato e sito consultato").

Il sistema consentiva, quindi, attraverso la possibilità di ricondurre la navigazione a uno specifico nome utente ("id utente"), di **effettuare un controllo individualizzato della navigazione in Internet dei singoli dipendenti, mediante estrazione di dati, ad opera dell'amministratore di rete, su richiesta dei dirigenti competenti**. Tanto, al fine di "generare evidenze per la sicurezza informatica della rete del Comune", la cui integrità dovrebbe essere assicurata per consentire l'esecuzione dei compiti di interesse pubblico propri dell'Ente (art. 6, par. 1, lett. e), del Regolamento).

Nel corso dell'istruttoria **il Comune ha dichiarato di aver fornito ai dipendenti**, anteriormente all'entrata in vigore del Regolamento, **l'informativa generale** sul trattamento dei dati personali e di averne predisposta un'altra, aggiornata al nuovo quadro normativo, "pubblicata sul sito istituzionale".

Tuttavia, nel corso delle verifiche è emerso che, sul sito web dell'Ente, **non era presente alcuna specifica informativa** relativa ai trattamenti dei dati personali dei dipendenti né, in quelle rese disponibili, vi era alcun riferimento al trattamento dei dati personali relativi alla navigazione in Internet da parte degli stessi.

Un riferimento alle operazioni di tracciamento delle connessioni ad Internet era invece presente in altri documenti messi a disposizione dei dipendenti, alcuni dei quali pubblicati nella intranet, quali, l'accordo sindacale, il codice di comportamento, alcune circolari interne dell'Ufficio del personale, nonché il modulo che ogni dipendente doveva firmare all'atto della richiesta per l'accesso ad Internet e agli altri servizi di rete. Tali atti, che non contenevano tuttavia tutti gli elementi informativi essenziali richiesti dall'art. 13 del Regolamento, essendo stati redatti per assolvere ad obblighi diversi rispetto a quelli derivanti dalla disciplina in materia di protezione dei dati, **non possono quindi sostituire l'informativa che il titolare deve rendere**, prima di iniziare il trattamento, agli interessati in merito alle caratteristiche essenziali dello stesso; ciò allo scopo di consentire all'interessato di esser pienamente consapevole della tipologia di operazioni di trattamento che potranno essere svolte anche attingendo, in un quadro di liceità, ai dati raccolti nel corso dell'attività lavorativa.

L'adempimento degli obblighi informativi nei confronti del dipendente costituisce una specifica condizione per il lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali (v. art. 4, comma 3, l. 20 maggio 1970, n. 300).

Ai fini della conformità del trattamento è quindi necessario fornire al dipendente un'adeguata informazione delle modalità d'uso degli strumenti e una specifica informativa dedicata ai trattamenti che, per esigenze organizzative e di sicurezza informatica, comportano il tracciamento delle attività dei dipendenti.



Il principio di minimizzazione dei dati e la raccolta di dati non attinenti all'attività lavorativa

In base al Regolamento, il trattamento deve essere "necessario" rispetto alla lecita finalità perseguita (art. 6, par. 1 del Regolamento) e avere ad oggetto i soli dati "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. c), del Regolamento).

Come emerge dagli atti, il sistema adottato dal Comune per finalità di sicurezza della rete, consentiva operazioni di filtraggio e tracciatura delle connessioni e dei collegamenti ai siti Internet esterni, la memorizzazione di tali dati e la loro conservazione, per trenta giorni, nonché l'estrazione di report, anche su base individuale.

In base a una complessiva valutazione degli elementi emersi nel corso dell'istruttoria, risulta che il trattamento dei dati personali raccolti e trattati dal Comune tramite il personale autorizzato e gli amministratori di sistema ("giorno, ora, sito consultato"), in presenza di un collegamento diretto e univoco con il dipendente e con la sua specifica postazione di lavoro (in quanto tra i dati raccolti figuravano anche "nome utente e PC utilizzato"), abbia dato luogo a una **raccolta sistematica di dati relativi all'attività e all'utilizzo dei servizi di rete da parte dipendenti direttamente identificabili**.

In tale contesto, il Comune aveva stipulato un accordo con le organizzazioni sindacali, dapprima nel 2000, aggiornato nel 2010, come prescritto dalla disciplina in materia di impiego di sistemi tecnologici sul posto di lavoro (art. 4 della legge n. 300 del 1970) che, anche a seguito delle modifiche disposte dal decreto legislativo 14 settembre 2015, n. 151, consente l'impiego di "impianti audiovisivi e di altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori... esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale", nel rispetto di specifiche condizioni, quali il previo accordo con la rappresentanza sindacale unitaria o le rappresentanze sindacali aziendali, ovvero, in alternativa, previa autorizzazione delle sedi territoriali dell'Ispettorato nazionale del lavoro (comma 1).

Peraltro anche il Garante, dopo le modifiche apportate nel 2015 a tale quadro di settore, si è espresso, proprio in merito all'utilizzo di **sistemi che comportano la tracciatura degli accessi a Internet** (si veda il provvedimento del 13 luglio 2016, n. 303, confermato dal Tribunale di Chieti con sentenza n. 672 del 24 ottobre 2019) precisando, tra l'altro, che tali sistemi richiedono le garanzie di cui all'art. 4, comma 1 della L. n. 300 del 1970, **non potendo essere ricompresi nel novero degli "strumenti di lavoro"**, ai sensi dell'art. 4, comma 2, diversamente dai sistemi di inibizione automatica di consultazione di contenuti in rete.

In ogni caso, il titolare del trattamento deve sempre rispettare i principi di protezione dei dati (art. 5 del Regolamento). Ciò comporta che **l'ambito dei controlli (indiretti o preterintenzionali), entro i limiti stabiliti dalla disciplina di settore, e i trattamenti di dati personali che possono essere lecitamente effettuati dal datore di lavoro, debbano essere comunque non massivi, graduali e ammissibili solo previo esperimento di misure meno limitative dei diritti lavoratori**.

Con riguardo al caso di specie, secondo quanto emerge dagli atti e confermato dal titolare del trattamento, risultava invece che **le caratteristiche originarie del sistema e le conseguenti operazioni di trattamento (raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti, memorizzazione per trenta giorni e possibilità di estrazione di reportistica relativa alla navigazione di singoli dipendenti) non fossero necessarie e proporzionate** rispetto alla finalità di protezione e sicurezza della rete interna invocata dall'Ente, avendo riguardato dati non "adeguati, pertinenti e limitati" a quanto necessario a





garantire la sicurezza della rete, in violazione dei principi di liceità e di minimizzazione di cui all'art. 5, par. 1, lett. a) e c), e dell'art. 6 del Regolamento.

Il sistema utilizzato dal Comune effettuando una raccolta sistematica dei dati di navigazione dei dipendenti comportava inevitabilmente il trattamento di informazioni anche estranee all'attività professionale, desumibili dagli URL visitati e risultava, pertanto, in contrasto con il divieto per il datore di lavoro di trattare dati "non attinenti alla valutazione dell'attitudine professionale del lavoratore" e dunque con l'art. 113 del Codice, in riferimento all'art. 8 della l. 20 maggio 1970, n. 300 e all'art. 10 del d.lgs. 10 settembre 2003, n. 276.

L'esigenza di ridurre il rischio di usi impropri della navigazione in Internet, da parte dei dipendenti, consistenti in attività non correlate alla prestazione lavorativa (ad esempio, la visione di siti web non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività lavorativa) non può, infatti, giustificare ogni forma di interferenza nella vita privata, ma **può essere soddisfatta mediante la predisposizione di misure tecniche e organizzative idonee a prevenire che eventuali informazioni relative alla sfera extralavorativa vengano raccolte**, dando luogo a trattamenti di informazioni personali, "non pertinenti" che ricadono nell'ambito di applicazione dell'art. 113 del Codice (con riguardo ai rischi per gli interessati e alle responsabilità per il titolare in ordine all'acquisizione di informazioni afferenti alla sfera privata dei dipendenti).

Il principio di limitazione della finalità e il mancato rispetto delle condizioni previste dalla disciplina di settore con riguardo all'utilizzo dei dati raccolti per altri fini connessi alla gestione del rapporto di lavoro

Stante il principio in base al quale i dati devono essere "raccolti per finalità determinate, esplicite legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità" (art. 5, par. 1, lett. b), del Regolamento) si osserva che il Comune si è riservato, fin dal 2000, la possibilità di consultare i dati relativi alla navigazione web dei propri dipendenti, su richiesta del dirigente competente e per il tramite dell'amministratore di sistema, per eventuali esigenze legate a procedimenti disciplinari. Ciò è in concreto avvenuto nei confronti di taluni dipendenti (indicati dal Comune nel numero di 27 lavoratori), tra i quali il reclamante, con conseguente utilizzo dei dati raccolti dal sistema nell'ambito del procedimento disciplinare a carico dello stesso.

Solo dal 2015 il quadro normativo vigente consente che i dati raccolti ai sensi dell'art. 4, commi 1 e 2 della legge n. 300/1970 possano essere utilizzati dal datore di lavoro "a tutti i fini connessi al rapporto di lavoro" a condizione che "sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n.196" (art. 4, comma 3 l. n. 300/1970).

Il quadro normativo consente quindi al titolare (datore di lavoro) di utilizzare, per ulteriori trattamenti necessari alla gestione del rapporto di lavoro, solo le informazioni raccolte nel rispetto delle condizioni e dei limiti previsti dall'art. 4, commi 1 o 2, della l. n. 300/70 e della disciplina di protezione dati. Tali successive ed eventuali operazioni di trattamento **presuppongono quindi la necessità di fornire agli interessati un'adeguata informativa** sui trattamenti che il datore di lavoro si riserva di effettuare e **l'opportuna configurazione dei sistemi in modo che siano poste in essere le sole operazioni necessarie e raccolti i soli dati pertinenti in relazione alla finalità principale per la quale i dati sono originariamente trattati**.

Nel caso di specie risulta, invece, che i dati relativi alla navigazione web del reclamante, originariamente raccolti e trattati tramite il citato sistema in modo non proporzionato e non conforme alla disciplina in materia di protezione dei dati personali, in violazione dell'art. 5, par.



1, lett. a) e c), 6 del Regolamento e dell'art. 113 del Codice, e senza un'adeguata informativa ai sensi dell'art. 13 del Regolamento, siano stati successivamente impiegati per contestare addebiti disciplinari allo stesso, non rispettando quindi i presupposti e le condizioni previste dalla richiamata disciplina di settore all'art. 4, comma 3, della legge n. 300 del 1970.

Mancata esecuzione di una valutazione d'impatto sulla protezione dei dati

In attuazione del principio di responsabilizzazione (che impone l'adozione di adeguate misure tecniche e organizzative atte a garantire che il trattamento avvenga in conformità alla normativa vigente; cfr. artt. 24 e 25 del Regolamento), **spetta al titolare valutare se i trattamenti che si intendono realizzare possano presentare un rischio elevato** per i diritti e le libertà delle persone fisiche, in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite, che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali.

Il trattamento dei dati personali degli interessati è stato effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati sul presupposto che il trattamento non presentasse rischi specifici per gli stessi.

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si rileva, invece, che il trattamento reso possibile dal descritto sistema, per come configurato, consistente nella raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti (originariamente associati in via diretta al nominativo, ad oggi, attraverso l'id macchina), nella memorizzazione per trenta giorni e nella possibilità di estrarre una reportistica relativa alla navigazione di singoli dipendenti, comporta rischi specifici per i diritti e le libertà degli interessati nel contesto lavorativo (art. 35 del Regolamento).

Tanto in considerazione della particolare "vulnerabilità" degli interessati nel contesto lavorativo e del fatto che in tale ambito l'impiego di sistemi che comportano il "monitoraggio sistematico", inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti

Date le caratteristiche del sistema implementato il Garante ha ritenuto che il Titolare avesse l'obbligo di effettuare una valutazione di impatto e quindi, in assenza ha violato l'art. 35 del Regolamento.

Alla luce dell'importante Provvedimento del Garante in materia, in qualità di RPD, **si indica e prescrive quanto segue:**

- risulta necessario attuare **con urgenza una verifica della conformità** del proprio sistema e delle misure in essere per la disciplina dell'uso di internet da parte dei dipendenti e dell'eventuale implementazione di uno strumento per la registrazione, la tracciatura e l'analisi degli accessi e della navigazione in internet dei dipendenti;
- **se tale strumento è implementato**, il suddetto strumento **deve, by default, prevedere mediante l'adozione di misure tecniche e organizzative, l'anonimizzazione del dato relativo al dipendente che effettua la navigazione**. Lo strumento deve consentire la possibilità di intraprendere rilevazioni di dati puntuali di navigazione in internet, solo a fronte di riscontrate anomalie di traffico web la cui entità sia tale da compromettere la sicurezza e l'integrità dei sistemi informativi;
- se tale strumento è implementato, necessita sia stato effettuato un accordo sindacale in quanto **i sistemi che comportano la tracciatura degli accessi a internet** richiedono le garanzie di cui all'art. 4, comma 1 della L. n. 300 del 1970, **non sono ricompresi nel**





- novero degli “strumenti di lavoro”, ai sensi dell’art. 4, comma 2, diversamente dai sistemi di inibizione automatica di consultazione di contenuti in rete;
- **se tale strumento è implementato**, l’ambito dei **controlli** previsti (indiretti o preterintenzionali) e i trattamenti di dati personali che possono essere lecitamente effettuati dal datore di lavoro, debbano essere comunque **non massivi, gradualmente e ammissibili solo previo esperimento di misure meno limitative dei diritti lavoratori**;
 - **in ogni caso ai fini della conformità del trattamento è necessario sia fornita ad ogni dipendente un’adeguata informazione** delle modalità d’uso degli strumenti e **una specifica informativa** dedicata ai trattamenti che, per esigenze organizzative e di sicurezza informatica, comportano il tracciamento delle attività dei dipendenti. Il Servizio privacy RPD fornirà a breve un modello di informativa ad hoc;
 - in ogni caso **si prescrive di effettuare una valutazione di impatto privacy** avente ad oggetto il trattamento dei dati personali relativi alla navigazione in internet dei dipendenti.

Si evidenzia che, se in esito a tale verifica di conformità **il sistema e le misure in essere non risultassero conformi alle prescrizioni sopra indicate** e da quanto contenuto nel citato provvedimento del Garante, **risulta necessario con urgenza disattivare tale sistema e tali strumenti**.

L’Ente provvederà quindi di seguito ad attuare le misure valutate adeguate e necessario a garantire la conformità del trattamento dei dati personali al Regolamento europeo 679/2016.

* * * * *

Coerentemente con l’approccio fino ad oggi adottato, rimane inteso che – qualora ritenuto da voi opportuno – la dott.ssa Federica Dallaporta all’Ufficio Segreteria dell’Area Innovazione (tel: 0461 987139 e-mail: serviziordp@comunitrentini.it) ed il personale dello staff è a disposizione per eventuali ulteriori informazioni in merito.

Il Responsabile
dell’Area Innovazione
Walter Merler
[documento firmato digitalmente]

Questo documento, se inviato in forma cartacea, costituisce copia dell’originale informatico firmato digitalmente conservato dal nostro Ente ai sensi del D. Lgs. 82/2005 (artt. 3-bis e 71). La firma autografa è sostituita dal nominativo del responsabile ai sensi del D. Lgs. 39/1993 (art. 3)."



Trento, 28 settembre 2020
GF/fd/ed

Ai segretari
Ai Referenti privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE/PEC

OGGETTO: Servizio privacy RPD – Approfondimento in merito alla figura del Titolare del trattamento e del Responsabile del trattamento alla luce di alcune nuove pronunce delle Autorità competenti

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto.
Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.
Cordiali saluti.

Il Direttore Generale
dott. Marco Riccadonna

Il Presidente
dott. Paride Giarmona



CIRCOLARE/RUNDSCHREIBEN

Alle Dirigenti e ai Dirigenti
delle Ripartizioni della
Regione autonoma Trentino Alto-Adige/Südtirol

Tramite PITre

e, p.c.

Al Responsabile della Protezione dei Dati
Consorzio dei Comuni trentini
Pec.: consorzio@pec.comunitrentini.it

All'Ufficio Informatica e digitalizzazione
Sede

Oggetto: Aggiornamento del registro dei trattamenti e nomina dei soggetti autorizzati (incaricati) ai sensi dell'art. 4. par. 1, n. 10, in combinato disposto con l'art. 29 del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679.

Gentili Dirigenti,

con Decreto del Presidente della Regione n. 77 di data 9 dicembre 2020 è stato approvato il nuovo assetto organizzativo dell'ente Regione autonoma Trentino-Alto Adige/Südtirol. In relazione a ciò, si rende necessario aggiornare il Registro dei trattamenti e le nomine dei soggetti autorizzati al trattamento dei dati.

Richiamo, a tal fine, la deliberazione della Giunta regionale 3 settembre 2019, n. 193 la quale, alla luce della struttura dell'ente Regione autonoma Trentino-Alto Adige/Südtirol nonché delle funzioni e competenze alla stessa attribuite, ha introdotto criteri e modalità organizzative, volte a garantire e comprovare che il titolare del trattamento, in ossequio al principio di responsabilizzazione, operi in modo che il trattamento dei dati personali sia effettuato in conformità alla vigente normativa in materia. L'invito che vi rivolgo, di voler aggiornare il Registro dei trattamenti e le nomine dei direttori d'ufficio e collaboratori autorizzati ai trattamenti di dati personali, è in esecuzione del punto 3) del dispositivo della sopracitata deliberazione.

La modifica della struttura organizzativa ha avuto un impatto anche da un punto di vista tecnico in quanto si è dovuto intervenire sull'organigramma dell'applicativo Pi.Tre. e sulle attribuzioni ai collaboratori dei diritti ai singoli applicativi e cartelle di rete.

In tale contesto, ritengo doveroso garantire e comprovare che il trattamento dei dati personali da parte dei direttori e dei collaboratori sia effettuato sulla base di formali autorizzazioni da parte dei

Dirigenti, aggiornate alla data dell'1 gennaio 2021. Chiedo, quindi, uno sforzo da parte di tutti affinché gli adempimenti richiesti dalla normativa in materia di privacy siano eseguiti tempestivamente.

Per agevolare le attività di vostra competenza vi vengono indicati, di seguito, i documenti da predisporre e le relative indicazioni operative.

1) Registro dei trattamenti.

Ogni Dirigente è tenuto verificare, aggiornare e trasmettere firmato il Registro dei trattamenti, alla Segreteria generale (220) mediante PITre, con protocollo interno, **entro il 31 gennaio 2021**.

2) Nomina dei soggetti autorizzati.

In allegato alla presente è inviato il nuovo modello di nomina, da personalizzare con le istruzioni che si devono impartire al singolo collaboratore, tenuto conto delle mansioni che in concreto svolge. Tale modello deve essere redatto per ogni direttore e collaboratore. E' inviato, inoltre, il modello di check list incaricati. La documentazione predisposta va trasmessa, **entro il 31 gennaio 2021**, tramite PITre con protocollo interno, alla Segreteria generale (220) inserendo come documento principale la check list incaricati e come allegati gli altri documenti.

3) Abilitazioni in PITre e verifica delle medesime.

La verifica delle abilitazioni dei collaboratori in PITre è un'attività che deve essere svolta regolarmente dai Dirigenti, per accertarsi che le abilitazioni assegnate siano sempre aggiornate. L'Ufficio Informatica e digitalizzazione ha predisposto una guida, che si allega alla presente, affinché questa attività possa essere effettuata da ogni Dirigente in autonomia utilizzando la gestione organigramma di PITre.

In seguito alla verifica vi invito a compilare e sottoscrivere il modello "Verifica abilitazioni PITre", allegato alla presente, ed a trasmetterlo alla Segreteria generale con le medesime modalità indicate nei paragrafi sopra. Considerata la delicatezza, ai fini privacy, delle abilitazioni concesse, vi chiedo di effettuare tale verifica urgentemente e di trasmettere il modello entro il **15 gennaio 2021**. Nulla è variato, invece, per quanto riguarda l'incarico ai collaboratori per l'utilizzo del sistema PITre, viene comunque allegato anche detto modello.

4) Abilitazioni alle cartelle ed applicativi e verifica delle medesime.

Per richiedere l'abilitazione a cartelle ed applicativi è stato predisposto un nuovo modello in formato excel che si allega alla presente. Essendo necessario effettuare annualmente una verifica delle abilitazioni già autorizzate, l'Ufficio Informatica e digitalizzazione ha elaborato un modello per ogni ufficio riportante tutti i dipendenti dell'ufficio e i diritti base attribuiti sulle cartelle. Ogni dirigente riceverà quanto prima, via mail, la lista relativa alla propria Struttura e agli Uffici dipendenti. Vi chiedo di verificare le informazioni riportate e, se necessario, di integrare l'autorizzazione ad operare su ulteriori cartelle o applicativi. Anche in questo caso, considerata la delicatezza, ai fini privacy, delle abilitazioni concesse, vi chiedo di effettuare tale verifica urgentemente e di trasmettere il documento sottoscritto entro il **15 gennaio 2021**.

Ritengo utile, infine, riassumere gli adempimenti da porre in essere, di regola, da parte dei dirigenti:

1) **Nuovo trattamento** (per assunzione, trasferimento, cambio ruolo all'interno dell'ufficio):

- aggiornamento del Registro dei trattamenti,
- nomina del soggetto autorizzato
- check list nomina soggetto autorizzato
- abilitazioni PITre
- prospetto attribuzione diritti ai singoli applicativi e sito web
- prospetto attribuzione diritti alle singole cartelle

2) **Verifiche da effettuare costantemente da parte dei dirigenti**

- verifica delle abilitazioni dei collaboratori in PITre
- verifica delle abilitazioni dei collaboratori alle cartelle ed applicativi

Per eventuali chiarimenti rimangono a disposizione i seguenti collaboratori: Rosabianca Gambini, Daniela Marconi, Sabrina Poli, Michele Zanotti.

Confido nella collaborazione di tutti voi per la positiva implementazione degli adempimenti in materia di privacy.

Cordiali saluti.

IL SEGRETARIO GENERALE

Michael Mayr

(firmato digitalmente)

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Allegati:

1. modello nomina soggetto autorizzato
2. modello check list
3. modello verifica abilitazioni in PITre
4. guida alla verifica delle abilitazioni in PITre
5. prospetto attribuzione diritti ai singoli applicativi e sito web
6. prospetto attribuzione diritti alle singole cartelle
7. Modello abilitazione PITre

ALLEGATO n. 2

**Circolare n. 11 del 2018 prot. n. 18085
concernente “Gestione delle istanze di
accesso civico generalizzato, accesso
civico (semplice), accesso documentale,
tramite sistema P.I.Tre. e registro degli
accessi civici generalizzati e relativi
Allegati.**

ANLAGE Nr. 2

**Rundschreiben Nr. 1/2018 Prot. Nr. 18085
betreffend „Abwicklung der Anträge auf
allgemeinen Bürgerzugang, auf
(einfachen) Bürgerzugang sowie auf
Zugang zu den Verwaltungsunterlagen
über das P.I.Tre.-System und Register der
allgemeinen Bürgerzugänge“ und
Anlagen**



Trento / Trient 4.09.2018 prot. n. 18085

CIRCOLARE/RUNDSCHREIBEN Nr. 11

Oggetto: gestione delle istanze di accesso civico generalizzato, accesso civico (semplice), accesso documentale, tramite il sistema P.I.Tre. e registro degli accessi civici generalizzati.

Alle Dirigenti ed ai Dirigenti di
Ripartizione e Strutture equiparate

Alle Direttrici ed ai Direttori degli Uffici

Al personale regionale
Alle Organizzazioni Sindacali

Betreff: Abwicklung der Anträge auf allgemeinen Bürgerzugang, auf (einfachen) Bürgerzugang sowie auf Zugang zu den Verwaltungsunterlagen über das P.I.Tre.-System und Register der allgemeinen Bürgerzugänge

An die Leiterinnen und Leiter der Abteilungen
und der gleichgestellten
Organisationsstrukturen
An die Direktorinnen und Direktoren der Ämter

An die Regionalbediensteten
An die Gewerkschaften

Si informa il personale regionale che è stata implementata nel sistema P.I.Tre la nuova funzionalità concernente la gestione delle diverse fasi procedurali connesse alle istanze di accesso civico generalizzato, istituto giuridico previsto dall'articolo 1, comma 1, lettera 0a) della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, concernente l'ostensibilità dei documenti detenuti dall'amministrazione, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria.

Es wird mitgeteilt, dass im P.I.Tre.-System eine neue Funktion implementiert wurde, welche die Abwicklung der verschiedenen Verfahrensphasen in Zusammenhang mit den Anträgen auf allgemeinen Bürgerzugang betrifft. Dieses neue Rechtsinstitut ist im Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10 – geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16 – vorgesehen und betrifft die Einsehbarkeit von bei der Verwaltung aufliegenden Dokumenten, die über die veröffentlichungspflichtigen Dokumente hinausgehen.

Tale nuova funzionalità introdotta nel sistema consente la gestione delle diverse fasi procedurali relative all'istanza di accesso

Mit dieser neuen Funktion können die verschiedenen Verfahrensphasen in Zusammenhang mit den Anträgen auf

civico generalizzato ovvero:

- protocollazione delle richieste;
- gestione della fase istruttoria;
- gestione della fase relativa agli eventuali rimedi giurisdizionali e non, da attivare da parte del richiedente, in caso di diniego parziale o totale dell'accesso e quindi richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) o alternativamente, ricorso al difensore civico o alternativamente ricorso al Tribunale amministrativo regionale;
- la verifica in ogni momento dello stato di avanzamento di ogni procedimento;
- la registrazione delle richieste di accesso civico generalizzato pervenute, sottoforma di "Registro degli accessi" ovvero l'estrazione automatica dei files riepilogativi delle richieste pervenute (in tre formati diversi xls, pdf, e xml) che verrà gestita dalla Segreteria generale. Ciò, in osservanza a quanto stabilito nel punto 9 delle Linee guida dell'Autorità nazionale Anticorruzione, approvate con delibera n. 1309 del 28 dicembre 2016, recanti *"Indicazioni operative, ai fini della definizione delle esclusioni e dei limiti di accesso civico di cui all'articolo 5, comma 2, del decreto legislativo n. 33 e successive modificazioni"*, (si legga per la Regione TAA articolo 1, comma 1, lettera 0a) della Legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16).

allgemeinen Bürgerzugang abgewickelt werden, d. h.:

- Protokollierung der Anträge;
- Bearbeitung der Anträge;
- Phase betreffend die eventuell von der antragstellenden Person eingeleiteten Rechtsbehelfe (Antrag an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz – RPCT auf Überprüfung der Entscheidung oder Rekurs bei der Volksanwaltschaft oder Rekurs beim Regionalen Verwaltungsgericht), falls der Zugangsantrag teilweise oder ganz abgelehnt wurde;
- jederzeit mögliche Überprüfung des Stands des jeweiligen Verfahrens;
- Erfassung der eingegangenen Anträge auf allgemeinen Bürgerzugang in Form eines „Registers der Zugänge“, d. h. automatische Extraktion der Dateien der eingegangenen Anträge (in den drei Dateiformaten .xls, .pdf und .xml). Dieser Schritt wird vom Generalsekretariat durchgeführt. Dadurch wird den Bestimmungen laut Z. 9 der mit Beschluss der nationalen Antikorruptionsbehörde (ANAC) vom 28. Dezember 2016, Nr. 1309 genehmigten Richtlinien entsprochen, die Anleitungen zur Bestimmung der Fälle enthalten, in denen der Bürgerzugang laut Art. 5 Abs. 2 des gesetzesvertretenden Dekrets Nr. 33 i.d.g.F. Ausnahmen und Einschränkungen unterliegt (in Bezug auf die Region Trentino-Südtirol siehe Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember

Nelle predette linee guida, l'Autorità raccomanda infatti, la raccolta organizzata delle richieste di accesso civico generalizzato sottoforma di "Registro" il quale deve contenere l'elenco delle richieste con l'oggetto e la data, il relativo esito con la data della decisione, da pubblicare nel sito istituzionale dell'Amministrazione regionale, oscurando i dati personali eventualmente presenti.

Il Registro degli accessi, oltre ad essere funzionale per il monitoraggio che in quest'ambito l'Autorità periodicamente intende svolgere, è anche utile per l'Amministrazione, al fine di rendere note le tipologie di documenti sulle quali è stato consentito l'accesso in una ottica di sempre maggiore semplificazione delle attività.

Con l'occasione dell'introduzione della nuova funzionalità finalizzata al monitoraggio delle istanze di accesso civico generalizzato, nel fascicolo tipizzato con classificazione 6.3 accesso ai documenti amministrativi, è stata inserita un'ulteriore tipologia di registrazione degli accessi ai documenti amministrativi, ovvero l'accesso agli atti o accesso documentale (tipologia fascicolo "Accesso documentale").

Pertanto, ogni richiesta di accesso dovrà preliminarmente essere ricondotta alla propria fattispecie giuridica e conseguentemente inserita nel sistema P.I.Tre nel fascicolo 6.3 accesso ai documenti amministrativi scegliendo uno dei fascicoli corrispondenti alla tipologia individuata.

Die Antikorruptionsbehörde empfiehlt in genannten Richtlinien nämlich die organisierte Erfassung der Anträge auf allgemeinen Bürgerzugang in Form eines „Registers“, das das Verzeichnis der eingegangenen Anträge mit Gegenstand und Datum sowie Ergebnis und Datum der diesbezüglichen Entscheidung enthält und auf der offiziellen Website der Regionalverwaltung zu veröffentlichen ist, wobei eventuell vorhandene personenbezogene Daten unkenntlich zu machen sind. Der Register der Zugänge ist nicht nur für das Monitoring nützlich, das die Antikorruptionsbehörde regelmäßig in diesem Bereich durchzuführen gedenkt, sondern im Hinblick auf die Vereinfachung der Tätigkeit auch für die Verwaltung, um die Art der Dokumente bekannt zu geben, auf die der Bürgerzugang erlaubt ist.

Anlässlich der Einführung dieser neuen Funktion zum Monitoring der Anträge auf allgemeinen Bürgerzugang wurde im Faszikeltyp „6.3 accesso ai documenti amministrativi“ zur Registrierung der Dokumentenzugänge ein weiterer Zugangstyp vorgesehen, nämlich der Zugang zu den Verwaltungsunterlagen (Faszikeltyp: *„Accesso documentale“*).

Dementsprechend muss jeder Zugangsantrag vorab der jeweiligen Kategorie zugeordnet und in das jeweilige Faszikel unter 6.3 „Accesso ai documenti amministrativi“ im P.I.Tre-System eingegeben werden.

Al fine di agevolare gli uffici nello svolgimento delle attività sopra descritte, si allegano per ogni utile consultazione i seguenti documenti:

- allegato A – breve sintesi sulle disposizioni in materia di accesso;
- allegato B – modalità di gestione delle domande di accesso tramite P.I.Tre;
- Allegato C - diagramma di flusso delle attività in cui sono indicati gli attori del processo e le operazioni da compiere con riferimento all'accesso civico generalizzato;
- modello per le richieste di accesso civico generalizzato, accesso documentale e accesso civico semplice (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico" unitamente alla presente circolare);
- modello per la richiesta di riesame al Responsabile per la prevenzione della corruzione e della trasparenza (RPCT) da parte del richiedente accesso in caso di diniego totale, parziale, differimento o mancata risposta dell'accesso civico generalizzato (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico unitamente alla presente circolare);
- modello per la richiesta di riesame al Responsabile per la prevenzione della corruzione e della trasparenza (RPCT) da parte dei controinteressati in caso di opposizione all'accoglimento dell'istanza di accesso civico generalizzato (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico unitamente alla presente circolare).

Um die Durchführung der oben beschriebenen Tätigkeiten zu erleichtern, werden nachstehende Unterlagen beigelegt:

- Anlage A – Übersicht über die Regelung des Zugangsrechts;
- Anlage B – Modalitäten für die Abwicklung der Zugangsanträge mittels Eingabe in das P.I.Tre-System;
- Anlage C – Flussdiagramm der Aktivitäten in Bezug auf den allgemeinen Bürgerzugang mit Angabe der Akteure und der durchzuführenden Schritte;
- Vordruck für die Anträge auf allgemeinen Bürgerzugang, Zugang zu den Verwaltungsunterlagen und einfachen Bürgerzugang (der Vordruck ist zusammen mit diesem Rundschreiben auf der offiziellen Website unter dem Bereich „Transparente Verwaltung – Sonstige Inhalte – Bürgerzugang“ veröffentlicht);
- Vordruck für den von der antragstellenden Person an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz (RPCT) zu richtenden Antrag auf Überprüfung für den Fall, dass der Antrag auf allgemeinen Bürgerzugang ganz oder teilweise abgelehnt oder der Zugang aufgeschoben oder keine Antwort erteilt wurde (der Vordruck ist zusammen mit diesem Rundschreiben auf der offiziellen Website unter dem Bereich „Transparente Verwaltung – Sonstige Inhalte – Bürgerzugang“ veröffentlicht);
- Vordruck für den von den Drittbetroffenen an den Verantwortlichen für die

Korruptionsvorbeugung und die
Transparenz (RPCT) zu richtenden
Antrag auf Überprüfung für den Fall,
dass gegen den Antrag auf allgemeinen
Bürgerzugang Einspruch erhoben
wurde (der Vordruck ist zusammen mit
diesem Rundschreiben auf der
offiziellen Website unter dem Bereich
„Transparente Verwaltung – Sonstige
Inhalte – Bürgerzugang“ veröffentlicht).

Cordiali saluti.

Mit freundlichen Grüßen

IL SEGRETARIO GENERALE
DER GENERALSEKRETÄR

Alexander Steiner

(firmato digitalmente - digital signiert)

AS/cg

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Dokument in Papierform übermittelt wird, stellt es die für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

ALLEGATO A

Breve sintesi sulle disposizioni in materia di diritto di accesso

Il diritto di accedere ai documenti detenuti dall'Amministrazione può essere esercitato mediante:

- a) **accesso agli atti (accesso documentale)** ai sensi di quanto previsto dalla legge regionale 31 luglio 1993, n. 13, e successive modificazioni, recante “*Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*” nonché dal Regolamento di esecuzione D.P.Reg. 16 novembre 2004, n. 7/L, e successive modificazioni;
- b) **accesso civico semplice**, inteso come richiesta di pubblicazione di documenti soggetti a pubblicazione obbligatoria, laddove sia stata omessa (art. 1, comma 1, della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, - riferimento: art. 5, comma 1, del decreto legislativo n. 33 del 2013 e successive modificazioni);
- c) **accesso civico generalizzato**, inteso come diritto di accedere ai DOCUMENTI detenuti dall'Amministrazione, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria (articolo 1, comma 1, lettera 0a) della Legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, - riferimento articolo 5, comma 2, del decreto legislativo n. 33 del 2013, e successive modificazioni).

Nel caso dell'**accesso agli atti “accesso documentale”** previsto dalla legge regionale 31 luglio 1993, n. 13, e successive modificazioni, la domanda di accesso deve essere motivata da parte del richiedente per far valere una situazione giuridicamente tutelata.

L'**accesso civico semplice, “accesso civico”**, è esercitabile unicamente presso il Responsabile della prevenzione della corruzione e della trasparenza (RPCT), al fine di verificare la presunta mancata pubblicazione, nella sezione “Amministrazione Trasparente” del sito istituzionale della Regione, di documenti che, in forza della vigente normativa in materia di trasparenza (legge regionale 29 ottobre 2014, n. 10 come modificata dalla legge regionale 15 dicembre 2016, n. 16) sono oggetto di pubblicazione obbligatoria.

L'inadempimento degli obblighi di pubblicazione, rilevato a seguito della presentazione di una domanda di accesso civico semplice comporta, per il Responsabile della prevenzione della corruzione e della trasparenza, l'obbligo di effettuare una segnalazione alla struttura competente in materia di procedimenti disciplinari, al Nucleo di valutazione dei dirigenti in funzione di Organismo Indipendente di Valutazione (O.I.V.) nonché al vertice politico dell'amministrazione (art. 43, comma 5, d. lgs. n. 33 del 2013, e successive modificazioni).

L'**accesso civico generalizzato, “accesso generalizzato”**, può essere esercitato da chiunque, senza bisogno di motivazione, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti (articolo 1, comma 1, lettera 0a) e seguenti della Legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16 - riferimento: articolo 5, comma 2, e art. 5-*bis* del decreto legislativo n. 33 del 2013, e successive modificazioni).

Il contesto normativo di riferimento è delineato inoltre, dalle Linee guida dell'Autorità nazionale Anticorruzione recanti “*Indicazioni operative ai fini della definizione delle esclusioni e dei limiti di accesso civico di cui all'articolo 5, comma 2, del decreto legislativo n. 33 e successive modificazioni*” approvate con delibera n. 1309 del 28 dicembre 2016 e dalla circolare del Dipartimento della Funzione pubblica presso la Presidenza del Consiglio dei Ministri n. 2 del 2017, alle quali si rinvia per ogni utile approfondimento.

L'accoglimento o il non accoglimento della domanda deve essere sempre motivato. In applicazione del principio della tutela preferenziale dell'interesse conoscitivo la motivazione del non accoglimento della domanda, nelle varie forme in cui esso può essere manifestato, richiede un'attenta valutazione degli interessi pubblici e privati che possono giustificare una sua limitazione. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine dei trenta giorni, il richiedente può presentare richiesta di riesame al Responsabile della prevenzione e della corruzione e della trasparenza (articolo 5, comma 7, del decreto legislativo n. 33 del 2013, e successive modificazioni) che decide con provvedimento motivato entro il termine di venti giorni, fatte salve le sospensioni del termine qualora si ritenga necessario acquisire l'avviso del Garante per la protezione dei dati personali.

Il differimento e la limitazione all'accesso civico generalizzato nei casi non previsti dalla citata normativa vigente, costituisce **elemento di valutazione della responsabilità dirigenziale**, anche ai fini della corresponsione della retribuzione di risultato.

Istruttoria (articolo 5, commi 5 e 6, e articolo 5-bis, commi 1 e 2 del decreto legislativo n. 33 del 2013 e successive modificazioni):

Assenza di controinteressati

Riscontrata l'assenza di controinteressati cui comunicare la domanda di accesso pervenuta il procedimento si conclude con:

- risposta motivata da comunicare al richiedente nel rispetto del termine di trenta giorni dalla data di presentazione della domanda.

Presenza di controinteressati

Nel caso di presenza di controinteressati, intesi quali soggetti portatori di uno degli interessi pubblici e/o privati tutelati:

- deve essere data comunicazione agli stessi mediante raccomandata con avviso di ricevimento o per via telematica, se dal richiedente è stato fornito nella domanda di accesso un indirizzo di posta elettronica certificata (PEC);
- devono essere contestualmente sospesi i termini per la risposta fino alla scadenza dei dieci giorni concessi ai controinteressati per fare opposizione;
- dalla ricezione della comunicazione inizia a decorrere il termine di dieci giorni concesso ai controinteressati per fare opposizione: in presenza di una pluralità di controinteressati la verifica deve essere compiuta rispetto alla ricezione di ciascuna comunicazione.

Scenari possibili:

A) Nessuno dei controinteressati fa opposizione

Accertata la data della ricezione della comunicazione ai fini della verifica dell'integrale decorrenza dei dieci giorni concessi per l'opposizione, il termine per la risposta ricomincia a decorrere e il procedimento si conclude con la comunicazione dell'esito al richiedente e con la tempestiva messa a disposizione dello stesso dei documenti richiesti, con le modalità indicate nella domanda. Dell'accoglimento della domanda deve essere data comunicazione ai controinteressati non opposti.

B) Uno o più controinteressati presentano opposizione

In via pregiudiziale deve essere verificato il rispetto del termine di 10 giorni dalla ricezione delle singole comunicazioni di opposizione, pena l'inammissibilità delle stesse: dall'integrale decorso del termine di dieci giorni riprende a decorrere il termine, precedentemente sospeso, per la risposta.

A seguito della valutazione dei motivi dell'opposizione, il procedimento può concludersi:

- con l'accoglimento della domanda di accesso nonostante l'opposizione dei controinteressati;
- con il non accoglimento della domanda di accesso, qualora si ravvisi in particolare l'esigenza di tutelare uno degli interessi previsti dall'art. 5-bis, commi 1 e 2, del d.lgs. n. 33 del 2013, e successive modificazioni.

Salvi i casi di comprovata indifferibilità (art. 5, comma 6, d.lgs. n. 33 del 2013 e successive modificazioni), deve essere data comunicazione dell'accoglimento della domanda di accesso al controinteressato, indicando che si procederà a trasmettere i documenti al richiedente non prima di quindici giorni dall'avvenuta ricezione della comunicazione stessa e che, avverso l'accoglimento, lo stesso controinteressato (ai sensi di quanto previsto dall'articolo 5, comma 9, d. lgs. n. 33 del 2013, e successive modificazioni) può presentare richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza o ricorso al Difensore civico (art. 5, commi 7, 8 e 9, d. lgs. n. 33 del 2013 e successive modificazioni). A tal riguardo, la citata circolare del Dipartimento della Funzione pubblica n. 2 del 2017 suggerisce: *"Anche al fine di evitare contestazioni, è opportuno che la comunicazione di accoglimento della richiesta di accesso (in caso di opposizione) contenga l'espressa precisazione che la trasmissione al richiedente dei dati o documenti avviene qualora, decorsi quindici giorni, non siano stati notificati all'amministrazione ricorsi o richieste di riesame sulla medesima domanda di accesso"*.

Anche in questo caso, il Responsabile della prevenzione della corruzione e della trasparenza decide motivatamente entro venti giorni dalla richiesta di riesame, fatta salva la sospensione di tale termine qualora si ritenga necessario acquisire l'avviso del Garante per la protezione dei dati personali.

Il Difensore civico invece, si pronuncia entro trenta giorni dalla presentazione del ricorso.

ANLAGE A

Übersicht über die Regelung des Zugangsrechts

Das Recht auf Zugang zu den bei der Verwaltung aufliegenden Dokumenten kann in verschiedenen Weisen ausgeübt werden:

a) Zugang zu den Verwaltungsunterlagen im Sinne des Regionalgesetzes vom 31. Juli 1993, Nr. 13 i.d.g.F. „*Bestimmungen auf dem Gebiet des Verwaltungsverfahrens und des Rechtes auf Zugang zu den Verwaltungsunterlagen*“ sowie der Durchführungsverordnung laut DPRReg. vom 16. November 2004, Nr. 7/L i.d.g.F.;

b) einfacher Bürgerzugang: Antrag auf Veröffentlichung von veröffentlichungspflichtigen Dokumenten, wenn diese unterlassen wurde (Art. 1 Abs. 1 des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16; Bezugsbestimmung: Art. 5 Abs. 1 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.);

c) allgemeiner Bürgerzugang: Recht auf Zugang zu bei der Verwaltung aufliegenden Dokumenten, die über die veröffentlichungspflichtigen hinausgehen (Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16; Bezugsbestimmung: Art. 5 Abs. 2 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.).

Der **Zugang zu den Verwaltungsunterlagen („accesso documentale“)** gemäß Regionalgesetz vom 31. Juli 1993, Nr. 13 i.d.g.F. kann beantragt werden, um eine rechtlich geschützte Situation geltend zu machen. Der Antrag muss von der ansuchenden Person entsprechend begründet werden.

Das Recht auf **einfachen Bürgerzugang („accesso civico“)** kann ausschließlich über einen Antrag an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz (RPCT) ausgeübt werden, welcher daraufhin die vermeintlich unterlassene Veröffentlichung von Dokumenten, die laut den geltenden Bestimmungen in Sachen Transparenz (Regionalgesetz vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16) veröffentlichungspflichtig sind, unter dem Bereich „Transparente Verwaltung“ der offiziellen Website der Region überprüft.

Stellt der Verantwortliche für die Korruptionsvorbeugung und die Transparenz infolge eines Antrags auf einfachen Bürgerzugang fest, dass die Veröffentlichungspflicht nicht erfüllt wurde, so muss er dies der für die Disziplinarverfahren zuständigen Struktur, dem Gremium zur Bewertung der Führungskräfte in seiner Funktion als Unabhängiges Bewertungsgremium (OIV) sowie dem politischen Führungsorgan der Verwaltung melden (Art. 43 Abs. 5 des GvD Nr. 33/2013 i.d.g.F.).

Das Recht auf **allgemeinen Bürgerzugang („accesso generalizzato“)** kann von einer jeden Person ohne Begründung innerhalb der Grenzen des Schutzes rechtlich relevanter öffentlicher und privater Interessen ausgeübt werden (Art. 1 Abs. 1 Buchst. 0a) ff. des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16; Bezugsbestimmungen: Art. 5 Abs. 2 und Art. 5-bis des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.).

Den rechtlichen Rahmen bilden ferner die mit Beschluss der Nationalen Antikorruptionsbehörde vom 28. Dezember 2016, Nr. 1309 erlassenen Richtlinien mit *Anleitungen zur Bestimmung der Fälle, in denen der Bürgerzugang laut Art. 5 Abs. 2 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F. Ausnahmen und Einschränkungen unterliegt*, sowie das Rundschreiben Nr. 2/2017 der Abteilung für das öffentliche Verwaltungswesen beim Präsidium des Ministerrats, auf die zur Vertiefung verwiesen wird.

Die Annahme bzw. Ablehnung des Antrags ist immer zu begründen. Gemäß dem Grundsatz des vorrangigen Schutzes des Informationsinteresses müssen bei der Begründung der in welcher Form auch immer bekundeten Ablehnung des Antrags die öffentlichen und privaten Interessen, die eine Einschränkung des Zugangsrechts rechtfertigen können, genau abgewogen werden.

Wird der Zugangsantrag ganz oder teilweise abgelehnt oder erfolgt keine Antwort binnen der Frist von 30 Tagen, so kann die antragstellende Person beim Verantwortlichen für die Korruptionsvorbeugung und die Transparenz einen Antrag auf Überprüfung der Entscheidung stellen (Art. 5 Abs. 7 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.). Dieser entscheidet binnen zwanzig Tagen mit begründeter Maßnahme, unbeschadet der Aussetzung dieser Frist, falls die Datenschutzbehörde angehört werden muss.

Der Aufschub und die Einschränkung des allgemeinen Bürgerzugangs in Fällen, die nicht in den oben genannten Bestimmungen vorgesehen sind, werden **bei der Bewertung der Verantwortung der Führungskraft**, u. a. auch im Hinblick auf das Ergebnisgehalt, **berücksichtigt**.

Bearbeitung (Art. 5 Abs. 5 und 6 und Art. 5-bis Abs. 1 und 2 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.):

Es sind keine Drittbetroffenen vorhanden:

Nach Feststellung des Nichtvorhandenseins von Drittbetroffenen, denen der eingegangene Zugangsantrag mitzuteilen ist, wird das Verfahren

- mit einer begründeten Antwort abgeschlossen, die der antragstellenden Person innerhalb 30 Tagen ab Einreichung des Antrags zu erteilen ist.

Es sind Drittbetroffene vorhanden:

Falls Drittbetroffene, d. h. Rechtsträger eines geschützten öffentlichen und/oder privaten Interesses, vorhanden sind, ist folgendermaßen vorzugehen:

- Die Drittbetroffenen sind per Einschreiben mit Rückschein oder auf digitalem Weg – falls die antragstellende Person im Zugangsantrag eine zertifizierte E-Mail-Adresse (PEC) angegeben hat – über den Antrag zu informieren.
- Gleichzeitig wird die Frist für die Beantwortung des Antrags bis zum Ablauf der zehntägigen Frist ausgesetzt, innerhalb deren die Drittbetroffenen Einspruch erheben können.
- Die den Drittbetroffenen gewährte zehntägige Einspruchsfrist läuft ab dem Datum, an dem sie die Mitteilung erhalten haben. Sind mehrere Drittbetroffene vorhanden, so muss zur Berechnung der Frist das Datum des Erhalts jeder einzelnen Mitteilung berücksichtigt werden.

Mögliche Szenarien:

A) Keiner der Drittbetroffenen erhebt Einspruch

Nachdem das Datum des Erhalts der Mitteilung überprüft und der vollständige Ablauf der zehntägigen Einspruchsfrist festgestellt wurde, beginnt die Frist für die Beantwortung des Antrags wieder zu laufen und das Verfahren wird abgeschlossen, indem der antragstellenden Person das Ergebnis mitgeteilt wird und ihr die beantragten Dokumente umgehend und nach den im Antrag angegebenen Modalitäten zur Verfügung gestellt werden. Die Annahme des Antrags ist den Drittbetroffenen, die keinen Einspruch erhoben haben, mitzuteilen.

B) Einer oder mehrere Drittbetroffene erheben Einspruch

Vor der Entscheidung muss überprüft werden, dass die zehntägige Frist für die Einspruchserhebung ab Erhalt der jeweiligen Mitteilungen eingehalten wurde, da ansonsten der Einspruch unzulässig ist. Wenn diese zehntägige Frist vollständig abgelaufen ist, beginnt die zuvor ausgesetzte Frist für die Beantwortung des Antrags wieder zu laufen.

Je nachdem, wie die Einspruchsgründe beurteilt werden, kann das Verfahren folgendermaßen abgeschlossen werden:

- Dem Zugangsantrag wird trotz Einspruch der Drittbetroffenen stattgegeben.
- Der Zugangsantrag wird abgelehnt, falls insbesondere der Schutz eines der im Art. 5-bis Abs. 1 und 2 des GvD Nr. 33/2013 i.d.g.F. vorgesehenen Interessen für notwendig erachtet wird.

Außer in nachweislich unaufschiebbaren Fällen (Art. 5 Abs. 6 des GvD Nr. 33/2013 i.d.g.F.) sind die Drittbetroffenen über die Annahme des Zugangsantrags zu informieren mit dem Hinweis, dass die angeforderten Dokumente an die antragstellende Person erst nach Ablauf von fünfzehn Tagen ab Erhalt der Mitteilung zugesandt werden und dass gemäß Art. 5 Abs. 9 des GvD Nr. 33/2013 i.d.g.F. die Drittbetroffenen gegen die Annahme einen Antrag auf Überprüfung der Entscheidung beim Transparenzverantwortlichen oder Rekurs bei der Volksanwaltschaft einlegen können (Art. 5 Abs. 7, 8, und 9 des GvD Nr. 33/2013 i.d.g.F.). Diesbezüglich wird im genannten Rundschreiben Nr. 2/2017 der Abteilung für das öffentliche Verwaltungswesen Nachstehendes empfohlen: „*Um im Einspruchsfall Beanstandungen zu vermeiden, sollte die Mitteilung über die Annahme des Zugangsantrags den ausdrücklichen Hinweis enthalten, dass die angeforderten Daten oder Dokumente an die antragstellende Person erst nach Ablauf von fünfzehn Tagen übermittelt werden, sofern der Verwaltung innerhalb dieser Frist kein Rekurs oder kein Antrag auf Überprüfung der Entscheidung betreffend den Zugangsantrag zugestellt wird.*“

Wird ein Antrag auf Überprüfung der Entscheidung eingereicht, so entscheidet der Verantwortliche für die Korruptionsvorbeugung und die Transparenz auch in diesem Fall binnen zwanzig Tagen ab Eingang des Antrags mit begründeter Maßnahme, unbeschadet der Aussetzung dieser Frist, falls die Datenschutzbehörde angehört werden muss.

Die Volksanwaltschaft entscheidet hingegen innerhalb von dreißig Tagen nach Einlegung des Rekurses.

ALLEGATO B

Modalità di gestione delle domande di accesso tramite inserimento in P.I.Tre

La domanda di accesso, qualunque sia la modalità scelta dal richiedente (posta elettronica o posta elettronica certificata, consegna a mano, invio tramite il servizio postale) può essere presentata alla Segreteria della Segreteria generale della Giunta e alle Segreterie delle strutture competenti per materia – Ripartizioni - che provvederanno a protocollarla immettendola nel sistema P.I. Tre.

Gli indirizzi di posta elettronica cui inviare le domande sono i seguenti:

Segreteria generale della Giunta	giunta@pec.regione.taa.it
Ripartizione I - Pianificazione e programmazione delle risorse	programmazione@pec.regione.taa.it
Ripartizione II – Enti locali, previdenza e competenze ordinamentali	ripaist@pec.regione.taa.it
Ripartizione III – Minoranze linguistiche, integrazione europea, e giudici di pace	ripmin@pec.regione.taa.it
Ripartizione IV- Gestione delle risorse umane	personale@pec.regione.taa.it
Ripartizione V- Gestione delle risorse strumentali	risorsestrumentali@pec.regione.taa.it

E' ulteriormente possibile trasmettere istanza di accesso alla casella generale di posta elettronica certificata della Regione Autonoma Trentino-Alto Adige/Südtirol regione.taa@regione.taa.legalmail.it .
Sarà cura del servizio protocollo trasmettere l'istanza all'Ufficio competente.

Gli addetti delle segreterie delle strutture competenti, sentito il dirigente, provvedono a trasmettere, per competenza, le richieste di accesso protocollate agli incaricati dell'istruttoria.

L'incaricato dell'istruttoria provvede alla creazione del "fascicolo tipizzato" secondo quanto di seguito specificato.

Come registrare le pratiche di accesso

Ogni richiesta di accesso è preliminarmente ricondotta alla propria fattispecie giuridica creando uno specifico fascicolo, con classificazione 6.3 *accesso ai documenti amministrativi*, nell'ambito delle seguenti tipologie:

1. accesso agli atti o accesso documentale (tipologia fascicolo "Accesso documentale");
2. accesso civico generalizzato e accesso civico semplice (tipologia fascicolo "Accesso generalizzato e civico");

Ciascun profilo del fascicolo, oltre ai campi comuni alle tre diverse tipologie, prevede specifici campi aggiuntivi, oggetto di compilazione nel corso della progressione del procedimento.

Per la rappresentazione del sistema di fascicolazione, relativa alle diverse tipologie di accesso, si rimanda al diagramma di flusso delle attività (**Allegato C**), in cui sono indicati gli attori del processo e le operazioni da compiere.

Nel presente allegato, sono descritti i campi tipici di ognuna delle due tipologie di fascicolo e sono riportate le indicazioni per la compilazione.

Si richiama la necessità di verificare attentamente, soprattutto nel campo *Descrizione*, che non vengano inseriti riferimenti alla sfera personale del richiedente in violazione delle vigenti disposizioni in materia di tutela della privacy.

Tipologia fascicolo: Accesso generalizzato e civico

Per la creazione del fascicolo selezionare Fascicoli, Crea nuovo fascicolo.

Scheda fascicolo

Contenuto
Struttura
Trasmissione
Visibilità
Eventi

Registro
RATAA
☐ Privato

Codice di Classificazione*

6.3
Accesso ai documenti amministrativi

Descrizione*
Caratteri disponibili 2000

Nessuna nota visibile

☐ Personale
☐ Ruolo
☒ Tutti

Caratteri disponibili 2000

Trasmissione rapida

Scegli un modello di trasmissione

Tipologia Fascicolo

Seleziona una tipologia

Accesso documentale

Accesso generalizzato e civico

Tipologia Fascicolo

Accesso generalizzato e civico

Progressivo

AOO

RATAA

Data di arrivo della domanda *

24

Nr protocollo della domanda *

Si seleziona la tipologia “Accesso generalizzato e civico” e il profilo del fascicolo viene arricchito di alcuni campi ovvero la **Data arrivo della domanda** e il **Numero di protocollo della domanda**, che sono già stati assegnati dalla segreteria al momento della protocollazione e che sono da inserire nuovamente.

Entrambi sono campi obbligatori (contrassegnati da *) e saranno compilati al momento dell'effettuazione del passo n. 3 del diagramma di flusso allegato (Allegato C).

L'indicazione della **Presenza controinteressati** sarà fatta al momento dell'effettuazione del passo n. 4 del diagramma di flusso delle attività.

Presenza controinteressati

☐ SI ☐ NO



Utilizzare il pulsante per correggere eventuali errori di selezione.

I campi relativi all'esito del procedimento saranno compilati dall'incaricato dell'istruttoria al momento dell'effettuazione del passo n. 7 del diagramma di flusso delle attività. In dettaglio, la compilazione del campo **Esito** sarà effettuata scegliendo uno dei valori ammessi: Accoglimento, Differimento, Rifiuto parziale, Rifiuto totale.

Esito

Seleziona

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

La compilazione del campo **Motivi del rifiuto parziale, del rifiuto totale o del differimento** sarà effettuata solo se l'esito non è Accoglimento. Per facilitare la compilazione del campo sono proposte alcune motivazioni che è possibile scegliere dalle voci del menu a tendina:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Seleziona

ALTRO - Motivi del rifiuto parziale, del rifiuto totale o del differimento**Data risposta** 24

Seleziona

a protezione di uno degli interessi previsti dall'art. 5 bis, comma 1, D. lgs. n. 33 del 2013

a protezione di interessi economici e commerciali

a protezione di dati personali

divieto di divulgazione per norma di legge

dati richiesti non sono detenuti dall'Amministrazione provinciale

dati richiesti richiedono un'elaborazione a cui l'Amministrazione non è tenuta

Se il motivo non è presente nella lista, selezionare *altri motivi* e inserire una descrizione a testo libero nel campo apposito. Si evidenzia che, in ogni caso, il campo altri motivi è stato inserito solamente in via cautelativa. Prima di procedere alla sua compilazione valutare attentamente di non essere in alcuna delle ipotesi di diniego non consentito descritte dalle linee guida ANAC approvate con delibera n. 1309 del 28 dicembre 2016 o dalla circolare del Dipartimento della Funzione pubblica della Presidenza del Consiglio dei Ministri n. 2 del 2017.

Motivi del rifiuto parziale, del rifiuto totale o del differimento

altri motivi (descriverli nel campo successivo) X

Il campo **Data risposta** sarà compilato con la data di protocollo della risposta al richiedente.

Data risposta 24

Il campo **Riesame – data di presentazione della domanda** sarà compilato al momento dell'effettuazione del passo n. 14 del diagramma di flusso delle attività.

Riesame - Data di presentazione della domanda 24

Il campo **Riesame – Esito** sarà compilato al momento dell'effettuazione del passo n. 16 del diagramma di flusso, scegliendo uno dei valori ammessi: Accoglimento, Differimento, Rifiuto parziale, Rifiuto totale

Riesame - Esito

Seleziona ▼

Riesame - Esito

Seleziona ▲

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

Nel caso di Esito Differimento, Rifiuto parziale, Rifiuto totale, si richiede la compilazione del campo **Motivi del rifiuto parziale, del rifiuto totale o del differimento**. Il campo prevede testo libero:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Il campo **Riesame – Data risposta** sarà compilato con la data di protocollo della risposta al richiedente.

Riesame - Data risposta

24

Il campo **Ricorso – Data di notificazione del ricorso all'Amministrazione** sarà compilato al momento dell'effettuazione del passo n. 21 del diagramma di flusso delle attività:

Ricorso – data di notificazione del ricorso

24

Il campo **Ricorso – Esito** sarà compilato al momento dell'effettuazione del passo n. 23 del diagramma di flusso delle attività, scegliendo uno dei valori ammessi: Accoglimento, Accoglimento parziale, Non accoglimento.

Ricorso - Esito

Seleziona ▼

Ricorso - Esito

Seleziona ▲

Accoglimento

Accoglimento parziale

Non accoglimento

Tipologia fascicolo: Accesso agli atti/ Accesso Documentale

Per la creazione del fascicolo selezionare Fascicoli, Crea nuovo fascicolo.

Scheda fascicolo

Contenuto | Struttura | Trasm.ni | Visibilità | Eventi

Registro RATAA ☐ Privato

Codice di Classificazione*

6.3 Accesso ai documenti amministrativi

Descrizione*

Caratteri disponibili 2000

Nessuna nota visibile

☐ Personale ☐ Ruolo ☒ Tutti

Caratteri disponibili 2000

Trasmissione rapida

Scegli un modello di trasmissione

Tipologia Fascicolo

Seleziona una tipologia

Accesso documentale

Accesso generalizzato e civico

Si seleziona la tipologia Accesso documentale. Il profilo del fascicolo viene arricchito di alcuni campi:

La **Data arrivo della domanda** e il **Nr protocollo della domanda**, sono campi obbligatori (contrassegnati da *) e saranno compilati al momento dell'effettuazione del passo n. 3 del diagramma di flusso delle attività (Allegato C) e sono da inserire nuovamente.

L'indicazione della **Presenza controinteressati** sarà fatta al momento dell'effettuazione del passo n. 4 del diagramma di flusso delle attività.

Presenza controinteressati

☐ SI ☐ NO



Utilizzare il pulsante  per correggere eventuali errori di selezione.

I campi relativi all'esito del procedimento saranno compilati al momento dell'effettuazione del passo n. 7 del diagramma di flusso delle attività. In dettaglio, la compilazione del campo **Esito** sarà effettuata scegliendo uno dei valori ammessi: Accoglimento, Differimento, Rifiuto parziale, Rifiuto totale.

Esito

Seleziona 

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

Nel caso di Esito Differimento, Rifiuto parziale, Rifiuto totale, si richiede la compilazione del campo a testo libero **Motivi del rifiuto parziale, del rifiuto totale o del differimento** :

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Il campo **Data risposta** sarà compilato con la data di protocollo della risposta al richiedente.

Data risposta

 24

Il campo **Ricorso – Data di notificazione del ricorso all'Amministrazione** sarà compilato al momento dell'effettuazione del passo n. 12 del diagramma di flusso delle attività:

Ricorso – data di notificazione del ricorso

 24

Il campo **Ricorso – Esito** sarà compilato al momento dell'effettuazione del passo n. 14 del diagramma di flusso delle attività, scegliendo uno dei valori ammessi: Accoglimento, Accoglimento parziale, Non accoglimento.

Ricorso - Esito

Seleziona 

Ricorso - Esito

Seleziona 

Accoglimento

Accoglimento parziale

Non accoglimento

Rapporti tra Fascicoli generati nel protocollo informatico e Registro degli accessi

La protocollazione, attraverso gli specifici fascicoli creati per le diverse tipologie di accesso delle domande e dei documenti relativi alle stesse (eventuale comunicazione ai controinteressati, la risposta di opposizione all'accesso, comunicazione della struttura con

l'indicazione dei motivi del rifiuto dell'accesso, ecc.) costituisce lo strumento per generare automaticamente il Registro degli accessi. Il Registro, gestito dalla Segreteria generale, pubblicato attraverso report periodici sul sito Amministrazione trasparente, costituisce la rappresentazione delle informazioni inserite nei vari campi del protocollo documentale.

ANLAGE B

Modalitäten für die Abwicklung der Zugangsanträge mittels Eingabe in das P.I.Tre.-System

Der Zugangsantrag kann – unabhängig von der gewählten Modalität (E-Mail, zertifizierte E-Mail, persönliche Übergabe, Post) – beim Sekretariat des Generalsekretariats der Regionalregierung oder der für das jeweilige Sachgebiet zuständigen Struktur/Abteilung eingereicht werden, das ihn zur Protokollierung in das P.I.Tre.-System eingibt.

Die Anträge können an nachstehende E-Mail-Adressen gesandt werden:

Generalsekretariat der Regionalregierung	giunta@pec.regione.taa.it
Abteilung I – Planung und Programmierung der Ressourcen	programmazione@pec.regione.taa.it
Abteilung II – Örtliche Körperschaften, Vorsorge und Ordnungsbefugnisse	ripaist@pec.regione.taa.i
Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte	ripmin@pec.regione.taa.it
Abteilung IV – Verwaltung der Humanressourcen	personale@pec.regione.taa.it
Abteilung V – Verwaltung der Technischen Ressourcen	risorsestrumentali@pec.regione.taa.it

Es ist außerdem möglich, den Zugangsantrag an die allgemeine zertifizierte E-Mail-Adresse der Autonomen Region Trentino-Südtirol regione.taa@regione.taa.legalmail.it zu senden. Der Protokolldienst leitet dann den Antrag an das zuständige Amt weiter.

Die Sekretariatsbediensteten der zuständigen Strukturen übermitteln die protokollierten Zugangsanträge nach Anhören der Abteilungsleiterin / des Abteilungsleiters je nach Zuständigkeit an die sachbearbeitende Person.

Die sachbearbeitende Person erstellt ein Klassifikationsfaszikel („fascicolo tipizzato“) gemäß den nachstehenden Anweisungen.

Die Zugangsanträge sind wie folgt zu registrieren:

Jeder Zugangsantrag muss vorab der jeweiligen Kategorie zugeordnet werden, indem ein spezifisches Faszikel im Rahmen der nachstehenden Faszikeltypen mit Klassifizierung „6.3 accesso ai documenti amministrativi“ zu erstellen ist:

1. Zugang zu den Verwaltungsunterlagen (Faszikeltyp „Accesso documentale“);
2. allgemeiner Bürgerzugang und einfacher Bürgerzugang (Faszikeltyp „Accesso generalizzato e civico“);

Jedes Faszikel enthält neben den allen zwei Typen gemeinsamen Feldern auch spezifische Zusatzfelder, die im Laufe des Verfahrens auszufüllen sind.

Die Faszikelanlegung für die verschiedenen Arten des Zugangs ist im Flussdiagramm der Aktivitäten dargestellt (**Anlage C**), auf das verwiesen wird und in dem die Akteure und die durchzuführenden Schritte angegeben sind.

Diese Anlage enthält hingegen die Beschreibung der spezifischen Felder der zwei Faszikeltypen und die Anweisungen für das Ausfüllen derselben.

Es ist sorgfältig darauf zu achten, dass – vor allem im Feld „Descrizione“ – keine Bezüge auf die Privatsphäre der antragstellenden Person eingegeben werden, was die geltenden Datenschutzbestimmungen verletzen würde.

Faszikeltyp: „Accesso generalizzato e civico“

Um ein Faszikel zu erstellen, wählt man „Fascicoli, Crea nuovo fascicolo“.

Nun wählt man den Typ „Accesso generalizzato e civico“. Es erscheinen weitere Felder: **„Data di arrivo della domanda“** und **„Numero di protocollo della domanda“**. Diese Daten wurden bereits vom Sekretariat bei der Protokollierung zugewiesen und sind erneut einzugeben.

Beide Felder sind Pflichtfelder (mit * markiert) und werden ausgefüllt, wenn Schritt 3 des beiliegenden Flussdiagramms (Anlage C) ausgeführt wird.

Das Vorhandensein von Drittbetroffenen wird im Feld **„Presenza controinteressati“** angegeben, wenn Schritt 4 des Flussdiagramms ausgeführt wird.



Mit der Schaltfläche können eventuelle Fehler bei der Auswahl korrigiert werden.

Die Felder betreffend den Ausgang des Verfahrens werden von der sachbearbeitenden Person ausgefüllt, wenn Schritt 7 des Flussdiagramms ausgeführt wird. Für das Feld „**Esito**“ muss eine der folgenden Optionen gewählt werden: „Accoglimento“, „Differimento“, „Rifiuto parziale“, „Rifiuto totale“.

Esito

Seleziona

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

Falls nicht die Option „Accoglimento“ gewählt wurde, muss das Feld „**Motivi del rifiuto parziale, del rifiuto totale o del differimento**“ ausgefüllt werden. Um das Ausfüllen zu erleichtern, enthält das Dropdown-Menü bereits einige Begründungsvorschläge:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Seleziona

ALTRO - Motivi del rifiuto parziale, del rifiuto totale o del differimento

Data risposta

24

Seleziona

a protezione di uno degli interessi previsti dall'art. 5 bis, comma 1, D. lgs. n. 33 del 2013

a protezione di interessi economici e commerciali

a protezione di dati personali

divieto di divulgazione per norma di legge

dati richiesti non sono detenuti dall'Amministrazione provinciale

dati richiesti richiedono un'elaborazione a cui l'Amministrazione non è tenuta

Wenn die Begründung nicht in der Liste enthalten ist, wählt man „*altri motivi*“ und beschreibt die Begründung mit freien Worten im entsprechenden Feld. Es wird darauf hingewiesen, dass das Feld „*altri motivi*“ rein vorsichtshalber eingefügt wurde. Bevor es ausgefüllt wird, sollte sorgfältig abgewogen werden, dass keiner der Fälle einer unzulässigen Ablehnung vorliegt, die in den mit Beschluss der Nationalen Antikorruptionsbehörde vom 28. Dezember 2016, Nr. 1309 erlassenen Richtlinien oder im Rundschreiben

Nr. 2/2017 der Abteilung für das öffentliche Verwaltungswesen beim Präsidium des Ministerrats beschrieben werden.

Motivi del rifiuto parziale, del rifiuto totale o del differimento

altri motivi (descriverli nel campo successivo)✕ ▾

Das Feld „**Data risposta**“ ist mit dem Protokollierungsdatum der Antwort an die antragstellende Person auszufüllen.

Data risposta

24

Das Feld „**Riesame – data di presentazione della domanda**“ ist auszufüllen, wenn Schritt 14 des Flussdiagramms ausgeführt wird.

Riesame - Data di presentazione della domanda

24

Das Feld „**Riesame – Esito**“ ist auszufüllen, wenn Schritt 16 des Flussdiagramms ausgeführt wird, wobei eine der folgenden Optionen zu wählen ist: „Accoglimento“, „Differimento“, „Rifiuto parziale“, „Rifiuto totale“.

Riesame - Esito

Seleziona ▾

Riesame - Esito

Seleziona ▲

🔍

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

Falls im Feld „Esito“ die Option „Differimento“, „Rifiuto parziale“ oder „Rifiuto totale“ gewählt wird, ist das Feld „**Motivi del rifiuto parziale, del rifiuto totale o del differimento**“ auszufüllen. Es handelt sich dabei um ein offenes Textfeld:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Das Feld „**Riesame – Data risposta**“ ist mit dem Protokollierungsdatum der Antwort an die antragstellende Person auszufüllen.

Riesame - Data risposta

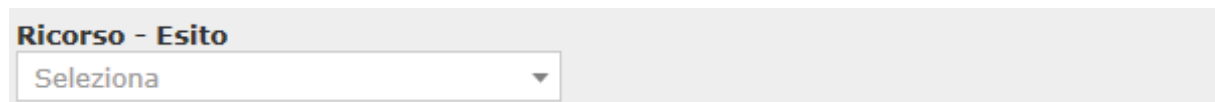
24

Das Feld „**Ricorso – Data di notificazione del ricorso all’Amministrazione**“ ist auszufüllen, wenn Schritt 21 des Flussdiagramms ausgeführt wird:

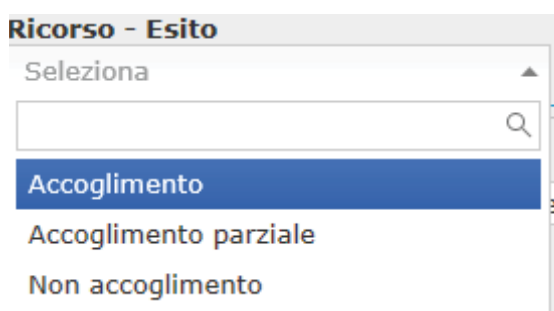


The screenshot shows a form field titled "Ricorso - Data di notificazione del ricorso giurisdizionale all'Amministrazione". Below the title is a text input box and a small red icon with the number "24".

Das Feld „**Ricorso – Esito**“ ist auszufüllen, wenn Schritt 23 des Flussdiagramms ausgeführt wird, wobei eine der folgenden Optionen zu wählen ist: „Accoglimento“, „Accoglimento parziale“, „Non accoglimento“.



The screenshot shows a dropdown menu titled "Ricorso - Esito". The menu is open, showing the text "Seleziona" and a downward arrow.



The screenshot shows the "Ricorso - Esito" dropdown menu with the following options: "Seleziona", "Accoglimento", "Accoglimento parziale", and "Non accoglimento". The "Accoglimento" option is highlighted in blue.

Faszikeltyp: „Accesso agli atti/ Accesso Documentale“

Um ein Faszikel zu erstellen, wählt man „Fascicoli, Crea nuovo fascicolo“.

Scheda fascicolo

Contenuto **Struttura** Trasm.ni Visibilità Eventi

Descrizione*

Caratteri disponibili 2000

Nessuna nota visibile

☐ Personale ☐ Ruolo ☐ RF ☒ Tutti

Caratteri disponibili 2000

Trasmissione rapida

Scegli un modello di trasmissione

Tipologia Fascicolo

Seleziona una tipologia

Accesso dei Consiglieri provinciali
Accesso documentale
Accesso generalizzato e civico

Nun wählt man den Typ „Accesso documentale“. Es erscheinen weitere Felder:

Tipologia Fascicolo

Accesso documentale

Progressivo

AOO

PAT

Data di arrivo della domanda *

24

Nr protocollo della domanda *

Die Felder „**Data di arrivo della domanda**“ und „**Nr protocollo della domanda**“ sind Pflichtfelder (mit * markiert) und müssen erneut eingegeben werden, wenn Schritt 3 des Flussdiagramms (Anlage C) ausgeführt wird.

Das Vorhandensein von Drittbetroffenen wird im Feld „**Presenza controinteressati**“ angegeben, wenn Schritt 4 des Flussdiagramms ausgeführt wird.

Presenza controinteressati

☐ SI ☐ NO



Mit der Schaltfläche  können eventuelle Fehler bei der Auswahl korrigiert werden.

Die Felder betreffend den Ausgang des Verfahrens werden ausgefüllt, wenn Schritt 7 des Flussdiagramms ausgeführt wird. Das Feld „**Esito**“ wird demnach ausgefüllt, indem eine der folgenden Optionen gewählt wird: „Accoglimento“, „Differimento“, „Rifiuto parziale“, „Rifiuto totale“.

Falls im Feld „Esito“ die Option „Differimento“, „Rifiuto parziale“ oder „Rifiuto totale“ gewählt wird, ist das offene Textfeld „**Motivi del rifiuto parziale, del rifiuto totale o del differimento**“ auszufüllen.

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Das Feld „**Data risposta**“ ist mit dem Protokollierungsdatum der Antwort an die antragstellende Person auszufüllen.

Data risposta



Das Feld „**Ricorso – Data di notificazione del ricorso all'Amministrazione**“ ist auszufüllen, wenn Schritt 12 des Flussdiagramms ausgeführt wird:

Ricorso - Data di notificazione del ricorso giurisdizionale all'Amministrazione



Das Feld „**Ricorso – Esito**“ ist auszufüllen, wenn Schritt 14 des Flussdiagramms ausgeführt wird, wobei eine der folgenden Optionen zu wählen ist: „Accoglimento“, „Accoglimento parziale“, „Non accoglimento“.

Ricorso - Esito

Ricorso - Esito

Seleziona ▲

Accoglimento
Accoglimento parziale
Non accoglimento

Zusammenhang zwischen den im P.I.Tre.-System erstellten Faszikeln und dem „Register der Zugänge“

Durch die Protokollierung der Zugangsanträge und der diesbezüglichen Unterlagen (eventuelle Mitteilungen an Drittbetroffene, Antwort auf den Einspruch gegen den Zugang, Mitteilung der zuständigen Struktur mit Angabe des Ablehnungsgrunds usw.) mittels der spezifischen je nach Art des Zugangs vorgesehenen Faszikel erfolgt zugleich die automatische Erstellung des Registers der Zugänge. In diesem Register, das vom Generalsekretariat verwaltet und regelmäßig auf der Website der Region im Bereich „Transparente Verwaltung“ veröffentlicht wird, werden die in die verschiedenen Felder des Protokolls zur Dokumentenverwaltung eingegebenen Informationen dargestellt.



**REGIONE AUTONOMA TRENTINO - ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENTINO-SÜDTIROL**

RICHIESTA DI ACCESSO

☐ **Alla Segreteria¹** _____
(in caso di accesso civico generalizzato e accesso documentale);

oppure

☐ **Al Responsabile per la prevenzione della corruzione e della trasparenza della Regione Autonoma Trentino-Alto Adige/Südtirol** (in caso di accesso civico semplice);

Il sottoscritto/a

(campi obbligatori: nome, cognome e almeno un dato di recapito o contatto)

Dati anagrafici	/ /			
	nome	cognome	luogo di nascita	data di nascita
Residenza				
	indirizzo	CAP	Comune	Prov./Stato estero

¹ In caso di accesso civico generalizzato e accesso documentale l'istanza va presentata alle segreterie delle Strutture competenti per materia (Ripartizioni e/o Segreteria generale della Giunta in quanto struttura equiparata). In caso di accesso civico semplice l'istanza va presentata al Responsabile per la prevenzione della corruzione e della trasparenza, per il tramite della Segreteria generale della Giunta.

Gli indirizzi di posta elettronica cui inviare le domande sono i seguenti:

Segreteria generale della Giunta	giunta@pec.regione.taa.it
Ripartizione I - Pianificazione e programmazione delle risorse	programmazione@pec.regione.taa.it
Ripartizione II - Enti locali, previdenza e competenze ordinarie	ripaist@pec.regione.taa.it
Ripartizione III - Minoranze linguistiche, integrazione europea, e giudici di pace	ripmin@pec.regione.taa.it
Ripartizione IV- Gestione delle risorse umane	personale@pec.regione.taa.it
Ripartizione V- Gestione delle risorse strumentali	risorsestrumentali@pec.regione.taa.it

E' ulteriormente possibile trasmettere istanze di accesso alla casella generale di posta elettronica certificata della Regione Autonoma Trentino - Alto Adige/Südtirol regione.taa@regione.taa.legalmail.it .
Sarà cura del servizio protocollo trasmettere l'istanza all'Ufficio competente

La richiesta di accesso può essere inviata con una delle seguenti modalità:

tramite posta elettronica, tramite posta elettronica certificata (PEC), tramite posta ordinaria all'indirizzo: Regione Autonoma Trentino-Alto Adige/Südtirol – Via Gazzoletti, 2 – 38122 TRENTO, tramite fax al n. 0461/201496, con consegna a mano presso la Segreteria Generale della Giunta regionale – secondo piano – Regione Autonoma Trentino – Alto Adige – Via Gazzoletti, 2 – 38122 TRENTO

Dati di contatto	@		
	indirizzo PEC/e-mail	telefono/cellulare	fax

in qualità di legale rappresentante della società/ditta/persona giuridica/ente		
	Denominazione società/ditta/persona giuridica/ente/altro (da precisare)	Dati inerenti la procura/incarico

in qualità di:		
	<i>campo facoltativo: solo per rilevazioni statistiche (a titolo meramente esemplificativo ricercatore, studente, giornalista, libero professionista, dipendente pubblico, ecc.)</i>	

CHIEDE
(barrare la casella corrispondente)

☐ **accesso civico generalizzato, ai sensi dell'articolo 1, comma 1, lettera 0a) della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16 (riferimento art. 5, comma 2, decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni) per i DOCUMENTI non soggetti ad obbligo di pubblicazione in base alla normativa vigente, detenuti dalla Regione Autonoma Trentino - Alto Adige/Südtirol, e di seguito specificati:**

Documenti	
	Specificare gli elementi necessari per consentire di identificare quanto richiesto.

mediante:

- ☐ **visione**
☐ **rilascio in copia semplice**
☐ **rilascio in copia autenticata**
☐ **rilascio in copia autenticata in bollo (il costo delle marche da bollo è a carico del richiedente);**



☐ **accesso ai documenti amministrativi, ai sensi degli artt. 26 e seguenti della legge regionale 31 luglio 1993, n. 13, e successive modificazioni, nonché D.P.Reg. 16 novembre 2004, n. /L (riferimento: legge n. 241 del 1990, e successive modificazioni.)**

Documenti	
	Specificare gli elementi necessari per consentire di identificare quanto richiesto.

mediante:

- ☐ **visione**
- ☐ **rilascio in copia semplice**
- ☐ **rilascio in copia autenticata**
- ☐ **rilascio in copia autenticata in bollo (il costo delle marche da bollo è a carico del richiedente)**

in quanto portatore dei seguenti interessi giuridicamente rilevanti e motivi di legittimazione collegati al documento richiesto:

Motivazione	



☐ **accesso civico semplice, ai sensi dell'art. 1 della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, per omessa pubblicazione obbligatoria, ai sensi della normativa regionale vigente, dei seguenti DOCUMENTI nella sezione "Amministrazione trasparente" del sito istituzionale della Regione Autonoma Trentino-Alto Adige/Südtirol:**

Documenti	
	<i>Specificare i dati, le informazioni, i documenti di cui è stata omessa, anche parzialmente, la pubblicazione obbligatoria; nel caso in cui il richiedente ne sia a conoscenza, specificare anche la norma che impone la pubblicazione di quanto richiesto.</i>

Tale accesso sarà assicurato tramite pubblicazione e contestuale comunicazione dell'avvenuta pubblicazione (con indicazione del collegamento ipertestuale).



Modalità di esercizio dell'accesso (indicare la modalità prescelta):

- ☐ **visione/ritiro presso la sede dell'Ufficio che detiene i documenti;**
- ☐ **invio al seguente indirizzo di posta elettronica (PEO) / posta elettronica certificata (PEC);**
- ☐ **invio per posta tramite raccomandata con avviso di ricevimento al seguente indirizzo:**

indirizzo _____ **località** _____
provincia _____ **CAP** _____ **Stato** _____;

Il sottoscritto/a, inoltre

DICHIARA

di essere informato/a che potrà essere richiesto il pagamento delle spese effettivamente sostenute e documentate per la riproduzione su supporti materiali (carta o CD)²;

di aver preso visione dell'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento europeo n. 679/2016.

ALLEGA

copia di documento di identità o di riconoscimento (non occorre per le istanze sottoscritte con firma digitale o elettronica qualificata o con identificazione tramite SPID nonché per le istanze consegnate direttamente all'addetto dell'Ufficio e sottoscritte in sua presenza).

(luogo e data)

(firma)

²La trasmissione telematica e la copia di file digitali su supporto fornito dal richiedente (CD o dispositivo USB) sono esenti da pagamento.



**REGIONE AUTONOMA TRENTINO - ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENTINO-SÜDTIROL**

ZUGANGSANTRAG

☐ **An das Sekretariat³**

(falls der allgemeine Bürgerzugang oder der Zugang zu den Verwaltungsunterlagen beantragt wird)

oder

☐ **An den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz der Autonomen Region Trentino-Südtirol** (falls der einfache Bürgerzugang beantragt wird)

Die/Der Unterfertigte

(Pflichtfelder: Vorname, Zuname und mindestens eine Kontaktangabe)

Personalien				
	Vorname	Zuname	Geburtsort	Geburtsdatum
Wohnsitz				
	Adresse	PLZ	Gemeinde	Provinz/ausländ. Staat
Kontakt- daten				
	E-Mail- oder zertifizierte E-Mail-Adresse		Telefon/Mobiltelefon	Fax

ERSUCHT

3 Anträge auf allgemeinen Bürgerzugang und auf Zugang zu den Verwaltungsunterlagen sind beim Sekretariat der für das jeweilige Sachgebiet zuständigen Struktur (Abteilungen und/oder Generalsekretariat der Regionalregierung als gleichgestellte Organisationsstruktur) einzureichen.

Anträge auf einfachen Bürgerzugang sind über das Generalsekretariat der Regionalregierung an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz zu richten.

Die Anträge können an nachstehende E-Mail-Adressen gesandt werden:

Generalsekretariat der Regionalregierung	giunta@pec.regione.taa.it
Abteilung I – Planung und Programmierung der Ressourcen	programmazione@pec.regione.taa.it
Abteilung II – Örtliche Körperschaften, Vorsorge und Ordnungsbefugnisse	ripaist@pec.regione.taa.it
Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte	ripmin@pec.regione.taa.it
Abteilung IV – Verwaltung der Humanressourcen	personale@pec.regione.taa.it
Abteilung V – Verwaltung der technischen Ressourcen	risorsestrumentali@pec.regione.taa.it

Es ist außerdem möglich, den Zugangsantrag an die allgemeine zertifizierte E-Mail-Adresse der Autonomen Region Trentino-Südtirol regione.taa@regione.taa.legalmail.it zu senden.

Der Protokolldienst leitet dann den Antrag an das zuständige Amt weiter.

Der Zugangsantrag kann mit einer der nachstehenden Modalitäten übermittelt werden:

E-Mail; zertifizierte E-Mail; Post an die Adresse: Autonome Region Trentino-Südtirol – Via Gazzoletti 2 – 38122 TRIENT; Fax an die Nr. 0461/201496; persönliche Übergabe beim Generalsekretariat der Regionalregierung – 2. Stock – Autonome Region Trentino-Südtirol – Via Gazzoletti 2 – 38122 TRIENT.

in ihrer Eigenschaft als gesetzliche Vertreterin / in seiner Eigenschaft als gesetzlicher Vertreter der Gesellschaft/Firma/juristischen Person/Körperschaft		
	Name der Gesellschaft/Firma/juristischen Person/Körperschaft o. ä. (bitte genau angeben)	Angaben zur Vollmacht/zum Auftrag

Beschäftigung:	
	Fakultatives Feld, nur für statistische Erhebungen (z. B. Forscher/in, Student/in, Journalist/in, Freiberufler/in, öffentliche/r Bedienstete/r usw.)

(Zutreffendes ankreuzen)

☐ **um allgemeinen Bürgerzugang** im Sinne des Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16, (Bezugsbestimmung: Art. 5 Abs. 2 des gesetzesvertretenden Dekrets vom 14. März 2013, Nr. 33 i.d.g.F) zu nachstehenden DOKUMENTEN, die aufgrund der geltenden Bestimmungen nicht veröffentlichungspflichtig sind und bei der Autonomen Region Trentino-Südtirol aufliegen

Dokumente	
	Die zur Identifizierung der beantragten Dokumente erforderlichen Daten genau angeben

durch:

- ☐ Einsichtnahme
- ☐ Ausstellung einer einfachen Kopie
- ☐ Ausstellung einer beglaubigten Kopie
- ☐ Ausstellung einer beglaubigten Kopie mit Stempelmarke (Die Gebühr für die Stempelmarke geht zu Lasten der antragstellenden Person)



☐ **um Zugang zu den Verwaltungsunterlagen** im Sinne des Art. 26 ff. des Regionalgesetzes vom 31. Juli 1993, Nr. 13 i.d.g.F. sowie des DPRReg. vom 16. November 2004, Nr. 7/L (Bezugsbestimmung: Gesetz Nr. 241/1990 i.d.g.F.)

Dokumente	
	Die zur Identifizierung der beantragten Dokumente erforderlichen Daten genau angeben

durch:

- ☐ Einsichtnahme

- ☐ Ausstellung einer einfachen Kopie
- ☐ Ausstellung einer beglaubigten Kopie
- ☐ Ausstellung einer beglaubigten Kopie mit Stempelmarke (Die Gebühr für die Stempelmarke geht zu Lasten der antragstellenden Person),

da in Zusammenhang mit den Dokumenten, zu denen der Zugang beantragt wird, sie/er Trägerin/Träger nachstehender rechtlich relevanter Interessen ist bzw. nachstehende Legitimierungsgründe bestehen:

Begründung	



☐ **um einfachen Bürgerzugang** im Sinne des Art. 1 des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch das Regionalgesetz vom 15. Dezember 2016, Nr. 16, da die nachstehenden im Sinne der geltenden Regionalbestimmungen der Veröffentlichungspflicht unterliegenden DOKUMENTE nicht unter dem Bereich „Transparente Verwaltung“ der offiziellen Website der Autonomen Region Trentino-Südtirol veröffentlicht wurden:

Dokumente	
	Die veröffentlichungspflichtigen Daten, Informationen, Dokumente angeben, deren Veröffentlichung – auch nur teilweise – unterlassen wurde; wenn bekannt, auch die Bestimmung angeben, in der die Veröffentlichungspflicht vorgesehen ist.

Der Zugang erfolgt durch Veröffentlichung der Dokumente und Mitteilung an die antragstellende Person über die erfolgte Veröffentlichung (mit Angabe des entsprechenden Hyperlinks).



Das Zugangsrecht wird wie folgt ausgeübt (Zutreffendes ankreuzen):

- ☐ Einsichtnahme/Abholen beim Amt, bei dem die Dokumente aufliegen
- ☐ Zusendung an die folgende E-Mail- bzw. zertifizierte E-Mail-Adresse: _____
- ☐ Zusendung mittels Einschreiben mit Rückschein an die folgende Adresse:

Straße/Platz _____ Ort _____
 Provinz _____ PLZ _____ Staat _____

Die/Der Unterfertigte

ERKLÄRT

ferner, dass sie/er darüber in Kenntnis ist, dass für die bestrittenen und nachgewiesenen Kosten für die Wiedergabe der Dokumente auf Datenträgern (Papier oder CD)⁴ eine Gebühr erhoben werden kann;

dass sie/er Einsicht in die Information über die Verarbeitung der personenbezogenen Daten im Sinne des Art. 13 der EU-Verordnung Nr. 679/2016 genommen hat,

und

LEGT

eine Kopie des Personalausweises bei. (Davon wird abgesehen, wenn der Antrag digital oder in einer anderen qualifizierten Form elektronisch signiert ist oder die antragstellende Person mittels SPID identifiziert wird oder wenn der Antrag unmittelbar der/dem Bediensteten des Amtes übergeben und vor dieser/diesem unterzeichnet wird.)

(Ort und Datum)

(Unterschrift)

⁴ Die digitale Übermittlung und das Kopieren von digitalen Dateien auf Datenträger (CD oder USB-Stick), die von der antragstellenden Person zur Verfügung gestellt werden, sind gebührenfrei.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENTINO-SÜDTIROL**

**RICHIESTA DI RIESAME
(per il richiedente accesso)**

Al Responsabile per la prevenzione della corruzione e della trasparenza della Regione Autonoma Trentino-Alto Adige/Südtirol

**per il tramite
della Segreteria della Segreteria generale della Giunta**

giunta@pec.regione.taa.it

e p.c.

**Al Responsabile _____
(dirigente responsabile a decidere in merito all'istanza di accesso civico generalizzato)**

Il sottoscritto/a

(campi obbligatori: nome, cognome e almeno un dato di recapito o contatto)

Dati anagrafici	_____ / ____ / ____			
	nome _____	cognome _____	luogo di nascita _____	data di nascita _____

Residenza	_____			
	indirizzo _____	CAP _____	Comune _____	Prov./Stato estero _____

Dati di contatto	_____ @ _____		
	indirizzo PEC/e-mail _____	telefono/cellulare _____	fax _____

*in riferimento all'istanza di accesso civico generalizzato presentata in data _____
prot. n. _____, con il seguente esito:*

- ☐ *diniego totale dell'accesso*
- ☐ *diniego parziale dell'accesso*
- ☐ *differimento dell'accesso*

*come da comunicazione a firma del Responsabile _____ prot. n. _____
del _____, inviata a mezzo _____ e ricevuto in
data _____;*

oppure

- ☐ è mancata dall'Ufficio la risposta nei termini previsti dalla legge,

CHIEDE

il **RIESAME dell'istanza presentata**, ai sensi dell'art. 5, comma 7, del decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni, con le seguenti motivazioni:

CHIEDE INOLTRE,

che le comunicazioni inerenti la presente richiesta di riesame siano inviate:
(barrare la modalità prescelta e compilare le parti relative)

- ☐ al seguente indirizzo di posta elettronica (PEO) / posta elettronica certificata (PEC);

- ☐ al seguente indirizzo postale;

indirizzo _____ località _____
_____ provincia _____ CAP _____ Stato
_____;

DICHIARA

- di essere informato/a che potrà essere richiesto il pagamento delle spese effettivamente sostenute e documentate per la riproduzione su supporti materiali dei documenti richiesti (carta o CD)⁵;
- di aver preso visione dell'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del d.lgs. n. 196 del 2003.

ALLEGA

copia di documento di identità o di riconoscimento (non occorre per le istanze sottoscritte con firma digitale o elettronica qualificata o con identificazione tramite SPID nonché per le istanze consegnate direttamente all'addetto dell'Ufficio e sottoscritte in sua presenza).

(luogo e data)

(firma)

⁵ La trasmissione telematica e la copia di file digitali su supporto fornito dal richiedente (CD o dispositivo USB) sono esenti da pagamento.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL**

**ANTRAG AUF ÜBERPRÜFUNG
(für die um Zugang ansuchende Person)**

An den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz der Autonomen Region Trentino-Südtirol

**über
das Sekretariat des Generalsekretariats der Regionalregierung**

giunta@pec.regione.taa.it

u. z. K.

**An die Verantwortliche / An den Verantwortlichen _____
(für die Entscheidung über den Antrag auf allgemeinen Bürgerzugang verantwortliche Führungskraft)**

Die/Der Unterfertigte

(Pflichtfelder: Vorname, Zuname und mindestens eine Kontaktangabe)

Personalien				
	Vorname	Zuname	Geburtsort	Geburtsdatum
Wohnsitz				
	Adresse	PLZ	Gemeinde	Provinz/ausländ. Staat
Kontaktdaten				
	E-Mail- oder zertifizierte E-Mail-Adresse	Telefon/Mobiltelefon	Fax	

ERSUCHT

in Bezug auf den Antrag auf allgemeinen Bürgerzugang vom _____, Prot. Nr. _____,

der mit Mitteilung der/des Verantwortlichen _____ Prot. Nr. _____ vom _____ (die mittels _____ zugesandt und am _____ erhalten wurde) mit folgendem Ergebnis beantwortet wurde:

- ☐ der Zugang wurde gänzlich verweigert
☐ der Zugang wurde teilweise verweigert
☐ der Zugang wurde aufgeschoben

bzw.

☐ der Antrag wurde in der gesetzlich vorgesehenen Frist vom zuständigen Amt nicht beantwortet

um **ÜBERPRÜFUNG des eingereichten Antrags** im Sinne des Art. 5 Abs. 7 des gesetzesvertretenden Dekrets vom 14. März 2013, Nr. 33 i.d.g.F. aus den nachstehenden Gründen:

Sie/Er

ERSUCHT FERNER

darum, dass die Mitteilungen in Zusammenhag mit diesem Antrag wie folgt zugesandt werden:
(Zutreffendes ankreuzen und ausfüllen)

☐ an die nachstehende E-Mail- bzw. zertifizierte E-Mail-Adresse:

☐ per Post an die nachstehende Adresse:

Straße/Platz _____ Ort _____
Provinz _____ PLZ _____ Staat _____

Die/Der Unterfertigte

ERKLÄRT

ferner, dass sie/er darüber in Kenntnis ist, dass für die bestrittenen und nachgewiesenen Kosten für die Wiedergabe der beantragten Dokumente auf Datenträgern (Papier oder CD)⁶ eine Gebühr erhoben werden kann;

dass sie/er Einsicht in die Information über die Verarbeitung der personenbezogenen Daten im Sinne des Art. 13 der EU-Verordnung Nr. 679/2016 genommen hat,

und

LEGT

eine Kopie des Personalausweises bei. (Davon wird abgesehen, wenn der Antrag digital oder in einer anderen qualifizierten Form elektronisch signiert ist oder die antragstellende Person mittels SPID identifiziert wird oder wenn der Antrag unmittelbar der/dem Bediensteten des Amtes übergeben und vor dieser/diesem unterzeichnet wird.)

(Ort und Datum)

(Unterschrift)

⁶ Die digitale Übermittlung und das Kopieren von digitalen Dateien auf Datenträger (CD oder USB-Stick), die von der antragstellenden Person zur Verfügung gestellt werden, sind gebührenfrei.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL**

**RICHIESTA DI RIESAME
(del controinteressato)**

Al Responsabile per la prevenzione della corruzione e della trasparenza della Regione Autonoma Trentino-Alto Adige/Südtirol

**per il tramite
della Segreteria della Segreteria generale della Giunta**

giunta@pec.regione.taa.it

e p.c.

**Al Responsabile _____
(dirigente responsabile che ha comunicato l'accoglimento dell'istanza di accesso)**

Il sottoscritto/a

(campi obbligatori: nome, cognome e almeno un dato di recapito o contatto)

Dati anagrafici	_____ / ____ / ____			
	nome _____	cognome _____	luogo di nascita _____	data di nascita _____

Residenza	_____			
	indirizzo _____	CAP _____	Comune _____	Prov./Stato estero _____

Dati di contatto	_____ @ _____		
	indirizzo PEC/e-mail _____	telefono/cellulare _____	fax _____

in riferimento al non accoglimento dell'opposizione presentata in data _____ prot. n. _____ come da comunicazione a firma del Responsabile _____ prot. n. _____ del _____, inviata a mezzo _____ e ricevuto in data _____,

e dell'accoglimento dell'istanza di accesso come da comunicazione a firma del Responsabile _____ prot. n. _____ del _____, inviata a mezzo _____ e ricevuto in data _____;

CHIEDE

il RIESAME dell'opposizione e del relativo accoglimento dell'istanza di accesso, ai sensi dell'art. 5, comma 9, del decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni, con le seguenti motivazioni:

CHIEDE INOLTRE,

che le comunicazioni inerenti la presente richiesta di riesame siano inviate:
(barrare la modalità prescelta e compilare le parti relative)

☐ al seguente indirizzo di posta elettronica (PEO) / posta elettronica certificata (PEC);

☐ al seguente indirizzo postale;

indirizzo _____ localit  _____
_____ provincia _____ CAP _____ Stato
_____;

DICHIARA

- di essere informato/a che potr  essere richiesto il pagamento delle spese effettivamente sostenute e documentate per la riproduzione su supporti materiali dei documenti richiesti (carta o CD)⁷;
- di aver preso visione dell'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del d.lgs. n. 196 del 2003.

ALLEGA

copia di documento di identit  o di riconoscimento (non occorre per le istanze sottoscritte con firma digitale o elettronica qualificata o con identificazione tramite SPID nonch  per le istanze consegnate direttamente all'addetto dell'Ufficio e sottoscritte in sua presenza).

(luogo e data) (firma)

⁷ La trasmissione telematica e la copia di file digitali su supporto fornito dal richiedente (CD o dispositivo USB) sono esenti da pagamento.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL**

**ANTRAG AUF ÜBERPRÜFUNG
(für Drittbetroffene)**

An den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz der Autonomen Region Trentino-Südtirol

**über
das Sekretariat des Generalsekretariats der Regionalregierung**

giunta@pec.regione.taa.it

u. z. K.

**An die Verantwortliche / An den Verantwortlichen _____
(verantwortliche Führungskraft, welche die Annahme des Zugangsantrags mitgeteilt hat)**

Die/Der Unterfertigte

(Pflichtfelder: Vorname, Zuname und mindestens eine Kontaktangabe)

Personalien				
	Vorname	Zuname	Geburtsort	Geburtsdatum
Wohnsitz				
	Adresse	PLZ	Gemeinde	Provinz/ausländ. Staat
Kontaktdaten				
	E-Mail- oder zertifizierte E-Mail-Adresse	Telefon/Mobiltelefon	Fax	

ERSUCHT

in Bezug auf die Ablehnung des Einspruchs vom _____, Prot. Nr. _____, laut Mitteilung der/des Verantwortlichen _____ Prot. Nr. _____ vom _____ (die mittels _____ zugesandt und am _____ erhalten wurde)

sowie in Bezug auf die Annahme des Zugangsantrags laut Mitteilung der/des Verantwortlichen _____ Prot. Nr. _____ vom _____ (die mittels _____ zugesandt und am _____ erhalten wurde)

um **ÜBERPRÜFUNG des eingelegten Einspruchs und der Annahme des Zugangsantrags** im Sinne des Art. 5 Abs. 9 des gesetzesvertretenden Dekrets vom 14. März 2013, Nr. 33 i.d.g.F. aus den nachstehenden Gründen:

Sie/Er

ERSUCHT FERNER

darum, dass die Mitteilungen in Zusammenhag mit diesem Antrag wie folgt zugesandt werden:
(Zutreffendes ankreuzen und ausfüllen)

☐ an die nachstehende E-Mail- bzw. zertifizierte E-Mail-Adresse:

☐ per Post an die nachstehende Adresse:

Straße/Platz _____ Ort _____
Provinz _____ PLZ _____ Staat _____

Die/Der Unterfertigte

ERKLÄRT

ferner, dass sie/er darüber in Kenntnis ist, dass für die bestrittenen und nachgewiesenen Kosten für die Wiedergabe der beantragten Dokumente auf Datenträgern (Papier oder CD)⁸ eine Gebühr erhoben werden kann;

dass sie/er Einsicht in die Information über die Verarbeitung der personenbezogenen Daten im Sinne des Art. 13 der EU-Verordnung Nr. 679/2016 genommen hat,

und

LEGT

eine Kopie des Personalausweises bei. (Davon wird abgesehen, wenn der Antrag digital oder in einer anderen qualifizierten Form elektronisch signiert ist oder die antragstellende Person mittels SPID identifiziert wird oder wenn der Antrag unmittelbar der/dem Bediensteten des Amtes übergeben und vor dieser/diesem unterzeichnet wird.)

(Ort und Datum)

(Unterschrift)

⁸ Die digitale Übermittlung und das Kopieren von digitalen Dateien auf Datenträger (CD oder USB-Stick), die von der antragstellenden Person zur Verfügung gestellt werden, sind gebührenfrei.

Informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento europeo n. 679/2016 connessa all' Istanza di Accesso/Riesame

Titolare del trattamento

Ai sensi dell'art. 13 del Regolamento (UE) n. 2016/679 – “Regolamento del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)” (di seguito denominato “Regolamento”), la Regione Autonoma Trentino -Alto Adige/Südtirol di seguito “Regione”, con sede via Gazzoletti n.2, Trento, in qualità di “Titolare” del trattamento dei dati personali, è tenuta a comunicare ai richiedenti accesso informazioni in merito all'utilizzo dei dati personali forniti.

Il Responsabile della protezione dei dati personali

Il Responsabile della Protezione dei Dati RPD-DPO della Regione è Il Consorzio dei comuni trentini

Telefono: 04611920717

E-mail: servizioRPD@comunitrentini.it

PEC: consorzio@pec.comunitrentini.it

Finalità e base giuridica del trattamento

Il trattamento dei dati personali viene effettuato dal Titolare, in relazione all'oggetto dell'istanza di accesso, per l'esecuzione di un compito di interesse pubblico connesso al rispetto del principio della pubblicità e della trasparenza cui soggiace l'attività dei pubblici poteri e pertanto, ai sensi dell'art. 6 comma 1 lett. e) del citato Regolamento non necessita di consenso. I dati personali sono trattati per la seguente finalità: assicurare l'esercizio del diritto di accesso.

Modalità di trattamento

I dati personali vengono trattati con sistemi informatici e/o manuali attraverso procedure adeguate a garantire la sicurezza e la riservatezza degli stessi.

Responsabili esterni del trattamento

La Regione può avvalersi di soggetti terzi per l'espletamento di attività e relativi trattamenti di dati personali di cui mantiene la titolarità. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli di esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati.

La Regione formalizza istruzioni, compiti ed oneri in capo a tali soggetti terzi con la designazione degli stessi a "Responsabili del trattamento" e sottopone tali soggetti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia.

Soggetti autorizzati al trattamento

I dati personali sono trattati da personale interno previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei dati personali.

Destinatari dei dati personali

I dati personali trattati non sono oggetto di comunicazione ad altri soggetti pubblici pubblici o privati o di diffusione.

Trasferimento dei dati personali a Paesi extra UE

I dati personali trattati non sono trasferiti al di fuori dell'Unione europea.

Periodo di conservazione

I dati personali sono conservati per il periodo strettamente necessario all'esecuzione del compito o della funzione di interesse pubblico e comunque sulla base della vigente normativa in materia di conservazione della documentazione e degli archivi della pubblica amministrazione e potrà protrarsi, nell'osservanza di tali disposizioni, anche a tempo indeterminato.

All'interessato al trattamento dei dati personali sono riconosciuti i seguenti diritti:

- richiedere la conferma dell'esistenza o meno dei dati che lo riguardano;
- ottenere la loro comunicazione in forma intelligibile;
- richiedere di conoscere le finalità e modalità del trattamento;
- ottenere la rettifica, la cancellazione, la limitazione o la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- richiedere la portabilità dei dati;
- aggiornare, correggere o integrare i dati che lo riguardano;
- opporsi, per motivi legittimi, al trattamento dei dati;
- di proporre reclamo al Garante per la protezione dei dati personali.

Conferimento dei dati

Il conferimento dei dati personali è obbligatorio e necessario per le finalità sopra indicate. Il suo mancato conferimento comporterà l'impossibilità di dare corso alla richiesta di accesso.

Information über die Verarbeitung personenbezogener Daten – Art. 13 der EU-Verordnung Nr. 679/2016 in Zusammenhang mit dem ZUGANGSANTRAG

Verantwortlicher für die Datenverarbeitung

Die Autonome Region Trentino-Südtirol, in der Folge „Region“ genannt, mit Sitz in Trient, Via Gazzoletti 2, in ihrer Eigenschaft als Inhaberin der Verarbeitung personenbezogener Daten ist im Sinne des Art. 13 des Verordnung (EU) Nr. 2016/679 – „Verordnung des Europäischen Parlaments zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“, in der Folge „Verordnung“ genannt, dazu verpflichtet, die Personen, die um Zugang ansuchen, über die Verwendung der bereitgestellten personenbezogenen Daten zu informieren.

Datenschutzbeauftragter

Der Datenschutzbeauftragte der Region ist der Gemeindenverband der Provinz Trient

Telefon: 04611920717

E-Mail: servizioRPD@comunitrentini.it

Zertifizierte E-Mail: consorzio@pec.comunitrentini.it

Zweck und Rechtsgrundlage der Datenverarbeitung

Die Verarbeitung der Daten, die Gegenstand des Zugangsantrag sind, wird vom Verantwortlichen für die Erfüllung einer Aufgabe im öffentlichen Interesse unter Beachtung des Grundsatzes der Bekanntmachung und der Transparenz, dem die Tätigkeit der öffentlichen Behörden unterliegt, wahrgenommen. Die personenbezogenen Daten werden zwecks Gewährleistung der Ausübung des Zugangsrechts verarbeitet.

Verarbeitungsmodalitäten

Die Verarbeitung der personenbezogenen Daten erfolgt mittels EDV und/oder händisch unter Anwendung von Verfahren, die die Sicherheit und die Vertraulichkeit der Daten gewährleisten.

Externe Auftragsverarbeiter

Die Region kann mit der Ausübung von Tätigkeiten und der entsprechenden Verarbeitung personenbezogener Daten, für die sie verantwortlich ist, Dritte beauftragen. Diese müssen gemäß den Gesetzesbestimmungen Erfahrungs-, Kompetenz- und Zuverlässigkeitsstandards unter Beachtung der geltenden Bestimmungen in Sachen Datenverarbeitung – Datensicherheit inbegriffen – gewährleisten.

Bei der Beauftragung Dritter als Auftragsverarbeiter legt die Region Anleitungen, Aufgaben und Pflichten für dieselben fest. Sie unterzieht diese Rechtssubjekte periodischen Kontrollen, um das Niveau der Garantien zu überprüfen.

Zur Datenverarbeitung befugte Personen

Die personenbezogenen Daten werden von internem Personal verarbeitet, das vorab als mit der Verarbeitung beauftragtes Personal ermächtigt und bestellt wurde und dem geeignete Anweisungen im Hinblick auf die anzuwendenden Maßnahmen, Vorkehrungen und Verfahrensweisen zum konkreten Schutz der personenbezogenen Daten erteilt wurden.

Empfänger der personenbezogenen Daten

Die personenbezogenen Daten werden nicht anderen öffentlichen oder privaten Rechtssubjekten oder Medien mitgeteilt.

Weitergabe personenbezogener Daten an Nicht-EU-Länder

Die personenbezogenen Daten werden nicht an Länder außerhalb der Europäischen Union übermittelt.

Dauer der Speicherung

Die Speicherung der personenbezogenen Daten erfolgt für die zur Erfüllung der Aufgabe oder Funktion im öffentlichen Interesse strikt notwendige Zeit und aufgrund der geltenden Bestimmungen in Sachen Aufbewahrung der Dokumente und Archive der öffentlichen Verwaltung. Sie kann unter Beachtung besagter Bestimmungen auch auf unbefristete Zeit erfolgen.

Rechte des von der Verarbeitung personenbezogener Daten betroffenen Person:

- Auskunft über das eventuelle Vorhandensein der sie betreffenden personenbezogenen Daten
- Mitteilung der personenbezogenen Daten in verständlicher Form;
- Informationen über Zwecke und Modalitäten der Datenverarbeitung;
- Berichtigung, Löschung, Einschränkung der Verarbeitung, Anonymisierung oder Sperrung von unrechtmäßig verarbeiteten Daten;
- die Datenübertragbarkeit verlangen;
- Aktualisierung, Berichtigung oder Vervollständigung der sie betreffenden personenbezogenen Daten;
- Widerspruch gegen die Verarbeitung der personenbezogenen Daten aus berechtigten Gründen;
- Einreichung einer Beschwerde bei der Datenschutzbehörde.

Bereitstellung der Daten

Die Bereitstellung der personenbezogenen Daten ist obligatorisch und für die oben genannten Zwecke notwendig. Bei unterlassener Bereitstellung der Daten kann dem Zugangsantrag nicht stattgegeben werden.



Trento / Trient, 4.9.2018

CIRCOLARE/RUNDSCHREIBEN Nr. 11

Oggetto: gestione delle istanze di accesso civico generalizzato, accesso civico (semplice), accesso documentale, tramite il sistema P.I.Tre. e registro degli accessi civici generalizzati.

Alle Dirigenti ed ai Dirigenti di
Ripartizione e Strutture equiparate

Alle Direttrici ed ai Direttori degli Uffici

Al personale regionale
Alle Organizzazioni Sindacali

Betreff: Abwicklung der Anträge auf allgemeinen Bürgerzugang, auf (einfachen) Bürgerzugang sowie auf Zugang zu den Verwaltungsunterlagen über das P.I.Tre.-System und Register der allgemeinen Bürgerzugänge

An die Leiterinnen und Leiter der Abteilungen
und der gleichgestellten
Organisationsstrukturen
An die Direktorinnen und Direktoren der Ämter

An die Regionalbediensteten
An die Gewerkschaften

Gentilissime Signore e gentilissimi Signori,

Sehr geehrte Damen und Herren,

al fine di semplificare le procedure a carico degli uffici e per garantire maggiore trasparenza e tracciabilità nelle procedure è stata implementata nel sistema P.I.Tre la nuova funzionalità concernente la gestione delle diverse fasi procedurali connesse alle istanze di accesso civico generalizzato, istituto giuridico previsto dall'articolo 1, comma 1, lettera 0a) della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, concernente l'ostensibilità dei documenti detenuti dall'amministrazione, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria.

zur Vereinfachung und Verbesserung der Transparenz und Rückverfolgbarkeit der von den Ämtern abzuwickelnden Verfahren wurde im P.I.Tre.-System eine neue Funktion implementiert, welche die Abwicklung der verschiedenen Verfahrensphasen in Zusammenhang mit den Anträgen auf allgemeinen Bürgerzugang betrifft. Dieses neue Rechtsinstitut ist im Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10 – geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16 – vorgesehen und betrifft die Einsehbarkeit von bei der Verwaltung aufliegenden Dokumenten, die über die veröffentlichungspflichtigen Dokumente hinausgehen.

Tale nuova funzionalità introdotta nel sistema consente la gestione delle diverse fasi procedurali relative all'istanza di accesso civico generalizzato ovvero:

- protocollazione delle richieste;
- gestione della fase istruttoria;
- gestione della fase relativa agli eventuali rimedi giurisdizionali e non, da attivare da parte del richiedente, in caso di diniego parziale o totale dell'accesso e quindi richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) o alternativamente, ricorso al difensore civico o alternativamente ricorso al Tribunale amministrativo regionale;
- la verifica in ogni momento dello stato di avanzamento di ogni procedimento;
- la registrazione delle richieste di accesso civico generalizzato pervenute, sottoforma di "Registro degli accessi" ovvero l'estrazione automatica dei files riepilogativi delle richieste pervenute (in tre formati diversi xls, pdf, e xml) che verrà gestita dalla Segreteria generale. Ciò, in osservanza a quanto stabilito nel punto 9 delle Linee guida dell'Autorità nazionale Anticorruzione, approvate con delibera n. 1309 del 28 dicembre 2016, recanti *"Indicazioni operative, ai fini della definizione delle esclusioni e dei limiti di accesso civico di cui all'articolo 5, comma 2, del decreto legislativo n. 33 e successive modificazioni"*, (si legga per la Regione TAA articolo 1, comma 1, lettera 0a) della Legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge

Mit dieser neuen Funktion können die verschiedenen Verfahrensphasen in Zusammenhang mit den Anträgen auf allgemeinen Bürgerzugang abgewickelt werden, d. h.:

- Protokollierung der Anträge;
- Bearbeitung der Anträge;
- Phase betreffend die eventuell von der antragstellenden Person eingeleiteten Rechtsbehelfe (Antrag an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz – RPCT auf Überprüfung der Entscheidung oder Rekurs bei der Volksanwaltschaft oder Rekurs beim Regionalen Verwaltungsgericht), falls der Zugangsantrag teilweise oder ganz abgelehnt wurde;
- jederzeit mögliche Überprüfung des Stands des jeweiligen Verfahrens;
- Erfassung der eingegangenen Anträge auf allgemeinen Bürgerzugang in Form eines „Registers der Zugänge“, d. h. automatische Extraktion der Dateien der eingegangenen Anträge (in den drei Dateiformaten .xls, .pdf und .xml). Dieser Schritt wird vom Generalsekretariat durchgeführt. Dadurch wird den Bestimmungen laut Z. 9 der mit Beschluss der nationalen Antikorruptionsbehörde (ANAC) vom 28. Dezember 2016, Nr. 1309 genehmigten Richtlinien entsprochen, die Anleitungen zur Bestimmung der Fälle enthalten, in denen der Bürgerzugang laut Art. 5 Abs. 2 des gesetzesvertretenden Dekrets Nr. 33 i.d.g.F. Ausnahmen und Einschränkungen unterliegt (in Bezug auf die Region Trentino-Südtirol siehe Art.

regionale 15 dicembre 2016, n. 16).

1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16).

Nelle predette linee guida, l'Autorità raccomanda infatti, la raccolta organizzata delle richieste di accesso civico generalizzato sottoforma di "Registro" il quale deve contenere l'elenco delle richieste con l'oggetto e la data, il relativo esito con la data della decisione, da pubblicare nel sito istituzionale dell'Amministrazione regionale, oscurando i dati personali eventualmente presenti.

Il Registro degli accessi, oltre ad essere funzionale per il monitoraggio che in quest'ambito l'Autorità periodicamente intende svolgere, è anche utile per l'Amministrazione, al fine di rendere note le tipologie di documenti sulle quali è stato consentito l'accesso in una ottica di sempre maggiore semplificazione delle attività.

Con l'occasione dell'introduzione della nuova funzionalità finalizzata al monitoraggio delle istanze di accesso civico generalizzato, nel fascicolo tipizzato con classificazione 6.3 accesso ai documenti amministrativi, è stata inserita un'ulteriore tipologia di registrazione degli accessi ai documenti amministrativi, ovvero l'accesso agli atti o accesso documentale (tipologia fascicolo "Accesso documentale").

Pertanto, ogni richiesta di accesso dovrà preliminarmente essere ricondotta alla propria fattispecie giuridica e conseguentemente inserita nel sistema P.I.Tre nel fascicolo 6.3 accesso ai documenti amministrativi

Die Antikorruptionsbehörde empfiehlt in genannten Richtlinien nämlich die organisierte Erfassung der Anträge auf allgemeinen Bürgerzugang in Form eines „Registers“, das das Verzeichnis der eingegangenen Anträge mit Gegenstand und Datum sowie Ergebnis und Datum der diesbezüglichen Entscheidung enthält und auf der offiziellen Website der Regionalverwaltung zu veröffentlichen ist, wobei eventuell vorhandene personenbezogene Daten unkenntlich zu machen sind.

Der Register der Zugänge ist nicht nur für das Monitoring nützlich, das die Antikorruptionsbehörde regelmäßig in diesem Bereich durchzuführen gedenkt, sondern im Hinblick auf die Vereinfachung der Tätigkeit auch für die Verwaltung, um die Art der Dokumente bekannt zu geben, auf die der Bürgerzugang erlaubt ist.

Anlässlich der Einführung dieser neuen Funktion zum Monitoring der Anträge auf allgemeinen Bürgerzugang wurde im Faszikeltyp „6.3 accesso ai documenti amministrativi“ zur Registrierung der Dokumentenzugänge ein weiterer Zugangstyp vorgesehen, nämlich der Zugang zu den Verwaltungsunterlagen (Faszikeltyp: „Accesso documentale“).

Dementsprechend muss jeder Zugangsantrag vorab der jeweiligen Kategorie zugeordnet und in das jeweilige Faszikel unter 6.3 „Accesso ai documenti amministrativi“ im P.I.Tre.-System eingegeben werden.

scegliendo uno dei fascicoli corrispondenti alla tipologia individuata.

Al fine di agevolare gli uffici nello svolgimento delle attività sopra descritte, si allegano per ogni utile consultazione i seguenti documenti:

- allegato A – breve sintesi sulle disposizioni in materia di accesso;
- allegato B – modalità di gestione delle domande di accesso tramite P.I.Tre;
- Allegato C - diagramma di flusso delle attività in cui sono indicati gli attori del processo e le operazioni da compiere con riferimento all'accesso civico generalizzato;
- modello per le richieste di accesso civico generalizzato, accesso documentale e accesso civico semplice (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico" unitamente alla presente circolare);
- modello per la richiesta di riesame al Responsabile per la prevenzione della corruzione e della trasparenza (RPCT) da parte del richiedente accesso in caso di diniego totale, parziale, differimento o mancata risposta dell'accesso civico generalizzato (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico unitamente alla presente circolare);

Um die Durchführung der oben beschriebenen Tätigkeiten zu erleichtern, werden nachstehende Unterlagen beigelegt:

- Anlage A – Übersicht über die Regelung des Zugangsrechts;
- Anlage B – Modalitäten für die Abwicklung der Zugangsanträge mittels Eingabe in das P.I.Tre-System;
- Anlage C – Flussdiagramm der Aktivitäten in Bezug auf den allgemeinen Bürgerzugang mit Angabe der Akteure und der durchzuführenden Schritte;
- Vordruck für die Anträge auf allgemeinen Bürgerzugang, Zugang zu den Verwaltungsunterlagen und einfachen Bürgerzugang (der Vordruck ist zusammen mit diesem Rundschreiben auf der offiziellen Website unter dem Bereich „Transparente Verwaltung – Sonstige Inhalte – Bürgerzugang“ veröffentlicht);
- Vordruck für den von der antragstellenden Person an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz (RPCT) zu richtenden Antrag auf Überprüfung für den Fall, dass der Antrag auf allgemeinen Bürgerzugang ganz oder teilweise abgelehnt oder der Zugang aufgeschoben oder keine Antwort erteilt wurde (der Vordruck ist zusammen mit diesem Rundschreiben auf der offiziellen Website unter dem Bereich „Transparente Verwaltung – Sonstige Inhalte – Bürgerzugang“ veröffentlicht);

- modello per la richiesta di riesame al Responsabile per la prevenzione della corruzione e della trasparenza (RPCT) da parte dei controinteressati in caso di opposizione all'accoglimento dell'istanza di accesso civico generalizzato (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico unitamente alla presente circolare).

- Vordruck für den von den Drittbetroffenen an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz (RPCT) zu richtenden Antrag auf Überprüfung für den Fall, dass gegen den Antrag auf allgemeinen Bürgerzugang Einspruch erhoben wurde (der Vordruck ist zusammen mit diesem Rundschreiben auf der offiziellen Website unter dem Bereich „Transparente Verwaltung – Sonstige Inhalte – Bürgerzugang“ veröffentlicht).

Cordiali saluti.

Mit freundlichen Grüßen

IL SEGRETARIO GENERALE
DER GENERALEKRETÄR

Alexander Steiner

(firmato digitalmente - digital signiert)

AS/RG/CG

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Dokument in Papierform übermittelt wird, stellt es die für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

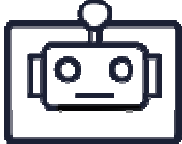
Informativa sui trattamenti di dati personali effettuati per la gestione delle procedure di selezione e concorsuali del personale

La informiamo che il Regolamento UE 2016/679 e il Decreto legislativo 196/2003 hanno ad oggetto la protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Gli artt. 13 e 14 del Regolamento UE 2016/679 prevedono che il soggetto i cui dati vengono trattati (Lei, in qualità di interessato) venga debitamente informato sul trattamento medesimo.

TITOLARE	TITOLARE
 Chi decide le modalità e le finalità del trattamento? L'Ente _____, in qualità di titolare/contitolare del trattamento, decide le modalità e le finalità del trattamento.	Ente _____ con sede a _____ in via _____ • e-mail _____ • sito internet _____ • PEC _____
RPD	RESPONSABILE PER LA PROTEZIONE DATI
 Chi è il RPD? Il Responsabile per la protezione dei dati (RPD) è il soggetto individuato dal titolare del trattamento che svolge funzioni di supporto e controllo, sull'applicazione del Regolamento UE.	Consorzio dei Comuni Trentini, con sede a Trento, in via Torre Verde 23 • e-mail servizioRPD@comunitrentini.it • sito internet www.comunitrentini.it
DATI	CATEGORIE DI DATI PERSONALI TRATTATI
 Quali dati raccogliamo? Raccogliamo diverse categorie di dati personali, a seconda della finalità del trattamento.	• <i>dati identificativi semplici (es. nome, cognome, data di nascita, telefono, e-mail, indirizzo, codice fiscale)</i> • <i>categorie particolari di dati (es. categorie protette, salute)</i> • <i>dati di localizzazione (es. indirizzo IP)</i> • <i>dati giudiziari (es. procedimenti/condanne penali; misure di sicurezza)</i>
FONTE	FONTE DEI DATI
 Dove sono stati raccolti i dati? I dati possono essere raccolti direttamente	☐ sono stati raccolti presso l'interessato (lei medesimo). In caso di verifiche sulla veridicità delle dichiarazioni rese, i dati possono essere raccolti presso altre Pubbliche Amministrazioni e/o Autorità giudiziaria.

presso l'interessato, oppure presso enti terzi che ne hanno fatto comunicazione al titolare del trattamento.	
SCOPO	FINALITÀ DEL TRATTAMENTO
 A che scopo trattiamo i Suoi dati? Il trattamento dei Suoi dati è realizzato per diverse finalità.	I dati personali vengono raccolti e trattati per le seguenti attività: - verifica del possesso dei requisiti di accesso alla selezione pubblica; - predisposizione della documentazione per la procedura selettiva/concorsuale; - verifiche legate al Covid-19 per l'accesso ai luoghi di svolgimento delle prove selettive/concorsuali (in particolare, autodichiarazione di non essere sottoposto a misure di isolamento); - redazione dei verbali di selezione e di valutazione da parte della Commissione giudicatrice; - espletamento delle prove d'esame e relativa valutazione; - formazione della graduatoria; - comunicazione dei dati a terzi nel caso di esercizio del diritto di accesso; - pubblicazione del dato sul sito web istituzionale dell'ente, alla pagina <i>Amministrazione trasparente</i>. Inoltre, i dati personali possono essere trattati per finalità diverse da quelle per le quali sono stati raccolti, garantendo in ogni caso la coerenza con i fini istituzionali.
CONDIZIONI	BASE GIURIDICA DEL TRATTAMENTO
 Quale condizione rende lecito il trattamento? Il trattamento, per essere lecito, deve essere fondato su un'adeguata base giuridica.	I dati sono trattati per l'esecuzione di un compito o di una funzione di interesse pubblico. In particolare, la base giuridica è rinvenibile nelle seguenti disposizioni: d.lgs. 33/2013 e legge regionale 10/2014 (normativa in materia di trasparenza amministrativa) legge regionale 2/2018 e ss. (Codice degli enti locali della Regione autonoma Trentino-Alto Adige) d.lgs. 82/2005 (Codice amministrazione digitale) Legge provinciale 23/1992 (legge provinciale attività amministrativa) Regolamento per le procedure di assunzione del personale Bando di concorso/selezione Ordinanza Ministero della salute d.d. 25.05.2022 (ultimo protocollo salute e sicurezza in periodo Covid-19)
MODALITÀ	MODALITÀ DEL TRATTAMENTO

 I Suoi dati sono al sicuro? Nel trattare i Suoi dati adottiamo specifiche misure di sicurezza per prevenire la perdita, gli usi illeciti o non corretti e gli accessi non autorizzati ai tuoi dati personali.	I dati sono trattati con strumenti informatici o manuali e tramite procedure adeguate a garantirne la sicurezza e la riservatezza. Il trattamento è effettuato, esclusivamente per le finalità sopra indicate, da personale specificamente autorizzato in relazione ai compiti e alle mansioni assegnate e nel rispetto del segreto professionale e del segreto di ufficio. Sono adottate specifiche misure di sicurezza per prevenire la perdita dei dati personali, usi illeciti o non corretti ed accessi non autorizzati.
CONSERVAZIONE	PERIODO DI CONSERVAZIONE DEI DATI
 Per quanto tempo conserviamo i Suoi dati? Conserviamo i Suoi dati per un periodo di tempo che varia in base alle finalità del trattamento.	I dati sono conservati per il periodo strettamente necessario all'esecuzione del compito o della funzione di interesse pubblico e comunque nei termini di legge. La conservazione dei dati, contenuti nei documenti oggetto di protocollazione, avviene secondo la disciplina dettata dall'art. 44 del Codice dell'Amministrazione digitale (D.lgs. 82/2005), tramite il Polo archivistico regionale dell'Emilia-Romagna - ParER, a tempo indeterminato.
DESTINATARI	A CHI POSSONO ESSERE COMUNICATI
 A chi potremmo trasmettere i Suoi dati? Per le finalità del trattamento indicate in questa Informativa potremmo trasmettere alcuni Suoi dati a soggetti esterni che agiscono come titolari e/o responsabili del trattamento.	I dati possono essere trasmessi a soggetti esterni operanti, ad esempio: - Autorità e organi di vigilanza e controllo - Pubbliche Autorità che ne facciano espressa richiesta per finalità amministrative o istituzionali - società, associazioni o professionisti che prestino attività di assistenza o consulenza (es. membri esterni commissioni) - fornitore della piattaforma informatica utilizzata (es. sito web o software per selezione/concorso) - altre pubbliche amministrazioni che usufruiscono della graduatoria. I dati sono oggetto di diffusione tramite sito web istituzionale, limitatamente agli obblighi di trasparenza amministrativa imposti ex lege.
AUTORIZZATI	CHI PUÒ TRATTARE I DATI
 Chi sono i soggetti autorizzati a trattare i Suoi dati? I Suoi dati potranno essere trattati dai dipendenti dell'Ente.	I dati possono essere conosciuti da personale specificamente autorizzato in relazione ai compiti e alle mansioni assegnate.

TRASFERIMENTO	TRASFERIMENTO DEI DATI IN PAESI EXTRA UE
 I Suoi dati potranno essere trasferiti all'estero in Paesi fuori dall'Unione Europea? I Suoi dati potrebbero essere trasferiti in Paesi extra-europei. In caso di trasferimento di dati all'estero Le garantiamo il rispetto dei requisiti di legge per il trasferimento.	I dati <i>sono/non sono</i> oggetto di trasferimento delle banche dati fuori dall'Unione Europea. <i>In caso di trasferimento i dati sono soggetti alle seguenti garanzie adeguate:</i> • <i>decisione di adeguatezza della Commissione Europea</i> • <i>clausole contrattuali standard</i> • <i>meccanismi di certificazione</i> • <i>codici di condotta</i>
OBBLIGATORIETÀ	OBBLIGATORIETÀ DEL CONFERIMENTO DEI DATI
 Perché è necessario il conferimento dei Suoi dati? Per alcune finalità del trattamento è necessario che Lei conferisca i Suoi dati, senza i quali non potremo fornirLe i nostri servizi. Per altre, Lei è libero di non conferire i Suoi dati; in tal caso, il servizio ulteriore non sarà erogato.	Il conferimento dei dati ha natura: ☐ obbligatoria. Non fornire i dati comporta non osservare obblighi di legge e/o impedire che l'Ente possa l'espletare le proprie funzioni istituzionali e/o erogare il servizio.
DIRITTI	I DIRITTI DELL'INTERESSATO
 Quali sono i Suoi diritti? Può esercitare i diritti che Le sono riconosciuti dal Regolamento Europeo. Ad esempio, può chiedere al titolare l'accesso ai dati che la riguardano, la loro cancellazione, rettifica, integrazione, nonché la limitazione del trattamento. Può inoltre proporre reclamo all'Autorità di controllo competente.	I diritti dell'interessato sono: – richiedere la conferma dell'esistenza o meno dei dati che lo riguardano; – ottenere la loro comunicazione in forma intelligibile; – richiedere di conoscere le finalità e modalità del trattamento; – ottenere la rettifica, l'eventuale cancellazione, la limitazione o la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge; – aggiornare, correggere o integrare i dati che lo riguardano; – opporsi, per motivi legittimi, al trattamento dei dati; – di proporre reclamo al Garante per la protezione dei dati personali.

MODIFICHE E AGGIORNAMENTI: la presente informativa può essere soggetta a modifiche e/o integrazioni.

Versione di data _____



Consorzio dei
Comuni Trentini

Trento, 09 agosto 2022
LM/MGT/PG/MG/GF/ed

Al Sindaco/Commissario
Al Segretario
Al Referente privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE

OGGETTO: Servizio privacy RPD – LINEE GUIDA su pubblicazione degli atti relativi alle procedure di selezione pubblica con riferimento al trattamento dei dati personali.

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto, elaborata anche grazie al contributo della **Commissione anticorruzione, trasparenza e accesso agli atti** dello Scrivente Consorzio.

Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse

rendersi necessario.

Cordiali saluti.

Il Direttore Generale
dott. Marco Riccadonna

Il Presidente
dott. Paride Gianfranceschi





La pubblicazione di documenti relativi a procedure concorsuali/selettive per il reclutamento, a qualsiasi titolo (ad es. anche in caso di avviso di mobilità e di selezioni per posti a tempo determinato), all'albo pretorio per finalità di pubblicità legale, così come la pubblicazione di documenti sul sito dell'ente per finalità di trasparenza e di altre disposizioni normative, anche di natura regolamentare aventi analoga finalità di trasparenza, devono rispettare la disciplina sulla protezione dei dati personali.

La pubblicazione sul sito internet di dati personali costituisce, infatti, un'operazione di diffusione degli stessi, anche nel caso delle pubblicazioni previste ex lege, in quanto comporta la conoscenza di dati personali da parte di un numero indeterminato di soggetti, quali sono i potenziali utenti della rete internet.

Dev'essere pertanto applicato il principio di "minimizzazione dei dati" personali, espresso dall'art. 5 del Regolamento (UE) n. 679/2016, per cui è consentita la diffusione dei soli dati personali la cui inclusione in atti e documenti sia realmente necessaria e proporzionata al raggiungimento delle finalità perseguite.

A. Modalità di regolamentazione del trattamento dei dati personali tramite bando/avviso

Qualora un Ente bandisca una procedura pubblica per il reclutamento è tenuto a:

- pubblicare il bando/avviso all'albo telematico per il periodo necessario a garantirne la pubblicità;
- pubblicare il bando/avviso sul sito istituzionale, nella sezione *Amministrazione trasparente – Bandi di concorso*, per 5 anni calcolati a partire dal 1° gennaio dell'anno successivo alla pubblicazione.

Le regole giuridiche che governano la **pubblicità legale all'albo telematico trentino**, nel caso delle procedure selettive e concorsuali, si rinviengono nell'art. 183 del Codice degli enti locali (legge regionale 3 maggio 2018, n. 2), secondo cui tutte le deliberazioni comunali sono pubblicate sull'albo telematico, per 10 giorni consecutivi, salvo specifiche disposizioni di legge. Tale pubblicazione deve avvenire entro dieci giorni dall'adozione della deliberazione e comporta, alla scadenza del decimo giorno, l'esecutività del provvedimento.

L'art. 1, comma 1, lettera g), della legge regionale 10/2014 attribuisce inoltre agli enti locali la facoltà di pubblicare in **Amministrazione trasparente** integralmente anche i provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti, in luogo dei meri elenchi.

Le regole giuridiche che disciplinano la sezione di **Amministrazione trasparente** dedicata alle procedure concorsuali si rinviengono nell'art. 19, co.1 e co.2 del d.lgs. n. 33/2013 e ss.mm, direttamente applicabile nell'ordinamento locale.

Secondo tale fonte debbono essere pubblicate in *Amministrazione trasparente* dei portali web istituzionali alcune informazioni e documenti:

- bandi di concorso per il reclutamento, a qualsiasi titolo, del personale presso l'amministrazione;
- criteri di valutazione stabiliti dalla Commissione;
- tracce delle prove;
- graduatorie finali, aggiornate con l'eventuale scorrimento degli idonei non vincitori (obbligo di trasparenza inserito dall'art. 1, comma 145, lett. a) della Legge 27.12.2019 n. 160, a decorrere dal 1° gennaio 2020).

La **base giuridica legittimante il trattamento** dei dati personali, oggetto delle pubblicazioni sopra citate, è costituita dalla norma di legge (l'art. 19 del D.lgs. 33/2013), ovvero – in virtù della novella introdotta nel Codice privacy italiano lo scorso anno – anche da **un atto amministrativo generale, rappresentato** – nel caso di specie – **dal bando/avviso di selezione** oppure da specifica norma **regolamentare (regolamento disciplinante le procedure di**





assunzione) nel caso in cui l'ente abbia provveduto alla relativa adozione. Infatti, l'articolo 9, comma 1, lett. a) del D.L. 8 ottobre 2021 n. 139 (convertito con legge 3 dicembre 2021, n. 205) ha innovato il comma 1 dell'articolo 2-ter del D.lgs. 196/2003 (Codice privacy italiano), ammettendo quale legittima base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, oltre alla norma di legge o di regolamento, anche l'emanazione di un atto amministrativo generale.

L'introduzione della nuova base giuridica dell'atto amministrativo generale permette, dunque, oggi la pubblicazione di dati personali comuni, ulteriori rispetto a quelli previsti ex lege, fermi restando i limiti generali di pertinenza, non eccedenza, proporzionalità vigenti per il trattamento dei dati personali¹.

Ad esempio, l'Ente potrebbe avere interesse a pubblicare documenti relativi alle diverse fasi di selezione, per comunicare, in sequenza, diverse informazioni, sia di carattere organizzativo (convocazioni), sia recanti gli esiti delle prove, quali:

- elenco dei soli candidati ammessi alla procedura concorsuale;
- elenco dei soli candidati ammessi alle prove successive.

In questo caso, si propone un fac-simile di paragrafo da inserire nell'avviso/bando di selezione oppure nel regolamento comunale disciplinante le procedure di assunzione per estendere l'utilizzo delle pubblicazioni nella sezione amministrazione trasparente per le fasi di gestione della procedura e delle relative comunicazioni ai candidati:

Nella sezione amministrazione trasparente del sito istituzionale sono pubblicati il nome e cognome () dei candidati che sono stati ammessi a partecipare alla procedura di concorso, selezione o mobilità indetta dal Comune e di coloro che sono stati ammessi a partecipare (**) alle prove di cui si compongono le predette procedure.*

I dati di cui al comma precedente, avendo la finalità di comunicare ai candidati l'avvenuta ammissione alla procedura e la convocazione alle singole prove, rimangono pubblicati fino alla data di pubblicazione della graduatoria finale.

*La graduatoria finale è pubblicata, riportando il nome e cognome del vincitore e dei candidati idonei, per il tempo previsto dalle vigenti disposizioni di legge (***).*

In caso di omonimia, la pubblicazione è integrata dalla data di nascita del candidato.

() Oppure, in alternativa, solamente le iniziali del nome e cognome.*

*(**) Si ricorda che non vanno pubblicati le generalità dei soggetti non ammessi ovvero che non hanno superato le prove.*

*(***) Per le graduatorie finali, rispetto alle quali è prevista espressamente la pubblicazione, non si pone un problema di riservatezza di dati personali, purché la durata della pubblicazione rispetti il termine di 5 anni a decorrere dal 1° gennaio successivo alla data di pubblicazione, ai sensi dell'art. 8 del d.lgs. 33/2013.*

¹La novità normativa richiamata interviene in un contesto nel quale il Garante per la protezione dei dati personali, con svariati provvedimenti, ha sanzionato la PA, censurando il trattamento di dati personali basato unicamente sul consenso espresso dal candidato in sede di iscrizione al concorso. Secondo il Garante (provvedimento del 25 novembre 2021, n. 9732406) "i soggetti pubblici, anche quando operino nello svolgimento di procedure concorsuali, selettive o comunque valutative, prodromiche all'instaurazione del rapporto di lavoro, possono trattare i dati personali degli interessati (art. 4, n. 1, del Regolamento) se il trattamento è necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" (si pensi a specifici obblighi previsti dalla normativa nazionale "per finalità di assunzione", artt. 6, par. 1, lett. c), 9, par. 2, lett. b) e 4; 88 del Regolamento) oppure "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6, par. 1, lett. c) ed e) del Regolamento e art. 2-ter del Codice nel testo vigente al tempo in cui si riferiscono i fatti e le condotte oggetto di contestazione, anteriormente alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139)".





Qualora l'ente non abbia adottato una norma regolamentare o inserito la previsione nel bando in modo da consentire la pubblicazione di nomi e cognomi per il tempo strettamente necessario alla gestione della procedura e decidesse di pubblicare anche altri dati, informazioni e documenti, ulteriori rispetto a quelli previsti dalla legge (ex art. 7 bis d.lgs. 33/2013), dovrà sempre procedere alla indicazione pseudonimizzata² dei dati personali eventualmente presenti.

Secondo la lettura resa dal Garante (cfr. provv.ti 29 aprile 2021, n. 170, doc. web n. [9681778](#); 25 marzo 2021, n. 106, doc. web n. [9584421](#) e 11 marzo 2021, n. 89, doc. web n. [9581028](#)), infatti, ad eccezione delle graduatorie finali di merito, il d.lgs. 33/2013 e le disposizioni in materia di trasparenza non possono costituire idonea base giuridica per la diffusione online della maggior parte degli atti e documenti relativi alle procedure concorsuali, in relazione ai quali, in base al quadro normativo vigente, non è infatti previsto alcun obbligo di pubblicazione obbligatoria per finalità di trasparenza³.

Sul tema il Garante si è pronunciato negli anni con vari provvedimenti di natura sanzionatoria; ex multis si ricorda il provvedimento n. 20 del 30 gennaio 2020, con cui è stata comminata una sanzione al Comune di Colledara (TE) per aver pubblicato illecitamente documenti con dati personali dei candidati ammessi a sostenere le prove scritte (data di nascita, luogo di residenza etc..) e dei candidati ammessi con riserva a sostenere le prove scritte o dei non idonei con indicazione dei motivi di esclusione. Secondo l'Autorità garante non rilevava, nel caso, nemmeno il motivo di uso-notificata del sito web, perché sarebbe stato comunque possibile utilizzare sistemi di password-login che limitino il trattamento dei dati ai diretti interessati. Ed ancora, con il provvedimento n. 154 del 3 settembre 2020 è stato sanzionato il Comune di Casaloldo per la pubblicazione in amministrazione

²Per inciso, a norma dell'art. 4, n. 5 del GDPR, per **pseudonimizzazione** si intende il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Per il concetto di dato anonimo o informazione anonima si veda Considerando 26: "I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato".

Quindi la differenza essenziale è che, mentre un dato pseudonimizzato può correre il rischio di essere ricostruito, tramite un dato anonimo non è possibile risalire/re-identificare l'identità dell'utente.

³Sul punto, già nelle *Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati* (provvedimento n. 243 del 15 maggio 2014), il Garante precisava che: "Con riguardo alla pubblicità degli esiti delle prove concorsuali e delle graduatorie finali – nonché, nei casi (e con le modalità) previsti, dei risultati di prove intermedie – di concorsi e selezioni pubbliche e di altri procedimenti che prevedono la formazione di graduatorie, restano salve le normative di settore che ne regolano tempi e forme di pubblicità (es. affissione presso la sede dell'ente pubblico, pubblicazione nel bollettino dell'amministrazione o, per gli enti locali, all'albo pretorio). **Tale regime di conoscibilità, come già rilevato in passato dal Garante, assolve alla funzione di rendere pubbliche le decisioni adottate dalla commissione esaminatrice e/o dall'ente pubblico procedente, anche al fine di consentire agli interessati l'attivazione delle forme di tutela dei propri diritti e di controllo della legittimità delle procedure concorsuali o selettive. Anche a questo riguardo devono essere diffusi i soli dati pertinenti e non eccedenti riferiti agli interessati.** ... Come già rilevato in passato dal Garante, **al fine di agevolare le modalità di consultazione delle graduatorie** oggetto di pubblicazione in conformità alla disciplina di settore (per finalità diverse dalla trasparenza), **le stesse possono altresì essere messe a disposizione degli interessati in aree ad accesso selezionato dei siti web istituzionali consentendo la consultazione degli esiti delle prove o del procedimento ai soli partecipanti alla procedura concorsuale o selettiva mediante l'attribuzione agli stessi di credenziali di autenticazione** (es. username o password, numero di protocollo o altri estremi identificativi forniti dall'ente agli aventi diritto, oppure mediante utilizzo di dispositivi di autenticazione, quali la carta nazionale dei servizi)."





trasparente degli esiti delle prove intermedie con indicazione dei nominativi dei non idonei, trattamento ritenuto illecito in assenza di idonea base giuridica.

In conclusione, **gli atti aventi valore di notifica personale ai candidati**, riportanti l'elenco dei candidati ammessi (mai gli esclusi) alle diverse fasi concorsuali intermedie debbono essere:

- pseudonimizzati con il ricorso, ad esempio, a codici che consentano solo agli interessati di essere identificati;

oppure:

- pubblicati in apposita area riservata del sito, accessibile solo ai diretti interessati tramite appositi sistemi di autenticazione;

oppure:

- comunicati direttamente agli interessati tramite altro canale istituzionale (es. email/PEC ..).

Solamente qualora questo ulteriore trattamento dei dati (pubblicazione sul sito web dei dati personali dei candidati per le fasi intermedie) sia esplicitamente previsto nel regolamento per la selezione del personale dell'ente o nello specifico bando di concorso e nella relativa informativa, può rinvenirsi idonea base giuridica a legittimare la pubblicazione dei nominativi per esteso, oppure delle iniziali delle generalità, con indicazione della data di nascita in caso di omonimia.

Tali pubblicazioni dovranno - in ogni caso - essere **rimosse dalla pagina *Amministrazione trasparente* al termine della fase cui si riferiscono**, non avendo copertura normativa per finalità di pubblicità oltre al tempo necessario alla mera comunicazione (e dunque mai oltre la chiusura della procedura concorsuale).

Non sono invece da pubblicare, in quanto difetta una specifica giustificazione normativa, in *Amministrazione trasparente*, nella sezione *Bandi di concorso*, i documenti afferenti alla Commissione di concorso/selezione, né riguardo ai curricula vitae, né riguardo alle dichiarazioni di assenza di conflitto di interesse, che andranno invece tenute agli atti.

Nello specifico, i curricula e le dichiarazioni rese dai commissari esterni, incaricati ad hoc dall'ente, andranno inseriti nella sezione *Titolari di incarichi di consulenza e di collaborazione*, mentre per i commissari interni non deve essere diffuso alcunché, in quanto l'attività svolta è considerata attività di servizio.

B. Applicazione dei principi di pertinenza e non eccedenza del trattamento

In tema di **pubblicazioni obbligatorie**, come quelle riferite alle procedure selettive, c'è però da dire che, pur in presenza di una fonte giuridica legittimante il trattamento e in particolare la diffusione dei dati, gli enti sono tenuti a rendere non intellegibili i dati personali non pertinenti e non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione, fermo restando il divieto assoluto di diffusione dei dati relativi allo stato di salute.

Il trattamento dei dati personali, contenuti nei documenti riferiti alle procedure concorsuali, in particolare la loro diffusione, deve dunque essere effettuato dall'ente pubblico, titolare del trattamento, alla luce del **principio di pertinenza e non eccedenza del trattamento** (art. 5, par. 1, lett. a) e c) del Regolamento europeo). Principio ribadito, a livello regionale, dall'art. 1,





comma 3, della LR 10/2014, secondo cui la pubblicazione di documenti, informazioni e dati viene effettuata nel rispetto delle norme in materia di tutela della riservatezza⁴.

Ne discende che i dati concernenti i recapiti degli interessati (utenze di telefonia fissa o mobile, indirizzo di residenza o di posta elettronica, codice fiscale) e quelli concernenti le condizioni di salute degli interessati, compresi i riferimenti a condizioni di invalidità, disabilità o handicap fisici e/o psichici (indicatore Isee, numero di figli disabili, risultati di test psicoattitudinali) non devono formare oggetto di pubblicazione⁵.

In particolare, i dati relativi alla salute, ossia quelli *“attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute”*, non possono essere diffusi in ragione della particolare delicatezza di tale categoria di dati (art. 2-septies, comma 8 e art. 166, comma 2, del Codice privacy e art. 9, parr. 1, 2, 4, del Regolamento europeo).

La pubblicazione dei dati personali contenuti nel provvedimento di approvazione della graduatoria finale di merito è limitata ai dati (nome e cognome) del vincitore e degli idonei inseriti nelle graduatorie finali di merito (con evidenza dello scorrimento della graduatoria medesima).

Si fa presente che le graduatorie finali eventualmente pubblicate anteriormente al 1° gennaio 2020 dovranno essere eliminate dalla sezione *Amministrazione trasparente*, in quanto prive di base giuridica ai fini della pubblicazione.

Nel caso, invece, di graduatorie che contengano dati particolari, che riguardano ad es. candidati appartenenti alle c.d. categorie protette, i dati personali (nome e cognome) non potranno mai essere oggetto di pubblicazione, salvo disporre la pseudonimizzazione (es. tramite codice alfa numerico, conoscibile solamente dall'ente e dal candidato).

⁴Sul punto il Garante per la protezione dei dati personali ha precisato che: *non può comportare alcun automatismo rispetto alla diffusione online dei dati e informazioni personali, né una deroga ai principi in materia di protezione dei dati personali, quali – fra gli altri – quello di “minimizzazione”, in base al quale i dati personali – anche contenuti in atti o documenti la cui diffusione online sia prevista da una specifica base normativa – devono essere non solo “adequati” e “pertinenti”, ma anche “limitati a quanto necessario rispetto alle finalità per le quali sono trattati”* (art. 5, par. 1, lett. c) del Regolamento). *La disciplina di protezione dei dati prevede infatti che il titolare debba mettere “in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento” e debba essere “in grado di dimostrare” di averlo fatto alla luce del principio di responsabilizzazione* (artt. 5, par. 2, 24 e 25, par. 2, del Regolamento).

⁵part II, par. 3.b Linee guida cit.; cfr anche le Linee guida in materia di trattamento di dati personali, di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, provv. del 14 giugno 2007, n.161, doc web [n.1417809](#).





C. Conclusioni

Gli atti gli atti aventi valore di notifica personale ai candidati, riportanti l'elenco dei candidati ammessi (mai gli esclusi) alle diverse fasi concorsuali intermedie debbono essere:

- pseudonimizzati con il ricorso, ad esempio, a codici che consentano solo agli interessati di essere identificati;
oppure:
- pubblicati in apposita area riservata del sito, accessibile solo ai diretti interessati tramite appositi sistemi di autenticazione;
oppure:
- comunicati direttamente agli interessati tramite altro canale istituzionale (es. email/PEC ..).

Solamente qualora questo ulteriore trattamento dei dati (pubblicazione sul sito web dei dati personali dei candidati per le fasi intermedie) sia esplicitamente previsto nel regolamento per la selezione del personale dell'ente o nello specifico bando di concorso e nella relativa informativa può rinvenirsi idonea base giuridica a legittimare la pubblicazione dei nominativi per esteso, oppure delle iniziali delle generalità, con indicazione della data di nascita in caso di omonimia.

Tali pubblicazioni dovranno - in ogni caso - essere **rimosse dalla sezione *Amministrazione trasparente* al termine della procedura concorsuale/selettiva**, non avendo copertura normativa per finalità di pubblicità, oltre tale termine.

Non sono invece da pubblicare, in quanto difetta una specifica giustificazione normativa, in *Amministrazione trasparente*, nella sezione *Bandi di concorso*, i documenti afferenti alla Commissione di concorso/selezione, né riguardo ai curricula vitae, né riguardo alle dichiarazioni di assenza di conflitto di interesse, che andranno invece tenute agli atti.

Nello specifico, i curricula e le dichiarazioni rese dai commissari esterni, incaricati ad hoc dall'ente, andranno inseriti nella sezione *Titolari di incarichi di consulenza e di collaborazione*, mentre per i commissari interni non deve essere diffuso alcunché, in quanto l'attività svolta è considerata attività di servizio.

Si allega alla presente *fac-simile di informativa* per il trattamento dati personali nelle procedure selettive pubbliche, da personalizzare in base alle scelte effettuate dall'ente.

* * * * *

Per ogni chiarimento doveste ritenere utile o necessario, potete contattare la dott.ssa Federica Dallaporta o la dott.ssa Marta Mattiello ai seguenti recapiti: tel. 0461 987139 - e-mail serviziordpd@comunitrentini.it.

Cordiali saluti.

Firmato
Il Responsabile della
protezione dei dati
dott. Gianni Festi

Firmato
Il Responsabile del procedimento
dott.ssa Laura Marinelli

All. ti: nr. 1

✓





Estratto del verbale della seduta del 27 novembre 2024

DELIBERAZIONE N. 211

Oggetto:

Valutazione di impatto della Regione autonoma Trentino-Alto Adige/Südtirol sulla protezione dei dati in materia di *whistleblowing* a norma dell'articolo 13, comma 6, del decreto legislativo 10 marzo 2023, n. 24.

Arno Kompatscher	Presidente	presente
Giulia Zanotelli	Vice Presidente sostituta del Presidente	assente
Franz Thomas Locher	Vice Presidente	presente
Carlo Daldoss	Assessore	presente
Angelo Gennaccaro	Assessore	presente
Luca Guglielmi	Assessore	presente
Gabriele Morandell	Segretaria generale della Giunta regionale	presente

Su proposta del Presidente Arno Kompatscher

Ripartizione II – Enti locali, previdenza e competenze ordinamentali

In riferimento all'oggetto la Giunta regionale ha discusso e deliberato quanto segue:

Premesso che:

- con il decreto legislativo 10 marzo 2023, n. 24, è stata recepita la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative;
- la disciplina in materia di *whistleblowing* sopra citata modifica la precedente disciplina, che era contenuta nel decreto legislativo 30 marzo 2001, n. 165, all'articolo 54-*bis*, il quale è stato abrogato in forza dell'articolo 23 del d.lgs. n. 24 del 2023;
- in vigore della normativa di cui al d.lgs. n. 165 del 2001, la Regione autonoma Trentino-Alto Adige/Südtirol aveva individuato i canali di segnalazione interna mediante la piattaforma informatica e per mezzo del modello cartaceo;
- con riferimento alla piattaforma informatica per la ricezione e la gestione delle segnalazioni di illeciti, il Consorzio dei comuni trentini (che fornisce alla Regione la citata piattaforma), con nota assunta al prot. n. 23324/ 28/08/2023-A, ha comunicato che, in conseguenza della nuova disciplina di cui al d.lgs. 23 del 2024, sono stati apportati adeguamenti, anche di tipo tecnologico, alla piattaforma informatica per renderla aderente alle nuove disposizioni legislative. Inoltre, con più specifico riferimento agli aspetti relativi alla tutela dei dati personali e alla riservatezza del segnalante, al fine di fornire le necessarie garanzie rispetto ai principi di privacy by design e by default, nonché di conformità della soluzione applicativa, sono state trasmesse, con la stessa nota, le misure di sicurezza adottate dal Consorzio in qualità di fornitore del servizio (prodotte da Isweb e da Trentino digitale, in qualità di sub-fornitori del servizio e sub-responsabili esterni del trattamento dei dati personali);
- con deliberazione della Giunta regionale del 15 novembre 2023, n. 208, ai sensi dell'articolo 4, comma 1, del citato d.lgs. n. 24 del 2023, la Regione ha adottato l'atto organizzativo relativo ai canali di segnalazione per la presentazione e per la gestione delle segnalazioni in materia di *whistleblowing*. Con il medesimo atto, da un lato, sono state confermate le modalità di inoltro della segnalazione mediante il modello cartaceo e mediante la piattaforma *whistleblowing* (la quale, come detto, era stata adeguata dal Consorzio dei comuni trentini anche per gli aspetti attinenti alla tutela della privacy) e, dall'altro lato, è stata introdotta la modalità di segnalazione orale, come previsto dallo stesso decreto legislativo n. 24 del 2023;
- come noto, le disposizioni del d.lgs. n. 24 del 2023, oltre alla necessità per le pubbliche amministrazioni di adottare degli atti organizzativi per la gestione delle segnalazioni, prevedono anche delle particolari misure di tutela dei dati personali e della riservatezza dei segnalanti. Più nello specifico, si fa riferimento alla disciplina dettata dall'articolo 13, comma 6, del medesimo d.lgs. n. 24 del 2023, secondo cui le amministrazioni *“definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018”*;

- sotto questo profilo, nella citata deliberazione della Giunta regionale del 15 novembre 2023, n. 108 di approvazione dell'atto organizzativo regionale in materia di *whistleblowing*, si evidenziava che la valutazione di impatto sulla protezione dei dati di cui all'articolo 13, comma 6, del d.lgs. n. 24 del 2023, era in corso di svolgimento e sarebbe stata ultimata all'esito dell'adozione dell'atto organizzativo stesso.

Dato atto che:

- la valutazione di impatto sulla protezione dei dati sopra detta, di seguito in sigla DPIA, è una procedura disciplinata dall'articolo 35 del UE/2016/679, volta a descrivere un trattamento dei dati personali, a valutarne la necessità e la proporzionalità nonché a valutarne i rischi per i diritti e libertà delle persone fisiche, allo scopo di determinare le misure per affrontarli, gestirli e se possibile eliminarli o comunque ridurli al minimo;
- la DPIA compete al titolare del trattamento, che si consulta con il responsabile della protezione dei dati;
- il titolare del trattamento dei dati personali è la Regione autonoma Trentino-Alto Adige/Südtirol e l'attuale responsabile della Protezione dei dati per la Regione è il Consorzio dei comuni trentini.

Rilevato che:

- con nota di data 11 luglio 2023 (ns. prot. n. 20323 di pari data), il Consorzio dei comuni trentini, Responsabile per la protezione dei dati della Regione, ha trasmesso all'amministrazione regionale un modello di DPIA in materia di *whistleblowing*, da personalizzare sulla base delle procedure di segnalazione adottate e delle caratteristiche degli strumenti di segnalazione utilizzati;
- secondo il paragrafo 6 del citato atto organizzativo della Regione in materia di *whistleblowing*, adottato con deliberazione n. 208 del 2023, la gestione delle segnalazioni di illeciti è affidata al Responsabile per la prevenzione della corruzione e per la trasparenza, incarico attualmente ricoperto dalla dirigente della ripartizione II, cui compete quindi il relativo trattamento;
- la ripartizione II della Regione ha effettuato pertanto l'istruttoria per la DPIA, utilizzando il modello fornito dal Consorzio dei comuni trentini. La stessa struttura regionale ha aggiornato il proprio registro dei trattamenti, ha valutato i possibili rischi che derivano dal trattamento con riferimento ai canali di segnalazione previsti nel citato atto organizzativo regionale in materia di *whistleblowing* e ha infine individuato le misure di trattamento che riducono tali rischi secondo quanto previsto dall'articolo 13, comma 6, del d.lgs. n. 24 del 2023.

Considerato che:

- all'esito di un primo esame della DPIA trasmessa dalla Regione al Consorzio dei comuni trentini, quest'ultimo, con nota del 20 maggio 2024 (ns. prot. n.14409 di pari data), ha fornito il parere preliminare sulla valutazione di impatto condotta dalla Regione, indicando le prescrizioni da adottare per ridurre il rischio e migliorare la valutazione trasmessa;

- la Regione ha accolto le indicazioni del Consorzio dei comuni trentini espresse nel parere preliminare e, con e-mail del 28 agosto 2024 e con successiva nota formale del 3 settembre 2024 (prot. n. 23181), ha trasmesso nuovamente al Consorzio dei comuni trentini la DPIA aggiornata con la relativa documentazione, al fine di acquisire il parere del Responsabile per la protezione dei dati.
- con nota del 4 ottobre 2024 (ns. prot. n. 26596 di pari data), il Consorzio dei comuni trentini ha trasmesso il parere favorevole alla DPIA del Servizio privacy – Responsabile per la protezione dei dati;
- il suddetto parere favorevole è stato condizionato alla osservanza delle seguenti prescrizioni e indicazioni che testualmente si riportano:
 - a) aggiornare l'informativa disponibile nella piattaforma informatizzata in modo da renderla omogenea all'informativa disponibile nella sezione "Amministrazione trasparente" del sito istituzionale;
 - b) aggiornare il nominativo del referente RPD nel registro delle attività trattamento;
 - c) verificare con il fornitore che le misure di sicurezza relative al 2023 siano adeguate ed aggiornate al fine di garantire la tutela dei dati personali in linea con l'art. 32 del GDPR;
- in accoglimento delle sopra riportate indicazioni, la Regione ha aggiornato l'informativa disponibile nella piattaforma automatizzata di segnalazione e ha modificato il registro delle attività di trattamento;
- la Regione ha altresì richiesto al Consorzio dei comuni trentini (fornitore della piattaforma *whistleblowing*) di verificare l'aggiornamento e l'adeguatezza delle misure di sicurezza rispetto a quanto già trasmesso dallo stesso Consorzio con la sopra citata nota del 28 agosto 2023 (ns prot. 23324 di pari data). Con e-mail del 14 novembre 2023, il Consorzio ha trasmesso l'ultima versione, datata 27 ottobre 2023, del documento contenente la "Dichiarazione sulle misure di sicurezza applicate" che sostituisce il documento in precedenza inviato.

Considerato altresì che:

- le misure di trattamento del rischio individuate nella DPIA, come modificate a seguito dei confronti e delle indicazioni del Responsabile per la protezione dei dati, si intendono ad oggi adeguate, in quanto è stata valutata la necessità e la proporzionalità del trattamento dei dati in materia di *whistleblowing*, sono stati valutati i rischi per i diritti e le libertà delle persone fisiche, nonché determinate le misure per affrontarli, gestirli e se possibile eliminarli o comunque ridurli al minimo;
- come da indicazioni del Responsabile per la protezione dei dati, la DPIA sulle medesime attività di trattamento sarà comunque nuovamente condotta se dovesse determinarsi una variazione delle caratteristiche delle attività trattamento, se l'attività di trattamento riguarda dati particolari che, per loro natura, richiedono una maggiore tutela e cura e, in ogni caso, periodicamente, alla modifica delle condizioni generali interne alla struttura organizzativa dell'Ente.

Ad unanimità di voti legalmente espressi,

delibera

- di approvare la valutazione di impatto della Regione autonoma Trentino-Alto Adige/Südtirol sulla protezione dei dati in materia di *whistleblowing* a norma dell'articolo 13, comma 6, del decreto legislativo 10 marzo 2023, n. 24 e la relativa documentazione, come registrata nel protocollo della Regione all'ID n. 28494825.

Letto, confermato e sottoscritto.

IL PRESIDENTE

Arno Kompatscher
firmato digitalmente

LA SEGRETARIA GENERALE
DELLA GIUNTA REGIONALE

Gabriele Morandell
firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).



Consorzio dei
Comuni Trentini

Trento, 11 luglio 2023
GF/FD/MAM/LM/lb

Al Sindaco/Presidente
Al Segretario/Direttore
Al Referente privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE

OGGETTO: Servizio privacy RPD – whistleblowing e tutela dei dati personali: novità previste dalla normativa a partire dal 15 luglio 2023.

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto.
Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.
Cordiali saluti.

Firmato
Il Direttore generale
Marco Riccadonna

Firmato
Il Vicepresidente
ing. Michele Cereghini



Consorzio dei Comuni Trentini società cooperativa

P.IVA e C.F.
01533550222

Iscritta al Registro delle Imprese
di Trento n. 01533550222

Via Torre Verde, 23
38122 TRENTO (TN)

Tel. 0461 987139

consorzio@pec.comunitrentini.it
info@comunitrentini.it

www.comunitrentini.it



Con il decreto legislativo n. 24 del 2023, che recepisce la direttiva UE 2019/1937, si introducono delle significative novità alla disciplina italiana dell'istituto del Whistleblowing.

La suddetta normativa è entrata in vigore il 30 marzo 2023 e **le sue disposizioni avranno effetto per gli enti pubblici a decorrere dal 15 luglio 2023.**

Le novità dettate dalla disciplina del Whistleblowing assumono rilievo e implicazioni per la tutela dei dati personali e la riservatezza dei diversi soggetti interessati ossia le persone segnalanti presunti illeciti, le persone segnalate e le persone terze eventualmente coinvolte.

Si ritiene utile di seguito rappresentarne ed evidenziarne gli aspetti più significativi, con particolare riferimento ai profili della riservatezza e del trattamento dei dati personali.

Whistleblowing, come è tutelato il segnalante

La Direttiva (UE) 2019/1937 pone come centrale il ruolo del *whistleblower* nella denuncia e nella prevenzione di violazioni di norme e al fine della salvaguardia del "benessere" della società.

Obiettivo del legislatore è impedire o contrastare condotte che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e accrescere il livello di osservanza delle norme giuridiche in ambiti e settori in cui le violazioni possono arrecare un grave pregiudizio al pubblico interesse.

Per perseguire tale obiettivo, la Direttiva europea Direttiva (UE) 2019/1937 impone agli Stati membri di obbligare un ampio numero di soggetti pubblici e privati a mettere a disposizione dei potenziali whistleblower canali di segnalazione efficaci, riservati e sicuri e a proteggere gli stessi da eventuali ritorsioni.

Per i lavoratori dipendenti l'esigenza di protezione deriva dalla loro "posizione di soggezione" verso il datore di lavoro.

Il decreto legislativo n. 24 del 2023 stabilisce ad esempio che il licenziamento conseguente alla segnalazione, alla denuncia all'autorità giudiziaria o contabile o alla divulgazione pubblica effettuate ai sensi del decreto stesso è nullo.

La medesima necessità di impedire ritorsioni vale peraltro anche per i lavoratori assunti con contratti atipici, compresi i lavoratori a tempo parziale e i lavoratori con contratti a tempo determinato e per tutte le persone che hanno un contratto di lavoro o un rapporto di lavoro con un'agenzia interinale.

La protezione si estende anche ai lavoratori indipendenti, ai contraenti, ai subappaltatori e ai fornitori.

Ambito della normativa

L'istituto e la disciplina del Whistleblowing non rappresentano una novità nel nostro ordinamento, essendo la stessa già prevista per il settore pubblico dal decreto legislativo n. 165 del 2001 e, per il settore privato, dal decreto legislativo n. 231 del 2001 in materia di prevenzione dei crimini d'impresa e dalla legge n. 179 del 2017 in materia di anticiclaggio.

Le principali novità sono:

- l'estensione dei destinatari degli obblighi;
- l'estensione delle condotte potenzialmente illecite ritenute meritevoli di segnalazione;
- la previsione del canale di segnalazione esterno gestito dall'Autorità anticorruzione (ANAC);
- il rafforzamento della tutela dei whistleblower con strumenti e garanzie finalizzate ad evitare il timore di effettuare le segnalazioni per le possibili conseguenze negative.

Destinatari della normativa sono tutti gli enti del settore pubblico.

Per il settore privato, invece, la stessa si applica ai soggetti che hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, a quelli che rientrano nell'ambito di applicazione delle normative europee indicate dalla direttiva (UE) 2019/1937 come rilevanti e a quelli che adottano modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo n. 231 del 2001.

Oggetto della segnalazione possono essere sia violazioni già occorse, che violazioni non ancora commesse ma che molto verosimilmente potrebbero esserlo nonché ancora atti od omissioni che il





whistleblower abbia fondato motivo di ritenere rappresentino violazioni nonché i tentativi di nascondere le stesse.

Con il decreto legislativo n. 24 del 2023 il legislatore si pone l'obiettivo di proteggere i whistleblowers sia dalle ritorsioni dirette (come ad esempio il licenziamento, il mobbing, la calunnia), sia dalle ritorsioni indirette sia da quelle destinate a persone fisiche o giuridiche diverse dai whistleblowers, ma ad essi "collegate o collegabili" (come ad esempio le persone operanti all'interno del medesimo contesto lavorativo che assistono i whistleblowers nel processo di segnalazione - i cosiddetti "facilitatori", i colleghi di lavoro o i parenti che sono in una relazione di lavoro con lo stesso datore di lavoro).

I canali per le segnalazioni

I whistleblowers avranno a disposizione due canali: la segnalazione interna all'ente e la segnalazione esterna all'Autorità nazionale anticorruzione (ANAC).

- **Il canale interno**

Gli enti pubblici hanno l'obbligo di attivare il canale di segnalazione, sentite le rappresentanze o le organizzazioni sindacali (art. 4, comma 1, d.lgs. 24/2023), nei soli casi di attivazione *ex novo* di un canale di segnalazione o di modifiche sostanziali del medesimo.

La segnalazione dovrà poter essere effettuata per iscritto o a voce (ad esempio a un numero telefonico dedicato), a scelta del whistleblower. Le segnalazioni possono essere effettuate in forma scritta, anche con modalità informatiche, oppure in forma orale (art. 4, comma 3).

Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

La segnalazione in forma orale, previo consenso della persona segnalante, è documentata a cura del personale addetto, mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.

Quanto alle segnalazioni scritte, sul punto si richiamano le linee guida ANAC (delibera n. 469 del 9 giugno 2021), 2.2. *Modalità di gestione delle segnalazioni*: procedure informatizzate e tradizionali, ove si dice che: Le Amministrazioni sono, quindi, tenute a disciplinare, in conformità alle presenti Linee guida, le procedure, preferibilmente informatizzate, per la ricezione e gestione delle segnalazioni. L'Amministrazione dà notizia dell'adozione del sistema applicativo informatico di gestione delle segnalazioni nella home page del proprio sito istituzionale in modo chiaro e visibile.

Tuttavia, anche al fine di evitare usi impropri del sistema, l'indirizzo web della piattaforma, sebbene raggiungibile da Internet, potrà non essere reso pubblico sul sito istituzionale dell'amministrazione. In tal caso, esso potrà essere reso noto ai soggetti interessati esterni all'amministrazione (lavoratori e collaboratori delle imprese che realizzano opere in favore della p.a.) per altre vie (ad es. mediante comunicazione diretta del link al momento della sottoscrizione del contratto). In assenza della pubblicazione sul proprio sito Internet, l'Amministrazione è comunque tenuta a garantire l'accesso non ristretto ai lavoratori e collaboratori delle imprese fornitrici che realizzano opere in favore dell'amministrazione pubblica, contemplati nel co. 2 del novellato art. 54-bis d.lgs. 165/2001.

Nel caso in cui l'applicativo utilizzato per acquisire e gestire le segnalazioni sia fornito da un soggetto terzo che offra anche altri servizi quali la manutenzione o la conduzione applicativa, o altri servizi informatici che comportano il trattamento di dati per conto dell'amministrazione, o nel caso in cui l'amministrazione si doti di un sistema offerto in Cloud o in modalità SaaS (Software as a Service) resta fermo che tale soggetto terzo opera in





qualità di “responsabile” del trattamento (ai sensi dell’art. 28 del Regolamento UE 2016/679).

Analogamente, opera in qualità di autorizzato al trattamento il personale dell’Amministrazione con mansioni di manutenzione e conduzione applicativa del sistema.

L’amministrazione che non ha automatizzato il processo di gestione delle segnalazioni, a causa di specifiche difficoltà organizzative da motivare adeguatamente, può, in via residuale, utilizzare canali e tecniche tradizionali da disciplinare nel PTPCTT o nell’atto organizzativo indicando, tuttavia, gli strumenti previsti per garantire la riservatezza dell’identità del segnalante, del contenuto delle segnalazioni e della relativa documentazione, in conformità a quanto previsto dalla legge. Ad esempio, può essere prevista la trasmissione cartacea della segnalazione in busta chiusa indirizzata al RPCT con la dicitura “riservata/personale”. Con riguardo alle segnalazioni pervenute mediante canali diversi dalla procedura informatica, si ritiene opportuno che queste siano protocollate in apposito registro riservato.

Si sottolinea come la lettura di ANAC, ancorché antecedente al nuovo decreto legislativo, sia ancora valida ma che permane la possibilità di optare tra i diversi canali (scritto, orale, piattaforma informatizzata).

Procedura di Gestione del canale di segnalazione interna

Nell’ambito della gestione del canale di segnalazione interna, il soggetto (RPCT/odV) cui è affidata la gestione del canale di segnalazione interna svolge le seguenti attività (art. 5):

1. rilascia alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;
2. mantiene le interlocuzioni con la persona segnalante e può richiedere a quest’ultima, se necessario, integrazioni;
3. dà diligente seguito alle segnalazioni ricevute;
4. fornisce riscontro alla segnalazione entro tre mesi dalla data dell’avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione;
5. mette a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne.

Le suddette informazioni sono pubblicate in una sezione dedicata del sito istituzionale ed esposte e rese facilmente visibili nei luoghi di lavoro.

- Il canale esterno

I whistleblower avranno la possibilità di effettuare una segnalazione all’ANAC, in presenza di una delle seguenti condizioni (art. 6):

1. se nello specifico contesto lavorativo l’attivazione del canale di segnalazione interna non è obbligatoria o se il canale non è attivo o non è attivato nel rispetto dei requisiti normativi;
2. se il whistleblower ha già fatto una segnalazione interna, ma la stessa non ha avuto seguito o si è conclusa con un provvedimento conclusivo negativo;
3. se il whistleblower ha fondato motivo di ritenere che, qualora effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
4. se il whistleblower ha fondato motivo di ritenere che la violazione segnalata possa costituire un pericolo imminente o palese per il pubblico interesse.

Entro tre mesi dalla data di entrata in vigore del decreto, l’ANAC, sentita l’Autorità Garante in materia di protezione dei dati personali, adoterà delle linee guida relative alle procedure per la presentazione e la gestione delle segnalazioni esterne.



L'ANAC ha l'obbligo di trasmettere eventuali segnalazioni relative a violazioni che esulano dalle proprie attribuzioni alle competenti autorità, amministrative o giurisdizionali.

La protezione dell'identità dei soggetti interessati nel canale di segnalazione interno

L'art. 4 del decreto legislativo n. 24 del 2023 prevede la tutela della riservatezza dell'identità del whistleblower ma anche della persona segnalata e di qualsiasi altra persona comunque menzionata nella segnalazione nonché la riservatezza del contenuto della segnalazione e della relativa documentazione, anche tramite il ricorso a strumenti di crittografia.

L'art. 12 del decreto legislativo n. 24 del 2023 disciplina la riservatezza dell'identità del whistleblower nel procedimento penale e innanzi alla Corte dei Conti.

Nel procedimento disciplinare l'identità della persona segnalante non potrà essere rivelata laddove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione (anche se conseguenti alla stessa).

La segnalazione potrà essere usata ai fini di un procedimento disciplinare nei confronti della persona segnalata solo se:

- il procedimento sia fondato, in tutto o in parte, sulla segnalazione;
- la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato;
- la persona segnalante, dopo aver ricevuto una comunicazione scritta delle ragioni della rivelazione, abbia dato il consenso alla rivelazione della propria identità.

L'identità della persona segnalante e qualsiasi altra informazione da cui possa evincersi tale identità (direttamente o indirettamente) potranno essere rivelate a persone diverse da quelle designate dagli enti a ricevere o a dare seguito alle segnalazioni solo previo consenso espresso del whistleblower, debitamente informato.

L'identità delle persone coinvolte e delle persone menzionate nella segnalazione dovrà essere tutelata fino alla conclusione dei procedimenti attivati in ragione della segnalazione nel rispetto delle medesime garanzie previste in favore della persona segnalante.

Ruoli dei soggetti privacy – misura da adottare

Il decreto legislativo n. 24 del 2023 individua in modo chiaro ruoli e responsabilità per i trattamenti dei dati personali connessi alla gestione delle segnalazioni.

L'art. 13 del decreto legislativo esplicita che i trattamenti di dati personali relativi al ricevimento e gestione delle segnalazioni sono svolti dagli enti destinatari della normativa in qualità di Titolari.

Le persone fisiche designate dall'ente a ricevere o a dare seguito alle segnalazioni (RPCT, OIV, detentore delle chiavi) devono essere autorizzate dal Titolare tramite un esplicito riferimento nella nomina a designato/incaricato oppure tramite l'associazione all'interno del registro delle attività del trattamento alla specifica attività di trattamento e potranno conoscere l'identità del whistleblower senza necessità del consenso dello stesso.

Se il servizio viene affidato *in toto* o in parte ad un soggetto "esterno" o dello stesso ci si avvalga quale fornitore della piattaforma informatica adottata come canale per la ricezione e gestione delle segnalazioni, ricorre la figura del Responsabile del trattamento. Il rapporto tra Titolare e Responsabile dovrà essere disciplinato da un apposito atto ai sensi dell'art. 28 del GDPR (nomina a responsabile del trattamento).

La necessità di effettuare la DPIA – misura da adottare

Il comma 6 dell'art. 13 decreto legislativo n. 24 del 2023 prescrive che nel definire il proprio modello di ricevimento e gestione delle segnalazioni interne, gli enti pubblici e privati devono effettuare la Valutazione d'impatto privacy (DPIA) ai sensi dell'art. 35 del GDPR finalizzata ad analizzare i rischi a carico di tutti i soggetti coinvolti (whistleblower, persone segnalate, terzi) e adottare misure tecniche



e organizzative idonee a garantire un livello di sicurezza adeguato alla probabilità e alla gravità dei rischi individuati.

Diritti degli interessati

I diritti degli interessati (specialmente delle persone segnalate) possono essere esercitati nei limiti di quanto previsto dall'articolo 2-*undecies* del D.lgs. 196/2003, che ne determina la sospensione qualora da essi possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del whistleblower.

Applicazione del principio di minimizzazione by default

I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, devono essere cancellati immediatamente.

La conservazione delle segnalazioni interne ed esterne e della relativa documentazione è legittima per il tempo necessario alla loro definizione e, comunque, per non più di cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza e del principio di limitazione della conservazione definito dal GDPR. A parere del Garante tale termine massimo di conservazione della documentazione della segnalazione è compatibile con la durata media del termine prescrizione dei principali illeciti suscettibili di verificarsi. Ad ogni modo, nel caso di eliminazione di documenti amministrativi, si richiama al rispetto delle regole di conservazione di cui al Codice dei Beni Culturali e del Paesaggio (d. lgs. 42/2004); sul punto è in corso un confronto con la Soprintendenza per i beni culturali della Provincia autonoma di Trento.

La tutela dei whistleblower dalle violazioni in materia di trattamento dei dati personali

I whistleblower sono autorizzati a diffondere informazioni anche personali riferite ai segnalati o a terzi (esempio fornendole ai media o pubblicandole sui canali social) quando (art. 15 del Decreto Legislativo 24/2023):

- hanno previamente effettuato una segnalazione interna ed esterna, ma non hanno ricevuto riscontro nei termini;
- hanno fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- hanno fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto.

Inoltre, qualora le segnalazioni abbiano per contenuto dati personali ai quali i whistleblower non erano autorizzati ad accedere, quali ad esempio una e-mail indirizzata a un terzo, gli stessi sono esenti da responsabilità purché non abbiano commesso un vero e proprio reato di trattamento illecito di dati personali.

In conclusione, si ritiene utile riepilogare brevemente quali sono gli adempimenti **in materia di protezione dei dati personali che gli enti sono chiamati a predisporre:**

- nomina ai designati/incaricati della gestione delle segnalazioni;
- nomina a responsabile del trattamento dell'eventuale fornitore e/o manutentore della piattaforma di gestione delle segnalazioni;
- inserimento, all'interno del registro delle attività del trattamento, della specifica attività di gestione delle segnalazioni – whistleblowing;
- predisposizione e messa a disposizione di una specifica informativa al trattamento dei dati personali inerente alla gestione delle segnalazioni (fac-simile allegato 1);





- formalizzare una procedura di gestione delle segnalazioni, contenente istruzioni circa i canali di comunicazione (piattaforma informatica/modalità orale, ...), nonché sui tempi di gestione delle segnalazioni (3 mesi);
- provvedere a comunicare ai soggetti legittimati ad effettuare la segnalazione, il canale mediante il quale è effettuabile e le eventuali credenziali d'accesso al medesimo;
- se ci si avvale di una piattaforma fornita da un soggetto esterno, si raccomanda di richiedere al fornitore garanzie circa la progettazione della stessa rispettando i principi di privacy by design e by default, nonché le misure di sicurezza adottate;
- sottoporre l'attività di trattamento a valutazione d'impatto obbligatoria. In merito a tale ultimo aspetto, lo Scrivente rende disponibile un modello di DPIA per la valutazione della procedura di segnalazione whistleblowing (fac-simile allegati 2 e 3), **da personalizzare sulla base delle procedure di segnalazione adottate dal singolo ente e delle caratteristiche dello strumento utilizzato.**

* * * * *

Per ogni chiarimento dovete ritenere utile o necessario, potete contattare la dott.ssa Federica Dallaporta o la dott.ssa Marta Mattiello ai seguenti recapiti: tel. 0461 987139 - e-mail serviziopd@comunitrentini.it.
Cordiali saluti.

Firmato
Il Referente
Responsabile della protezione dei dati
dott. Gianni Festi

Firmato
Il Responsabile del procedimento
dott.ssa Laura Marinelli





Consorzio dei
Comuni Trentini

Trento, 25 agosto 2023
MAM/LM/ed

Al Sindaco/Presidente
Al Segretario/Direttore
Al Referente privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE

OGGETTO: Servizio privacy RPD – l'informativa privacy: specificità sul whistleblowing alla luce del D. Lgs. 24/2023.

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto. Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.
Cordiali saluti.

Il Direttore Generale
dott. Marco Riccadonna

Il Presidente
dott. Paride Gianmoena



Consorzio dei Comuni Trentini società cooperativa

P.IVA e C.F.
01533550222

Iscritta al Registro delle Imprese
di Trento n. 01533550222

Via Torre Verde, 23
38122 TRENTO (TN)

Tel. 0461 987139

consorzio@pec.comunitrentini.it
info@comunitrentini.it

www.comunitrentini.it



Facendo seguito alla nostra precedente circolare dd. 11.07.2023, avente ad oggetto *"whistleblowing e tutela dei dati personali: novità previste dalla normativa a partire dal 15 luglio 2023"*, e alla luce dei primi orientamenti dottrinali in merito, siamo a specificare quanto segue con riferimento al tema dell'informativa al trattamento dei dati personali.

L'art. 13 del D. Lgs. 24/2023 (cd. decreto whistleblowing) prevede che si debbano fornire *"idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14"* del GDPR, ossia nei casi in cui i dati siano raccolti presso l'interessato o presso terzi (da fornire qualora i dati personali non siano stati ottenuti presso l'interessato).

Vengono, infatti, trattati sia i dati forniti dall'interessato (il segnalante ed eventualmente il facilitatore), sia i dati riguardanti terzi (il segnalato ed i soggetti menzionati nella segnalazione).

Ne deriva che ciascun Ente è tenuto a produrre e rendere conoscibile ai potenziali segnalanti una informativa ex art. 13 GDPR (unitamente alle indicazioni su come procedere per una eventuale segnalazione, da rendere note ai propri dipendenti, così come a tutti i soggetti individuati dal decreto) e, analogamente, ex art. 14 GDPR, una informativa a favore del segnalato e dei terzi menzionati dal whistleblower.

Si allega, pertanto, **un fac-simile di informativa, completa sia delle informazioni necessarie ex art. 13 a favore del segnalante sia ai sensi dell'art. 14, a favore del segnalato** (e degli altri eventuali soggetti coinvolti nella segnalazione), in quanto le informazioni da rendere agli interessati sono relative a un medesimo processo e sono di tenore analogo.

L'informativa andrà resa disponibile a tutti i potenziali interessati tramite pubblicazione sulla piattaforma "whistleblowing" e anche sul sito istituzionale dell'Ente, affinché anche il segnalato sia in grado di venirne a conoscenza, in coerenza con le Linee guida sulla trasparenza (W260 del 2018), elaborate dal Gruppo di Lavoro art. 29, ove affermano che *"l'interessato dovrebbe essere in grado di determinare in anticipo quali siano la portata del trattamento e le relative conseguenze e non dovrebbe successivamente essere colto di sorpresa dalle modalità di utilizzo dei dati personali che lo riguardano"*.

La scelta di predisporre un'unica informativa e di renderla pubblica avrebbe anche il vantaggio di informare preventivamente il (potenziale) segnalato senza la necessità di inviare allo stesso una informativa ad hoc, con il rischio di compromettere la riservatezza della procedura.

A memoria del GDPR, infatti, nel caso in cui rendere l'informativa ex art. 14 (par. 5) *"rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni"* (art.14).

È rimessa, pertanto, al singolo Ente la scelta se redigere due diverse informative ex art. 13 e a ex art. 14, come sopra precisato, oppure se utilizzare l'informativa allegata, che si invita ad adattare alle esigenze dell'Ente e, per quanto sopra precisato, a pubblicare sul sito internet istituzionale (in sostituzione del modello precedentemente trasmesso con nostra circolare d.d. 11.07.2023).





Consorzio dei
Comuni Trentini

Per ogni chiarimento doveste ritenere utile o necessario, potete contattare la dott.ssa Federica Dallaporta o la dott.ssa Marta Mattiello ai seguenti recapiti: tel. 0461 987139 - e-mail serviziordp@comunitrentini.it.

Cordiali saluti.

Firmato
Il Referente
Responsabile della protezione dei dati
dott. Gianni Festi

Firmato
Il Responsabile del procedimento
dott.ssa Laura Marinelli

All. ti:1



Consorzio dei Comuni Trentini società cooperativa

P.IVA e C.F.
01533550222

Iscritta al Registro delle Imprese
di Trento n. 01533550222

Via Torre Verde, 23
38122 TRENTO (TN)

Tel. 0461 987139

consorzio@pec.comunitrentini.it
info@comunitrentini.it

www.comunitrentini.it



Consorzio dei
Comuni Trentini

Trento, 13 maggio 2022
LM/FD/MAM/GF/ed

Al Sindaco/Commissario
Al Segretario
Al Referente privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE

E, p.c.

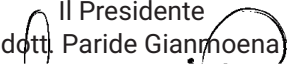
Spett.le
Trentino Digitale spa

interoperabilità PITRE

OGGETTO: Servizio privacy RPD – informazioni circa le misure di sicurezza informatiche adottate da Trentino Digitale nell'erogazione dei propri servizi.

Siamo con la presente a trasmettere la circolare relativa all'argomento in oggetto.
Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.
Cordiali saluti.

 Il Direttore Generale
dott. Marco Riccadonna

 Il Presidente
dott. Paride Gianmoena



Nel corso degli audit annuali effettuati dal Servizio privacy – RPD del Consorzio dei Comuni trentini, durante il 2021, è emerso che molti Enti fruiscono dei servizi informatici offerti da Trentino Digitale. Tali enti, quali titolari del trattamento, hanno inquadrato la medesima società nel ruolo di responsabile del trattamento e hanno ad essa richiesto, in quanto fornitore dei servizi informatici, di conoscere la tipologia e/o l'aggiornamento delle misure di sicurezza, in modo da poterne valutare l'adeguatezza e di documentarne il rispetto.

Considerato che lo scrivente Responsabile per la Protezione dei Dati, nell'espletamento delle proprie funzioni, affianca gli enti nell'assolvimento della accountability, il Consorzio dei Comuni Trentini ha ritenuto di provvedere a richiedere un confronto con Trentino Digitale in merito all'implementazione delle misure di sicurezza necessarie.

In ragione della collaborazione in essere tra le due società di sistema, si è scelto di **condividere un iter per mettere a disposizione dei titolari del trattamento le misure di sicurezza aggiornate, adottate da Trentino Digitale, nel contesto della erogazione dei propri servizi**, in modo che ne sia apprezzabile e verificabile l'adeguatezza.

Il documento, che si intende mettere a disposizione degli enti in indirizzo in allegato alla presente, riporta pertanto le generali "*Misure di sicurezza relative alle infrastrutture di Trentino Digitale SPA*", con evidenza specifica della diversa natura delle stesse: **Sicurezza perimetrale, Sicurezza dei servizi di connettività, Sicurezza dei servizi di Data Center, Sicurezza degli accessi fisici, SOC (Security Operation Center)** e con specifica menzione delle certificazioni ottenute dalla società:

- ISO 9001:2015 Progettazione, sviluppo ed erogazione di servizi informatici applicativi, di sicurezza, tecnologici e di telecomunicazione;
- ISO 27001:2013 per la gestione della sicurezza delle informazioni, estesa ai controlli aggiuntivi;
- ISO 27017:2015 e 27018:2014 per la gestione della sicurezza e la privacy delle informazioni in Cloud;
- ISO 22301:2019 a garanzia della continuità operativa dei servizi.

Tra le informazioni rilevanti si riporta inoltre che:

- Trentino Digitale applica attualmente inoltre una misura di **filtraggio della navigazione Internet** che implementa il blocco di specifiche liste e categorie di siti Internet (URL filtering) con costanti aggiornamenti. Si tratta di siti palesemente illeciti o non attinenti alle attività lavorativa (ad es. pedofilia, contenuti sessuali, armi, violenza, razzismo, trading on line, etc.). Nel rispetto delle linee guida del Garante per la protezione dei dati personali per l'utilizzo della rete internet e della posta elettronica da parte dei lavoratori:
 - le attività di filtraggio vengono realizzate attraverso apposite policy sui firewall perimetrali della rete;
 - in generale vengono applicati vari livelli di filtraggio per tutti gli Enti pubblici del sistema Trentino a seconda delle specifiche esigenze (ad esempio per le scuole);
 - sono esclusi dalle attività di filtraggio alcuni soggetti (ad esempio Operatori di telecomunicazione) ed alcuni Enti su specifiche richieste ed esigenze.
- Trentino Digitale, in qualità di Operatore di Telecomunicazioni, è tenuta a raccogliere e conservare i **log relativi al traffico di navigazione Internet** (ora e data, IP del client,



userid, indirizzo o URL di destinazione e protocollo). Tali informazioni sono trattate in ottemperanza a quanto disposto dal Provvedimento del Garante per la protezione dei dati personali "Sicurezza dei dati di traffico telefonico e telematico" del 17 gennaio 2008. Nelle informazioni raccolte non viene memorizzata nessuna informazione che permetta l'identificazione immediata dell'utente e possono essere consultate esclusivamente per motivi di sicurezza della rete Telpat o su richiesta dell'Autorità Giudiziaria.

I dati raccolti non vengono in alcun modo utilizzati per effettuare la profilazione delle abitudini di traffico degli utenti ma, in caso di necessità, e comunque nel rispetto dei principi di pertinenza e non eccedenza, i suddetti dati possono essere analizzati per le seguenti legittime finalità:

- tutelare la sicurezza e preservare l'integrità degli strumenti informatici;
 - evitare la commissione di illeciti;
 - verificare la funzionalità del sistema e degli strumenti informatici;
 - rispondere alle richieste delle autorità giudiziarie;
 - garantire l'assenza di interferenze o violazioni ingiustificate dei diritti e delle libertà fondamentali degli utenti, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.
- Trentino Digitale garantisce comunque l'esclusione di controlli prolungati, costanti o indiscriminati, coerentemente con quanto previsto dal Provvedimento generale del Garante per la protezione dei dati personali del 1° marzo 2007. Il Responsabile dei controlli, eseguiti solamente per le finalità dichiarate, è la struttura responsabile della gestione della sicurezza delle informazioni.
- Trentino Digitale effettua una conservazione per settantadue mesi dei dati di traffico telefonico e telematico (riferimenti sulla navigazione su Internet), in base all'obbligo previsto dall'art. 24 della Legge 167/2017, al fine di garantire strumenti di indagine efficaci a fronte delle straordinarie esigenze di contrasto al fenomeno del terrorismo.

Le misure di sicurezza informatica saranno inoltre reperibili alla pagina web: <https://www.trentinodigitale.it/Societa/Privacy/Enti>, che contiene anche i fac-simile di nomina a responsabile del trattamento dei dati personali per i servizi erogati da Trentino Digitale. Alla pagina è possibile accedere secondo quanto indicato nella nota del 3 giugno 2021 inviata agli enti locali dalla medesima società (per accedere utilizzare **Nome utente:** Privacy e **Password:** Privacy01).

Si precisa che il non fornire e divulgare da parte di Trentino Digitale ulteriori e dettagliate informazioni tecnico-informatiche in merito alle misure di sicurezza implementate costituisce policy aziendale e ulteriore garanzia per il Titolare di conformità del livello di sicurezza alla normativa in materia di protezione dei dati personali.

Come specificato nello schema di nomina a responsabile del trattamento, predisposto – a suo tempo- congiuntamente allo scrivente Servizio, il responsabile del trattamento è tenuto a fornire al titolare tutte le informazioni necessarie ad accertare *"l'adequatezza delle misure di sicurezza, l'osservanza delle istruzioni impartite e in generale il rispetto della normativa in materia"*.

L'occasione della consultazione della pagina indicata per l'acquisizione delle misure di sicurezza aggiornate, può essere quindi utile alla verifica - da parte Vostra – di aver effettuato





la/le nomina/e a responsabile del trattamento per i servizi forniti e, in difetto, alla pronta trasmissione della nomina sottoscritta a Trentino Digitale.

Ricordiamo infatti che, a norma dell'art. 28 GDPR e come specificato nelle Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR, versione 2.0, adottate dall'European Data Protection Board il 7 luglio 2021:

Il titolare del trattamento deve avvalersi unicamente di responsabili del trattamento che presentino garanzie sufficienti per l'attuazione di misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR.

Gli elementi di cui tenere conto potrebbero essere le conoscenze specialistiche del responsabile del trattamento (ad esempio, le competenze tecniche in materia di misure di sicurezza e di violazione dei dati), il grado di affidabilità, le risorse di cui dispone il responsabile e l'adesione di quest'ultimo a un codice di condotta o a un meccanismo di certificazione riconosciuti.

Qualsivoglia trattamento di dati personali da parte di un responsabile del trattamento deve essere disciplinato da un contratto o da un atto giuridico di altra natura, redatto per iscritto, anche in formato elettronico, con carattere di vincolatività.

* * * * *

Per ogni chiarimento doveste ritenere utile o necessario, potete contattare il Servizio privacy – RPD ai seguenti recapiti: tel. 0461 987139 - e-mail serviziordp@comunitrentini.it.

Cordiali saluti.

Firmato
Il Referente
Responsabile della protezione dei dati
dott. Gianni Festi

Firmato
Il Responsabile del procedimento
dott.ssa Laura Marinelli





Consorzio dei
Comuni Trentini

Trento, 21 agosto 2023
GF/FD/MAM/LM/ed

Al Sindaco/Presidente
Al Segretario/Direttore
Al Referente privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE

OGGETTO: Servizio privacy RPD – Amministratore di sistema: nuovo modello di nomina e facsimile di relazione annuale.

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto. Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.
Cordiali saluti.

Il Direttore Generale
dott. Marco Riccadonna

Il Presidente
dott. Paride Gianmoena



Consorzio dei Comuni Trentini società cooperativa

P.IVA e C.F.
01533550222

Iscritta al Registro delle Imprese
di Trento n. 01533550222

Via Torre Verde, 23
38122 TRENTO (TN)

Tel. 0461 987139

consorzio@pec.comunitrentini.it
info@comunitrentini.it

www.comunitrentini.it



L'amministratore di sistema, pur non essendo esplicitamente richiamato nel GDPR, rappresenta un soggetto che riveste un ruolo essenziale nella gestione della "privacy" dell'Ente.

Si tratta di una figura professionale che assume e può assumere diversi compiti e funzioni. Di norma lo stesso sovrintende e "governa" la sicurezza e l'efficienza della rete informatica dell'Ente o di un software dello stesso, si occupa delle architetture informatiche ed in particolare, dell'utilizzo e della condivisione dei dati attraverso le reti di comunicazione, comprese quelle a cui non si accede via web, come le reti intranet.

Altresì all'amministratore di sistema sono affidati delicati compiti quali l'implementazione dei sistemi di sicurezza e la definizione delle procedure di autenticazione alla rete e di autorizzazione all'accesso ai dati da parte degli utenti, la cura degli interventi di conservazione dei dati attraverso soluzioni di *backup* e la progettazione delle attività di supporto al *disaster recovery*.

Inoltre, ha un ruolo importante nel supportare l'Ente ad adottare le misure cosiddette di *privacy by design* e *privacy by default* nelle fasi di progettazione e di innovazione dei processi organizzativi e di protezione dei dati ed assume un ruolo fondamentale per quanto riguarda la prevenzione e la gestione di eventuali *data breach*.

Le funzioni che l'amministratore di sistema assume comportano quindi, di regola, la concreta capacità dello stesso di accedere in modo privilegiato a dati personali dell'Ente. È pertanto necessario adottare specifiche cautele nell'individuare le mansioni svolte dagli amministratori di sistema e nell'individuare accorgimenti e misure che agevolino l'esercizio dei doveri di controllo da parte del titolare.

Vale rammentare che la figura dell'amministratore di sistema era già prevista agli albori della privacy nella disciplina in materia di protezione dei dati preesistente al Codice del 2003, laddove si definiva lo stesso quale *"soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione"* (art. 1, comma 1, lett. c) d.P.R. 318/1999).

Risale al 27 novembre 2008 l'adozione da parte del Garante per la Protezione dei Dati Personali di un Provvedimento Generale denominato *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema con l'intento di promuovere presso Titolari e pubblico la consapevolezza della delicatezza del ruolo di "amministratore di Sistema"* (modificato e integrato con un Provvedimento del 25 giugno 2009) che richiamava in particolar modo l'attenzione sulla necessità di prestare la massima attenzione ai rischi incombenti sui dati personali e alle criticità relative alle misure di sicurezza adottate connesse allo svolgimento di tale attività.

Con tale provvedimento il Garante Privacy ha inteso, infatti, dare rilievo al ruolo dell'amministratore di sistema all'interno del sistema di gestione privacy, evidenziandone l'importanza e imponendo ai Titolari una selezione dei candidati e una scelta del soggetto individuato sulla base di comprovate capacità tecniche ed esperienze, l'assegnazione allo stesso di precise responsabilità nonché la definizione e l'implementazione di procedure tecniche di supervisione e controllo sul suo operato.

Il Regolamento europeo sulla protezione dei dati personali 679/2016 non contiene uno specifico ed esplicito riferimento alla figura dell'amministratore di sistema. Tuttavia, l'articolo 32, par. 1, del Regolamento sancisce che i titolari *"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle"*





persone fisiche, [...] mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio", l'articolo 29 del Regolamento prevede che "chiunque agisca sotto l'autorità del Titolare del trattamento, che abbia accesso a dati personali, non può trattarli se non è istruito in tal senso dal titolare del trattamento" e, infine, l'articolo 28 del Regolamento stabilisce che "Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato".

Se ne deduce che l'individuazione, l'autorizzazione e il controllo dei soggetti idonei a svolgere le mansioni di amministratore di sistema è fondamentale per la protezione dei dati personali.

Al fine di porre in essere le prescrizioni previste dal Regolamento, il Servizio Privacy RPD ha ritenuto opportuno rivedere il **fac-simile di nomina ad Amministratore di sistema** proposto agli Enti, con l'obiettivo di fornire due diversi modelli di nomina: **uno per il caso di autorizzazione interna e l'altro nel caso di esternalizzazione del servizio**. Si ricorda che tali modelli devono essere "personalizzati" dall'Ente in relazione all'effettivo incarico affidato alla figura o alle figure che per lo stesso svolgono tali funzioni e compiti.

Inoltre, rende disponibile un **modello di relazione** che l'amministratore di sistema incaricato dovrà compilare e restituire al titolare almeno con cadenza **annuale** per essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali.

Per ogni chiarimento doveste ritenere utile o necessario, potete contattare la dott.ssa Federica Dallaporta o la dott.ssa Marta Mattiello ai seguenti recapiti: tel. 0461 987139 - e-mail serviziordp@comunitrentini.it.

Cordiali saluti.

Firmato
Il Referente
Responsabile della protezione dei dati
dott. Gianni Festi

Firmato
Il Responsabile del procedimento
dott.ssa Laura Marinelli





**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Ufficio _____
☎ 0461 20 _____
@ _____@regione.taa.it
pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Oggetto: **Nomina a responsabile del trattamento e amministratore di sistema di _____** *(indicare il nominativo del responsabile "esterno")*, ai sensi degli artt. 28 e 32 del Regolamento europeo sul trattamento dei dati personali n. 679/2016 e Provvedimento a carattere generale del Garante per la protezione dei dati personali di data 27 novembre 2008.

IL DIRIGENTE _____

- ✓ visto il Regolamento europeo sulla protezione dei dati 27 aprile 2016, n. 679;
- ✓ visto il Decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" come modificato dal decreto legislativo 8 agosto 2018, n. 101;
- ✓ visto il Provvedimento a carattere generale del Garante per la protezione dei dati personali di data 27 novembre 2008, avente ad oggetto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- ✓ vista la Circolare dell'Agenzia per l'Italia Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l'Amministrazione Digitale;
- ✓ visto il punto 8) del paragrafo 1 dell'art. 4 del Regolamento UE 2016/679 che definisce «responsabile del trattamento» la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- ✓ visto il paragrafo 1 dell'art. 28 del Regolamento UE 2016/679 che prevede che "qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato";
- ✓ visto il paragrafo 3 dell'art. 28 del Regolamento UE 2016/679 che prevede che "I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento”;

- ✓ considerato che per capacità, esperienza ed affidabilità _____ (*indicare il nominativo del responsabile “esterno”*) fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nel trattamento dei dati personali;
- ✓ in data _____ tra la Regione Autonoma Trentino-Alto Adige/Südtirol e il fornitore _____ (*indicare il nominativo del responsabile “esterno”*), è stato stipulato il contratto riferimento _____ (*indicare i riferimenti del contratto*) avente ad oggetto il servizio di assistenza e consulenza informatica, di gestione della sicurezza informatica e di gestione delle misure minime di sicurezza informatica;
- ✓ per lo svolgimento di tale attività e/o servizio, _____ (*indicare il nominativo del responsabile “esterno”*) tratta dati personali di cui è titolare la Regione Autonoma Trentino-Alto Adige/Südtirol;
- ✓ visto il Codice degli Enti Locali della Regione autonoma Trentino-Alto Adige approvato con Legge regionale 3 maggio 2018 n. 2;

NOMINA

_____ (**INDICARE IL NOMINATIVO DEL RESPONSABILE “ESTERNO”**)

QUALE

RESPONSABILE DEL TRATTAMENTO E AMMINISTRATORE DI SISTEMA

per lo svolgimento del servizio di assistenza e consulenza informatica, di gestione della sicurezza informatica e di gestione delle misure minime di sicurezza informatica dell’ente

effettuato con strumenti elettronici o comunque automatizzati o con strumenti diversi a decorrere dal _____ e fino alla cessazione del contratto

L’elenco completo dei soggetti autorizzati a prestare le attività di assistenza informatica alla Regione Autonoma Trentino-Alto Adige/Südtirol è riportato nell’allegato A, parte integrante del presente atto di nomina.

In relazione a tale incarico, il fornitore dovrà opportunamente autorizzare, istruire e monitorare i soggetti indicati nell’Allegato A, che avranno il compito di sovrintendere e gestire le risorse del sistema informativo e del sistema di basi di dati dell’amministrazione regionale, in base alle prescrizioni e indicazioni date dal Titolare.

In qualità di amministratore di sistema e responsabile del trattamento, il fornitore può accedere ed effettuare il trattamento dei dati gestiti nel sistema informatico unicamente per finalità di gestione, manutenzione e limitando le operazioni a quelle necessarie a tali fini, trattando i dati personali di cui viene a conoscenza nell’ambito dello svolgimento delle operazioni di manutenzione in modo lecito, con assoluta riservatezza e secondo correttezza.

In particolare, nell’effettuare operazioni di gestione e manutenzione:

- se è necessario eseguire stampe per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, quando non strettamente necessario relativamente al test in oggetto, si devono utilizzare files di prova privi di dati personali;



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

- eventuali stampe di prova di dati personali vanno immediatamente distrutte, così come vanno cancellate o restituite le registrazioni di dati personali su supporti di registrazione;
- se è strettamente necessario accedere a files già esistenti contenenti dati personali (ad esempio files di log o per il recupero di un testo) trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito e secondo correttezza ed ai soli fini della gestione e manutenzione;
- se vi è necessità è consentito prelevare e trasferire presso il proprio centro di assistenza tecnica apparecchiature elettroniche, parti di esse o supporti contenenti i dati oggetto della manutenzione ed assistenza. Se l'oggetto della manutenzione ed assistenza non sono i dati stessi o il loro recupero, e se tecnicamente possibile, i supporti di registrazione devono essere cancellati prima dell'asporto (verificando se è necessario o utile consegnare un backup agli addetti). Ove prevista, la password di accesso è comunicata dall'incaricato il quale provvede a cambiarla al termine delle operazioni di manutenzione;
- i dati sono consegnati al solo fine della manutenzione ed assistenza e non devono essere utilizzati per scopi diversi da quelli per i quali è stato richiesto l'intervento;
- l'accesso per la tele-assistenza deve avvenire esclusivamente se motivato da oggettive necessità dipendenti dall'oggetto dell'incarico e richiede che l'incaricato attivi il programma che consente la teleassistenza.

È compito del fornitore implementare una misura idonea alla registrazione degli accessi compiuti dai propri autorizzati al sistema informativo (access log) dell'amministrazione regionale, che comprenda i riferimenti temporali e la descrizione dell'evento e che consenta di conservare tali registrazioni in maniera completa e inalterata per un periodo minimo di sei mesi.

Collaborando con il Titolare del trattamento, il fornitore deve osservare e adempiere alle seguenti prescrizioni:

- impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dall'art. 32 del Regolamento europeo 679/2019; in particolare, deve:
 1. attribuire a ciascun incaricato del trattamento le credenziali univoche di autenticazione composte da codice per l'identificazione dell'incaricato e password per l'utilizzazione del sistema e, dove previsto, dei singoli applicativi o sistemi componenti;
 2. prevedere password composte, ove tecnicamente possibile, da almeno otto caratteri;
 3. prevedere che uno stesso codice non possa, neppure in tempi diversi, essere riassegnato a persone diverse;
 4. prevedere un sistema che obblighi gli incaricati alla modifica delle credenziali univoche di autenticazione con una cadenza trimestrale;
 5. operare la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi o in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- impostare e gestire un sistema di autorizzazione informatica per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme dall'art. 32 del Regolamento europeo 679/2019; in particolare deve:
 1. configurare d'intesa con il titolare un sistema di autorizzazione;
 2. configurare i profili di autorizzazione degli incaricati e dei responsabili prima dell'inizio del trattamento;
 3. periodicamente e almeno annualmente verificare le condizioni per la conservazione dei profili di autorizzazione da parte degli incaricati e dei responsabili
 4. verificare costantemente che l'amministrazione regionale abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dalla Circolare dell'Agenzia per l'Italia



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l'Amministrazione Digitale provvedendo senza indugio agli adeguamenti eventualmente necessari e supportarlo nel loro aggiornamento;

- suggerire l'adozione e l'aggiornamento delle misure di tecniche e organizzative adeguate a garantire il livello di sicurezza adeguato al rischio atte a realizzare quanto previsto all'art. 32 del Regolamento europeo 679/2016;
- curare l'adozione e l'aggiornamento delle eventuali misure adeguate di cui al punto precedente;
- attivare e aggiornare con cadenza almeno semestrale idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornare periodicamente, con frequenza almeno semestrale, i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi (operazioni di backup e recovery dei dati);
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, dell'efficacia delle misure di sicurezza adottate;
- consegnare copia delle credenziali di autenticazione quale Amministratore di sistema al Titolare, incluse le password di accesso al server e alle risorse informatiche.

È compito del fornitore riferire periodicamente, ed in ogni caso con cadenza almeno annuale al Titolare sullo svolgimento dei propri compiti, mediante presentazione di dettagliata relazione degli interventi effettuati corredata dalla dimostrazione necessaria per dimostrare conformità a tutti i propri obblighi.

Il fornitore è tenuto a fornire piena collaborazione al Titolare nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

Il fornitore è tenuto ad assistere il Titolare nell'adempimento dell'obbligo di rispondere alle richieste di esercizio dei diritti degli interessati e delle istanze del Garante per la protezione dei dati personali.

L'amministratore di sistema, nell'espletamento delle sue funzioni, ha l'obbligo di rispettare anche le disposizioni e prescrizioni di cui all'art. 28 del Reg. Ue 679/2016, destinate ai responsabili del trattamento in quanto per il servizio di assistenza e consulenza informatica, di gestione della sicurezza informatica e di gestione delle misure minime di sicurezza informatica dell'ente si configura anche quale responsabile "esterno" del trattamento; in particolare:

Subresponsabili:

Il fornitore, per l'erogazione delle attività affidate e dei relativi trattamenti di dati personali, *(scegliere una delle due opzioni)*

- a. non è legittimato a ricorrere a un altro responsabile senza previa specifica autorizzazione scritta. La richiesta deve indicare le specifiche attività di trattamento affidate all'altro responsabile.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

b. è autorizzato ad affidare a un altro responsabile specifiche attività di trattamento, fornendo di seguito l'elenco degli eventuali subresponsabili:

a. subresponsabile 1: _____ (indicare il nominativo del subresponsabile)

b. subresponsabile 2: _____ (indicare il nominativo del subresponsabile)

c.

Il fornitore deve informare tempestivamente il titolare di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri subresponsabili del trattamento; il titolare può opporsi a tali modifiche.

Si ricorda che, se il fornitore ricorre ad un subresponsabile per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, il fornitore deve nominare il subresponsabile con contratto o altro atto giuridico, prescrivendo gli stessi obblighi in materia di protezione dei dati contenuti nel presente atto, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento UE 2016/679.

Istruzioni

Il fornitore ha l'obbligo di osservare le istruzioni che sono e saranno impartite dal titolare del trattamento con il presente atto e con comunicazioni successive in materia di trattamento dei dati personali.

Il fornitore ha l'obbligo di osservare la normativa speciale in materia di trattamento dei dati relativa al servizio oggetto del contratto.

Incaricati al trattamento

Il fornitore ha l'obbligo di individuare, secondo idonee modalità, i soggetti incaricati al trattamento che agiscono sotto la sua autorità.

Il fornitore ha l'obbligo di impartire le disposizioni organizzative e operative e fornire ai soggetti autorizzati le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, eseguendo gli opportuni controlli.

Misure di sicurezza

Il fornitore si impegna ad adottare e attuare, in via autonoma, le misure di sicurezza tecniche e organizzative più adeguate a garantire un livello di tutela dei dati adeguato al rischio, tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento effettuato in esecuzione del Contratto.

Il fornitore provvede affinché vengano rigorosamente adottate tutte le misure idonee a garantire la disponibilità, l'integrità e la riservatezza dei dati; vale a dire misure che permettano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati trattati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità per le quali i dati sono stati



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

raccolti e di modifiche o cancellazioni a seguito di errori o di azioni volontarie, ma anche a seguito di malfunzionamenti o danni dei sistemi tecnologici.

Il fornitore verifica periodicamente lo stato di applicazione del D.lgs. 30 giugno 2003 n. 196 e del Regolamento Europeo 2016/679, nonché la corretta applicazione, il buon funzionamento dei sistemi e, ai sensi dell'art. 32 del GDPR, delle misure adottate per la tutela dei dati personali e la conformità alle indicazioni dell'Autorità Garante e del Titolare.

I dati personali, trattati in esecuzione del contratto, devono essere tenuti separati rispetto a quelli eventualmente trattati per conto di altre terze parti applicando una segregazione fisica e logica, ove possibile.

Il fornitore garantisce la stretta osservanza dell'incarico ricevuto, escludendo qualsiasi trattamento o utilizzo dei dati personali che esuli dalle attività previste nel Contratto.

Il fornitore ha l'obbligo di provvedere alla formazione e tenuta del registro delle attività di trattamento svolte per conto del Titolare, se previsto dall'art. 30 del Regolamento UE 2016/679.

Il fornitore ha l'obbligo di designare un Responsabile della protezione dei dati, se previsto dall'art. 37 del Regolamento UE 2016/679 e di comunicarne il nominativo e riferimento al Titolare entro 10 giorni dalla nomina.

Il fornitore si impegna a supportare il titolare nella predisposizione e aggiornamento della valutazione di impatto del trattamento sui diritti e sulle libertà delle persone.

Trasferimento dati extra UE

Se i dati contenuti nelle banche dati vengono trasferiti in Paesi extraeuropei o se il fornitore si avvale di un subresponsabile che trasferisce i dati in Paesi extraeuropei, il fornitore deve verificare che il Paese extraeuropeo sia destinatario di una decisione di adeguatezza della Commissione Europea oppure, in mancanza, il fornitore deve offrire garanzie adeguate e verificare che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi ai sensi dell'art. 46 GDPR.

In quest'ultimo caso, il fornitore deve verificare, caso per caso, in collaborazione con il subresponsabile che trasferisce i dati, se la legge o la prassi del Paese terzo incidono sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento.

Il fornitore dovrà, se necessario, attuare misure supplementari che andranno identificate, caso per caso, conformemente alle raccomandazioni adottate dall'European Data Protection Board (raccomandazioni 01/2020; raccomandazioni 02/2020) e ne dovrà fornire puntuale rendicontazione nei termini del paragrafo Controlli e ispezioni.

Assistenza

- esercizio dei diritti dell'interessato

Il fornitore ha l'obbligo di prestare la propria collaborazione al Titolare nella predisposizione, ai sensi degli artt. 13 e 14 Regolamento UE 2016/679, dell'informativa agli interessati, della modulistica e delle altre forme idonee di informazione, inerenti al proprio servizio.



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Il fornitore ha l'obbligo di assistere il Titolare del trattamento con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo dello stesso di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento UE 2016/679.

Il fornitore ha l'obbligo di prestare la propria collaborazione per consentire al Titolare di rispondere in modo esaustivo e tempestivo alle richieste e prescrizioni delle Autorità di controllo e dell'Autorità Giudiziaria.

- **misure di sicurezza**

Il fornitore notifica al Titolare del trattamento ogni violazione di dati a carattere personale nel termine massimo di 36 ore dopo esserne venuto a conoscenza. Tale notifica è accompagnata da ogni documentazione utile per permettere al Titolare del trattamento, se necessario, di notificare la violazione all'autorità di controllo competente.

Spetta solo al Titolare decidere di non effettuare la notifica all'Autorità di controllo competente, in presenza di semplice incidente che non ha comportato perdita, distruzione, diffusione o modifica dei dati e/o, nonostante la violazione dei dati personali, sia improbabile che essa comporti un rischio per i diritti e le libertà degli Interessati. Il fornitore provvederà a fornire al Titolare del trattamento tutte le informazioni di propria competenza al fine di consentire a quest'ultimo di effettuare tale valutazione.

Previo accordo con il Titolare del trattamento, il fornitore comunica, in nome e per conto del Titolare del trattamento, la violazione di dati a carattere personale alla persona interessata al più presto, qualora, in base alla valutazione del Titolare, tale violazione sia suscettibile di generare un rischio elevato per i diritti e le libertà di una persona fisica.

- **informazioni accountability (responsabilizzazione)**

Il fornitore ha l'obbligo di mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del Regolamento UE 2016/679 e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal Titolare del trattamento o da un altro soggetto dallo stesso incaricato.

Il fornitore ha l'obbligo di informare il Titolare del trattamento di ogni comunicazione o attività di controllo o ispettiva dell'Autorità di controllo.

Controlli e ispezioni

Il fornitore ha l'obbligo di permettere al Titolare del trattamento di porre in essere controlli periodici finalizzati ad accertare l'adeguatezza delle misure di sicurezza, l'osservanza delle istruzioni impartite e in generale il rispetto della normativa in materia. Queste verifiche possono essere condotte mediante preavviso scritto di minimo 7 giorni lavorativi.

Il Titolare garantisce che:

- i controlli, le ispezioni e le verifiche di cui al paragrafo che precede avranno luogo durante il normale orario di lavoro e senza ostacolare l'attività del fornitore e di altri clienti del fornitore;



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

- tutte le informazioni ottenute o generate dal Titolare o dal/i proprio/i auditor in relazione a tali controlli, ispezioni e verifiche saranno mantenute strettamente confidenziali (salvo richieste da parte delle Autorità di controllo o, se altrimenti richiesto, dalla legge applicabile);
- conviene che il costo di siffatti controlli, verifiche o ispezioni, sarà a proprio carico, a meno che dai predetti accertamenti, controlli o ispezioni non risultino inadempimenti e/o violazioni del fornitore agli obblighi su di lui incombenti.

Manleve

Il fornitore s'impegna a risarcire, manlevare e tenere indenne il Titolare per qualsiasi danno, pretesa, risarcimento, sanzione e/o pregiudizio che possa derivargli dalla mancata osservanza degli obblighi di cui al presente atto, delle istruzioni impartite e della normativa vigente.

Il fornitore è altresì responsabile per ogni pregiudizio cagionato al Titolare da parte degli eventuali subresponsabili da lui nominati.

Qualora il fornitore eroghi ulteriori servizi o espleti ulteriori attività per conto del Titolare del trattamento che non rientrano nel contratto oggetto della presente nomina, il medesimo sarà nominato con sperato atto di nomina quale responsabile del trattamento.

IL FORNITORE

IL DIRIGENTE DELLA ____ RIPARTIZIONE

Firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Ufficio _____
☎ 0461 20 _____
@ _____@regione.taa.it
pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Gentile Signore/Gentile Signora

Oggetto: in grassetto.

Oggetto: Nomina ad Amministratore di sistema –il/la Signor/a _____ dipendente dell'ufficio _____.

IL TITOLARE

visto il Regolamento europeo sulla protezione dei dati 27 aprile 2016, n. 679;

visto il decreto legislativo 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali" come modificato dal decreto legislativo 8 agosto 2018, n. 101;

visto il Provvedimento a carattere generale del Garante per la protezione dei dati personali di data 27 novembre 2008, avente ad oggetto "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

vista la Circolare dell'Agenzia per l'Italia Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l'Amministrazione Digitale;

considerato che per capacità, esperienza ed affidabilità ill/la Signor/a _____ dipendente dell'ufficio _____ fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, con particolare riferimento al profilo relativo alla sicurezza nel trattamento dei dati personali;

visto il Codice degli Enti Locali della Regione autonoma Trentino-Alto Adige approvato con Legge regionale 3 maggio 2018 n. 2;

visto lo Statuto;



NOMINA

il/la Signor/a _____,

AMMINISTRATORE DI SISTEMA
PER LA GESTIONE E MANUTENZIONE DI _____

In relazione a tale incarico Lei ha il compito di sovrintendere e gestire le risorse del sistema informativo e del sistema di basi di dati dell'Ente, in base alle prescrizioni e indicazioni date dal Titolare.

In qualità di amministratore di sistema **Lei può accedere e effettuare il trattamento dei dati gestiti nel sistema informatico unicamente per finalità di gestione, manutenzione e limitando le operazioni a quelle necessarie a tali fini, trattando i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito, con assoluta riservatezza e secondo correttezza.**

In particolare, nell'effettuare operazioni di gestione e manutenzione:

- se è necessario eseguire stampe per controllare il funzionamento di stampanti o per verificare il funzionamento di strumenti o programmi installati, quando non strettamente necessario relativamente al test in oggetto, deve utilizzare files di prova privi di dati personali;
- eventuali stampe di prova di dati personali vanno immediatamente distrutte, così come vanno cancellate o restituite le registrazioni di dati personali su supporti di registrazione;
- se è strettamente necessario accedere a files già esistenti contenenti dati personali (ad esempio files di log o per il recupero di un testo) trattare tutti i dati personali di cui viene a conoscenza nell'ambito dello svolgimento delle operazioni di manutenzione in modo lecito e secondo correttezza ed ai soli fini della gestione e manutenzione;
- se vi è necessità Le è consentito prelevare e trasferire presso il Suo centro di assistenza tecnica apparecchiature elettroniche, parti di esse o supporti contenenti i dati oggetto della manutenzione ed assistenza. Se l'oggetto della manutenzione ed assistenza non sono i dati stessi o il loro recupero, e se tecnicamente possibile, i supporti di registrazione devono essere cancellati prima dell'asporto (verificando se è necessario o utile consegnare un backup agli addetti). Ove prevista, la password di accesso è comunicata dall'incaricato il quale provvede a cambiarla al termine delle operazioni di manutenzione;
- i dati sono consegnati al solo fine della manutenzione ed assistenza e non devono essere utilizzati per scopi diversi da quelli per i quali è stato richiesto l'intervento;
- l'accesso per la tele-assistenza deve avvenire esclusivamente se motivato da oggettive necessità dipendenti dall'oggetto dell'incarico e richiede che l'incaricato attivi il programma che consente la tele-assistenza.

È suo compito implementare una **misura idonea alla registrazione degli accessi** da Lei compiuti



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

al sistema informativo (access log), che comprenda i riferimenti temporali e la descrizione dell'evento e che consenta di conservare tali registrazioni in maniera completa e inalterata per un periodo minimo di sei mesi.

Collaborando con il Titolare del trattamento, deve osservare e adempiere alle seguenti prescrizioni:

- impostare e gestire un **sistema di autenticazione informatica** per i trattamenti di dati personali effettuati con strumenti elettronici, conforme a quanto previsto dall'art. 32 del Regolamento europeo 679/2019; in particolare, deve:
 1. attribuire a ciascun incaricato del trattamento le credenziali univoche di autenticazione composte da codice per l'identificazione dell'incaricato e password per l'utilizzazione del sistema e, dove previsto, dei singoli applicativi o sistemi componenti;
 2. prevedere password composte, ove tecnicamente possibile, da almeno otto caratteri;
 3. prevedere che uno stesso codice non possa, neppure in tempi diversi, essere riassegnato a persone diverse;
 4. prevedere un sistema che obblighi gli incaricati alla modifica delle credenziali univoche di autenticazione con una cadenza trimestrale;
 5. operare la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi o in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- impostare e gestire un **sistema di autorizzazione informatica** per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conforme dall'art. 32 del Regolamento europeo 679/2019; in particolare deve:
 1. configurare d'intesa con il titolare un sistema di autorizzazione;
 2. configurare i profili di autorizzazione degli incaricati e dei responsabili prima dell'inizio del trattamento;
 3. periodicamente e almeno annualmente verificare le condizioni per la conservazione dei profili di autorizzazione da parte degli incaricati e dei responsabili
 4. verificare costantemente che l'Ente abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dalla Circolare dell'Agenzia per l'Italia Digitale (AgID) 18 aprile 2017, n. 2, che detta le misure minime di sicurezza ICT per le Pubbliche Amministrazioni nel rispetto del Codice per l'Amministrazione Digitale provvedendo senza indugio agli adeguamenti eventualmente necessari;
- suggerire **l'adozione e l'aggiornamento delle misure di tecniche e organizzative adeguate** a garantire il livello di sicurezza adeguato al rischio atte a realizzare quanto previsto all'art. 32 del Regolamento europeo 679/2016;
- curare **l'adozione e l'aggiornamento delle eventuali misure adeguate** di cui al punto precedente;



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

- attivare e aggiornare idonei strumenti elettronici atti a proteggere i dati trattati attraverso gli elaboratori del sistema informativo contro il rischio di intrusione e contro l'azione dei virus informatici;
- aggiornare periodicamente i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- adottare procedure per la **custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi (operazioni di backup e recovery dei dati)**;
- predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno semestrale, dell'efficacia delle misure di sicurezza adottate;
- consegnare copia delle credenziali di autenticazione quale Amministratore di sistema al Titolare.

È Suo compito riferire periodicamente, ed in ogni caso con cadenza **almeno annuale** al Titolare sullo svolgimento dei Suoi compiti, mediante presentazione di **dettagliata relazione degli interventi effettuati corredata dalla dimostrazione necessaria per dimostrare conformità a tutti i suoi obblighi**.

È tenuto a fornire piena collaborazione al Titolare nello svolgimento delle verifiche periodiche circa il rispetto delle disposizioni di legge e l'adeguatezza delle misure di sicurezza adottate.

È tenuto ad assistere il Titolare nell'adempimento dell'obbligo di rispondere alle richieste di esercizio dei diritti degli interessati e delle istanze del Garante per la protezione dei dati personali.

LUOGO E DATA

PER RICEVUTA

IL CONTRAENTE

IL TITOLARE

Corpo del testo con rientro a 1.

Inserire sempre alla fine del testo la frase: "per ulteriori informazioni è a disposizione il sig./la sig.ra (cognome e nome, telefono e mail)".



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

IL SEGRETARIO GENERALE

Michael Mayr

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

MM

Allegati:

Relazione dell'amministratore di sistema riferita all'anno _____

Relativamente all'incarico di Amministratore di Sistema dell'Ente _____ contratto nr di data _____ ed in particolare al compito di riferire al _____ nome Ente _____ sullo svolgimento dei compiti svolti, mediante presentazione di relazione degli interventi effettuati corredata dalla dimostrazione di conformità a tutti i suoi obblighi in materia di protezione dei dati personali, è stata eseguita una verifica e mappatura della struttura informatica dell'Ente al fine di garantire il regolare funzionamento dell'infrastruttura tecnologica e il corretto utilizzo della stessa da parte degli utenti interni ed esterni alla rete. La relazione fornisce inoltre una panoramica sui livelli di sicurezza e di protezione dei dati.

La presente relazione intende illustrare le principali attività svolte nel corso del 2023, i problemi riscontrati e le relative soluzioni adottate, nonché sottoporre all'Ente proposte di miglioramento.

L'amministratore di sistema ha adottato una serie di misure generali per proteggere i dati personali dell'Ente, in particolare:

- Limitazione dell'accesso ai dati solo al personale autorizzato
- Aggiornamento delle politiche di sicurezza dei dati personali
- Analisi dei rischi per identificare eventuali vulnerabilità del sistema
- Utilizzo di password complesse e sicure
- Backup regolari dei dati
- Crittografia dei dati in transito e di storage (chi lo fa?)
- Monitoraggio costante delle attività
- Segnalazione delle criticità riscontrate
- Proposte di miglioramento
- Supporto per la gestione di eventuali violazioni dati personali
- Formazione del personale in materia di cybersecurity

DESCRIZIONE DELL'INFRASTRUTTURA

RETE: nome rete e descrizione

SOGGETTI/DITTE ESTERNE CHE ACCEDONO ALLA RETE: ad es. Trentino Digitale per connettività

FIGURE INTERNE INCARICATE CON RUOLI SPECIFICI: ad es. per il cambio dei dischi rimovibili di backup

SERVER FISICI: nome server principale e di replica, loro collocazione

SERVER VIRTUALI: nome server

BACKUP: tempistiche e ridondanze

DISASTER RECOVERY: nome software utilizzato e apparato di salvataggio, tempistiche di schedulazione, tempistiche di conservazione

CONNETTIVITÀ: Linea TELPAT, Conservazione dei log di accesso

CONNESSIONI PER L' ACCESSO DA REMOTO: connessioni protette con canali cifrati, tramite software appositi professionali (LogMeIn, Livecare Support). La connessione ad apparati di rete come firewall, switch e router avviene tramite protocolli https e/o SSH

CREDENZIALI DI ACCESSO/GESTIONE DEI PERMESSI UTENTE SULLE CARTELLE E LORO DISMISSIONE: tempistica/procedura per la verifica dei profili da rimuovere

AGGIORNAMENTI DI SICUREZZA AUTOMATICI: aggiornamenti automatici attivati di default su tutti i dispositivi, anche se per l'installazione di patch di software specifici potrebbe essere necessario l'intervento dell'operatore

Sono stati effettuati test di vulnerabilità e analisi del rischio per individuare eventuali punti deboli nella rete e nelle applicazioni?

- a) Sì ☐
- b) No ☐
- c) Altro:

.....

.....

Sono state aggiornate tutte le patch di sicurezza dei sistemi operativi, delle applicazioni e dei dispositivi di rete?

- a) Sì ☐
- b) No ☐
- c) Altro:

.....

.....

Sono state attuate politiche di sicurezza robuste, come l'utilizzo di password complesse, l'attivazione della crittografia dei dati sensibili e la restrizione degli accessi privilegiati?

- a) Sì ☐
- b) No ☐
- c) Altro:

.....

.....

Sono state implementate, dove possibile, delle politiche di accesso a sistemi, applicazioni, dati ecc., basate sui principi del "meno privilegiato" e della "necessità di conoscenza".

- a) Sì ☐
- b) No ☐
- c) Altro:

.....

.....

Sono stati eseguiti backup regolari e test di ripristino per garantire la disponibilità dei dati in caso di necessità e/o incidenti?

- a) Sì ☐
- b) No ☐
- c) Altro:

.....

.....

Sono stati implementati metodi di sicurezza nella configurazione della rete wi-fi? (Ad esempio Nat e log di traffico)

- a) Sì ☐
- b) No ☐
- c) Altro:

.....

.....

Sono stati aggiornati i criteri di accesso alla rete locale (Ad esempio per utenti non più in servizio)

- a) Sì ☐
- b) No ☐
- c) Altro:

.....

.....

È stata consegnata la configurazione relativa alla rete, completa di nome utente e password amministrativa?

- a) Sì ☐
- b) No ☐

c) Altro:

.....
.....

È stato aggiornato l'elenco dei software in black list?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

Sono stati configurati e aggiornati tutti i sistemi operativi e i software con patch di sicurezza e qualsiasi altro correttivo al fine di contenere le vulnerabilità di sistema?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

Il sistema firewall hardware è stato correttamente aggiornato ed implementato con nuovi plug-in di sicurezza necessari per aumentare il grado di protezione della rete?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

È stato aggiornato l'elenco dei siti web in black list?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

Sono stati forniti ai dipendenti corsi di formazione sulla sicurezza informatica e sono state adottate politiche di utilizzo responsabile della rete e degli strumenti informatici?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

Il firewall hardware, se presente, è stato aggiornato e configurato per garantire un livello elevato di controllo sulla rete senza l'utilizzo di tracciamento dati relativi agli utenti?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

Sono stati implementati piani futuri per migliorare la sicurezza informatica dell'Ente?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

È presente un "Piano di Disaster Recovery"?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

È stata effettuato una valutazione del rischio informatico nell'ultimo anno?

a) Sì ☐

b) No ☐

c) Altro:

.....
.....

SEGNALAZIONI, PROPOSTE DI SVILUPPO E MIGLIORAMENTO

.....

CONCLUSIONI

L' amministratore di sistema ritiene che le misure adottate siano adeguate per garantire la sicurezza dei dati personali degli utenti. In caso di eventuali cambiamenti normativi o tecnologici, l'amministratore di sistema si impegna a revisionare le politiche e le misure di sicurezza esistenti per garantire la conformità continua al GDPR.

Firma dell'amministratore di sistema

.....

**REGIONE AUTONOMA
TRENTINO-ALTO ADIGE/SÜDTIROL**

GIUNTA REGIONALE



**AUTONOME REGION
TRENTINO-SÜDTIROL**

REGIONALREGIERUNG

Estratto del verbale della seduta del

31.10.2019

Auszug aus dem Protokoll der Sitzung
vom

DELIBERAZIONE N.

BESCHLUSS Nr.

237

Oggetto:

Betreff:

Disciplinare per l'utilizzo dei dispositivi elettronici della Regione Autonoma Trentino-Alto Adige/Südtirol

Anweisungen für die Verwendung der elektronischen Geräte der Autonomen Region Trentino-Südtirol

Arno Kompatscher	Presidente/ Präsident	presente/anwesend
Maurizio Fugatti	Vice Presidente sostituto del Presidente / Vizepräsident-Stellvertreter des Präsidenten	presente/anwesend
Waltraud Deeg	Vice Presidente / Vizepräsidentin	assente/abwesend
Claudio Cia	Assessore / Assessor	presente/anwesend
Giorgio Leonardi	Assessore / Assessor	presente/anwesend
Manfred Vallazza	Assessore / Assessor	assente/abwesend
Michael Mayr	Segretario Generale della Giunta regionale / Generalsekretär der Regionalregierung	presente/anwesend

Su proposta dell'Assessora Waltraud Deeg
Ripartizione V – Gestione risorse strumentali
Ufficio Informatica e digitalizzazione

Auf Vorschlag der Assessorin Waltraud Deeg
Abteilung V – Verwaltung der technischen
Ressourcen
Amt für Informatik und Digitalisierung

In riferimento all'oggetto la Giunta regionale ha discusso e deliberato quanto segue:

Premesso che la diffusione delle tecnologie informatiche e telematiche ed il progressivo passaggio della società verso modelli di comunicazione sempre più integrati ed interconnessi, rende fondamentale per ogni realtà organizzativa e lavorativa, lo sviluppo di una cultura della sicurezza del proprio patrimonio informativo e della tutela dei diritti degli interessati;

Preso atto che è dovere dell'Ente individuare il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione per il trattamento dei dati personali, nonché adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi, anche per prevenire utilizzi indebiti;

Ritenuto che l'elevato uso della tecnologia informatica e in particolare l'accesso alla rete informatica, Internet e posta elettronica come strumento di lavoro, impone la necessità di regolamentarne l'utilizzo, allo scopo di fornire agli utenti un'adeguata informazione circa le modalità da seguire per un corretto utilizzo degli strumenti e delle risorse informatiche messe loro a disposizione per lo svolgimento delle proprie mansioni istituzionali;

Visto l'art. 13 "Formazione informatica dei dipendenti pubblici" del D.Lgs. 7 marzo 2005, n. 82 e s.m.;

Viste le "Linee guida per posta elettronica e internet" del Garante della privacy del 1 marzo 2007;

Visti i Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza" (in particolare il provvedimento generale del 27 novembre

Die Regionalregierung hat über die oben genannte Angelegenheit beraten und Folgendes beschlossen:

Vorausgeschickt, dass für jede Organisations- und Arbeitsstruktur angesichts des weitverbreiteten Einsatzes von Informations- und Telekommunikationstechnologien und des schrittweisen Übergangs unserer Gesellschaft zu immer stärker integrierten und verknüpften Kommunikationsmodellen die Entwicklung einer Kultur der Sicherheit des eigenen Datenbestandes und der Schutz der Rechte der Betroffenen fundamental sind;

Nach Kenntnisnahme der Tatsache, dass die Körperschaft sämtliche technischen, informatischen, organisatorischen, logistischen und prozeduralen Mindestsicherheitsmaßnahmen ergreifen muss, um den Schutz personenbezogener Daten sowie die Verfügbarkeit und Integrität der Informationssysteme zu garantieren und um eine unbefugte Nutzung zu verhindern;

Nach Dafürhalten, dass der starke Einsatz von Informationstechnologien als Arbeitsinstrument – insbesondere der Zugriff auf das Informationsnetz, auf Internet und die elektronische Post – eine Regelung erfordert, um die Nutzer über die korrekte Verwendung der ihnen für die Abwicklung ihrer institutionellen Aufgaben zur Verfügung gestellten IT-Instrumente und -Ressourcen angemessen zu informieren;

Aufgrund des Art. 13 („Digitale Ausbildung der öffentlichen Bediensteten“) des GvD vom 7. März 2005, Nr. 82 i.d.g.F.;

Nach Einsichtnahme in die von der Datenschutzbehörde erlassenen „Richtlinien für die Nutzung der elektronischen Post und von Internet“ vom 1. März 2007;

Aufgrund der von der Datenschutzbehörde erlassenen „Sicherheitsmaßnahmen“ zum Datenschutz (insbesondere der allgemeinen Maßnahme vom 27. November 2008

2008 riguardante gli Amministratori di Sistema);

Visto il Contratto collettivo 1.12.2008 e s. m.;

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;

Vista la CIRCOLARE 18 aprile 2017, n. 2/2017, recante: "Misure minime di sicurezza ICT per le pubbliche amministrazioni" dell'Agenzia per l'Italia Digitale;

Visto il Decreto Legislativo 10 agosto 2018, n. 101;

Visto il contratto repertorio n. 392 d.d. 20 dicembre 2018 stipulato tra l'amministrazione regionale e la società Informatica Alto Adige S.p.A.;

Vista la deliberazione della Giunta Regionale del 3 settembre 2019 n. 193;

Ad unanimità di voti legalmente espressi,

delibera

di approvare il "Disciplinare per l'utilizzo dei dispositivi elettronici e degli strumenti informatici, di Internet e della posta elettronica" composto da numero 12 punti (allegato A), che costituisce parte integrante della presente deliberazione;

di disporre che il Disciplinare sia portato a conoscenza di tutto il personale regionale, dei collaboratori e consulenti con qualsiasi tipologia di contratto o incarico, nonché degli Amministratori regionali e in generale di tutti coloro che utilizzano dispositivi elettronici e strumenti informatici messi a disposizione dalla Regione;

betreffend die Systemverwalter);

Aufgrund des Tarifvertrags vom 1.12.2008 i.d.g.F.;

Aufgrund der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016;

Aufgrund des Rundschreibens der Agenzia per l'Italia Digitale vom 18. April 2017, Nr. 2/2017 „ICT-Mindestsicherheitsmaßnahmen für die öffentlichen Verwaltungen“;

Aufgrund des gesetzvertretenden Dekrets vom 10. August 2018, Nr. 101;

Aufgrund des zwischen der Regionalverwaltung und der Gesellschaft Südtiroler Informatik AG unterzeichneten Vertrags vom 20. Dezember 2018, Rep. Nr. 392;

Aufgrund des Beschlusses der Regionalregierung vom 3. September 2019, Nr. 193;

beschließt die Regionalregierung

mit Einhelligkeit gesetzmäßig abgegebener Stimmen,

die Anweisungen für die Verwendung der elektronischen Geräte und der IT-Instrumente, von Internet und der elektronischen Post, die 12 Punkte umfassen (Anlage A) und ergänzender Bestandteil dieses Beschlusses sind, zu genehmigen;

zu verfügen, sämtliche Regionalbediensteten, Mitarbeiter und Berater mit jedwedem Vertrag oder Auftrag, die Regionalverwalter und im Allgemeinen alle Personen, die von der Region zur Verfügung gestellte elektronische Geräte und IT-Instrumente verwenden, über diese Anweisungen in Kenntnis zu setzen;

di disporre che il predetto Disciplinare deve essere osservato da tutti gli utilizzatori di dispositivi;

di dare atto che le prescrizioni contenute nell'allegato A potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

Letto, confermato e sottoscritto.

IL PRESIDENTE

DER PRÄSIDENT

Arno Kompatscher

firmato digitalmente / digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

zu verfügen, dass diese Anweisungen von allen Nutzern der Geräte zu befolgen sind;

zu bestätigen, dass die Inhalte der Anlage A im Lichte der gesammelten Erfahrung und der technischen Innovation aktualisiert werden können.

Gelesen, bestätigt und unterzeichnet

IL SEGRETARIO GENERALE
DELLA GIUNTA REGIONALE

DER GENERALSEKRETÄR
DER REGIONALREGIERUNG

Michael Mayr

firmato digitalmente / digital signiert

Falls dieses Dokument in Papierform übermittelt wird, stellt es die für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).



Disciplinare

Utilizzo Dispositivi Elettronici



Sommario

1. PREMESSA	3
2. GLOSSARIO	4
3. CONTESTO E NORME DI RIFERIMENTO	5
3.1 Normative di riferimento.....	5
3.2 Principi generali	6
4. GESTIONE, ASSEGNAZIONE E REVOCA DELLE CREDENZIALI DI ACCESSO.....	6
5. UTILIZZO INFRASTRUTTURA DI RETE E FILESYSTEM	7
6. UTILIZZO DEGLI STRUMENTI ELETTRONICI.....	9
6.1 Dispositivi mobili e Personal Computer Portatili.....	10
6.2 Supporti di Memorizzazione Removibili	11
7. USO DI ATTREZZATURE PRIVATE	12
8. UTILIZZO DI INTERNET	13
9. UTILIZZO DELLA POSTA ELETTRONICA.....	14
9.1 Posta elettronica ordinaria	14
9.2 Posta Elettronica Certificata - PEC	16
10. UTILIZZO DEI TELEFONI, FOTOCOPIATRICI, SCANNER E STAMPANTI	16
11. ASSISTENZA AGLI UTENTI E MANUTENZIONI	17
12. NORME FINALI	19



1. PREMESSA

È solamente con la collaborazione di tutti gli utilizzatori del sistema informatico che è possibile garantire un adeguato livello di sicurezza e protezione dei dati trattati dalle Strutture regionali. Uno dei rischi più elevati per la sicurezza di un sistema informatico è, infatti, costituito dal comportamento umano.

Spesso la scarsa conoscenza o più semplicemente il sottovalutare i pericoli correlati all'utilizzo poco responsabile delle risorse tecnologiche comporta gravi, a volte irreparabili, danni alle Organizzazioni.

La crescente diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete internet dai personal computer, espone l'Amministrazione e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità conseguenti alla violazione di specifiche disposizioni normative.

Posto che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, e che tutte le risorse ICT (Information and Communication Technology), fornite dall'Amministrazione agli Utenti devono essere utilizzate in modo appropriato, efficiente, rispettoso e per motivi lavorativi, la Regione adotta il presente regolamento interno al fine di evitare che comportamenti scorretti e/o inconsapevoli possano innescare problemi o minacce alla sicurezza informatica e al trattamento dei dati.

Considerato inoltre che la Regione, nell'ottica di uno svolgimento più agevole della propria attività, mette a disposizione dei propri collaboratori che ne necessitano per il tipo di funzioni svolte, telefoni e mezzi di comunicazione efficienti (computer portatili, tablets, telefoni cellulari, smartphone, etc.), sono state inserite nel regolamento alcune clausole relative alle modalità e ai doveri che ciascun collaboratore deve osservare nell'utilizzo di detta strumentazione.

Il presente documento si prefigge di tutelare le risorse ICT dell'Amministrazione e di fornire indicazioni agli utenti circa il corretto ed appropriato uso delle stesse. L'Amministrazione, in particolare, intende perseguire i seguenti obiettivi:

- ridurre i rischi relativi alle minacce di sicurezza informatica, preservando la disponibilità, integrità e confidenzialità dei dati e la continuità dei servizi erogati;
- garantire il rispetto della normativa in materia.



2. GLOSSARIO

Di seguito un elenco delle definizioni dei principali termini utilizzati all'interno di tale Regolamento:

Trattamento: Qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modifica, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati, siano essi strutturati e/o destrutturati.

Dato personale: Qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. In questa categoria rientrano informazioni quali dati di geolocalizzazione, targhe, indirizzo IP, immagini, registrazioni audio, etc.

Dati particolari o sensibili: I dati personali idonei a rivelare informazioni soggettive (perizie, valutazioni sul personale, pareri medici), dati che identificano origine razziale ed etnica, convinzioni religiose, filosofiche, politiche. Dati che identificano adesione a partiti politici, sindacati, stato di salute, vita ed orientamento sessuale. Dati genetici e biometrici.

Dati giudiziari: I dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Dato anonimo: Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

Titolare: La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.

Responsabile: La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Autorizzato: La persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile.

Interessato: La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

Banca di dati: Qualsiasi complesso organizzato di dati personali, siano essi strutturati e/o destrutturati, ripartito in una o più unità dislocate in uno o più siti.



Misure adeguate: Il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di Sicurezza che configurano il livello adeguato di protezione di cui viene fatta menzione all'interno del GDPR (General Data Protection Regulation).

Strumenti elettronici: Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

RPD: Responsabile Protezione dei Dati (Data Protection Officer - DPO) è un professionista con conoscenze specialistiche della normativa e delle prassi in materia di protezione dati che deve essere nominato dal Titolare formalizzandone l'incarico presso il Garante.

3. CONTESTO E NORME DI RIFERIMENTO

Il presente regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o di livello, nonché a tutti i collaboratori dell'Ente a prescindere dal rapporto contrattuale con la stessa intrattenuto.

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "utente" deve intendersi ogni dipendente e collaboratore in possesso di specifiche credenziali di autenticazione.

3.1 Normative di riferimento

Questo documento fa riferimento al seguente quadro normativo:

- Decreto Legislativo 10 agosto 2018, n. 101 - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- "Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE";
- Direttiva n. 2/2009 del Dipartimento Funzione Pubblica ad oggetto "Utilizzo di internet e della casella di posta elettronica istituzionale sul luogo di lavoro".
- Provvedimenti del Garante per la protezione dei dati personali in materia di "misure di sicurezza", in particolare con riguardo agli Amministratori di Sistema (Provvedimento generale del 27 novembre 2008);
- Garante della privacy "Linee guida per posta elettronica e internet" del 01.03.2007;.



- Decreto .Legislativo. 30 giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”(d’ora in poi “Codice”);
- Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), recante “Norme sulla tutela della libertà e dignità dei lavoratori, della libertà sindacale e dell’attività sindacale nei luoghi di lavoro e norme sul collocamento”;

3.2 Principi generali

I principi che sono a fondamento del presente disciplinare sono gli stessi espressi nel GDPR, e, precisamente:

- a) il **principio di necessità**, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 5 e 6 del Reg. UE 679/16);
- b) il **principio di pertinenza e non eccedenza** secondo il quale i **trattamenti devono essere effettuati per finalità determinate, esplicite e legittime** (art. 5 commi 1 e 2). Il datore di lavoro deve trattare i dati "nella misura meno invasiva possibile"; le attività di monitoraggio devono essere svolte solo da soggetti preposti ed essere "mirate sull'area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza".

4. GESTIONE, ASSEGNAZIONE E REVOCA DELLE CREDENZIALI DI ACCESSO

L’accesso ai sistemi dell’Amministrazione è vincolato all’utilizzo di un codice di identificazione e di una password. Quest’ultime, comunemente chiamate credenziali di autenticazione:

- vengono assegnate dall’Ufficio Informatica e digitalizzazione, previa formale richiesta del Dirigente della struttura nell’ambito della quale verrà inserito ed andrà ad operare il nuovo utente. La richiesta di attivazione delle credenziali dovrà essere completa di generalità dell’utente e dell’elenco dei sistemi informativi per i quali deve essere abilitato l’accesso. Ogni successiva variazione delle abilitazioni di accesso ai sistemi informativi dovrà essere richiesta formalmente all’Ufficio Informatica e digitalizzazione;
- consistono in un codice per l’identificazione dell’utente (altresì nominati username, nome utente o userid), assegnato dall’Ufficio Informatica e digitalizzazione, ed una password. Quest’ultima è personale e riservata e dovrà essere conservata e custodita dall’incaricato



con la massima diligenza senza divulgarla. La password deve essere di adeguata robustezza; nello specifico dovrà essere formata come minimo da otto caratteri, tra i quali dovranno essere utilizzati almeno tre di questi simboli: una maiuscola, una minuscola, un segno speciale o un numero. Non deve contenere riferimenti agevolmente riconducibili all'utente (username, nomi o date relative alla persona). L'utente dovrà procedere alla modifica della password al primo accesso e, successivamente, almeno ogni tre mesi.

Nel caso di cessazione del rapporto di lavoro con il dipendente, il Responsabile dell'Ufficio/Struttura di riferimento dovrà comunicare formalmente e preventivamente all'Ufficio Informatica e digitalizzazione la data effettiva a partire dalla quale le credenziali saranno disabilitate.

5. UTILIZZO INFRASTRUTTURA DI RETE E FILESYSTEM

Per l'accesso alle risorse informatiche dell'Ente attraverso la rete locale, ciascun utente deve essere in possesso di credenziali di autenticazione secondo quanto definito al paragrafo precedente e si fa assoluto divieto di utilizzare le credenziali di altre persone per accedere alla rete ed ai sistemi informativi regionali.

L'accesso alla rete garantisce all'utente la disponibilità di condivisioni di rete (cartelle su server) nelle quali vanno inseriti e salvati i files di lavoro, organizzati per struttura/ufficio o per diversi criteri o per obiettivi specifici di lavoro. Gli strumenti informatici e tutte le cartelle di rete possono ospitare esclusivamente contenuti professionali. Pertanto è vietato il salvataggio sui server dell'Ente di documenti non inerenti l'attività lavorativa, quali a titolo esemplificativo files e/o pratiche personali, fotografie, video, musica e quant'altro.

Ogni materiale personale rilevato dall'Ufficio Informatica e digitalizzazione a seguito di interventi di sicurezza informatica ovvero di manutenzione/aggiornamento dei sistemi verrà rimosso, ferma ogni ulteriore responsabilità civile, penale e disciplinare.

I dati risiedono sui dischi magnetici dei server di rete e su storage dedicati all'interno di cartelle e sottocartelle organizzate in maniera logica e gerarchica. In particolare:

- per ogni Ripartizione/Struttura e Ufficio esiste una cartella, che non può essere cancellata o rinominata che è identificata con la lettera M , il codice ufficio e quattro caratteri del nome ufficio (ad esempio: M:\723_INFO);



- all'interno di queste ultime possono esistere "n" sottocartelle che vengono create ed eventualmente cancellate direttamente dai dipendenti dell'ufficio, in base ai diritti loro attribuiti dal responsabile del trattamento;
- tutti i dipendenti di un ufficio hanno accesso unicamente alla cartella dell'ufficio cui sono assegnati in base ai diritti loro attribuiti dal responsabile del trattamento;
- nella cartella M:\CondivisioneStrutture ci sono delle sotto cartelle denominate con il codice di struttura/ripartizione, ogni cartella è accessibile agli utenti assegnati a quella struttura e sono utilizzate per lo scambio di documenti che devono essere visibili agli uffici appartenenti alla stessa struttura/ripartizione;
- a richiesta del responsabile del trattamento, in relazione ad attività lavorative particolari, può essere creata una cartella individuale riservata ad un singolo dipendente (R:\nomeutente) i cui diritti sono assegnati in via esclusiva e non condivisa con alcuno. Anche per questa cartella è garantito il backup dei dati.

La cartella "M:\comune" è accessibile a tutti gli utenti e si utilizza per poter scambiare dei files tra Uffici di Ripartizioni diverse. Tale cartella deve essere utilizzata esclusivamente per il tempo strettamente necessario allo scambio della documentazione, immediatamente dopo i files devono essere cancellati. **I dati sensibili, giudiziari e quelli riservati NON devono assolutamente transitare su questa cartella.**

La cartella "M:\TRADUZIONI", che è esclusivamente di "transito" per i documenti da tradurre, dispone di una sottocartella dedicata all'uso esclusivo di ogni singola Ripartizione e Ufficio. All'interno della cartella dell'ufficio possono essere create altre sottocartelle nelle quali inserire i documenti da tradurre. **Una volta terminata la traduzione i documenti interessati devono essere cancellati.**

Tutte le risorse di memorizzazione, diverse da quelle appena citate al punto precedente, non sono oggetto di backup periodici. A titolo di esempio e non esaustivo si citano: il disco C: o altri dischi locali dei singoli PC, la cartella "Documenti" o "Desktop" dell'utente, gli eventuali dispositivi di memorizzazione locali o di disponibilità personale come Hard disk portatili o NAS ad uso esclusivo. Tutte queste aree di memorizzazione non devono ospitare dati, poiché non sono garantite la sicurezza e la protezione contro una loro eventuale perdita. Pertanto la responsabilità dei salvataggi dei dati ivi contenuti è a carico del singolo utente. Si ricorda a tal proposito che è vietato



connettere alla rete locale qualsiasi dispositivo (PC esterni, router, switch, modem, stampanti, etc.) non autorizzato preventivamente dall'Ufficio Informatica e digitalizzazione.

Con regolare periodicità (almeno una volta al mese), ciascun utente provvede alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

L'Ufficio Informatica e digitalizzazione si riserva la facoltà di negare o interrompere l'accesso alla rete mediante dispositivi non adeguatamente protetti e/o aggiornati, che possano costituire una concreta minaccia per la sicurezza informatica.

6. UTILIZZO DEGLI STRUMENTI ELETTRONICI

Il personale è responsabile delle attrezzature informatiche fornite in dotazione dalla Regione; tali attrezzature devono essere utilizzate esclusivamente per attività connesse alla prestazione lavorativa. L'utilizzo non inerente l'attività lavorativa è vietato in quanto può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza. Ciascun dipendente/collaboratore si deve quindi attenere alle seguenti regole di utilizzo degli Strumenti e deve collaborare al mantenimento della loro efficienza segnalando tempestivamente all'Ufficio Informatica e digitalizzazione ogni incidente (ad es. malfunzionamento PC, indisponibilità dei servizi applicativi e di rete). Quest'ultimo, raccolta la segnalazione, avvierà il relativo processo di classificazione e risoluzione dell'incidente medesimo al fine di minimizzare gli eventuali impatti negativi sul normale svolgimento delle attività lavorative.

Tutti gli incidenti che possono determinare una violazione dei dati personali, cioè la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati ("databreach"), saranno trattati secondo le modalità previste dalla normativa vigente (GDPR).

Protezione degli strumenti informatici: le attrezzature devono essere protette da password e screen-saver (le specifiche delle quali sono riportate alla voce "4. Gestione, assegnazione e revoca delle credenziali di accesso"), e non devono essere lasciate incustodite e accessibili durante la sessione di lavoro ed al termine della stessa devono essere lasciate in condizioni di sicurezza, in modo che i dati siano protetti.



Hardware: sono vietati interventi o modifiche (aggiunte, rimozioni, sostituzioni), ai componenti delle attrezzature informatiche, in quanto tali compiti sono riservati esclusivamente ai tecnici dell'Ufficio Informatica e digitalizzazione o ai tecnici esterni incaricati dall'Ufficio medesimo, ciò per non compromettere la sicurezza del sistema informatico regionale, e per evitare violazioni a contratti di manutenzione o garanzia in essere. Non è consentita l'attivazione della password di accensione (BIOS), senza preventiva autorizzazione da parte Ufficio Informatica e digitalizzazione.

Installazione di dispositivi e/o di software: l'installazione di dispositivi e/o di software sulla rete o sui PC in dotazione al personale deve essere preventivamente autorizzata dall'Amministratore di sistema ed eseguita esclusivamente dal personale tecnico dell'Ufficio Informatica e digitalizzazione. Ogni altra modalità di installazione è vietata. È obbligatorio consentire l'installazione degli aggiornamenti di sistema che vengono proposti automaticamente, al primo momento disponibile, in modo tale da mantenere il PC sempre protetto. È vietato connettere al PC qualsiasi periferica non autorizzata preventivamente dall'Ufficio Informatica e digitalizzazione (ad esempio, ma non limitatamente a, smartphone, fotocamere, webcam, stampanti). Inoltre è vietato utilizzare il PC per l'acquisizione, la duplicazione e/o la trasmissione illegale di opere protette da copyright.

Nel caso in cui l'utente dovesse notare anomalie nel comportamento del PC, l'utente è tenuto a comunicarlo tempestivamente all'Ufficio Informatica e digitalizzazione.

Furto o smarrimento di strumenti informatici: il dipendente ha l'obbligo di segnalare tempestivamente il fatto al proprio superiore gerarchico, all'Ufficio Informatica e digitalizzazione e all'Ufficio Appalti, contratti, patrimonio ed economato, provvedendo contemporaneamente alla denuncia presso l'Autorità giudiziaria.

6.1 Dispositivi mobili e Personal Computer Portatili

Fatte salve le regole generali indicate al punto precedente, l'utilizzo di dispositivi cellulari e computer portatili, all'esterno dei locali dell'Ente, deve essere oggetto di particolare cura ed attenzione da parte degli utenti perché tale utilizzo rappresenta una fonte di rischi particolarmente rilevante in termini di sicurezza, sia delle risorse in sé sia dei dati nelle stesse contenuti. Tali dispositivi, infatti, possono essere soggetti a smarrimento, furti, distruzione o compromissione dei dati, tentativi di frode e/o accesso non autorizzato ovvero essere "infettati" da virus o codice malevole. Peraltro un'eventuale contaminazione da virus informatici potrebbe diffondersi e



ripercuotersi all'intera rete informatica dell'Amministrazione, una volta che tali dispositivi siano collegati direttamente alla rete interna. È necessario, pertanto, adottare ulteriori norme comportamentali nonché specifiche procedure, di seguito descritte, che gli utenti sono chiamati ad applicare in modo scrupoloso:

- sul disco fisso del portatile possono essere temporaneamente mantenuti solamente i dati necessari, esclusivamente per il tempo strettamente indispensabile al loro utilizzo, dati che successivamente devono essere trasferiti sulla rete locale della Regione, affinché siano regolarmente sottoposti alle procedure di backup;
- Il possessore del portatile è tenuto a controllare la presenza, l'aggiornamento ed il regolare funzionamento del software antivirus, ciò anche se il PC non è stato utilizzato. Per la verifica dell'avvenuta installazione delle più recenti versioni dei software di protezione i PC portatili sono sottoposti alla seguente procedura:
 - i portatili in dotazione agli Uffici della sede devono essere collegati alla rete locale almeno una volta alla settimana, per gli aggiornamenti automatici di sicurezza e per la manutenzione da parte dell'Ufficio Informatica e digitalizzazione;
 - i portatili in dotazione agli Uffici del Giudice di Pace, previo appuntamento concordato mensilmente con i tecnici dell'Ufficio Informatica e digitalizzazione, dovranno essere connessi alla rete locale presso l'ufficio del Giudice di Pace per la verifica degli aggiornamenti;
 - per quanto riguarda i portatili in dotazione agli Assessori od alle loro Segreterie saranno, previ appuntamenti mensili concordati con i tecnici dell'Ufficio Informatica e digitalizzazione, connessi alla rete locale.
- è consentito l'utilizzo di reti WI-FI solo se protette da crittografia;
- è vietato installare sul telefono di servizio firmware non ufficiali ed è inoltre vietato sbloccare il telefono stesso ovvero attivare i diritti di root. (autenticarsi nel sistema con privilegi elevati in modo da bypassare le restrizioni e modificare liberamente le impostazioni che normalmente risultano inaccessibili);
- sul telefono possono essere installate esclusivamente applicazioni provenienti dall'Android Market o dal Market del produttore. Non sono consentite applicazioni installate in altro modo (via file apk o simili).

6.2 Supporti di Memorizzazione Removibili

I supporti di memorizzazione removibili (CD, DVD, Memorie di massa e USB, ecc.) sono dati in uso ai dipendenti che li richiedono per scopi legati all'attività lavorativa. Essi devono essere custoditi con diligenza in luoghi sicuri (cassaforte o armadi dotati di serratura), inaccessibili a



persone non autorizzate al trattamento dei dati, in modo da evitarne lo smarrimento o il furto. Tali supporti non possono essere utilizzati per scopi personali.

Tali supporti devono essere collegati esclusivamente ad attrezzature informatiche dotate di protezioni antivirus attive ed aggiornate al fine di impedire la diffusione di virus informatici all'interno del sistema informativo regionale. Una delle cause prevalenti di diffusione di virus informatici da una macchina ad un'altra è, ad esempio, lo scambio di supporti rimovibili contenenti file infetti. Per questo motivo devono essere utilizzati esclusivamente dispositivi portatili e supporti di massa dati in dotazione dall'Ente e preventivamente sottoposti alla scansione dell'antivirus.

I supporti rimovibili sono da considerarsi supporti per il trasferimento dati e non per l'archiviazione degli stessi. Si ricorda, infatti, che i dati devono risiedere su server di rete muniti di sistema di backup, eseguita l'operazione di salvataggio sul server i dati memorizzati nei supporti di cui trattasi devono essere immediatamente eliminati.

I supporti informatici rimovibili devono essere formattati prima del loro riutilizzo, allo scopo di evitare che personale non autorizzato al trattamento dei dati memorizzati su tali supporti abbia la possibilità di prenderne visione. Le penne USB devono essere protette da password utilizzando appositi software in grado di criptarne il contenuto e renderlo così inaccessibile da chi non conosce la password.

Nel caso in cui il supporto non fosse più utilizzato è obbligatorio distruggerlo con strumenti idonei. Qualora gli uffici non fossero dotati di apparecchiature distruggi CD, DVD, queste dovranno essere richieste all'Ufficio appalti, contratti, patrimonio ed economato.

Il trasporto di dati sensibili su supporti di memoria/media (dischi fissi, stick di memoria, CD, ecc.) deve essere operato tramite memorizzazione cifrata di tali dati. Tale cifratura potrà essere realizzata per mezzo di meccanismi proprietari. In alternativa possono essere impiegati prodotti di crittografia gratuito (es. "TrueCrypt").

In ogni caso il trasporto di dati sensibili o personali su tali supporti deve essere autorizzato dal proprio superiore gerarchico.

7. USO DI ATTREZZATURE PRIVATE

All'interno degli Uffici regionali sono utilizzate attrezzature informatiche di proprietà della Regione.

L'uso di attrezzature informatiche private può essere consentito esclusivamente per lo svolgimento di particolari attività (ad es. presentazioni, convegni, collaboratori esterni, corsi), e deve essere



previamente autorizzato dall'Ufficio Informatica e digitalizzazione, che verificherà preliminarmente, unitamente al proprietario del bene, modalità di utilizzo e aggiornamento dei sistemi antivirus. Eventuali danni che si dovessero riscontrare al sistema informativo regionale a causa dell'utilizzo di hardware privato non protetto ed infetto da virus saranno risarciti dal proprietario dell'hardware medesimo.

8. UTILIZZO DI INTERNET

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente/collaboratore si deve attenere alle seguenti regole di utilizzo della rete Internet e dei relativi servizi.

È ammessa solo la navigazione in siti considerati correlati con la prestazione lavorativa, ad es. i siti istituzionali, i siti degli Enti locali, di fornitori e partner. L'accesso è regolato dal proxy con le sue policy di sicurezza debitamente implementate e aggiornate.

È vietato compiere azioni che siano potenzialmente in grado di arrecare danno all'Ente, ad esempio, il download o l'upload di file audio e/o video, l'uso di servizi di rete con finalità ludiche o, comunque, estranee all'attività lavorativa.

È vietato a chiunque il download di qualunque tipo di software gratuito (freeware) o shareware prelevato da siti Internet, se non espressamente autorizzato dall'Ufficio Informatica e digitalizzazione.

L'Ente si riserva di bloccare l'accesso a siti "a rischio" attraverso l'utilizzo di blacklist pubbliche in continuo aggiornamento e di predisporre filtri, basati su sistemi euristici di valutazione del livello di sicurezza dei siti web remoti, tali da prevenire operazioni potenzialmente pericolose o comportamenti impropri. In caso di blocco accidentale di siti di interesse, potrà contattare l'Ufficio Informatica e digitalizzazione per uno sblocco selettivo.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili, salvo i casi direttamente autorizzati dal superiore gerarchico, con il rispetto delle normali procedure di acquisto.

È assolutamente vietato l'utilizzo di abbonamenti privati per effettuare la connessione a Internet tranne in casi del tutto eccezionali e previa autorizzazione dell'Ufficio Informatica e digitalizzazione.



È assolutamente vietata la partecipazione a Forum non professionali, a Social Network, all'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Per motivi tecnici e di buon funzionamento del sistema informatico è buona norma, salvo comprovata necessità, non accedere a risorse web che impegnino in modo rilevante banda, come a titolo esemplificativo: filmati (tratti da youtube, siti di informazione, siti di streaming ecc.) o web radio, in quanto possono limitare e/o compromettere l'uso della rete agli altri utenti.

9. UTILIZZO DELLA POSTA ELETTRONICA

Le regole di seguito specificate sono adottate anche ai sensi delle "Linee guida del Garante per posta elettronica e internet" pubblicate in Gazzetta Ufficiale n. 58 del 10 marzo 2007.

Ciascun dipendente si deve attenere alle seguenti regole di utilizzo dell'indirizzo di Posta elettronica.

9.1 Posta elettronica ordinaria

Ad ogni utente viene fornito un account e-mail nominativo, generalmente coerente con il modello nome.cognome@regione.taa.it. L'utilizzo dell'e-mail deve essere limitato esclusivamente a scopi lavorativi, ed è assolutamente vietato ogni utilizzo di tipo privato. L'utente a cui è assegnata una casella di posta elettronica è responsabile del corretto utilizzo della stessa.

L'Ente fornisce, altresì, delle caselle di posta elettronica associate a ciascuna unità organizzativa, ufficio o gruppo di lavoro il cui utilizzo è da preferire rispetto alle e-mail nominative qualora le comunicazioni siano di interesse collettivo: questo per evitare che degli utenti singoli mantengano l'esclusività su dati.

L'iscrizione a mailing-list o newsletter esterne con l'indirizzo ricevuto è concessa esclusivamente per motivi professionali. Prima di iscriversi occorre verificare anticipatamente l'affidabilità del sito che offre il servizio.

Allo scopo di garantire sicurezza alla rete, evitare di aprire messaggi di posta in arrivo da mittenti di cui non si conosce l'identità o con contenuto sospetto o insolito, oppure che contengano allegati di tipo *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif. È necessario porre molta attenzione, inoltre, alla credibilità del messaggio e del mittente per evitare casi di phishing o frodi informatiche. In



qualunque situazione di incertezza contattare l'Ufficio Informatica e digitalizzazione per una valutazione dei singoli casi.

Non è consentito diffondere messaggi del tipo "catena di S. Antonio" o di tipologia simile anche se il contenuto sembra meritevole di attenzione; in particolare gli appelli di solidarietà e i messaggi che informano dell'esistenza di nuovi virus. In generale è vietato l'invio di messaggi pubblicitari di prodotti di qualsiasi tipo.

Nel caso in cui fosse necessario inviare a destinatari esterni messaggi contenenti allegati con dati personali o dati personali sensibili, è obbligatorio che questi allegati vengano preventivamente resi inintelligibili attraverso crittazione con apposito software (archiviazione e compressione con password ad esempio 7-Zip ecc.). La password di cifratura deve essere comunicata al destinatario attraverso un canale diverso dalla mail (ad esempio per telefono) e mai assieme ai dati criptati. Tutte le informazioni, i dati personali e/o sensibili di competenza possono essere inviati soltanto a destinatari - persone o Enti – qualificati e competenti.

Non è consentito l'invio automatico di e-mail all'indirizzo e-mail privato (attivando per esempio un "inoltro" automatico delle e-mail entranti), anche durante i periodi di assenza (es. ferie, malattia, infortunio ecc.). In questa ultima ipotesi, è raccomandabile utilizzare un messaggio "Out of Office" facendo menzione di chi, all'interno dell'Ente, assumerà le mansioni durante l'assenza, oppure indicando un indirizzo di mail alternativo preferibilmente l'indirizzo dell'Ufficio o Struttura.

La diffusione massiva di messaggi di posta elettronica deve essere effettuata esclusivamente per motivi inerenti il servizio, su autorizzazione del Dirigente responsabile competente.

È vietato inviare messaggi di posta elettronica in nome e per conto di un altro utente, salvo sua espressa autorizzazione.

La casella di posta elettronica personale deve essere mantenuta in ordine, cancellando messaggi e documenti la cui conservazione non è più necessaria. Anche la conservazione di messaggi con allegati pesanti è da evitare per quanto possibile, preferendo, in alternativa, il salvataggio dell'allegato sulle condivisioni.

I messaggi in entrata vengono sistematicamente analizzati da strumenti automatici alla ricerca di virus, malware o di qualsiasi altro elemento potenzialmente dannoso. Tutti quelli che il sistema identifica come pericolosi vengono spostati nella casella SPAM, quelli che vengono etichettati come virati sono automaticamente cancellati. Il sistema permette inoltre di ricategorizzare tutti i messaggi presenti nella cartella SPAM ritenuti attendibili dall'utente.



Si informa che, in caso di cessazione del rapporto lavorativo, la mail affidata all'incaricato verrà disattivata immediatamente. Il sistema in ogni caso genererà una risposta automatica al mittente, informando che la casella di posta elettronica è stata disattivata.

Si informa che per motivi di sicurezza è autorizzato l'utilizzo della casella di posta elettronica della Regione solo sui dispositivi mobili forniti dall'Ente. Il device adibito a tale accesso dovrà essere successivamente autorizzato. Previa approvazione del proprio dirigente l'accesso alla posta sarà consentito anche sui propri dispositivi personali (BYOD – Bring Your Own Device). A tal fine i Dirigenti segnaleranno le specifiche esigenze all'Ufficio Informatica e digitalizzazione.

Tali richieste comporteranno applicazione tassativa sul device di policy volte a garantire un adeguato livello di sicurezza. L'installazione e l'uso di software (App) sui dispositivi mobili (smartphone e tablet), sia BYOD che quelli di servizio, avviene sotto la completa responsabilità e gestione autonoma dell'utente stesso. L'Ente non risponde di un utilizzo illecito di software su dispositivi di proprietà personale nello svolgimento del proprio lavoro (BYOD).

9.2 Posta Elettronica Certificata - PEC

Per ogni casella sono stati individuati: un responsabile giuridico; alcuni soggetti utilizzatori per i casi di assenza o impedimento del responsabile.

Il contenuto della casella, in considerazione delle conseguenze giuridiche derivanti dall'uso della stessa (decorrenza dei termini), deve essere controllato quotidianamente dalla Ripartizione e/o ufficio individuato come responsabile giuridico.

10. UTILIZZO DEI TELEFONI, FOTOCOPIATRICI, SCANNER E STAMPANTI

Il dipendente è consapevole che gli strumenti di stampa, così come anche le altre apparecchiature, sono di proprietà dell'Ente e sono resi disponibili all'utente per rendere la prestazione lavorativa. Pertanto ne viene concesso l'uso esclusivamente per tale fine.

Qualora venisse assegnato un cellulare all'utente, quest'ultimo sarà responsabile del suo utilizzo e della sua custodia. Gli smartphone si applicano le medesime regole sopra previste per gli altri



dispositivi informatici, per quanto riguarda il mantenimento di un adeguato livello di sicurezza informatica. In particolare si raccomanda il rispetto delle regole per una corretta navigazione in Internet, se consentita.

L'Ente, per tutte le utenze telefoniche assegnate al personale, ha richiesto l'attivazione del servizio Dual Billing, al fine di consentire di effettuare con tale utenza chiamate personali e inviare SMS personali anteposendo un codice al numero telefonico di destinazione. Il dipendente che intenda usufruire delle utenze di servizio per le chiamate personali riceverà una fattura specifica a lui intestata relativa al traffico personale.

11. ASSISTENZA AGLI UTENTI E MANUTENZIONI

I tecnici dell'Ufficio Informatica e digitalizzazione possono accedere ai dispositivi informatici sia direttamente, sia mediante software di accesso remoto, per i seguenti scopi:

- verifica e risoluzione di problemi sistemistici ed applicativi, su segnalazione dell'utente finale;
- verifica del corretto funzionamento dei singoli dispositivi in caso di problemi rilevati nella rete;
- richieste di aggiornamento software e manutenzione preventiva hardware e software.

A questo fine, in data 21 dicembre 2005 è stato sottoscritto tra l'Amministrazione regionale e le Organizzazioni Sindacali l'accordo ai sensi dell'art. 4 della Legge 20 maggio 1970, n. 300 (Statuto dei lavoratori), in base al quale l'Amministrazione è stata autorizzata ad utilizzare il software di assistenza remota VNC e gli strumenti di assistenza integrati a Windows XP. Di tale accordo è stata data preventiva informazione con nota prot. n. 12294 del 14 ottobre 2005, e successivamente alla stipulazione dello stesso con circolare n. 11 di data 10 maggio 2006.

In data 14 aprile 2010, come previsto dalla lettera d) dell'Accordo del 21 dicembre 2005, stipulato ai sensi dell'art. 4 della Legge 20 maggio 1970, n. 300, le Organizzazioni Sindacali sono state preventivamente informate in merito all'aggiornamento della versione del software Microsoft e alle stesse sono state illustrate le nuove modalità operative di invito e offerta di assistenza remota.

A questo proposito si ritiene opportuno ribadire che:



- gli strumenti di assistenza remota rispettano la normativa vigente in particolare con riferimento all'obbligo di non adibire tali strumenti a finalità di controllo dei lavoratori, ed alla salvaguardia della privacy;
- i tecnici informatici sono appositamente istruiti in merito a compiti, limiti e responsabilità di intervento relativamente all'uso della metodologia di assistenza a distanza;
- tale metodologia presenta numerosi vantaggi per i dipendenti, dato che permette di eseguire un elevato numero di interventi di ripristino della funzionalità del sistema operativo, di assistenza e manutenzione nell'arco della stessa giornata;
- l'operatore informatico cui perviene una richiesta di assistenza inoltrata da un dipendente in difficoltà, è abilitato a provvedere in merito solamente se il dipendente medesimo esprimerà, per mezzo di una procedura informatizzata (diversa a seconda del software utilizzato), il proprio consenso affinché l'operatore informatico assuma il controllo del pc al solo scopo di verificare gli inconvenienti segnalati e provvedere alla loro soluzione;
- mentre l'operatore informatico svolgerà i servizi necessari, il dipendente potrà osservare in tempo reale sul proprio schermo ogni azione compiuta dal tecnico ed interrompere il collegamento in qualsiasi momento, molto semplicemente premendo un unico tasto.

Si ricorda che:

- per le sedi di Bolzano e Trento nella cartella "M:\comune\MANUALI" è depositato, per la consultazione in caso di necessità, il manuale "Documentazione Assistenza Remota";
- per gli Uffici del Giudice di Pace nella cartella "GdPcomune\MANUALI" è depositato, per la consultazione in caso di necessità, il manuale "Documentazione Assistenza Remota".

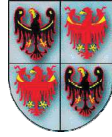
L'accesso in teleassistenza sui PC della rete richiesto da terzi (fornitori e/o altri) deve essere autorizzato dall'Ufficio Informatica e digitalizzazione, per le verifiche delle modalità di intervento per il primo accesso. Le richieste successive, se effettuate con la medesima modalità, possono essere gestite autonomamente dall'utente finale.

Durante gli interventi in teleassistenza da parte di operatori terzi, l'utente richiedente o i tecnici dell'Ufficio Informatica e digitalizzazione devono presenziare la sessione remota, in modo tale da verificare ed impedire eventuali comportamenti non conformi al presente regolamento.



12. NORME FINALI

La pubblicazione del presente documento, a cura dell'Ufficio Informatica e digitalizzazione, avverrà nelle seguenti forme: trasmissione per posta elettronica interna a tutti i Dirigenti e Direttori, e a tutti i dipendenti provvisti di e-mail e attraverso la rete informatica interna e sarà consultabile in qualsiasi momento nella seguente cartella M:\Comune\SICUREZZA\Disposizioni interne in materia di sicurezza informatica e pubblicato nella sezione "Amministrazione trasparente" del sito della Regione.



ANLAGE A)

ANWEISUNGEN FÜR DIE VERWENDUNG DER ELEKTRONISCHEN GERÄTE



Inhaltsverzeichnis

1. EINLEITUNG	3
2. Glossar	4
3. INHALT UND BEZUGSBESTIMMUNGEN	5
3.1 Bezugsbestimmungen	5
3.2 Allgemeine Grundsätze	6
4. VERWALTUNG, ERTEILUNG UND WIDERRUF DER ZUGANGSDATEN.....	6
5. NUTZUNG DER NETZINFRASTRUKTUR UND DES DATEISYSTEMS.....	7
6. VERWENDUNG DER ELEKTRONISCHEN GERÄTE.....	9
6.1 Mobile Geräte und Laptops.....	11
6.2 ENTFERNBARE DATENTRÄGER	12
7. VERWENDUNG PRIVATER GERÄTE	13
8. NUTZUNG VON INTERNET	13
9. NUTZUNG DER ELEKTRONISCHEN POST	14
9.1 Normale E-Mail-Postfächer	15
9.2 Zertifizierte elektronische Post – PEC.....	17
10. VERWENDUNG VON TELEFONEN, KOPIERGERÄTEN, SCANNERN UND DRUCKERN.....	17
11. NUTZERBETREUUNG UND WARTUNG.....	17
12. SCHLUSSBESTIMMUNGEN	19



1. EINLEITUNG

Die Sicherheit und der Schutz der von den Regionalämtern verarbeiteten Daten kann nur dann angemessen gewährleistet werden, wenn alle Nutzer des IT-Systems dazu beitragen. Das menschliche Verhalten stellt nämlich eines der größten Risiken für ein Informationssystem dar.

Eine mangelhafte Sachkenntnis oder einfach nur die Unterschätzung der mit der unverantwortlichen Nutzung technologischer Instrumente zusammenhängenden Gefahren bringt schwere, manchmal nicht wieder gutzumachende Schäden mit sich.

Der zunehmende Einsatz der neuen Informationstechnologien – insbesondere der freie Zugriff auf Internet über die zugewiesenen PCs – setzt die Verwaltung und die Nutzer (Bedienstete und Mitarbeiter) Gefahren vermögensrechtlicher Art und zudem der Haftung für die Verletzung spezifischer Bestimmungen aus.

Vorausgesetzt, dass die informatischen und telematischen Ressourcen stets nach dem Prinzip der Sorgfalt und Korrektheit einzusetzen sind, nach dem sich normalerweise das Verhalten am Arbeitsplatz richtet, und die Nutzer alle von der Verwaltung zur Verfügung gestellten ICT-Ressourcen angemessen, effizient, mit Sorgfalt und nur zu Arbeitszwecken verwenden müssen, erlässt die Region diese internen Anweisungen, um unkorrekte und/oder unbewusste Verhaltensweisen zu vermeiden, die zu Problemen oder Gefahren für die Datensicherheit und -verarbeitung führen könnten.

Die Region stellt ihren Mitarbeitern effiziente Telefone und Kommunikationsmittel (Laptops, Tablets, Mobiltelefone, Smartphones usw.) für eine reibungslose Abwicklung der Tätigkeit zur Verfügung, sofern diese für die Ausübung ihrer Funktionen notwendig sind, weshalb in den Anweisungen einige Klauseln bezüglich der Modalitäten und Pflichten enthalten sind, die ein jeder beim Gebrauch dieser Instrumente beachten muss.

Mit diesen Anweisungen wird auch auf den Schutz der ICT-Ressourcen der Verwaltung abgezielt, indem die Nutzer über deren korrekte und angemessene Verwendung informiert werden. Die Verwaltung verfolgt insbesondere nachstehende Ziele:

- Verringerung der Risiken der Gefährdung der Informationssicherheit und Absicherung der Verfügbarkeit, Integrität und Vertraulichkeit der Daten sowie der Kontinuität der Dienstleistungen;
- Gewährleistung der Berücksichtigung der einschlägigen Bestimmungen.



2. Glossar

In der Folge ein Verzeichnis mit den Definitionen der wichtigsten in den Anweisungen verwendeten Begriffe:

Datenverarbeitung: Jeder Vorgang oder jede Vorgangsreihe – auch ohne Nutzung elektronischer Mittel – in Zusammenhang mit Erhebung, Speicherung, Organisation, Aufbewahrung, Abfrage, Verarbeitung im engeren Sinn, Änderung, Auswahl, Auszug, Vergleich, Verwendung, Verknüpfung, Sperrung, Übermittlung, Verbreitung, Löschung und Vernichtung von strukturierten und/oder nicht strukturierten Daten, auch wenn sie nicht in einer Datenbank gespeichert sind.

Personenbezogene Daten: Jegliche Informationen über eine bestimmte oder auch nur indirekt – durch Bezugnahme auf irgendeine andere Information, auch auf eine persönliche Kennnummer – bestimmbare natürliche Person, juristische Person, Körperschaft oder Vereinigung. Unter diese Kategorie fallen Informationen wie z. B. Geolokalisierung, Autokennzeichen, IP-Adressen, Bilder, Audioaufzeichnungen usw.

Besondere oder sensible Daten: Personenbezogene Daten, die subjektive Informationen (Gutachten, persönliche Bewertungen, ärztliche Zeugnisse) offenbaren; Daten, die über rassische und ethnische Herkunft, religiöse, philosophische oder politische Weltanschauung, die Mitgliedschaft bei politischen Parteien und Gewerkschaften, Gesundheitszustand, Sexualleben und –orientierung Aufschluss geben können; genetische und biometrische Daten.

Gerichtsdaten: Personenbezogene Daten, die über Verfügungen und Maßnahmen in Zusammenhang mit dem Strafregister, dem Register über die anhängigen Verwaltungsstrafverfahren und die verhängten Verwaltungsstrafen oder über die Eigenschaft einer Person als Angeklagter oder als Beschuldigter im Sinne der Art. 60 und 61 der Strafprozessordnung Aufschluss geben können.

Anonyme Daten: Daten, die von Anfang an oder nach entsprechender Verarbeitung nicht beziehungsweise nicht mehr einer bestimmten oder bestimmbaren betroffenen Person zugeordnet werden können.

Verantwortlicher: Die natürliche Person, juristische Person, öffentliche Verwaltung oder jede andere Körperschaft, Vereinigung oder Einrichtung, die das Recht hat, auch zusammen mit einem anderen Verantwortlichen, über den Zweck der Verarbeitung personenbezogener Daten, über die jeweilige Verfahrensweise und über die dafür verwendeten Mittel, einschließlich der Datensicherung, zu entscheiden;

Auftragsverarbeiter: Die natürliche Person, juristische Person, öffentliche Verwaltung oder jede andere Körperschaft, Vereinigung oder Einrichtung, die vom Verantwortlichen mit der Verarbeitung personenbezogener Daten betraut wird.



Beauftragter: Die natürliche Person, die vom Verantwortlichen oder vom Auftragsverarbeiter mit der Datenverarbeitung beauftragt wird.

Betroffene Person: Die natürliche Person, juristische Person, Körperschaft oder Vereinigung, auf die sich die personenbezogenen Daten beziehen.

Datenbank: Jede geordnete Gesamtheit personenbezogener – strukturierter und/oder nicht strukturierter – Daten, die an einem oder mehreren Orten in eine oder mehrere Einheiten unterteilt ist.

Angemessene Maßnahmen: Sämtliche technischen, informatischen, organisatorischen, logistischen und prozeduralen Sicherheitsmaßnahmen, die ein angemessenes Datenschutzniveau gemäß der Datenschutz-Grundverordnung (General Data Protection Regulation) gewährleisten.

Elektronische Mittel: Computer, Computerprogramme und jede andere elektronische oder sonst wie automatisierte Vorrichtung, mit der Daten verarbeitet werden.

Datenschutzbeauftragter: Datenschutzbeauftragter (Data Protection Officer – DPO) ist eine Person mit spezifischem Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis. Er muss vom Verantwortlichen ernannt werden, welcher der Datenschutzbehörde die Auftragserteilung mitteilt.

3. INHALT UND BEZUGSBESTIMMUNGEN

Diese Anweisungen gelten – unabhängig von Rolle und Rang – für alle Bediensteten sowie für alle Mitarbeiter der Körperschaft unabhängig von dem mit dieser eingegangenen Arbeitsvertrag.

Im Rahmen dieser Anweisungen für die Nutzung der informatischen und telematischen Ressourcen ist unter „Nutzer“ jeder Bedienstete/Mitarbeiter zu verstehen, der über spezifische Zugangsdaten verfügt.

3.1 Bezugsbestimmungen

Rechtlicher Bezugsrahmen dieser Anweisungen:

- Gesetzesvertretendes Dekret vom 10. August 2018, Nr. 101 – Bestimmungen zur Anpassung der nationalen Regelung an die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten,



zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“

- Richtlinie Nr. 2/2009 der Abteilung für öffentliches Verwaltungswesen „Nutzung von Internet und der institutionellen E-Mail-Adressen am Arbeitsplatz“
- „Sicherheitsmaßnahmen“ betreffend insbesondere die Systemverwalter (Allgemeine Maßnahme vom 27. November 2008), erlassen von der Datenschutzbehörde
- „Richtlinien für die Nutzung der elektronischen Post und von Internet“ vom 1.3.2007, erlassen von der Datenschutzbehörde,
- Gesetzesvertretendes Dekret vom 30. Juni 2003, Nr. 196 „Datenschutzkodex“ (in der Folge „Kodex“)
- Gesetz vom 20. Mai 1970, Nr. 300 (Arbeiterstatut) „Vorschriften über den Schutz der Freiheit und Würde der Arbeitnehmer, der Gewerkschaftsfreiheit und der gewerkschaftlichen Tätigkeit am Arbeitsplatz und Vorschriften über die Arbeitsvermittlung“.

3.2 Allgemeine Grundsätze

Diesen Anweisungen liegen folgende Grundsätze zugrunde, die den in der Datenschutz-Grundverordnung (DSGVO) enthaltenen entsprechen:

- a) Der **Grundsatz der Notwendigkeit**, gemäß dem bei der Konfigurierung der Informationssysteme und Informatikprogramme die Verwendung von personenbezogenen und von Identifizierungsdaten – im Rahmen der verfolgten Ziele – auf ein Minimum zu beschränken ist (Art. 5 und 6 der Verordnung EU 679/2016);
- b) Der **Grundsatz der Einschlägigkeit und Angemessenheit**, laut dem **die Verarbeitung für festgesetzte, eindeutige und legitime Zwecke erfolgen muss** (Art. 5 Abs. 1 und 2). Der Arbeitgeber muss den Umfang der Datenverarbeitung „möglichst auf ein Minimum“ beschränken; die Überwachungstätigkeit darf nur von Vorgesetzten vorgenommen werden und muss „gezielt auf die Risikobereiche unter Berücksichtigung der Datenschutzbestimmungen und – sofern zutreffend – des Grundsatzes der Geheimhaltung der Korrespondenz durchgeführt werden“.

4. VERWALTUNG, ERTEILUNG UND WIDERRUF DER ZUGANGSDATEN

Der Zugang zu den Systemen der Verwaltung erfolgt nur unter Verwendung eines Identifizierungscodes und eines Kennwortes, im Allgemeinen Zugangsdaten genannt.



- Die Zugangsdaten werden vom Amt für Informatik und Digitalisierung auf formellen Antrag des Leiters der Struktur erteilt, in welcher der neue Nutzer arbeiten wird. Der Antrag auf Aktivierung der Zugangsdaten muss die Personalien und das Verzeichnis der IT-Systeme enthalten, zu denen der Zugriff zu gewähren ist. Jegliche Änderung der Zugriffsrechte zu den IT-Systemen ist formell beim Amt für Informatik und Digitalisierung zu beantragen.
- Sie bestehen aus einem Code für die Identifizierung des Nutzers (auch Username, Nutzernamen oder Userid genannt), der vom Amt für Informatik und Digitalisierung zugewiesen wird, und einem Passwort. Letzteres ist persönlich und geheim und muss von der beauftragten Person mit größter Sorgfalt aufbewahrt werden. Das Passwort muss solide sein, d. h. es muss aus mindestens acht Schriftzeichen bestehen, wobei mindestens drei der folgenden Zeichen zu verwenden sind: ein Großbuchstabe, ein Kleinbuchstabe, ein Sonderzeichen oder eine Zahl. Es darf keine auf den Nutzer leicht zurückführbaren Bezüge (Username, Namen oder Datumsangaben zur Person) enthalten. Der Nutzer muss das Passwort beim ersten Zugang und danach alle drei Monate ändern.

Bei Beendigung des Arbeitsverhältnisses des Bediensteten muss der für das jeweilige Amt/die jeweilige Struktur Verantwortliche dem Amt für Informatik und Digitalisierung formell das effektive Datum mitteilen, ab dem die Zugangsdaten zu sperren sind.

5. NUTZUNG DER NETZINFRASTRUKTUR UND DES DATEISYSTEMS

Für den Zugang zu den IT-Ressourcen der Körperschaft über das Lokalnetz muss jeder Nutzer über die Zugangsdaten gemäß dem vorstehendem Abschnitt verfügen. Es ist strengstens verboten, die Zugangsdaten anderer Personen für den Zugriff auf das Netz und die IT-Systeme der Region zu verwenden.

Der Zugriff auf das Netz garantiert dem Nutzer die Möglichkeit des Austausches im Netz über auf Servern gespeicherten Ordnern, in die die nach Struktur/Amt oder nach anderen Kriterien für spezifische Arbeitsziele organisierten Arbeitsdateien einzufügen und zu speichern sind. Die IT-Instrumente und alle Netzordner dürfen ausschließlich zu Arbeitszwecken verwendet werden. Daher ist es verboten, auf den Servern der Körperschaft Dokumente zu speichern, die nicht die Arbeitstätigkeit betreffen, wie z. B. persönliche Dateien und/oder Unterlagen, Bilder, Videos, Musik usw.



Sämtliches persönliches Material, das vom Amt für Informatik und Digitalisierung aufgrund von Eingriffen für die Informationssicherheit bzw. die Wartung und Aktualisierung der Systeme erhoben wird, wird – unbeschadet jeglicher zivil-, straf- und disziplinarrechtlicher Haftung – gelöscht.

Die Daten werden auf die Datenträger der Netzserver und dedizierte Storages nach logischen und hierarchischen Kriterien in Ordner und Unterordner gespeichert. Im Einzelnen:

- Jeder Abteilung/Struktur und jedem Amt ist ein Ordner zugewiesen, der nicht gelöscht oder umbenannt werden kann, und der durch den Buchstaben M, den Code des Amtes und vier Schriftzeichen des Amtsnamens identifizierbar ist (z. B.: M:\723_INFO).
- In den letztgenannten Ordnern können beliebig viele Unterordner existieren, die direkt von den Bediensteten des jeweiligen Amtes – je nach den ihnen vom Auftragsverarbeiter erteilten Rechten – erstellt und eventuell gelöscht werden.
- Alle Bediensteten eines Amtes haben – je nach den ihnen vom Auftragsverarbeiter erteilten Rechten – nur Zugriff auf den Ordner des Amtes, dem sie zugeteilt sind.
- Im Ordner M:/CondivisioneStrutture existieren Unterordner, die mit dem Code der Struktur/Abteilung benannt sind. Auf den einzelnen Ordner haben alle der jeweiligen Struktur zugeteilten Nutzer Zugriff; er wird ausschließlich für den Austausch von Dateien unter den Ämtern derselben Struktur/Abteilung verwendet.
- Auf Antrag des Auftragsverarbeiters kann in Bezug auf besondere Tätigkeitsbereiche ein individueller Ordner erstellt werden, der einem einzelnen Bediensteten (R:\Nutzername) vorbehalten ist, der das ausschließliche Zugriffsrecht auf diesen Ordner hat. Auch für diesen Ordner wird stets ein Datenbackup erstellt.

Auf den Ordner „M:\comune“ haben alle Nutzer Zugriff; er ist für den Austausch von Dateien unter den Ämtern verschiedener Abteilungen zu verwenden. Dieser Ordner ist ausschließlich für die für den Datenaustausch unbedingt erforderliche Zeit zu benutzen; danach müssen die Dateien sofort gelöscht werden. **Sensible, gerichtliche und vertrauliche Daten dürfen absolut NICHT über diesen Ordner ausgetauscht werden.**

Der Ordner „M:\TRADUZIONI“, der ebenfalls nur ein „Übergangsordner“ für die zu übersetzenden Dokumente ist, enthält für jede Abteilung und jedes Amt einen Unterordner. Innerhalb der Ordner der Ämter können weitere Unterordner erstellt werden, um die zu übersetzenden Dokumente zu speichern. **Nach erfolgter Übersetzung müssen die entsprechenden Dokumente gelöscht werden.**



Von allen anderen Speicherressourcen als die oben genannten wird kein regelmäßiger Backup erstellt. Dazu zählen zum Beispiel: die Festplatte C oder andere lokale Festplatten der einzelnen PCs, der Ordner „Documenti“ oder „Desktop“ des Nutzers, die eventuellen lokalen Speichervorrichtungen oder zum ausschließlichen Gebrauch eigens zur Verfügung gestellten tragbaren Festplatten oder NAS-Geräte usw. In all diesen Speicherbereichen dürfen keine Daten gespeichert werden, weil weder die Sicherheit noch der Schutz der Daten bei eventuellem Verlust gewährleistet sind. Jeder Nutzer trägt die Verantwortung für die Speicherung der darin enthaltenen Daten. In diesem Zusammenhang wird daran erinnert, dass es verboten ist, jegliche Vorrichtung (externer PC, Router, Switch, Modem, Drucker usw.), die nicht zuvor vom Amt für Informatik und Digitalisierung genehmigt wurde, mit dem lokalen Netz zu verbinden.

Jeder Nutzer muss regelmäßig (mindestens einmal monatlich) die veralteten oder unnötigen Dateien löschen. Besondere Aufmerksamkeit ist bei der Vervielfältigung der Daten empfohlen, um eine überflüssige Archivierung zu vermeiden.

Das Amt für Informatik und Digitalisierung behält sich vor, den Zugriff auf das Netz über nicht ausreichend geschützte oder aktualisierte Vorrichtungen, die eine Gefahr für die Informationssicherheit darstellen könnten, zu verweigern oder zu unterbrechen.

6. VERWENDUNG DER ELEKTRONISCHEN GERÄTE

Das Personal ist für die von der Region zur Verfügung gestellten IT-Geräte verantwortlich; diese sind ausschließlich für die mit der Arbeitsleistung verbundenen Tätigkeiten zu verwenden. Die nicht arbeitsbedingte Nutzung ist verboten, weil dies zu Fehlfunktionen und Wartungskosten und vor allem zu Sicherheitsproblemen führen kann. Jeder Bedienstete/Mitarbeiter muss sich daher an die folgenden Anweisungen für die Verwendung der Instrumente halten und zur Erhaltung ihrer Effizienz beitragen, indem er dem Amt für Informatik und Digitalisierung jeglichen Vorfall unverzüglich meldet (z. B. Fehlfunktion des PC, Nichtverfügbarkeit von Anwendungs- und Netzdiensten). Nach Erhalt der Meldung klassifiziert und löst besagtes Amt den Vorfall, wobei es die möglichen negativen Auswirkungen auf die normale Arbeitstätigkeit minimiert.

Alle Vorfälle, die eine Verletzung der personenbezogenen Daten, d. h. eine Verletzung der Sicherheit darstellen können, welche – unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung, unbefugte Offenlegung von oder unbefugten Zugriff auf personenbezogene Daten,



die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden, bewirkt („Databreach“), werden gemäß den in den geltenden Bestimmungen (DSGVO) vorgesehenen Modalitäten behandelt.

Schutz der IT-Instrumente: Die Geräte müssen durch Passwort und Bildschirmschoner geschützt sein (Einzelheiten dazu im Abschnitt „4. Verwaltung, Erteilung und Widerruf der Zugangsdaten“). Sie dürfen während der Arbeitssession nicht unbeaufsichtigt und zugänglich sein und müssen am Ende derselben abgesichert werden, um die Daten zu schützen.

Hardware: Es ist verboten, Komponenten der IT-Geräte durch Ergänzungen, Entfernungen oder Ersetzungen zu ändern. Dafür sind ausschließlich die Techniker des Amtes für Informatik und Digitalisierung oder die von diesem Amt beauftragten externen Fachleuten zuständig, um die Sicherheit des IT-Systems der Region nicht zu beeinträchtigen und Verletzungen von Wartungs- oder Garantieverträgen zu vermeiden. Ohne vorherige Genehmigung seitens des Amtes für Informatik und Digitalisierung darf kein BIOS-Passwort angelegt werden.

Installation von Hard- und/oder Software: Die Installation von Hard- und/oder Software im Netz oder auf den PC der Bediensteten muss zuvor vom Systemverwalter genehmigt werden und darf ausschließlich von den Technikern des Amtes für Informatik und Digitalisierung vorgenommen werden. Jede andere Art der Installation ist verboten. Die automatisch vorgeschlagenen Systemaktualisierungen sind zum frühestmöglichen Zeitpunkt vorzunehmen, damit der PC stets geschützt ist. Es ist verboten, den Computer mit jeglichem Peripheriegerät zu verbinden, das nicht zuvor vom Amt für Informatik und Digitalisierung genehmigt wurde (z. B. – jedoch nicht beschränkt auf – Smartphone, Fotoapparat, Webcam, Drucker). Es ist auch verboten, den Computer für die rechtswidrige Anschaffung, Vervielfältigung und/oder Übermittlung von durch Copyright geschützten Werken zu verwenden.

Sollte der Nutzer Computeranomalien feststellen, so muss er dies unverzüglich dem Amt für Informatik und Digitalisierung melden.

Diebstahl oder Verlust von IT-Instrumenten: In diesem Fall muss der Bedienstete seinen Vorgesetzten, das Amt für Informatik und Digitalisierung sowie das Amt für Vergabeverfahren, Verträge, Vermögen und Ökonomat unverzüglich davon in Kenntnis setzen und gleichzeitig Anzeige bei der Gerichtsbehörde erstatten.



6.1 Mobile Geräte und Laptops

Unbeschadet der im vorhergehenden Abschnitt erläuterten allgemeinen Regeln müssen außerhalb des Gebäudes der Körperschaft verwendete Mobiltelefone und Laptops von den Nutzern mit besonderer Sorgfalt und Aufmerksamkeit gehandhabt werden, weil die Sicherheit der Ressourcen und der in diesen enthaltenen Daten einem relevanten Risiko ausgesetzt ist. Diese Geräte können verloren gehen oder entwendet werden, die Daten können vernichtet oder kompromittiert sowie Betrugsversuchen und/oder unbefugtem Zugriff ausgesetzt bzw. durch Viren oder Malware infiziert werden. Eine eventuelle Infizierung durch Computerviren kann sich auf das gesamte Informatiknetz der Verwaltung ausbreiten und niederschlagen, wenn diese direkt mit dem internen Netz verbunden werden. Es ist demnach notwendig, weitere Verhaltensregeln sowie spezifische Prozeduren anzuwenden, die von den Nutzern strikt zu befolgen sind, und zwar:

- Auf der Festplatte des Laptops dürfen nur die notwendigen Daten vorübergehend – d. h. ausschließlich für die für ihre Verarbeitung unbedingt erforderliche Zeit – gespeichert werden. Die Daten müssen sodann im lokalen Netz der Region gespeichert werden, damit sie regelmäßig den Backup-Verfahren unterzogen werden können.
- Der Nutzer des Laptops muss überprüfen, ob das Antivirus-Programm aktiv sowie aktualisiert ist und richtig funktioniert, auch wenn der PC nicht verwendet wurde. Für die Überprüfung der erfolgten Installation der jüngsten Versionen der Schutzsoftware werden die Laptops folgender Prozedur unterzogen:
 - Die in den Ämtern des Hauptgebäudes verwendeten Laptops müssen mindestens einmal wöchentlich an das lokale Netz für die automatische Sicherheitsaktualisierung und die Wartung seitens des Amtes für Informatik und Digitalisierung angeschlossen werden.
 - Die Laptops der Friedensgerichte müssen nach Vereinbarung eines monatlichen Termins mit den Technikern des Amtes für Informatik und Digitalisierung beim jeweiligen Friedensgericht zwecks Überprüfung der Aktualisierungen an das lokale Netz angeschlossen werden.
 - Die Laptops der Assessoren oder deren Sekretariate werden nach der Vereinbarung monatlicher Termine mit den Technikern des Amtes für Informatik und Digitalisierung an das lokale Netz angeschlossen.
- Es ist lediglich die Nutzung von verschlüsselten Wi-Fi-Netzen erlaubt.
- Es ist verboten, auf Diensttelefone nicht offizielle Firmware zu installieren. Es ist ferner verboten, dass Telefon zu entsperren bzw. Root-Rechte zu aktivieren (sich im Betriebssystem mit erweiterten Rechten anmelden, um so Einschränkungen zu umgehen und die ansonsten blockierten Einstellungen zu ändern).



- Auf das Telefon dürfen ausschließlich Android-Market-Anwendungen oder vom jeweiligen Hersteller angebotene Anwendungen installiert werden. Auf andere Art installierte Anwendungen (mittels APK Files o. Ä.) sind nicht erlaubt.

6.2 ENTFERNBARE DATENTRÄGER

Entfernbarer Datenträger (CD, DVD, Massenspeicher, USB-Sticks usw.) werden den Bediensteten zur Verfügung gestellt, die diese für mit ihrer Arbeit zusammenhängende Zwecke beantragen. Diese Datenträger müssen mit größter Sorgfalt an einem sicheren zur Datenverarbeitung nicht befugten Personen unzugänglichen Ort (in Safes oder Schränken mit Schloss) aufbewahrt werden, um deren Verlust oder Diebstahl zu vermeiden. Sie dürfen nicht zu privaten Zwecken verwendet werden.

Entfernbarer Datenträger dürfen ausschließlich an IT-Geräte mit einem aktiven und aktualisierten Antivirus-Programm angeschlossen werden, um die Einschleusung von Computerviren in das IT-System der Region zu vermeiden. Der Austausch von entfernbaren Datenträgern, die infizierte Dateien enthalten, ist nämlich einer der Hauptgründe dafür, dass Computerviren von einem Gerät auf ein anderes gelangen. Deshalb dürfen ausschließlich von der Körperschaft zur Verfügung gestellte und zuvor auf Viren überprüfte tragbare Geräte und Massenspeicher verwendet werden.

Die entfernbaren Datenträger dienen nur zur Datenübertragung und nicht zur Datenarchivierung. Es wird daran erinnert, dass alle Daten auf einem Netzserver, der ein Backup-System enthält, zu speichern sind. Die auf den entfernbaren Datenträgern enthaltenen Daten sind – sobald sie im Server gespeichert wurden – umgehend zu löschen.

Vor ihrer Wiederverwendung müssen die tragbaren Datenträger neu formatiert werden, um zu vermeiden, dass Bedienstete, die nicht zur Verarbeitung der auf diesen Datenträgern gespeicherten Daten ermächtigt sind, Einsicht in diese erhalten. USB-Sticks sind mit einem Passwort zu schützen. Dafür ist eine besondere Software zu verwenden, die den Inhalt verschlüsselt und somit Unbefugten nicht zugänglich macht.

Wird ein Datenträger nicht mehr verwendet, so muss er mit entsprechenden Geräten vernichtet werden. Sollte ein Amt nicht über Vernichtungsgeräte für CDs und DVDs verfügen, so müssen diese beim Amt für Vergabeverfahren, Verträge, Vermögen und Ökonomat angefordert werden.

Die Übertragung sensibler Daten auf Datenträger/Speichermedien (Festplatten, Speichersticks, CDs usw.) muss durch verschlüsselte Speicherung dieser Daten erfolgen. Diese kann durch proprietäre Verschlüsselungsverfahren vorgenommen werden. Alternativ können unentgeltliche Verschlüsselungssoftwares (z. B. „TrueCrypt“) verwendet werden.



Die Übertragung von sensiblen oder personenbezogenen Daten auf diese Art von Trägern muss auf jeden Fall vom Vorgesetzten genehmigt werden.

7. VERWENDUNG PRIVATER GERÄTE

In den Ämtern der Region werden IT-Geräte verwendet, die Eigentum der Region sind.

Die Verwendung privater IT-Geräte darf ausschließlich für die Ausführung besonderer Tätigkeiten (z. B. im Fall von Präsentationen, Tagungen, externen Mitarbeitern, Lehrgängen) genehmigt werden. Dafür ist zuvor eine Ermächtigung beim Amt für Informatik und Digitalisierung einzuholen, das vor dem Einsatz des Gerätes zusammen mit dessen Eigentümer die Verwendungsmodalitäten und den aktuellen Stand der Antivirus-Systeme überprüft. Für eventuelle Schäden, die im Informationssystem der Region durch die Verwendung ungeschützter und mit Viren infizierter privater Hardware entstehen, haftet der Eigentümer dieser Hardware.

8. NUTZUNG VON INTERNET

Die nachstehenden Vorschriften wurden auch im Sinne der im Gesetzblatt der Republik vom 10. März 2007, Nr. 58 veröffentlichten „Richtlinien der Datenschutzbehörde für die Nutzung der elektronischen Post und von Internet“ festgesetzt.

Jeder Bedienstete/Mitarbeiter muss sich an die folgenden Regeln für die Nutzung von Internet und der entsprechenden Dienste halten.

Es dürfen nur Websites aufgerufen werden, die als mit der Arbeitstätigkeit verbunden gelten, z. B. institutionelle Websites, Websites der örtlichen Körperschaften, von Lieferanten und Partnern. Der Zugang wird über einen Proxy-Server geregelt, dessen Sicherheitseinstellungen ordnungsgemäß implementiert sind und aktualisiert werden.

Es sind u. a. das Download oder Upload von Audio- und/oder Videodateien sowie die Nutzung von Netzdiensten zu Spielzwecken oder zu nicht mit der Arbeitstätigkeit zusammenhängenden Zwecken verboten, weil dadurch der Körperschaft potentiell ein Schaden verursacht werden kann.

Es ist verboten, jegliche Art unentgeltlicher Software (Freeware) oder Shareware von Internet ohne ausdrückliche Ermächtigung seitens des Amtes für Informatik und Digitalisierung herunterzuladen.



Die Körperschaft behält sich vor, den Zugriff auf „risikoreiche“ Websites über öffentliche stets aktualisierte Blacklists zu blockieren und Filter einzusetzen, die auf heuristischen Systemen für die Bewertung der Sicherheitsebene der remoten Websites basieren, um potentiell gefährlichen Aktionen oder unangemessenen Verhaltensweisen vorzubeugen. Bei versehentlicher Sperrung einer Website ist das Amt für Informatik und Digitalisierung für eine eventuelle Entsperrung zu kontaktieren.

Jede Art finanzieller Transaktionen – einschließlich Remote Banking, On-line Einkäufen u. Ä. – ist strengstens verboten, unbeschadet der direkt vom Vorgesetzten unter Einhaltung der ordnungsgemäßen Beschaffungsverfahren genehmigten Fälle.

Es ist absolut verboten, private Abonnements für den Anschluss an Internet zu verwenden, unbeschadet außerordentlicher Fälle und nach vorheriger Genehmigung seitens des Amtes für Informatik und Digitalisierung.

Es ist absolut verboten, an Foren, die keine Berufsforen sind, sowie an sozialen Netzwerken teilzunehmen; es dürfen keine Chat-lines (mit Ausnahme der genehmigten) und elektronische Anschlagtafeln verwendet und Eintragungen in Guestbooks auch mit Pseudonym (oder Nickname) vorgenommen werden.

Aus technischen Gründen und für den reibungslosen Betrieb des IT-Systems ist es – vorbehaltlich nachgewiesener Notwendigkeit – nicht angebracht, auf Web-Ressourcen zuzugreifen, die die Bandbreite belasten, wie z. B. Filme (aus Youtube, Information Websites, Streaming Websites usw.) oder Web Radio, da sie die Nutzung des Netzes seitens der anderen Nutzer einschränken und/oder beeinträchtigen können.

9. NUTZUNG DER ELEKTRONISCHEN POST

Die nachstehenden Vorschriften wurden auch im Sinne der im Gesetzblatt der Republik vom 10. März 2007, Nr. 58 veröffentlichten „Richtlinien der Datenschutzbehörde für die Nutzung der elektronischen Post und von Internet“ festgesetzt.

Jeder Bedienstete muss sich an die folgenden Regeln für die Nutzung der elektronischen Post halten.



9.1 Normale E-Mail-Postfächer

Jeder Nutzer erhält einen persönlichen E-Mail-Account, der folgendem Modell entspricht: Vorname.Zuname@regione.taa.it. Das elektronische Postfach ist ausschließlich für Arbeitszwecke zu nutzen; jegliche private Nutzung ist absolut verboten. Der Nutzer ist für die korrekte Nutzung des ihm zugewiesenen elektronischen Postfachs verantwortlich.

Die Körperschaft stellt ferner jeder Organisationsstruktur, jedem Amt bzw. jeder Arbeitsgruppe ein elektronisches Postfach zur Verfügung, deren Nutzung jener der persönlichen Postfächer vorzuziehen ist, wenn die Mitteilungen von allgemeinem Interesse sind, um den Exklusivzugriff auf Daten seitens einzelner Nutzer zu vermeiden.

Die Eintragung in externe Mailinglisten oder Newsletters mit der erhaltenen Adresse ist ausschließlich aus Arbeitsgründen erlaubt. Vor der Eintragung ist die Zuverlässigkeit der anbietenden Website zu überprüfen.

Zur Gewährleistung der Sicherheit des Netzes ist das Öffnen von E-Mails seitens unbekannter Absender oder mit verdächtigem oder ungewöhnlichem Inhalt, oder die *.exe, *.com, *.vbs, *.htm, *.scr, *.bat, *.js e *.pif Anlagen enthalten, zu vermeiden. Auch die Glaubwürdigkeit der Mitteilung und des Absenders muss sorgfältig überprüft werden, um Phishing oder Computerbetrug zu vermeiden. Bei jeglicher Unsicherheit ist für die Bewertung der einzelnen Vorfälle das Amt für Informatik und Digitalisierung zu kontaktieren.

Es ist verboten, Kettenbriefe oder ähnliche Botschaften zu verbreiten, auch wenn der Inhalt lobenswert erscheint, insbesondere Solidaritätsaufrufe oder Nachrichten betreffend neue Viren. Es ist im Allgemeinen verboten, Werbebotschaften von Produkten aller Art zu versenden.

Sollte es notwendig sein, externen Adressaten E-Mails mit Anlagen zu schicken, die personenbezogene oder sensible Daten enthalten, so müssen diese zuvor durch Verschlüsselung mit einer spezifischen Software unkenntlich gemacht werden (Archivierung und Kompression mit Passwort z. B. 7-Zip usw.). Das entsprechende Passwort ist dem Adressaten über einen anderen Kanal als die E-Mail (z. B. telefonisch) und nie zusammen mit den verschlüsselten Daten mitzuteilen. Alle in den Zuständigkeitsbereich fallenden Informationen, personenbezogenen und/oder sensiblen Daten dürfen nur qualifizierten und zuständigen Empfängern – Personen oder Körperschaften – gesandt werden.

Die automatische Sendung von E-Mails an die private E-Mail-Adresse (z. B. durch Aktivierung der automatischen „Weiterleitung“ der eingehenden E-Mails) auch bei Abwesenheiten (z. B. Urlaub, Krankheit, Unfall usw.) ist nicht erlaubt. In diesem Fall wird empfohlen, eine Out of Office-Nachricht mit Angabe des Namens der Person, die während der Abwesenheitszeit die



entsprechenden Aufgaben wahrnimmt, oder der alternativen E-Mail-Adresse – möglichst jene des Amtes oder der Struktur – einzurichten.

Der Massenversand von E-Mails darf ausschließlich aus Dienstgründen und nach Genehmigung der zuständigen verantwortlichen Führungskraft vorgenommen werden.

Es ist verboten, E-Mails im Namen und auf Rechnung eines anderen Nutzers zu verschicken, sofern dieser keine ausdrückliche Ermächtigung erteilt hat.

Das persönliche elektronische Postfach muss in Ordnung gehalten werden, indem Nachrichten und Dokumente gelöscht werden, deren Aufbewahrung nicht mehr notwendig ist. Es ist möglichst auch die Aufbewahrung von E-Mails mit großen Anlagen zu vermeiden. Anlagen sollten vorzugsweise in freigegebenen Ordner gespeichert werden.

Die eingehenden E-Mails werden systematisch auf Viren, Malware oder jegliche andere potentiell schadhafte Elemente überprüft. Alle vom System als gefährlich eingestuften E-Mails werden in das SPAM-Postfach weitergeleitet, und die, die Viren enthalten, werden automatisch gelöscht. Zudem bietet das System die Möglichkeit, die im SPAM-Postfach vorhandenen vom Nutzer als zuverlässig betrachteten E-Mails neu zu kategorisieren.

Bei Auflösung des Dienstverhältnisses wird das der beauftragten Person anvertraute Postfach unmittelbar automatisch deaktiviert. Das System generiert in jedem Fall eine automatische Antwort, die den Absender über die Deaktivierung des elektronischen Postfachs informiert.

Aus Sicherheitsgründen wurde die Nutzung des elektronischen Postfachs der Region nur durch von der Körperschaft zur Verfügung gestellte mobile Geräte genehmigt. Das Device für den Zugriff ist anschließend zu genehmigen. Es darf – nach vorheriger Genehmigung der Führungskraft – auch mit privaten Geräten (BYOD – Bring Your Own Device) auf die Post zugegriffen werden. Zu diesem Zweck müssen die Führungskräfte dem Amt für Informatik und Digitalisierung die spezifischen Erfordernisse mitteilen.

Diese Anträge bewirken die ausdrückliche Anwendung von Policies auf das Gerät, um ein angemessenes Sicherheitsniveau zu gewährleisten. Die Installation und die Verwendung von Software (Apps) auf mobilen Geräten (Smartphones und Tablets) – sowohl BYOD als auch Dienstgeräte – fallen unter die volle Verantwortung und autonome Verwaltung des Nutzers. Die Körperschaft haftet nicht für die rechtswidrige Nutzung von Software auf den privaten Geräten (BYOD) während der Ausübung der eigenen Arbeit.



9.2 Zertifizierte elektronische Post – PEC

Für jedes Postfach wurden ein rechtlich Verantwortlicher und einige Nutzer bei dessen Abwesenheit oder Verhinderung bestimmt.

Der Inhalt des Postfachs muss in Anbetracht der rechtlichen Folgen, die sich aus dessen Nutzung ergeben (Ablauf der Fristen), täglich von der Abteilung und/oder dem Amt überprüft werden, die/das als rechtlich verantwortlich bestimmt wurde.

.

10. VERWENDUNG VON TELEFONEN, KOPIERGERÄTEN, SCANNERN UND DRUCKERN

Die Bediensteten sind sich bewusst, dass die Drucker sowie alle weiteren Geräte Eigentum der Körperschaft sind und ihnen für die Ausübung ihrer Tätigkeit zur Verfügung gestellt werden. Die Verwendung ist daher ausschließlich für diesen Zweck erlaubt.

Bei Zuweisung eines Mobiltelefons ist der jeweilige Nutzer für dessen Verwendung und Aufbewahrung verantwortlich. Auch für Smartphones gelten die für alle anderen IT-Geräte vorgesehenen Regeln bezüglich eines angemessenen IT-Sicherheitsniveaus. Es wird insbesondere empfohlen, die Vorschriften für eine korrekten Navigation in Internet (sofern erlaubt) zu beachten.

Die Körperschaft hat für die dem Personal zugewiesenen Telefone die Aktivierung des Dual-Billing-Dienstes angefordert, damit es private Anrufe tätigen sowie private SMS durch Eingabe eines Codes vor der gewünschten Telefonnummer senden kann. Die Bediensteten, die private Anrufe mit dem Diensttelefon vorzunehmen beabsichtigen, erhalten eine auf ihren Namen ausgestellte Rechnung für die private Nutzung.

11. NUTZERBETREUUNG UND WARTUNG

Die Techniker des Amtes für Informatik und Digitalisierung können auf alle IT-Geräte sowohl direkt als auch über Software für den Fernzugriff zu folgenden Zwecken zugreifen:



- Überprüfung und Lösung von System- und Anwendungsproblemen auf Meldung des Endnutzers;
- Überprüfung des korrekten Betriebs der einzelnen Geräte bei Netzstörungen;
- Antrag auf Aktualisierung von Software und vorbeugende Wartung von Hardware und Software.

Hierfür wurde am 21. Dezember 2005 zwischen der Regionalverwaltung und den Gewerkschaften die Vereinbarung im Sinne des Art. 4 des Gesetzes vom 20. Mai 1970, Nr. 300 (Arbeitnehmerstatut) unterzeichnet, aufgrund deren die Verwaltung zur Verwendung der für die Fernwartung bestimmten VNC-Software und der Hilfsmittel für Windows XP ermächtigt wurde. Über diese Vereinbarung wurde im Vorab mit Schreiben vom 14. Oktober 2005, Prot. Nr. 12294 und nach deren Abschluss mit Rundschreiben vom 10. Mai 2006, Nr. 11 informiert.

Am 14. April 2010 wurden die Gewerkschaften gemäß Buchst. d) der im Sinne des Art. 4 des Gesetzes vom 20. Mai 1970, Nr. 300 am 21. Dezember 2005 unterzeichneten Vereinbarung über die aktualisierte Version der Microsoft-Software und über die neuen Aufforderungs- und Angebotsmodalitäten für die Fernwartung vorab informiert.

In diesem Zusammenhang wird auf Folgendes aufmerksam gemacht:

- Die für die Fernwartung bestimmten Instrumente berücksichtigen die geltenden Bestimmungen, insbesondere was die Pflicht, diese nicht für die Kontrolle der Arbeitnehmer zu verwenden, sowie den Schutz der Privatsphäre anbelangt.
- Die Informatiktechniker sind über ihre Aufgaben, Grenzen und Verantwortung bei den Eingriffen bezüglich der Fernwartung entsprechend ausgebildet.
- Diese Modalität bringt zahlreiche Vorteile für die Bediensteten mit sich, da sie eine hohe Anzahl von Eingriffen für die Wiederherstellung der Betriebsfähigkeit des Systems, die Betreuung und die Wartung im Laufe ein und desselben Tages ermöglicht.
- Der Informatiktechniker, der von einem Bediensteten mit IT-Schwierigkeiten kontaktiert wird, ist nur zum Eingriff ermächtigt, wenn der Bedienstete mittels eines elektronischen Verfahrens (welches je nach der verwendeten Software unterschiedlich sein kann) der Überprüfung und Behebung der gemeldeten Störung durch den Techniker zustimmt.
- Während der Informatiktechniker die notwendigen Handlungen vornimmt, kann der Bedienstete in Echtzeit auf dem eigenen Bildschirm jeden vom Techniker durchgeführten Vorgang verfolgen und die Verbindung zu jedem Zeitpunkt unterbrechen, indem er eine einzige Taste betätigt.



Es wird auf Folgendes hingewiesen:

- Für die Amtsgebäude in Trient und Bozen ist für die eventuell notwendige Einsichtnahme im Ordner „M:\comune\MANUALI“ das Handbuch betreffend die Fernwartung hinterlegt.
- Für die Friedensgerichte ist für die eventuell notwendige Einsichtnahme im Ordner „GdPcomune\MANUALI“ das Handbuch betreffend die Fernwartung hinterlegt.

Die von Dritten (Lieferanten und/oder anderen) angeforderte Fernunterstützung der Computer des Netzes muss vom Amt für Informatik und Digitalisierung genehmigt werden, um die Modalitäten des ersten Zugriffs zu überprüfen. Die weiteren Eingriffe können – sofern sie gemäß derselben Modalität erfolgen – autonom vom Endnutzer verwaltet werden.

Während der seitens Dritter durchgeführten Fernunterstützung müssen die antragstellenden Nutzer oder die Techniker des Amtes für Informatik und Digitalisierung der Fernwartung beiwohnen, um so eventuelle nicht diesen Anweisungen entsprechende Verhaltensweisen zu überprüfen und zu vermeiden.

12. SCHLUSSBESTIMMUNGEN

Diese Anweisungen werden vom Amt für Informatik und Digitalisierung wie folgt veröffentlicht: durch interne elektronische E-Mail an alle Leiterinnen und Leiter sowie Direktorinnen und Direktoren, an alle Bediensteten, denen ein elektronisches Postfach zugewiesen wurde, im internen IT-Netz, wo sie jederzeit im Ordner „M:\Comune\SICUREZZA\Disposizioni interne in materia di sicurezza informatica“ eingesehen werden können, sowie unter „Transparente Verwaltung“ der Website der Region.



Consorzio dei
Comuni Trentini

Trento, 08 marzo 2023
MAM/FD/LM/GF/ed

Al Sindaco/Presidente
Al Segretario/Direttore
Al Referente privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE

OGGETTO: Servizio privacy RPD – Disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica.

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto. Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.

Cordiali saluti.

Firmato
Il Direttore generale
dott. Marco Riccadonna

Firmato
Il Presidente
dott. Paride Gianmoena





Secondo quanto previsto dall'art. 32 del Regolamento Europeo 679/2016 (GDPR), il titolare del trattamento, *tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio, deve adottare le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.*

Il titolare del trattamento, in virtù del principio di *accountability* di cui all'art. 5 par. 2 del GDPR, è quindi tenuto ad adottare tutte le misure e gli strumenti che siano adeguati per il contesto di riferimento e che garantiscano altresì un livello di sicurezza adeguato, considerando che le misure devono essere personalizzate in ragione del proprio specifico contesto.

Al fine di fornire uno strumento di riferimento, **il Servizio privacy RPD ha elaborato un modello di "Disciplinare delle misure di sicurezza tecniche e organizzative e di utilizzo dei dispositivi informatici, internet e posta elettronica"**, che deve essere integrato/modificato/adattato in ragione della specificità del proprio Ente. Si suggerisce di coinvolgere anche gli amministratori di sistema nella sua implementazione per verificare che le misure inserite nel disciplinare siano coerenti con il sistema organizzativo e informatico dell'Ente.

Il disciplinare ha l'obiettivo di fornire ad amministratori, dipendenti, collaboratori e a tutti coloro che, a vario titolo, utilizzano il sistema informatico dell'Ente e/o che si avvalgono degli strumenti e spazi di lavoro, le indicazioni per una corretta e adeguata gestione dei dati personali. In particolare, il disciplinare ha ad oggetto l'uso di sistemi, applicazioni e strumenti informatici dell'Ente (PC, tablet, notebook ed altri strumenti con relativi software e applicativi, smartphone, ...), nonché regola l'utilizzo della posta elettronica e di internet.

Il disciplinare costituisce altresì strumento per la corretta regolazione del rapporto di lavoro, atteso che tale disciplina costituisce adeguata informazione delle modalità d'uso degli strumenti di lavoro e di effettuazione dei controlli nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 sulla protezione dei dati personali e dal Codice Privacy (d. lgs. 196/2003).

Newsletter

I contenuti del disciplinare verranno approfonditi con newsletter periodiche, dedicate ai medesimi temi, che seguiranno nelle settimane immediatamente successive. La rassegna di newsletter sarà chiamata *"pillole di sicurezza"*.

Per ogni chiarimento doveste ritenere utile o necessario, potete contattare la dott.ssa Federica Dallaporta o la dott.ssa Marta Mattiello ai seguenti recapiti: tel. 0461 987139 - e-mail serviziordp@comunitrentini.it.

Cordiali saluti.

Firmato
Il Referente
Responsabile della protezione dei dati
dott. Gianni Festi

Firmato
Il Responsabile del procedimento
dott.ssa Laura Marinelli

All. n. 1



DISCIPLINARE
MISURE DI SICUREZZA TECNICHE E
ORGANIZZATIVE E DI UTILIZZO DEI
DISPOSITIVI INFORMATICI, INTERNET E
POSTA ELETTRONICA
DEL _____*NOME ENTE*_____

Sommario

PREMESSA.....	3
1. Misure di sicurezza fisiche.....	3
2. Misure per il trattamento con ausilio di supporti cartacei.....	3
3. Misure di sicurezza - strumenti informatici	4
3.1 Postazioni informatiche.....	4
3.2 Credenziali e password.....	4
3.3 Banche dati, software, applicazioni e cartelle del server	5
3.4 Sistema di backup.....	5
3.5 Sistema antivirus e antispam	5
3.6 Sistema firewall	6
3.7 Server.....	6
3.8 Personal Computer	6
3.9 Supporti di memorizzazione.....	7
3.10 Fotocopiatrici e scanner	7
3.11 Misure di sicurezza per altri strumenti elettronici	7
4. Misure di sicurezza - posta elettronica, internet e videoconferenza	7
4.1 Posta Elettronica.....	7
4.2 Internet.....	8
4.3 Sistemi di telefonia.....	9
4.4 Videoconferenza.....	9
5. Strumentazione informatica in Smart Working/Lavoro Agile.....	9
6. Fine vita (documenti cartacei e dispositivi elettronici).....	10
6.1 Smaltimento dei documenti cartacei	10
6.2 Smaltimento di rifiuti elettrici ed elettronici	10
7. Interventi di assistenza e manutenzione.....	10
8. Monitoraggio e controlli	10
9. Responsabilità e sanzioni	11
ALLEGATO 1 - GLOSSARIO.....	12
ALLEGATO 2 - INVENTARIO DELLA STRUMENTAZIONE INFORMATICA, DEI SOFTWARE E DELLE APPLICAZIONI IN DOTAZIONE ALL'ENTE.....	14

PREMESSA

Il presente disciplinare ha l'obiettivo di fornire ad amministratori, dipendenti, collaboratori e a tutti coloro che, a vario titolo, utilizzano il sistema informatico dell'Ente (di seguito "utenti"), le indicazioni per una corretta e adeguata gestione dei dati personali, trattati in particolare attraverso l'uso di sistemi, applicazioni e strumenti informatici dell'Ente (PC, tablet, notebook, e-mail ed altri strumenti con relativi software e applicativi, smartphone, ...), posta elettronica ed internet che sono messi a disposizione per le attività lavorative.

I dati personali e le altre informazioni dell'utente presenti all'interno dei suddetti strumenti, o che si possono eventualmente raccogliere tramite il loro uso, sono utilizzati per finalità istituzionali, per esigenze organizzative e produttive, per la sicurezza sul lavoro e per la tutela del patrimonio dell'Ente. Per tutela del patrimonio dell'Ente, si intende la sicurezza fisica, informatica e la tutela del sistema informatico e fisico-organizzativo dell'Ente. Tali informazioni sono utilizzabili anche a fini connessi al rapporto di lavoro, visto che il presente manuale costituisce adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli, sempre nel rispetto di quanto disposto dal Regolamento Europeo 679/2016 sulla protezione dei dati personali, e dal Codice Privacy (d. lgs. 196/2003), come adeguato dal d. lgs. n. 101/2018 e ss.mm..

In via preliminare, occorre precisare che compete al datore di lavoro assicurare la funzionalità e il corretto impiego della rete di internet e della posta elettronica da parte dei lavoratori. Il datore di lavoro deve definire le modalità d'uso di tali strumenti nell'organizzazione dell'attività lavorativa, e deve adottare idonee misure di sicurezza per assicurare la disponibilità e l'integrità dei sistemi informativi e dei dati, anche al fine di prevenire utilizzi indebiti che possono essere fonte di responsabilità per i dipendenti e per l'amministrazione. Quindi le disposizioni sono in primo luogo adottate a garanzia degli interessati, e debbono altresì contemperare le esigenze degli utenti del sistema informativo con quelle dell'amministrazione.

Il presente disciplinare ha lo scopo di:

- assicurare la funzionalità ed il corretto impiego delle strumentazioni informatiche e telematiche da parte degli utenti, definendone le modalità d'uso nell'organizzazione dell'attività lavorativa;
- prevenire rischi alla sicurezza del sistema;
- responsabilizzare gli utilizzatori sulle conseguenze di un uso improprio delle strumentazioni;
- rendere noti gli strumenti messi a disposizione dell'azienda e i software disponibili indicati nell'allegato 2 "inventario della strumentazione informatica";
- definire in maniera trasparente le modalità di effettuazione dei controlli e le conseguenze, anche disciplinari, di un utilizzo indebito;
- porre in essere adeguate misure organizzative e tecnologiche volte a prevenire il rischio di utilizzi impropri degli strumenti informatici, della rete informatica e del sistema di telefonia fissa e mobile, nel rispetto dei diritti dei lavoratori e del diritto alla riservatezza.

Per chiarezza le definizioni di interesse per il presente disciplinare sono contenute nell'allegato 1 "Glossario".

1. Misure di sicurezza fisiche

Accesso alla sede: per l'accesso fisico ai locali e la disattivazione dell'allarme dell'Ente, quest'ultimo individua i soggetti autorizzati e li dota di una chiave (ad es. trasponder, chiavi semplici, codice, ...), la quale deve essere personale, univoca e non utilizzabile da altri e conservata con l'opportuna diligenza a cura dell'assegnatario.

Accesso alle sale adibite ad uso comune (riunioni o aule corso), per minimizzare i rischi relativi ad accesso fisico non autorizzato e furto, gli utenti devono seguire le seguenti regole:

- le sale riunioni e le aule corsi, quando non utilizzate, sono chiuse a chiave. Le chiavi sono custodite da personale dell'Ente incaricato per la gestione della sala o dell'aula;
- qualora le chiavi siano assegnate a personale esterno all'ente, va debitamente autorizzata e documentata la consegna e la restituzione e devono essere fornite le misure di sicurezza da osservare nell'utilizzo della sala.

2. Misure per il trattamento con ausilio di supporti cartacei

Per tutelare la riservatezza e prevenire furti, copie e/o la distruzione dei dati contenuti nei **documenti cartacei**, l'Ente applica le seguenti regole:

- i documenti cartacei possono essere consultati esclusivamente dagli utenti autorizzati;

- la consultazione è consentita esclusivamente nei limiti in cui è necessaria per lo svolgimento delle mansioni e dei compiti assegnati;
- la consultazione dei documenti cartacei è consentita per il tempo strettamente necessario allo svolgimento delle mansioni e dei compiti assegnati. Una volta espletati tali mansioni e tali compiti, i documenti devono essere riposti nella posizione dalla quale erano stati prelevati;
- i documenti cartacei non devono essere lasciati incustoditi;
- se l'utente si allontana dalla propria postazione di lavoro, i documenti presenti devono essere riposti in modo tale da tutelare la riservatezza dei dati in essi contenuta.

Gli **archivi dei documenti cartacei** sono **custoditi in locali** o in elementi di arredo muniti di serratura e chiusi a chiave. Le chiavi sono custodite dal personale autorizzato.

L'accesso alle banche dati cartacee da parte degli utenti è autorizzato dall'Ente (dal Segretario generale o dai Responsabili di Servizio/Ufficio) in ragione delle mansioni e dei compiti loro assegnati.

L'utente deve attenersi ai profili di autorizzazione assegnati in modo da garantire che il trattamento dei dati personali sia svolto esclusivamente con riferimento ai dati necessari. A fronte di modifiche organizzative dell'Ente i profili di autorizzazione dei singoli autorizzati devono essere rivisti.

Per proteggere gli archivi di documenti cartacei dal rischio di accesso fisico non autorizzato, furto e distruzione, l'accesso da parte di soggetti esterni all'Ente è consentito esclusivamente in presenza di personale dell'Ente.

3. Misure di sicurezza - strumenti informatici

3.1 Postazioni informatiche

Ciascuna postazione di lavoro è assegnata nominalmente ad un utente. In caso di necessità operativa è sempre possibile, da parte di ciascun utente, accedere alla rete tramite un'altra postazione utilizzando le proprie credenziali.

Per accedere ai servizi informatici da una postazione di lavoro, l'utente deve utilizzare un codice identificativo (id utente) e una parola chiave segreta (password). Superato il sistema di autenticazione, l'utente è collegato alla rete dell'Ente e ad internet.

Le attività di gestione e manutenzione dei personal computer dell'Ente fanno capo all'amministratore di sistema e non è permesso agli utenti di intervenire personalmente sulle apparecchiature informatiche. In particolare:

- l'Ente mette a disposizione degli utenti differenti sistemi di memorizzazione su cui effettuare il salvataggio e la condivisione dei documenti e dei files di lavoro: i dischi di rete, identificati sulle postazioni di lavoro da lettere _____ (ad es. O:, Y:, ...) ed il sistema in cloud denominato _____ (ad es, OneDrive/Google Drive, ...), utilizzabile attraverso un browser web. Su queste unità vengono svolte attività di amministrazione e salvataggio periodico (backup). Per il trasferimento dei file interni l'Ente mette a disposizione la cartella di scambio denominata _____ (ad es. Condivisa, Pubblica, Transit, ...); i file dovranno essere tagliati e incollati nella cartella di destinazione in modo da svuotare la cartella di transit;
- tutti i documenti relativi all'attività lavorativa devono essere salvati sui sistemi di memorizzazione in rete definiti al punto precedente, in aree private o condivise. I files salvati su differenti unità di memorizzazione (dischi interni alle postazioni di lavoro, chiavette USB, etc..) non sono recuperabili in caso di guasto dell'unità di memorizzazione e non saranno salvati e/o ricopiati in caso di sostituzione delle postazioni di lavoro;
- nell'utilizzo di programmi, materiali audiovisivi, documenti ed ogni altra informazione protetta a norma di legge, gli utenti devono rispettare diritti d'autore, copyright e licenze d'uso di software;
- non è permesso l'utilizzo e/o la connessione alla propria postazione di lavoro o in rete di sistemi o periferiche hardware private non autorizzate;
- è vietato pubblicare o diffondere, anche tramite social network, notizie e informazioni di cui l'utente sia venuto a conoscenza per ragione di ufficio, fatti salvi i casi in cui lo stesso sia autorizzato dall'Amministrazione;
- non è consentito utilizzare le chat interne (ad es. Teams) per farne uso non consono alla attività lavorativa.

3.2 Credenziali e password

Il sistema di autenticazione serve a regolamentare l'accesso agli strumenti informatici utilizzati dagli utenti ed a proteggere gli strumenti ed i dati in essi contenuti da accessi non autorizzati. Le **credenziali di autenticazione** permettono agli utenti di gestire solo trattamenti di dati a cui sono autorizzati.

Gli utenti autorizzati possono accedere tramite le proprie credenziali di autenticazione, costituite da un nome utente e una password e, in casi specifici, da un ulteriore codice OTP (one time password) rilasciato via SMS, App o e-mail.

Le credenziali di autenticazione sono rilasciate dall'amministratore di sistema o dal fornitore dei servizi informatici previa richiesta del segretario/responsabile dell'ufficio dell'utente interessato. La stessa procedura deve essere seguita per la disattivazione delle utenze per coloro che cessano la propria attività nell'Ente.

L'utente deve essere consapevole del fatto che "cedere" le proprie credenziali ossia comunicarle a terzi significa autorizzare terzi a proprio nome al trattamento dei dati dell'Ente, con effetti potenzialmente dannosi, e che possono esporre a responsabilità disciplinare, civile e penale.

Le credenziali di autenticazione sono strettamente personali, non devono essere condivise con altri utenti e se ne deve garantire la loro segretezza:

- non si possono utilizzare credenziali di altri utenti, anche se conosciute casualmente o fornite volontariamente da altri colleghi;
- le credenziali di autenticazione devono essere modificate o disattivate se cambia la posizione dell'utente all'interno dell'Ente (promozione, spostamento organizzativo, sospensione dell'attività o dimissioni);
- la **password** deve essere composta da almeno 8 caratteri nei quali devono essere presenti almeno un carattere speciale, un numero e un carattere maiuscolo;
- la password non deve contenere riferimenti agevolmente riconducibili all'utente;
- la password deve essere modificata dall'utente al primo utilizzo e, successivamente, con cadenza almeno trimestrale. Il sistema di autenticazione (server) deve prevedere che ogni nuova password sia diversa almeno dalle tre precedenti;
- la password deve essere mantenuta riservata, non deve essere lasciata incustodita o in vista sulla propria postazione di lavoro, non deve essere trascritta su supporti facilmente accessibili a terzi (es. post-it);
- se la password viene salvata in un file dedicato, è importante proteggere il file con password (ad es. file ZIP o RAR protetto da password).

Al fine di accrescere ulteriormente la sicurezza, l'utente:

- non deve permettere che, in propria assenza, terzi non autorizzati utilizzino gli strumenti informatici a lui assegnati;
- se si assenta temporaneamente dalla propria postazione (ad esempio nelle pause pranzo) deve spegnere o rendere non possibile l'utilizzo dello strumento informatico a lui assegnato (chiudere a chiave la porta dell'ufficio, bloccare il Pc o far partire lo screen saver sbloccabile solo con l'introduzione della password);
- sul proprio pc deve impostare l'avvio dello screen saver in automatico dopo l'inutilizzo per breve tempo, ad esempio 10 minuti.

3.3 Banche dati, software, applicazioni e cartelle del server

Il segretario/il responsabile dell'ufficio autorizza l'accesso alle banche dati informatiche dell'Ente, ai software, alle applicazioni e alle cartelle del server ed in particolare:

- decide a quali cartelle del server l'utente può avere accesso (l'abilitazione all'accesso non può essere generica a tutte le cartelle del server);
- decide a quali banche dati informatiche, software e/o applicazioni l'utente può avere accesso;
- provvede alla revisione dei profili di autorizzazione dei singoli autorizzati a fronte di modifiche organizzative, in applicazione del principio di necessità del trattamento ossia che gli autorizzati sono legittimati ad accedere ai soli dati personali pertinenti e non eccedenti per le mansioni e attività agli stessi affidate.

3.4 Sistema di backup

L'Ente dota il proprio sistema informatico di un sistema automatico di salvataggio dei dati. Il salvataggio viene eseguito a cadenza stabilita e comunque non superiore ad un giorno. Pertanto, gli utenti devono salvare tutti i dati sul server, evitando di mantenerli in locale sui singoli PC (ad es. desktop).

3.5 Sistema antivirus e antispam

Il sistema antivirus previene l'azione di programmi (malware, virus) che hanno l'obiettivo di rubare un sistema informatico, i dati o i programmi in esso contenuti, nonché danneggiare file o software, anche al fine di interrompere in modo totale o parziale il funzionamento del sistema.

Il sistema antispam serve a prevenire la ricezione di messaggi di posta elettronica indesiderati (messaggi spam). L'Ente provvede a far installare programmi antivirus e antispam che sono mantenuti automaticamente aggiornati dall'amministratore di sistema o da altri fornitori di servizi informatici.

La maggior parte dei virus sono diffusi tramite la posta elettronica e Internet, ad esempio tramite tecniche di phishing, malvertising, domain squatting, ecc.

Al fine di minimizzare il rischio di introdurre virus nel sistema informatico dell'Ente gli utenti devono:

- non aprire allegati che contengano un'estensione doppia;
- prima di aprire una e-mail, in particolare se non richiesta o nel caso in cui si ritenga quantomeno insolita, verificare il mittente ed eventualmente non aprire allegati o collegarsi a siti internet contenuti nel testo della e-mail;
- anche se l'e-mail proviene da indirizzo istituzionale o noto (ad es. INPS, Agenzia Entrate, Poste, banche ...) imitandone l'interfaccia, verificare comunque la veridicità dell'indirizzo e l'autenticità del mittente oltre al contenuto;
- prima di utilizzare supporti esterni (chiavette Usb, Hard disk esterni o CD) di qualsiasi provenienza, procedere

con un controllo da parte dell'antivirus.

3.6 Sistema firewall

Il sistema firewall permette di separare la rete informatica dell'Ente e le reti informatiche esterne (Internet e Telpat). Il sistema firewall, controllando il traffico in entrata ed in uscita dalla rete riesce a minimizzare i rischi intrusione e accesso non autorizzato alla rete informatica dell'Ente e quindi agli strumenti informatici e ai dati in essi contenuti. Il firewall dell'Ente è mantenuto aggiornato dall'amministratore di sistema.

Previsione da inserire nel caso in cui l'Ente si sia dotato di firewall interno

3.7 Server

I server sono protetti dai rischi di accesso fisico non autorizzato, distruzione o perdita di dati dovuta ad eventi fisici e all'interruzione della fornitura elettrica (prevenibile con gruppo di continuità adeguatamente dimensionato).

L'Ente assicura le seguenti misure di sicurezza:

- i server sono ospitati in appositi locali/armadi, destinati a contenere unicamente i server stessi ed eventualmente le apparecchiature di rete;
- i locali in cui sono ospitati i server/armadi, se situati in posizioni tali da rendere possibili intrusioni, sono muniti di adeguate protezioni (chiusure sicure, sistemi antintrusione, ...);
- gli accessi ai locali/armadi in cui sono ospitati server sono chiusi a chiave. Le chiavi sono custodite da utenti autorizzati che le custodisce in sicurezza;
- l'accesso ai locali in cui sono ospitati i server/armadi è consentito solo ad utenti autorizzati;
- l'accesso è documentato da un sistema automatico o manuale:
 - o Registro di accesso configurato nel sistema di apertura: registro degli accessi automatico tramite conservazione dei log di apertura della porta tramite codici/trasponder personali;
 - o Registro di accesso cartaceo: registro degli accessi indicante data, ora, firma e motivo dell'accesso, qualora non vi sia una chiave personale univoca.
- *ulteriore misura da indicare se prevista: È attivo un sistema che monitora costantemente il funzionamento dei dispositivi e degli applicativi collegati alla rete informatica. Il sistema si basa su un apposito dispositivo hardware/software che consente il tempestivo rilevamento di malfunzionamenti o guasti dei dispositivi e degli applicativi monitorati che in automatico arriva all'amministratore di sistema inviandone appositi log di allert.*

Gli utenti che hanno accesso ai locali/armadi in cui sono ospitati i server devono informare l'Ente nel caso in cui riscontrino il mancato rispetto delle misure di sicurezza.

Per prevenire i rischi di incendio, surriscaldamento e anomalia dell'alimentazione elettrica delle apparecchiature elettroniche, sono stabilite le seguenti misure di sicurezza:

- in prossimità dei locali/armadi in cui sono ospitati i server è installato un estintore a CO2 o a polvere o dispositivo antincendio munito di allarme;
- nei locali/armadi in cui sono ospitati i server è installato un sensore di temperatura che segnala se la temperatura dell'aria supera i 30° celsius;
- le copie di backup sono custodite in luoghi sicuri e diversi da dove sono presenti i server;
- la rete elettrica di alimentazione dei server è collegata ad un gruppo di continuità. L'Ente si è dotato di un gruppo elettrogeno che si attiva automaticamente in caso di mancata alimentazione della rete elettrica dell'Ente.

3.8 Personal Computer

Per proteggere i dati contenuti nei PC:

- gli utenti devono mantenere la corretta configurazione del PC; è vietato alterarne le componenti hardware e software e installare software non autorizzati;
- è vietato scaricare sul PC file audio, video o di altro tipo non necessari per lo svolgimento delle mansioni e dei compiti assegnati;
- il PC portatile, quando non utilizzato, deve essere custodito in locali o in elementi di arredo muniti di serratura e chiusi a chiave;
- è vietato scaricare sul PC portatile file audio, video o di altro tipo non necessari per lo svolgimento delle mansioni e dei compiti assegnati;
- è vietato connettere il PC portatile a reti diverse dalla rete informatica dell'Ente, se non strettamente necessario per svolgimento delle mansioni e dei compiti assegnati.
- *eventuali ulteriori misure di sicurezza: i dischi sono criptati, il bios è protetto da password, è installato un modulo antivirus aggiuntivo per le connessioni fuori rete dell'Ente.*

3.9 Supporti di memorizzazione

Gli utenti nello svolgimento delle attività a loro assegnate, se autorizzati, possono utilizzare supporti rimovibili (chiavetta Usb - Pendrive Memoria Flash, CD, cassette, ecc...). In tal caso devono rispettare le seguenti regole:

- prima di utilizzare qualsiasi tipo di memoria esterna dev'essere eseguita una scansione manuale dell'antivirus;
- se i supporti rimovibili sono adoperati anche da altri autorizzati, prima della consegna ad altro autorizzato, deve essere eseguita la formattazione del supporto al fine di cancellare tutti i dati presenti e nel caso in cui, per motivi tecnici, non possa essere eseguita la formattazione, il supporto deve essere distrutto;
- i supporti rimovibili, se contengono dati dell'Ente, devono essere conservati in modo sicuro (contenitori chiusi a chiave);
- è inibito dall'amministratore di sistema utilizzare chiavette USB autopartenti/avviabili/bootables;
- è sconsigliato l'uso di chiavette USB per il trasferimento di file in assenza di antivirus e antimalware e di PIN protettivo/sistema biometrico.

3.10 Fotocopiatrici e scanner

Gli utenti nello svolgimento delle attività a loro assegnate se utilizzano una fotocopiatrice devono seguire le seguenti regole:

- non dimenticare sotto il coperchio della fotocopiatrice o dello scanner il documento da duplicare;
- nel caso di uso di fotocopiatrici centralizzate o multifunzioni di rete dotate di disco rigido autonomo, è necessaria l'autenticazione di manutenzione da parte dell'amministratore di sistema;
- verificare la correttezza dell'esecuzione, la leggibilità del documento od eventuali errori di acquisizione del testo;
- *possibile misura aggiuntiva: introdurre codici individuali di stampa o di ufficio/area/settore in modo da pseudonimizzare e segregare le attività di stampa.*

3.11 Misure di sicurezza per altri strumenti elettronici

Agli utenti nello svolgimento delle attività possono essere assegnati o utilizzare, se autorizzati, strumenti elettronici quali cellulari, smartphone, fotocamere, videocamere, ecc....

In tal caso, al fine di minimizzare il rischio furto o perdita di detti strumenti e degli eventuali dati in loro contenuti, si devono rispettare le seguenti regole:

- gli strumenti, se contengono dati dell'Ente, devono essere conservati in modo sicuro (contenitori chiusi a chiave);
- se lo strumento è predisposto, inserire un PIN per proteggere i dati memorizzati. Tale PIN può essere condiviso solo con altre persone autorizzate al trattamento dei dati memorizzati o consegnato a responsabile incaricato della gestione degli strumenti;
- se gli strumenti sono adoperati anche da altri utenti non autorizzati al trattamento dei dati memorizzati, prima della consegna, deve essere eseguita la cancellazione di tutti i dati presenti e nel caso in cui, per motivi tecnici, non possa essere eseguita, il supporto deve essere consegnato al responsabile incaricato della gestione degli strumenti che valuta la sua eventuale distruzione;
- se sono effettuate foto o riprese, le stesse dovranno essere scaricate e memorizzate nel sistema informatico dell'Ente e dovranno essere cancellate dalla memoria dello strumento.

Vale quanto indicato precedentemente sia per il caso di un telefono fornito dall'Ente sia di un dispositivo proprio dell'utente per cui l'Ente fornisce la SIM card.

Nel caso in cui sia utilizzato un dispositivo personale (smartphone/portatile/tablet, ...) per accedere a informazioni lavorative, ad es. utilizzo della posta elettronica, tramite app o direttamente via web, l'utente è tenuto ad aggiornare costantemente il sistema operativo e applicazioni, e ad adottare idonee misure di protezione all'accesso (biometria, password, PIN), antivirus con scansioni periodiche.

4. Misure di sicurezza - posta elettronica, internet e videoconferenza

4.1 Posta Elettronica

Il servizio di posta elettronica è disponibile per ogni utente in forma centralizzata: l'indirizzo di posta elettronica può essere nominale, individuale o condiviso fra più utenti.

Nell'utilizzo della posta elettronica devono essere adottate le seguenti misure:

- l'assegnazione della casella di posta avviene unicamente per ragioni di servizio;
- le caselle nominali sono da ritenersi personali e accessibili esclusivamente da parte dell'utente proprietario attraverso l'inserimento di una password; la password deve essere mantenuta riservata e non deve essere

comunicata. L'utente, utilizzando le apposite funzioni di delega fornite dal sistema di posta elettronica può comunque concedere, in caso di necessità e per ragioni di servizio, l'accesso e l'utilizzo della propria casella ad altri colleghi;

- è a disposizione di ciascun utente una apposita funzionalità di sistema che consente di inviare automaticamente, in caso di assenze programmate, messaggi di risposta personalizzabili segnalando eventualmente l'indirizzo della persona da contattare;
- è doveroso informare tempestivamente il Referente privacy/data breach e l'amministratore di sistema su potenziali rischi o problemi inerenti alla sicurezza informatica della posta elettronica;
- verificare il destinatario del messaggio prima dell'invio e non utilizzare la modalità 'rispondi a tutti' se non realmente necessaria.
- nel caso di ricezione e-mail da destinatari sospetti è necessario procedere alla loro immediata eliminazione;
- inserire l'informativa breve per il trattamento dei dati personali e nota di riservatezza in calce all'e-mail;
- per il caso di invio tramite e-mail di dati particolari (ad es. salute, orientamenti politici, razziali, sessuali, religiosi, ecc., dati biometrici, dati giudiziari,...):
 - verificare che l'indirizzo del destinatario sia correttamente digitato;
 - l'oggetto del messaggio non deve contenere direttamente categorie particolari di dati.

In ogni caso è tassativamente vietato:

- utilizzare tecniche di "e-mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione esterne o di azioni equivalenti;
- utilizzare il servizio di posta elettronica per inoltrare 'catene di S. Antonio', appelli e petizioni (anche se possono sembrare veritieri e socialmente utili), giochi, scherzi, barzellette, messaggi inerenti a virus, etc...;
- utilizzare la casella personale per l'iscrizione a dibattiti, forum o mailing-list se non inerenti alla propria attività lavorativa;
- utilizzare il servizio di posta elettronica per trasmettere pubblicità personale o commerciale.

Nel caso di cessazione dell'attività lavorativa dell'utente della casella di posta elettronica, sia nel caso di indirizzo nominale che di funzione (ad es. presidente, sindaco, segretario...), dev'essere bloccato l'accesso dal giorno successivo/settimana e il contenuto dev'essere cancellato entro un congruo termine dando previamente la possibilità di recuperare le informazioni strettamente personali. Tempi maggiori di conservazione possono essere autorizzati dal Segretario/Direttore generale per motivi di necessità opportunamente giustificati.

Contestualmente, devono essere implementati sistemi automatici volti ad informare i terzi e a fornire indirizzi alternativi, oltre ad una policy informativa di avviso della scadenza a tempo della casella per l'utilizzatore. Nel caso invece di caselle e-mail condivise per servizio/ufficio e non riconducibili ad un unico soggetto (ad es. segreteria, anagrafe, info...) non è prevista la chiusura e la cancellazione della casella e dei dati in essa contenuti.

4.2 Internet

Tutti gli utenti in possesso di credenziali per accedere alla rete interna dell'Ente possono collegarsi alla rete internet il cui utilizzo è consentito unicamente per ragioni di servizio.

L'utente è direttamente responsabile dell'uso di internet, dei contenuti che vi ricerca, dei siti che contatta, delle informazioni che vi immette e delle modalità con cui opera.

L'utilizzo imprudente di alcuni servizi della rete internet può essere fonte di particolari minacce alla sicurezza del sistema (ad es. virus informatici) e all'immagine dell'Ente.

L'Ente ha provveduto ad inibire i siti ritenuti non pertinenti all'attività lavorativa, adottando una apposita policy di black list.

Nell'utilizzo di internet è vietato:

- lo scarico (upload e/o download) di files e/o programmi software, se non esplicitamente autorizzati;
- la partecipazione a forum non autorizzati, l'utilizzo di chat line, di bacheche elettroniche e la registrazione in guestbooks anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di questi servizi Internet se non strettamente connessi all'attività lavorativa;
- l'utilizzo del collegamento ad Internet per attività in violazione del diritto d'autore o altri diritti tutelati dalla normativa vigente;
- l'utilizzo di sistemi peer to peer (P2P), di file sharing, podcasting, webcasting o similari non pertinenti all'attività lavorativa.

Si raccomanda all'Ente di valutare limiti e modalità di un utilizzo per fini personali di internet – in tal senso si legga il capoverso seguente:

Tuttavia, l'utilizzo di internet per svolgere attività che non rientrano tra i compiti istituzionali può essere consentito ai dipendenti per assolvere incombenze amministrative e burocratiche senza allontanarsi dal luogo di lavoro purché contenuta nei tempi strettamente necessari allo svolgimento di tali transazioni (ad esempio, per effettuare adempimenti on line nei confronti di pubbliche amministrazioni e di concessionari di servizi pubblici, ovvero per tenere rapporti con istituti bancari e assicurativi).

4.3 Sistemi di telefonia

Tutti gli utenti dotati di un telefono fisso connesso alla postazione di lavoro sono collegati alla rete internet tramite VOIP. L'utente è direttamente responsabile dell'uso del telefono, dei soggetti che contatta, delle informazioni che fornisce all'interlocutore.

Nell'utilizzo del telefono è necessario:

- qualificarsi all'interlocutore
- accertarsi dell'identità dell'interlocutore prima di fornire informazioni o dati personali relativi ad una persona fisica.

4.4 Videoconferenza

Nell'utilizzo del sistema di videoconferenza reso disponibile dall'Ente, è necessario ricordare:

- che i sistemi di videoconferenza sono strumenti di lavoro da utilizzare in alternativa a riunioni in presenza o come alternativa alla chiamata telefonica, di dotarsi di cuffie con microfono (per esempio anche quelle del telefono cellulare); questo migliora sensibilmente la qualità del segnale audio;
- di spegnere il proprio microfono quando non utilizzato per evitare di introdurre rumori, brusii o interferenze;
- che nel caso ci si connetta dalla propria abitazione e non si disponga di una zona riservata è possibile utilizzare sfondi virtuali, o, se si preferisce, disattivare la videocamera testando preventivamente l'illuminazione;
- che nel caso in cui non si disponga di banda sufficiente a garantire un adeguato segnale audio- video è conveniente disattivare la videocamera;
- di scollegarsi sempre al termine della videoconferenza, la stessa stanza potrebbe essere utilizzata successivamente per altre riunioni.

5. Strumentazione informatica in Smart Working/Lavoro Agile

Al fine di rendere possibile lo svolgimento della prestazione lavorativa il dipendente potrà essere dotato dall'Ente di un personal computer, da utilizzarsi nel totale rispetto delle regole determinate dalla regolamentazione e in conformità con le indicazioni che gli saranno fornite.

Gli strumenti di lavoro affidati al dipendente devono essere usati esclusivamente per lo svolgimento dell'attività lavorativa, nel rispetto di quanto previsto dai regolamenti dell'Ente e non per scopi personali o non connessi all'attività lavorativa.

Il dipendente ha l'obbligo di utilizzare e custodire gli strumenti di lavoro affidatigli con la massima cura e diligenza e di scegliere sempre un luogo che garantisca la riservatezza, ovvero che sia impedita la visualizzazione delle informazioni sullo schermo o l'ascolto delle conversazioni da parte di persone non autorizzate. In caso di guasto delle attrezzature in dotazione il lavoratore dovrà dare immediato avviso al proprio responsabile, all'assistenza informatica e dovrà consegnare lo strumento guastato non appena possibile. Il dipendente che effettua attività di smart-working/lavoro agile può collegare il pc messo a disposizione dall'Ente alla propria rete WI-FI.

Per l'accesso alla rete dell'Ente viene utilizzato un programma installato sul pc (VPN), che garantendo un accesso sicuro ai sistemi informatici dell'Ente, permette al dipendente di svolgere l'attività lavorativa in modalità analoga a quella dell'ufficio.

Il dipendente potrà utilizzare, nel caso in cui non possa disporre di strumentazione fornita dall'Ente, apparecchiature di proprietà per svolgere attività lavorativa previa specifica autorizzazione dell'Ente.

Nel caso di utilizzo di sistemi di proprietà verrà fornita assistenza solo sulle componenti software che saranno fornite dall'Ente.

In particolare, si richiama la necessità di verificare che l'antivirus installato sul computer sia attivo, aggiornato e connesso.

Nel caso in cui ci sia necessità di connettersi a rete wireless diverse da quella della propria abitazione si raccomanda, al

fine di prevenire l'esposizione a cyber attacchi, di evitare il collegamento a reti non sicure o sulle quali non si siano presenti adeguati sistemi di protezione e sicurezza.

6. Fine vita (documenti cartacei e dispositivi elettronici)

6.1 Smaltimento dei documenti cartacei

I documenti cartacei per cui non è più obbligatorio provvedere alla loro conservazione (cfr. manuale di scarto dell'Ente), possono essere di due tipi:

- documenti che hanno esaurito la propria utilità giuridico-amministrativa;
- documenti che non possiedono più apprezzabile interesse come fonte storica.

I documenti non più utili, contenenti dati, devono essere distrutti in tutta sicurezza e in modo tempestivo, senza lasciare traccia dei dati in essi contenuti ed eliminando, perciò, il rischio che tali dati possano essere utilizzati in seguito in modo fraudolento.

Per ottenere ciò l'Ente si dota di macchine distruggi-documenti.

La macchina distruggi-documenti scelta ha sicurezza di livello su una scala che va da 2 a 7, in cui 2 corrisponde alla sicurezza base e 7 ad alta sicurezza, classificazione che dipende dalla dimensione dei frammenti di carta prodotti dalla macchina. Ad esempio, il livello DIN P-4 è un livello medio che è in grado di produrre frammenti della dimensione di 4 x 38 mm. Praticamente, da un foglio di dimensioni A4, vengono generati ben 421 frammenti. Il livello P-4 è indicato per documenti confidenziali il cui trattamento renderà impossibile riuscire ad assemblare e a leggere anche la più piccola parte del documento originario.

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

6.2 Smaltimento di rifiuti elettrici ed elettronici

In caso di smaltimento di rifiuti elettrici ed elettronici (ad es. pc, smartphone, tablet), l'effettiva cancellazione dei dati personali dai supporti contenuti nelle apparecchiature elettriche ed elettroniche è obbligatoria in modo da impedire l'acquisizione indebita di dati personali.

La distruzione dei supporti prevede il ricorso a metodologie diverse a seconda del loro tipo, quali:

- sistemi di punzonatura¹ o deformazione meccanica;
- distruzione fisica o di disintegrazione (usata per i supporti ottici come i CD-ROM e i dvd);
- demagnetizzazione ad alta intensità.

Tali misure e accorgimenti possono essere attuate anche con l'ausilio o conferendo incarico a terzi tecnicamente qualificati, quali centri di assistenza, produttori e distributori di apparecchiature che attestino l'esecuzione delle operazioni effettuate o che si impegnino ad effettuarle.

7. Interventi di assistenza e manutenzione

Gli interventi di assistenza, installazione e aggiornamento dei software e, in generale, quelli volti a fronteggiare guasti nel funzionamento delle postazioni di lavoro, qualora possibile, sono di norma effettuati dagli amministratori di sistema tramite il servizio di assistenza e amministrazione remota. Il sistema di assistenza in remoto consente, previa autorizzazione del dipendente/utente, di condividere a distanza con l'operatore del supporto tecnico l'utilizzo di tastiera, mouse e schermo, senza che l'utente stesso perda il controllo di quanto avviene al proprio strumento in dotazione e ai dati eventualmente accessibili attraverso lo stesso.

Se invece sono necessari interventi di manutenzione sulla macchina o di assistenza, adeguamento, ecc., presso la postazione di lavoro, è necessario che l'utente o, in sua assenza, altro dipendente del servizio o struttura, assista alle operazioni di manutenzione.

8. Monitoraggio e controlli

L'Ente ha predisposto il proprio sistema informativo ed internet per esclusive esigenze organizzative e di servizio. A tal fine si avvale legittimamente di sistemi che consentono un monitoraggio continuo di eventi potenzialmente pericolosi sulla rete.

¹ Ad esempio, utilizzando un perno d'acciaio temprato, che tramite una leva, perfora l'hard disk in una o più zone distruggendolo definitivamente.

Non saranno utilizzati sistemi hardware e/o software idonei ad effettuare un controllo a distanza dei lavoratori, in particolare mediante:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura o la registrazione dei caratteri inseriti tramite la tastiera e analogo dispositivo.

Il trattamento dei dati contenuti nei LOG **può avvenire esclusivamente in forma anonima in modo tale da precludere l'identificazione dei lavoratori e/o delle loro attività.**

Potrà essere attivato un controllo dei LOG, **non in forma anonima**, in via eccezionale e tassativamente, nelle seguenti ipotesi:

1. per corrispondere ad eventuali richieste della polizia postale e/o dell'autorità giudiziaria;
2. su richiesta del datore di lavoro, quando si verifichi un evento dannoso o una situazione di pericolo che richieda un immediato intervento;
3. su richiesta del datore di lavoro, limitatamente al caso di riscontrate anomalie di traffico web, la cui entità sia tale da compromettere la sicurezza e l'integrità dei sistemi informativi.

Nei casi 2 e 3 sopra descritti, verrà preventivamente inviato un avviso a tutti i lavoratori per preallertare rispetto al controllo attivato nei giorni ed ore specificati. I dati contenuti nei LOG sono conservati per il tempo strettamente necessario al perseguimento di finalità organizzative, di servizio e di sicurezza, comunque non superiore a 30 giorni, e sono periodicamente cancellati automaticamente dal sistema. Un eventuale prolungamento dei tempi di conservazione viene valutato come eccezionale e avverrà solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all'indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- all'obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria e della polizia giudiziaria.

L'Ente, inoltre, per ragioni di necessità e urgenza legate in ogni caso all'espletamento delle funzioni istituzionali dell'ente, potrà accedere agli strumenti lavorativi del dipendente, previa opportuna e motivata notifica a quest'ultimo.

In tutti questi casi, il trattamento dei dati personali sarà limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità esplicitati.

9. Responsabilità e sanzioni

L'utente che abbia violato il presente disciplinare o la normativa ivi richiamata, potrà essere soggetto ad azione disciplinare in conformità a quanto stabilito dal Codice etico e di comportamento, dai contratti collettivi di lavoro e dalla normativa in materia di pubblico impiego, fatta salva la possibilità per l'Ente di esercitare le opportune azioni giudiziarie nelle sedi competenti, a tutela dei propri diritti giuridicamente tutelati.

In caso di danno, la violazione espone altresì l'utente responsabile ad azioni legali di carattere civile o penale da parte dei danneggiati e a richieste di risarcimento anche da parte dell'Ente.

ALLEGATO 1 - GLOSSARIO

Dato personale

Qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati particolari

Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale della persona, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Dati giudiziari

Dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Trattamento di dati personali

Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Comunicazione di dati personali

Il dare conoscenza di dati personali ad uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione o mediante interconnessione.

Diffusione di dati personali

Il dare conoscenza di dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Vi è diffusione, ad esempio, in caso di pubblicazione in internet di dati personali (es. sito web, albo pretorio).

Violazione di dati personali (data breach)

Violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Autorizzato al trattamento

La persona fisica che tratta i dati personali sotto la diretta autorità del titolare e sulla base delle istruzioni dagli stessi impartite. Gli autorizzati si possono suddividere in designati ed incaricati, in base al ruolo rivestito all'interno dell'Ente.

Amministratore di sistema

In ambito informatico, è la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti.

Strumenti Informatici

Strumenti tecnologici utilizzati per la gestione di informazioni e dati, forniti e/o inventariati dall'Ente (es. computer, tablet, supporti di memoria esterni rimovibili, firma digitale remota e token, smartphone, bodycam, dashcam, droni ed altri strumenti con relativi software e applicativi...)

Pseudonimizzazione

Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

Backup

il termine, che significa copia di sicurezza, indica l'operazione di duplicare su differenti supporti di memoria le informazioni (dati o programmi) presenti sui dischi di una stazione di lavoro o di un server. Normalmente viene svolta con una periodicità stabilita.

Chat

(letteralmente, "chiacchierata") è un servizio informatico che permette attraverso internet, di attivare e gestire un dialogo in tempo reale fra due o più utenti utilizzando principalmente messaggi testuali.

File sharing

condivisione di file all'interno di una rete comune.

Forum

Generalmente si riferisce ad un archivio informatico contenente discussioni e messaggi scritti dagli utenti oppure al software utilizzato per fornire questo archivio. Ci si riferisce comunemente ai forum anche come board, message board, bulletin board, gruppi di discussione, bacheche e simili.

ID utente

Codice identificativo personale per l'accesso ai sistemi informatici. Normalmente è formato dal cognome o dal cognome e parte del nome.

LOG

Il termine, che significa giornale di bordo o semplicemente giornale, viene utilizzato nell'informatica per indicare la registrazione cronologica delle operazioni man mano che vengono eseguite ed il file su cui tali registrazioni sono memorizzate.

Mailing-list: (letteralmente, lista per corrispondenza traducibile in italiano con lista di diffusione) è un sistema organizzato per la partecipazione di più persone in una discussione tramite posta elettronica.

Mail spamming: è l'invio di grandi quantità di messaggi indesiderati. Può essere messo in atto attraverso qualunque media, ma il più usato è internet attraverso l'e-mail.

Ondemand (in differita)

Modalità di accesso in rete a file audiovisivi che vengono resi disponibili su richiesta di un utente.

Password (“parola chiave”, “parola d'ordine”, o anche “parola d'accesso”)

È una sequenza di caratteri utilizzata per accedere ad una risorsa informatica.

Podcasting

Sistema che permette di scaricare in modo automatico documenti (generalmente audio o video) chiamati podcast, utilizzando un programma generalmente gratuito chiamato aggregatore o feeder. Con podcast si intende un file (generalmente audio o video), messo a disposizione su Internet e scaricabile automaticamente.

Software freeware

Programmi software distribuiti in modo gratuito.

Software peer-to-peer

Programmi utilizzati per la condivisione e lo scambio di files fra elaboratori. Questi programmi vengono utilizzati principalmente per scambiarsi file di tipo mp3, (file musicali) e DivX (contenenti i film) spesso in violazione dei diritti d'autore.

Stand – alone

Si riferisce ad un'apparecchiatura capace di funzionare da sola, indipendentemente dalla presenza di altre apparecchiature con cui potrebbe comunque interagire.

Streaming (in diretta)

Modalità di accesso in rete a file audiovisivi di cui si può fruire in tempo reale.

Virtual Private Network (VPN)

VPN (Virtual Private Network), Terminal Server o applicativi Web sono tecnologie che permettono di accedere alle risorse della rete locale del Consiglio provinciale attraverso la rete internet.

Voice over IP (Voip)

Si può parlare di tecnologia VoIP, ovvero voce tramite protocollo internet, quando si effettua una telefonata utilizzando la stessa connessione sia per dati che per voce.

Webcast/Web casting

Descrive la trasmissione di segnale audio o video, in tempo reale o ritardato, mediante tecnologie web. Il suono o il video sono catturati con sistemi audio-video convenzionali, quindi digitalizzati e inviati in streaming su un web server. Un client webcast consente agli utenti di connettersi ad un server che sta distribuendo (operazione detta di web casting) e di ascoltare o visualizzare il contenuto audio/video.

ALLEGATO 2 - INVENTARIO DELLA STRUMENTAZIONE INFORMATICA, DEI SOFTWARE E DELLE APPLICAZIONI IN DOTAZIONE ALL'ENTE

STRUMENTAZIONE INFORMATICA

Elencare qui la strumentazione informatica dell'Ente (computer, tablet, supporti di memoria esterni rimovibili, firma digitale remota e token, smartphone, bodycam, dashcam, droni ed altri strumenti)

SOFTWARE E APPLICAZIONI

Elencare qui i software e le applicazioni in dotazione all'Ente (servizio di posta elettronica e relative applicazioni disponibili, servizio di videoconferenza, gestionali in uso presso i singoli servizi/uffici, sistema di protocollo, etc.) con una descrizione che chiarisca all'utilizzatore quali sono le funzionalità.

Trento, 16 ottobre 2023
MAM/lb

Al Sindaco/Al Presidente
Al Segretario
Al Referente Privacy
degli Enti aderenti al Servizio
Privacy RPD

interoperabilità PITRE

OGGETTO: Servizio Privacy RPD – Novità sui trasferimenti di dati personali verso gli Stati Uniti.

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto.
Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.

Cordiali saluti.

Firmato
Il Direttore generale
dott. Marco Riccadonna

Firmato
Il Presidente
dott. Paride Gianmoena

Facendo seguito alle richieste di chiarimento pervenute negli scorsi mesi da parte degli Enti che hanno ricevuto molteplici comunicazioni da parte di MonitoraPA, gruppo di attivisti informatici, si rendono alcuni aggiornamenti.

MonitoraPA ha diffidato le pubbliche amministrazioni dall'utilizzo di svariati servizi (ad esempio, Google Analytics, Google Workspace, Amazon WEB Service, ...) forniti da società statunitensi, in quanto questi strumenti avrebbero potuto determinare un trasferimento sistematico di dati personali degli utenti verso gli Stati Uniti e dunque, secondo MonitoraPA, non sarebbero stati conformi alle disposizioni del Regolamento europeo 679/2016 (GDPR) in ordine al trasferimento transfrontaliero dei dati.

Infatti, con riferimento al trasferimento dei dati personali verso Paesi terzi, per assicurare che i dati personali vengano trattati con standard di tutela adeguati, se non equivalenti, a quelli garantiti all'interno dell'Unione, il GDPR prevede che il trasferimento possa aver luogo solamente nei casi tassativamente previsti agli artt. 45 e seguenti dello stesso, quali, ad esempio, la presenza di una decisione di adeguatezza della Commissione Europea, l'utilizzo di clausole contrattuali standard, di meccanismi di certificazione, di norme vincolanti d'impresa o di codici di condotta. Il trasferimento di dati personali verso paesi terzi, infatti, non può essere un mezzo per minare o indebolire la protezione che viene garantita nello Spazio Economico Europeo. Tali strumenti dovrebbero appunto garantire la soggezione dei dati trasferiti a garanzie adeguate con riferimento al livello di tutela dei dati personali cui si è impegnato il paese terzo, o il soggetto sito nel paese terzo. Adottando uno dei sopra menzionati strumenti di garanzia, dunque, il trasferimento avviene in modo lecito e conforme alla normativa in materia di protezione dei dati personali.

Fino a poco tempo fa, il trasferimento dei dati verso gli Stati Uniti avveniva prevalentemente utilizzando lo strumento delle clausole contrattuali standard, le quali (come anche gli altri strumenti di trasferimento), tuttavia, non operano in modo isolato: la Corte di Giustizia dell'Unione Europea afferma che i titolari o responsabili del trattamento, in qualità di esportatori, hanno la responsabilità di verificare, caso per caso e, ove necessario, in collaborazione con l'importatore nel paese terzo, se la legge o la prassi di quest'ultimo incidono sull'efficacia delle garanzie adeguate contenute negli strumenti di trasferimento citati. In tali casi la Corte lascia comunque aperta la possibilità per gli esportatori di attuare misure supplementari che colmino queste lacune nella protezione e la portino al livello richiesto dal diritto dell'UE. La Corte non specifica di quali misure potrebbe trattarsi, ma sottolinea che gli esportatori dovranno identificarle caso per caso, conformemente alle raccomandazioni adottate dall'European Data Protection Board e consultabili ai seguenti link: [raccomandazioni 01/2020](#); [raccomandazioni 02/2020](#). In concreto, tuttavia, risultava complesso imporre alle grandi società statunitensi l'adozione di ulteriori misure di sicurezza al fine di rendere effettiva la protezione dei dati personali trasferiti, che dunque rimanevano inapplicate.

In tale contesto, la **Commissione Europea**, il 10 luglio 2023, ha adottato la **decisione di adeguatezza sul quadro UE-USA per la protezione dei dati personali**, la quale sancisce che gli Stati Uniti garantiscono un livello di protezione adeguato - comparabile a quello dell'Unione europea - per i dati personali trasferiti dall'UE alle imprese statunitensi nell'ambito del nuovo accordo-quadro (cd. Data Privacy Framework).

Sulla base della nuova decisione di adeguatezza, dunque, **i dati personali possono circolare in modo sicuro dall'UE verso le imprese statunitensi che partecipano all'accordo Data Privacy Framework, senza la necessità di ulteriori garanzie per la protezione dei dati**. Pertanto, affinché un trasferimento verso gli Stati Uniti possa dirsi lecito senza la necessità di adottare ulteriori garanzie e misure di sicurezza (cfr. art. 46 e ss. GDPR e raccomandazioni 01/2020; raccomandazioni 02/2020 dell'EDPB), è oggi sufficiente che le imprese statunitensi a cui si intende trasferire i dati personali abbiano aderito al Data Privacy Framework.



I principali attori economici statunitensi (Google, Microsoft e Amazon), che possono interessare codeste amministrazioni, hanno aderito al predetto quadro impegnandosi a rispettare un insieme dettagliato di obblighi in materia di protezione dei dati personali (è possibile verificare l'adesione delle società al Data Privacy Framework al link: <https://www.dataprivacyframework.gov/s/participant-search>).

Ad oggi, pertanto, **le segnalazioni di Monitora-PA devono essere lette alla luce del nuovo quadro giuridico**, per il quale tali strumenti possono essere liberamente utilizzati previa opportuna richiesta al fornitore circa l'adesione del medesimo (o del suo sub-fornitore/sub-responsabile) al Data Privacy Framework in relazione al servizio offerto.

In ogni caso, è prudente considerare che, come già accaduto nel recente passato, la decisione di adeguatezza potrebbe essere oggetto di ricorso in annullamento e di vaglio da parte della Corte di Giustizia qualora ricorrano i presupposti richiesti dall'art. 263 del Trattato sul Funzionamento dell'Unione Europea (inerente all'annullamento degli atti giuridici delle istituzioni europee da parte della Corte di giustizia). Sono già state annullate - con le medesime modalità - due precedenti decisioni di adeguatezza nei confronti degli Stati Uniti e i relativi accordi Safe Harbor e Privacy Shield – cfr. cd. sentenze Schrems I (Causa C-362/14) e II (Causa C-311/18) della Corte di Giustizia.

Orientare la preferenza su prodotti che garantiscano la conservazione dei dati personali all'interno dello Spazio Economico Europeo rimane, comunque, la scelta più tutelante.

* * * * *

Per ogni chiarimento doveste ritenere utile o necessario, potete contattare la dott.ssa Federica Dallaporta o la dott.ssa Marta Mattiello ai seguenti recapiti: tel. 0461 987139 - e-mail serviziordpd@comunitrentini.it.

Cordiali saluti.

Firmato
Il Referente
Responsabile della protezione dei dati
dott. Gianni Festi

Firmato
Il Responsabile del procedimento
dott.ssa Laura Marinelli



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Segreteria generale
Generalsekretariat
Ufficio affari generali
Amt für allgemeine Angelegenheiten

☎ 0461 201323
@ affgen@regione.taa.it
pec: affgen@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Protokollnummer und Registrierungsdatum sind dem Dokument als Metadaten zugeordnet (Dekret des Präsidenten des Ministerrates vom 3.12.2013, Art. 20). Gegenstand der zertifizierten E-Mail bzw. beigefügte Dateien überprüfen.

Alle Dirigenti e ai Dirigenti delle strutture organizzative

Alle Direttrici ed ai Direttori degli Uffici

Al Capo della Segreteria del Presidente

Ai Segretari particolari dei componenti della Giunta regionale

e, p.c.

Al

Responsabile della protezione dei dati della Regione autonoma Trentino-Alto Adige/Südtirol
consorzio@pec.comunitrentini.it

An die Leiterinnen und Leiter der regionalen Organisationsstrukturen

An die Amtsdirektorinnen und Amtsdirektoren

An den Leiter des Sekretariats des Präsidenten der Region

An die persönlichen Referenten der Mitglieder der Regionalregierung

u. z. K.

An den

Datenschutzbeauftragten der Autonomen Region Trentino-Südtirol
consorzio@pec.comunitrentini.it

Oggetto: Ulteriori disposizioni organizzative in materia di privacy.

Con la circolare n. 2 di data 11 gennaio 2021 sono state fornite le indicazioni e la modulistica per agevolare gli adempimenti in materia di *privacy* previsti dal Regolamento generale sulla Protezione dei Dati (UE) n. 2016/679 (GDPR), dal decreto legislativo n. 196/2003 e ss.mm., nonché dalla deliberazione della Giunta regionale n. 193/2019.

Betreff: Weitere organisatorische Maßnahmen in Sachen Datenschutz

Mit Rundschreiben vom 11. Jänner 2021, Nr. 2 wurden Informationen und Formulare bereitgestellt, um die Einhaltung der Verpflichtungen laut EU-Datenschutz-Grundverordnung Nr. 2016/679, gesetzesvertretendem Dekret Nr. 196/2003 i.d.g.F. sowie Beschluss der Regionalregierung Nr. 193/2019 zu erleichtern.

Per ottimizzare la gestione delle diverse attività facenti capo alle strutture ed agli uffici, si è ritenuto opportuno introdurre dei nuovi modelli organizzativi che si provvede ad illustrare, unitamente ad un breve richiamo alle relative indicazioni operative.

Ritengo preliminarmente utile precisare che gli Uffici del Giudice di Pace e gli Uffici giudiziari del distretto della Corte d'Appello di Trento, sono, per quanto riguarda le rispettive attribuzioni giurisdizionali, titolari singolarmente del trattamento di dati personali e, per tanto, non sono destinatari delle disposizioni dettate dalla scrivente Struttura (giusta deliberazione n. 193/2019).

ABILITAZIONI A CARTELLE ED APPLICATIVI.

Per velocizzare il processo di attribuzione ai collaboratori delle abilitazioni alle cartelle ed applicativi l'Ufficio affari generali, in collaborazione con l'Ufficio informatica e digitalizzazione, ha predisposto una procedura informatizzata. Questa è stata realizzata in Pi.Tre ed è denominata "PROFILI INFORMATICI". Si individua scorrendo il menù a tendina del campo "Tipologie", dopo aver scelto "nuovo documento". Va utilizzato ogni qualvolta nelle Ripartizioni, nelle Segreterie politiche e negli Uffici si realizzino i seguenti eventi:

- nuove assunzioni di collaboratori;
- cessazioni di collaboratori;
- attribuzione o rimozione di diverse abilitazioni (pec, pitre, cartelle informatiche, utilizzo e accesso a base di dati).

La procedura prevede un flusso automatizzato che invia all'Ufficio affari generali le richieste di abilitazione prodotte

Um die verschiedenen den Strukturen und den Ämtern obliegenden Tätigkeiten zu optimieren, wurden nun neue Organisationsmodelle eingeführt, die in der Folge nebst kurzer operativer Anweisungen erläutert werden.

Es sei in diesem Zusammenhang darauf hingewiesen, dass die Friedensgerichte sowie die Gerichtsämter des Oberlandesgerichtssprengels Trient im jeweiligen Zuständigkeitsgebiet selbst für die Verarbeitung personenbezogener Daten verantwortlich sind und demnach von den von dieser Struktur erteilten Anweisungen nicht betroffen sind (siehe Beschluss Nr. 193/2019).

ZUGRIFFSBERECHTIGUNG AUF ORDNER UND ANWENDUNGEN

Um das Verfahren zur Gewährung der Zugriffsberechtigung auf Ordner und Anwendungen zu beschleunigen, hat das Amt für allgemeine Angelegenheiten in Zusammenarbeit mit dem Amt für Informatik und Digitalisierung ein elektronisches Verfahren eingerichtet. Es handelt sich um die „PROFILI INFORMATICI“-Funktion im Pi.Tre-System, welches man aus dem Dropdown-Menü im Feld „Tipologie“ auswählen kann, nachdem man „Nuovo documento“ gewählt hat. Dieses Verfahren ist immer dann zu verwenden, wenn Abteilungen, politische Sekretariate oder Ämter Nachstehendes vornehmen müssen:

- Neueinstellung von Mitarbeitern;
- Dienstaustritt von Mitarbeitern;
- Zu- oder Aberkennung bestimmter Zugriffsberechtigungen (PEC, elektronische Ordner, Verwendung und Zugang zu Datenbanken).

Das Verfahren sieht eine automatische Übermittlung der von den Strukturen, den politischen Sekretariaten und den Ämtern

dalle strutture, dalle Segreterie politiche e dagli Uffici, affinché ne possa essere verificata la correttezza formale; i documenti vengono poi automaticamente trasmessi all'Ufficio informatica e digitalizzazione, per l'esecuzione della richiesta. Nel caso in cui, dalle verifiche effettuate, non risulti possibile procedere all'abilitazione, il flusso informatico prevede la restituzione all'ufficio proponente della richiesta, con specificazione delle motivazioni del mancato accoglimento. Tra le cause del rifiuto della richiesta vi sono, a titolo esemplificativo: l'assenza della firma digitale del responsabile; il mancato aggiornamento del Registro delle attività di trattamento e l'assenza della lettera di autorizzazione al trattamento dei dati.

Con l'occasione è stata revisionata e semplificata la modulistica.

In allegato alla presente si trasmette anche l'inventario delle banche dati digitali rilevate presso l'amministrazione. Tale elenco costituisce, per voi, uno strumento utile per la compilazione della *"Lettera di autorizzazione al trattamento dei dati"* nella parte *"Specificazioni relative ad accessi particolari"* nel cui campo andrà riportato il nome delle banche dati a cui è autorizzato ad accedere il dipendente. Trattandosi di un documento che andrà tenuto costantemente aggiornato, vi invito ad effettuare una verifica delle banche dati di competenza e di comunicare le eventuali variazioni.

Le indicazioni operative per l'utilizzo della nuova procedura sono riportate nell'allegata scheda tecnica.

angeforderten Zugriffsberechtigungen an das Amt für allgemeine Angelegenheiten vor, damit deren formale Korrektheit überprüft werden kann; anschließend werden diese automatisch dem Amt für Informatik und Digitalisierung weitergeleitet, das dem Antrag stattgibt. Sollte sich im Zuge der Überprüfungen herausstellen, dass keine Zugriffsberechtigung erteilt werden kann, wird der Antrag automatisch an das Amt zurückgesandt, von dem er ausgegangen war, wobei die Gründe für die Ablehnung anzugeben sind. Zu den Gründen für eine Ablehnung zählen beispielsweise: das Fehlen der digitalen Signatur des Verantwortlichen, ein nicht aktualisiertes Verzeichnis der Verarbeitungstätigkeiten oder das Fehlen des Ermächtigungsschreibens für die Verarbeitung personenbezogener Daten.

Bei dieser Gelegenheit wurden die bestehenden Formulare überarbeitet und vereinfacht.

In der Anlage zu diesem Schreiben wird ebenfalls ein Inventar der bei der Verwaltung erhobenen Datenbanken übermittelt. Dieses Verzeichnis ist hilfreich, um das Ermächtigungsschreiben für die Verarbeitung personenbezogener Daten auszufüllen, insbesondere den Abschnitt *„Specificazioni relative ad accessi particolari“*, wo die Bezeichnung der Datenbanken anzugeben ist, zu denen man Zugriff hat. Da dieses Dokument ständig aktualisiert werden muss, werden Sie ersucht, die Datenbanken im eigenen Zuständigkeitsbereich zu überprüfen und eventuelle Änderungen mitzuteilen.

Die operativen Anweisungen betreffend die Verwendung des neuen Verfahrens sind in der beiliegenden technischen Übersicht

angeführt.

REGISTRO DELLE ATTIVITA' DI TRATTAMENTO.

Il Registro delle attività di trattamento deve essere redatto ai sensi dell'art. 30 del Regolamento (UE) n. 679/2016 e mantenuto costantemente aggiornato ai fini dell'esibizione all'Autorità Garante in caso di ispezione. Ad ogni modifica, il documento, firmato digitalmente dalla/dal dirigente competente o dal soggetto responsabile, va trasmesso all'Ufficio affari generali via Pi.tre. (221COLL) anziché alla Segreteria generale, come precedentemente indicato nella circolare 2/2019.

NOMINA A RESPONSABILE ESTERNO DEL TRATTAMENTO.

Sono designati Responsabili esterni del trattamento di dati personali i soggetti esterni all'amministrazione che siano tenuti a effettuare trattamenti di dati personali per conto del Titolare, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina.

Poiché i contratti di nomina a Responsabile esterno al trattamento, sottoscritti dai Dirigenti ai sensi della deliberazione 193/2019, possono costituire materia di verifica da parte del Responsabile della protezione dei dati (DPO), si è ritenuto opportuno individuare una modalità di archiviazione che consenta una veloce estrazione degli stessi. Si raccomanda, quindi, di archiviare tali contratti non solo nel fascicolo riguardante l'affidamento dell'incarico, ma anche nel fascicolo concernente la privacy, apponendo una duplice classificazione ai documenti di nomina dell'incaricato. Di quest'ultimo fascicolo se ne forniscono i dettagli nella

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Gemäß Art. 30 der Verordnung (EU) Nr. 679/2016 ist ein Verzeichnis der Verarbeitungstätigkeiten zu führen und ständig zu aktualisieren, das auf Anfrage der Aufsichtsbehörde zur Verfügung gestellt wird. Dieses von der zuständigen Leiterin/vom zuständigen Leiter oder vom Verantwortlichen digital signierte Verzeichnis ist nach jeder Änderung mittels Pi.Tre. (221 COLL) an das Amt für allgemeine Angelegenheiten und nicht – wie zuvor im Rundschreiben Nr. 2/2019 angegeben – an das Generalsekretariat zu übermitteln.

ERNENNUNG ZUM EXTERNEN VERANTWORTLICHEN FÜR DIE DATENVERARBEITUNG

Als externe Verantwortliche für die Datenverarbeitung werden verwaltungsexterne Personen bezeichnet, die aufgrund einer Vereinbarung, eines Vertrags, eines Vergabeprotokolls oder einer Ernennungsmaßnahme personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeiten müssen.

Da die gemäß Beschluss Nr. 193/2019 von den Leiterinnen/Leitern unterzeichneten Verträge über die Ernennung zum externen Verantwortlichen für die Datenverarbeitung vom Datenschutzbeauftragten (DSB) überprüft werden können, wurde eine Ablagemethode eingeführt, die ein schnelles Auffinden dieser Verträge ermöglicht. Diese Verträge sind demnach nicht nur im Faszikel betreffend die Auftragserteilung, sondern auch in jenem betreffend den Datenschutz abzulegen, wobei eine doppelte Klassifizierung der

scheda tecnica allegata.

Dokumente über diese Ernennungen vorzunehmen ist. In der beiliegenden technischen Übersicht werden die Einzelheiten betreffend letztgenannten Faszikel erläutert.

ARCHIVIAZIONE DOCUMENTI.

L'articolo 7 del *Regolamento generale per gli archivi regionali*, approvato con d.P.Reg. 20 settembre 2012, n. 10/L, dispone che ogni ufficio sia responsabile della gestione documentale durante lo svolgimento delle proprie attività. Con riferimento a tale aspetto, ritengo opportuno individuare una modalità di archiviazione omogenea dei documenti concernenti la *privacy* prodotti dall'Ente, in quanto trattasi di materia trasversale alle strutture e agli uffici. Questo faciliterà anche le operazioni di esibizione al Responsabile della protezione dei dati (DPO) e all'Autorità Garante nella loro, eventuale, veste ispettiva. Nella scheda tecnica allegata sono riportate le modalità di redazione degli oggetti e il sistema di fascicolazione.

DISABILITAZIONE ACCESSI.

Faccio presente come sia importante procedere, ove se ne rilevi la necessità (a titolo esemplificativo per cambio di ruolo, di competenze o d'ufficio), a rimuovere le autorizzazioni concesse al fine di disabilitare l'accesso ad applicativi e cartelle.

Vi invito a portare a conoscenza dei direttori e dei collaboratori il contenuto della presente circolare. L'Ufficio affari generali è a disposizione per eventuali chiarimenti (*tel. 0461 201323 Martina Bisoffi*).

DOKUMENTENABLAGE

Gemäß Art. 7 der mit DPREg. vom 20. September 2012, Nr. 10/L erlassenen „*Allgemeinen Verordnung für die Regionalarchive*“ ist jedes Amt für die Dokumentenverwaltung im Rahmen der eigenen Tätigkeiten verantwortlich. Diesbezüglich sollte eine einheitliche Ablagemethode für die von der Region erstellten datenschutzrelevanten Dokumente festgelegt werden, da es sich hierbei um eine struktur- und ämterübergreifende Frage handelt. Auch wäre damit im Fall einer Kontrolle die Aushändigung an den Datenschutzbeauftragten und an die Aufsichtsbehörde einfacher. In der beiliegenden technischen Übersicht wird die Vorgehensweise bei der Verfassung des Gegenstands sowie die Faszikelanlegung erläutert

DEAKTIVIERUNG VON ZUGRIFFSBERECHTIGUNGEN

Es wird auf die Bedeutung hingewiesen, bei Bedarf (z. B. bei Änderungen der Rolle, der Zuständigkeiten oder des Amtes) die erteilten Zugriffsberechtigungen auf Ordner oder Anwendungen zu deaktivieren.

Sie werden gebeten, die Amtsdirektorinnen und -direktoren sowie alle Mitarbeiter vom Inhalt dieses Rundschreibens in Kenntnis zu setzen. Das Amt für allgemeine Angelegenheiten steht für eventuelle Auskünfte gerne zur Verfügung. (*Tel. 0461*

201323 Martina Bisoffi).

Cordiali saluti.

Mit freundlichen Grüßen

IL SEGRETARIO GENERALE/
DER GENERALSEKRETÄR

Michael Mayr
firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Schreiben in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

MM/RG/MB

Allegati/Anlagen:

- scheda tecnica/technische Übersicht

- modelli/Vorlagen:

- modello lettera di incarico al trattamento dei dati
- Modello PITRE
- Modello disabilitazione cartelle di rete
- Modulo richiesta abilitazione e disabilitazione utenze-casella PEC
- Abilitazioni cartelle e stampanti
- Modello per abilitazione sito
- Richiesta_accesso_QLIK_Regione

SCHEDA TECNICA

Di cui alla circolare avente ad oggetto: “Ulteriori disposizioni organizzative in materia di privacy”.

■ ABILITAZIONE A CARTELLE ED APPLICATIVI.

La procedura informatica di Pi.Tre “Profili informatici” si individua scorrendo il menù a tendina del campo “*Tipologia*”, dopo aver scelto “nuovo documento”. Vanno caricati, per ogni collaboratore -a seconda dell'evento e della tipologia di abilitazione da attribuire o variare- i documenti di autorizzazione firmati digitalmente. I files dei nuovi modelli sono archiviati nella cartella condivisa *M:\Comune\Privacy\Modelli* e precisamente:

- a. Lettera di incarico al trattamento dei dati;
- b. *Abilitazione/disabilitazione a PiTre*;
- c. *Abilitazione/disabilitazione alle cartelle di rete e stampanti*,: il file in formato excel deve essere **sempre** allegato alla trasmissione, in quanto Trentino Digitale, che effettua l'abilitazione, accetta solamente questo formato;
- d. *Abilitazione e disabilitazione utenze della casella PEC*;
- e. *Abilitazione/disabilitazione al caricamento di dati del sito*;
- f. *Richiesta di abilitazione alla consultazione dei capitoli in contabilità finanziaria*;

Per snellire le operazioni, nella sotto riportata tabella sono indicati: il nome del file archiviato nella cartella M, la tipologia di documento e il campo di Pi.Tre. “oggetto della richiesta” da selezionare per ogni tipo di documento.

NOME FILE	UTILIZZO	OGGETTARIO
modello lettera di incarico al trattamento dei dati	Autorizzazione firmata dal Dirigente di Ripartizione al trattamento dei dati	Incarico
Modello PITRE	Modello per l'abilitazione e/o la disabilitazione dai ruoli di Pitre	PITRE
Modello disabilitazione cartelle di rete	Modello per la sola disabilitazione dell'accesso alle cartelle di rete	Cartelle
_Modulo richiesta abilitazione e disabilitazione utenze-casella PEC	Modello da utilizzare per abilitazione e/o disabilitazione pec	Cartelle
Abilitazioni cartelle e stampanti	Modello da utilizzare per l'abilitazione dell'accesso del collaboratore alle cartelle e alle stampanti*	Cartelle
Modello per abilitazione sito	Per autorizzare/rimuovere le autorizzazioni per operare sul sito (caricamento di dati a vario titolo)	Sito
Richiesta_accesso_QLIK_Regione	Modello di autorizzazione/revoca accesso a documenti Qlik	Sap
	Attraverso comunicazione asincrona, ad es. variazione accesso a data base	Altro

*firmare il documento pdf, ed allegare in P.I.Tre il file compilato in excell

Si raccomanda di utilizzare esclusivamente i file indicati, salvandoli e personalizzandoli (Ripartizione e Ufficio) per utilizzarli nelle successive trasmissioni.

✚ I campi da compilare (metadati) sono essenziali per il buon esito della procedura pertanto si invita cortesemente a compilare tutti i dati richiesti.

✚ Qualora in P.i.Tre sia necessario caricare più richieste di abilitazioni per uno stesso utente, è possibile evitare di reinserire i dati utilizzando la funzione “RIPROPONI” tenendo presente che:

- i documenti in stato finale non possono essere riproposti;
- i documenti ottenuti con la funzione *riproponi* da documenti non in stato finale partono sempre dallo stato iniziale (mantenendo cioè compilati i campi oggetto, mittente e classifica)
- i file devono essere di volta in volta caricati.

✚ Per agevolare la compilazione del modulo è stato creato il seguente oggettario:

OGGETTARIO	DESCRIZIONE
Incarico	Autorizzazione al trattamento dei dati del/la sig.re/ra _____ con decorrenza dal _____
PITRE	Richiesta abilitazione/disabilitazione a Pi.Tre del/la sig.re/ra _____ con decorrenza dal _____
Cartelle	Richiesta abilitazione/disabilitazione alle cartelle, applicativi e pec del/la sig.re/ra _____ con decorrenza dal _____
Sito	Richiesta abilitazione/disabilitazione alle funzionalità del sito del/la sig.re/ra _____ con decorrenza dal _____
Sap	Richiesta abilitazione/disabilitazione alla consultazione dei capitoli in contabilità finanziaria del/la sig.re/ra _____ con decorrenza dal _____
Altro	Richiesta abilitazione/disabilitazione a _____ del/la sig.re/ra _____ con decorrenza dal _____

Per completezza è stato creato anche l'oggettario per il Registro delle Attività di Trattamento dei dati:

OGGETTARIO	DESCRIZIONE
Registro	Registro delle Attività di Trattamento dei dati aggiornato alla data del _____ (inserire anche una breve descrizione della ragione dell'aggiornamento, es. assunzione Mario Rossi con decorrenza 01/01/2022)

✚ Ogni documento in partenza è destinato alla validazione da parte dell'Ufficio affari generali, avrà la caratteristica di essere un “documento grigio”.

In calce al presente allegato è riportato il manuale per l'utilizzo del tipo documento in Pi.Tre.

✚ ARCHIVIAZIONE DOCUMENTI.

Ogni Ripartizione è tenuta ad organizzare e fascicolare in maniera autonoma tutta la documentazione in Pi.Tre..

I documenti vanno classificato con il nodo di titolario *6.4. Protezione dei dati personali*

Si raccomanda di fascicolare i documenti utilizzando il seguente oggetto: *“Adempimenti in materia di privacy – Ripartizione..... oppure Ufficio*”.

E' a discrezione delle strutture e uffici l'utilizzo dei sottofascicoli, in tal caso si suggerisce di crearli nel modo seguente:

- *Registro dei trattamenti*
- *Lettere di incarico al trattamento dei dati;*
- *Abilitazioni/disabilitazioni a PiTre;*
- *Abilitazioni/disabilitazioni alle cartelle ed applicativi e pec;*
- *Abilitazioni/disabilitazioni al caricamento di dati del sito;*
- *Richieste di abilitazione alla consultazione dei capitoli in contabilità finanziaria;*
- *Nomine a responsabile esterno al trattamento dei dati.*



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Struttura

Ufficio _____

Tel: 0461 20

e-mail: _____@regione.taa.it

pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Gentile Signore / Gentile Signora

Oggetto: Autorizzazione al trattamento dei dati

Il _____

ai sensi dell'art. 29 GDPR (Reg. n. 2016/679), dell'art. 2-quaterdecies del Codice della privacy (D.Lgs. 196 del 2003) come novellato dal D.Lgs. 10 agosto 2018, n. 101 e della deliberazione della Giunta regionale 3 settembre 2019, n. 193

autorizza

al trattamento dei dati personali e di categorie particolari di dati, indicati nel Registro dei trattamenti, ex art. 9 del GDPR effettuato con l'utilizzo di strumenti cartacei, informatici e telematici, il seguente soggetto incardinato e preposto presso l'Ufficio _____:

Il soggetto autorizzato è tenuto a rispettare rigorosamente i principi GDPR e la normativa di settore, nonché ad attenersi alle circolari, policy in materia di sicurezza informatica, istruzioni impartite dal Titolare o da suo delegato.

Il soggetto autorizzato è tenuto a seguire le seguenti istruzioni organizzative e tecniche:

- trattare i dati personali in modo lecito e secondo correttezza;
- accedere solo ai dati strettamente necessari all'esercizio delle proprie funzioni;
- raccogliere e registrare i dati personali per scopi determinati, espliciti e legittimi;
- verificare che siano esatti e, se necessario, aggiornarli;
- verificare che siano pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti e successivamente trattati;
- conservarli in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti e successivamente trattati;
- comunicare o trasferire all'estero i dati personali esclusivamente ai soggetti autorizzati e riceverli legittimamente per le finalità per le quali gli stessi sono stati raccolti e comunque nel rispetto delle istruzioni ricevute;
- non comunicare a terzi, al di fuori dell'ambito lavorativo, o in difformità dalle istruzioni ricevute, qualsivoglia dato personale;
- ove necessario, prima di iniziare il trattamento di dati personali, consegnare/trasmettere il documento definito Informativa e raccogliere il Consenso al trattamento;
- informare prontamente il Dirigente di ogni circostanza idonea a determinare pericolo di dispersione o

utilizzazione non autorizzata dei dati stessi;

- informare prontamente il Dirigente qualora si verificasse la necessità di porre in essere operazioni di trattamento di dati personali per finalità o con modalità diverse da quelle risultanti dalle istruzioni ricevute, nonché di ogni istanza di accesso ai dati personali da parte di soggetti interessati e di ogni circostanza che esuli dalle istruzioni impartite dal Dirigente o dal Titolare;
- seguire le attività di formazioni organizzate dalla Regione Autonoma Trentino-Alto Adige/Südtirol per gli autorizzati al trattamento dei dati;
- accedere, per esigenze di servizio, esclusivamente alle banche dati informatiche o cartacee della propria Struttura o Ufficio a cui è stato autorizzato dal Dirigente;
- mantenere riservate le proprie credenziali di autenticazione;
- in presenza di dati particolari (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) e giudiziari (es. condanne penali) effettuare i trattamenti strettamente necessari ed eventualmente inseriti in regolamenti, procedure e/o disciplinari;
- effettuare i trattamenti sulla base di ogni ulteriore disciplinare o regolamento che il presente Ente emetterà in materia di privacy;

Specificazioni relative ad accessi particolari:

- il soggetto è autorizzato ad accedere a banche dati online, in particolare:

-
-
-

Il soggetto è autorizzato ad accedere alle cartelle ed agli applicativi come da documentazione sottoscritta e depositata presso l'amministrazione.

Il soggetto è altresì autorizzato ad utilizzare tutti i software, programmi, applicativi accessibili (programmi elaborazione testi, dati ecc...), installati per finalità d'ufficio, dall'Ufficio Informatica e digitalizzazione sul PC, al quale egli ha accesso.

La presente nomina di Autorizzato al trattamento dei dati personali può essere revocata in qualsiasi momento.

La presente nomina si intende automaticamente revocata alla data di cessazione del rapporto di lavoro con questa Amministrazione, per trasferimento ad altra Amministrazione o cessazione del rapporto di lavoro.

Successivamente a tale data, il soggetto destinatario della presente lettera non è più autorizzato ad effettuare alcun tipo di trattamento di dati per conto dell' Amministrazione.

In presenza di eventuali sanzioni legate a specifiche inosservanze il Titolare ed il Responsabile del trattamento si riservano di agire secondo le norme vigenti.

Si rappresenta che la conoscenza dei dati personali da parte di un Autorizzato, nell'ambito dei trattamenti assegnati al suo Servizio/Ufficio, non è considerata comunicazione di dati personali.

Il presente atto sostituisce le eventuali nomine al trattamento dei dati personali precedenti.

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Il/La sottoscritto/a _____ dichiara di aver ricevuto la presente nomina ad Autorizzato al trattamento dei dati personali e si impegna a seguirne e rispettarne il contenuto

Data,

firma dell'autorizzato al trattamento



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Struttura

Ufficio _____

Tel: 0461 20

e-mail: _____@regione.taa.it

pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Alla c.a.

Ufficio Informatica e digitalizzazione

Oggetto: richiesta di abilitazione/disabilitazione a P.I. Tre

A partire dalla data del _____, si chiede di abilitare / disabilitare il collaboratore:

NOMINATIVO		CODICE FISCALE	

in servizio presso:

STRUTTURA	Scegliere la struttura	UFFICIO	Scegliere l'ufficio

ATTIVITÀ RICHIESTA

	NUOVO INSERIMENTO DI COLLABORATORE NEL RUOLO (codice e descrizione)	

	CANCELLAZIONE DEL COLLABORATORE DAL RUOLO (codice e descrizione)	

	CANCELLAZIONE DEL COLLABORATORE DA TUTTI I RUOLI

IL/LA DIRIGENTE

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Struttura

Ufficio _____

Tel: 0461 20

e-mail: _____@regione.taa.it

pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Alla c.a.

Ufficio Informatica e digitalizzazione

Oggetto: richiesta di disabilitazione dalle cartelle di rete

Si chiede di abilitare / disabilitare il collaboratore:

NOMINATIVO		CODICE FISCALE	

in servizio presso:

STRUTTURA	Scegliere la struttura	UFFICIO	Scegliere l'ufficio

ATTIVITÀ RICHIESTA

	DISABILITAZIONE DEL COLLABORATORE DALLE CARTELLE DI RETE (codice e descrizione)	

	DISABILITAZIONE DEL COLLABORATORE DA TUTTE LE CARTELLE DI RETE

con decorrenza dal _____.

IL/LA DIRIGENTE

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (Art. 3-bis D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (Art. 3 D. Lgs. 39/93).

____/____



Legalmail

RICHIESTA DI ATTIVAZIONE
Servizio Legalmail – Posta Elettronica Certificata
Convenzione Consip



Il Cliente

Pubblica Amministrazione* _____ **Cod.Fisc/P.IVA*** _____

Telefono _____ **Via/P.zza*** _____

CAP* _____ **Comune*** _____ **Sigla Prov.*** _____

Indirizzo e-mail per comunicazioni tecniche o commerciali* _____

Nel presente ordine rappresentato da (sindaco direttore, dirigente, amministratore, ecc.) :

Cognome e Nome** _____ **Matricola** _____

Cittadinanza** _____ **Codice Fiscale**** _____

con la sottoscrizione del presente atto, consapevole che chiunque rilascia dichiarazioni mendaci è punito ai sensi del codice penale e delle leggi speciali in materia (art.76, D.P.R. 445/2000), dichiara di agire in qualità di rappresentante del soggetto giuridico indicato nel presente atto come Cliente o comunque di soggetto incaricato da quest'ultimo alla sottoscrizione del presente atto (art.46, lett. u), D.P.R. 445/2000) e richiede, nell'ambito del Servizio Legalmail, l'attivazione della/e casella/e di Posta Elettronica Certificata indicate nell'**APPENDICE AL PIANO DEI FABBISOGNI**

NOME INDIRIZZO CASELLA A SINGOLA UTENZA indicare se collegata ad applicazioni (es. Pi3):

Collegata ad applicazioni (si/no) _____

Disciplina contrattuale

Il Servizio Legalmail – Posta Elettronica Certificata è un servizio erogato da InfoCert. Nel presente documento, i termini indicati con l'iniziale maiuscola assumono lo stesso significato di cui alle relative definizioni contenute nelle Condizioni Generali di Contratto predisposte da InfoCert e disponibili sul sito internet di InfoCert www.infocert.it, nella sezione "PEC Legalmail", alla pagina "Documentazione".

La disciplina del Servizio Legalmail è contenuta nella presente Richiesta di attivazione, nelle Condizioni Generali di Contratto predisposte da InfoCert, nel Manuale Operativo, nell'Allegato Tecnico Casella Legalmail Massiva (limitatamente alle caselle massive) nonché nell'offerta commerciale. Con la sottoscrizione del presente atto, si dichiara di aver preso visione e di conoscere ed accettare tutte le clausole contenute nei sopra citati documenti, ivi comprese quelle relative alle tariffe indicate nell'offerta commerciale.

Trattamento dei dati personali rilasciati nella presente Richiesta di Attivazione

Il Cliente dichiara di aver letto e compreso il contenuto dell'Informativa della "Privacy Policy – Attivazione Servizi InfoCert", pubblicata nella pagina "Documentazione", sul sito www.infocert.it.

In particolare, il Cliente è stato reso edotto del trattamento dei propri dati personali necessario ai fini dell'erogazione del Servizio e, spuntando le caselle in basso e firmando dove richiesto, il Cliente può liberamente prestare il suo consenso e, di conseguenza, autorizzare:

a) al trattamento dei suoi dati personali per le finalità di marketing / vendita diretta di prodotti o servizi di InfoCert, sia con modalità automatizzate (es., posta elettronica, fax, sms), sia con modalità tradizionali di contatto (telefono, posta cartacea)

☐ **Presta il consenso**

☐ **Non presta il consenso**

b) al trattamento dei suoi dati personali per le finalità di marketing / vendita diretta di prodotti o servizi di soggetti terzi in qualità di autonomi titolari, sia con modalità automatizzate (es., posta elettronica, fax, sms), sia con modalità tradizionali di contatto (telefono, posta cartacea)

☐ **Presta il consenso**

☐ **Non presta il consenso**

Atto di affidamento della Conservazione e nomina di InfoCert a Responsabile del trattamento dei dati personali inviati in conservazione (in caso di acquisto del Servizio Aggiuntivo di Conservazione nell'ambito della presente Richiesta di Attivazione)

Il Cliente, con la sottoscrizione della presente Richiesta di Attivazione affida ad InfoCert il servizio di conservazione dei messaggi trasmessi e ricevuti, ai sensi del DPCM 3.12.2013 e dell'art. 1.3 delle Condizioni Generali di Contratto Legalmail, e in qualità di Titolare del trattamento dei dati personali inviati in conservazione, autorizza InfoCert ad effettuare le operazioni di trattamento di cui all'art. 8.2 delle Condizioni Generali di Contratto Legalmail. Pertanto, il Cliente nomina InfoCert quale responsabile del trattamento dei dati personali, ai sensi dell'art. 28 del Regolamento (UE) 679/2016 e dell'art. 8.2. delle Condizioni Generali di Contratto Legalmail.

DATA

IL CLIENTE (timbro e firma)

* i campi contrassegnati con un asterisco sono obbligatori

** da compilare se il richiedente è Impresa/Studio/Pubblica Amministrazione/Associazione

Spazio riservato

Numero Contratto _____



Il Cliente dichiara inoltre di approvare specificamente ai sensi degli artt. 1341 e 1342, c.c., le Condizioni Generali di Contratto “*Servizio Legalmail – Posta Elettronica Certificata*” di seguito indicate: art. 3 (Durata); art. 5 (Connettività e trasmissione dei dati); art. 6 (Corrispettivi); art. 9 (Responsabilità dei contenuti e dei dati); art. 10 (Responsabilità di InfoCert); art. 11 (Responsabilità dell'Utilizzatore); art. 12 (Risoluzione); art. 14 (Legge applicabile e disposizioni generali. Variazioni delle condizioni contrattuali); art. 15 (Procedure di reclamo e di risoluzione delle controversie)

DATA

IL CLIENTE (timbro e firma)

PER CASELLA MULTIUTENTE SPECIFICARE UTENZE DA ATTIVARE O DISATTIVARE:

UTENZE DA ABILITARE

Cognome	Nome	Email

UTENZE DA DISABILITARE

Cognome	Nome	Email

Note:

* i campi contrassegnati con un asterisco sono obbligatori

** da compilare se il richiedente è Impresa/Studio/Pubblica Amministrazione/Associazione

Spazio riservato

Numero Contratto _____

Domini personalizzati

Il Cliente ha la possibilità di richiedere l'attivazione di un dominio di posta diverso da quello previsto nell'offerta standard: **@legalmail.it**.

InfoCert può garantire l'attivazione di tale componente in due diverse modalità, sia utilizzando un ulteriore livello nei domini esistenti di InfoCert, sia utilizzando un dominio proprio.

Dominio personalizzato interno Legalmail

Il sottodominio interno Legalmail è configurato come un dominio di terzo livello del tipo **nomedominio.legalmail.it** all'interno del quale verranno definite caselle di posta elettronica certificata del tipo **nome.cognome@nomedominio.legalmail.it**.

Il nome del dominio è proposto dal Cliente, ma deve essere confermato da InfoCert sulla base di verifiche di congruità (Domini/Nominativi già registrati, ecc.).

La scelta di questo tipo di sottodominio non comporta nessun coinvolgimento operativo da parte del provider/maintainer del cliente.

InfoCert provvederà a:

- pubblicare i domini nell'Indice CNIPA (come previsto dalla Normativa)
- attivare le caselle di Posta Certificata, all'interno del nuovo Dominio personalizzato.

Dominio personalizzato esterno

La personalizzazione di un sottodominio esterno consiste nella definizione di un dominio del tipo **legal.propriodominio.it** (o simile), all'interno del quale verranno definite caselle di posta elettronica certificata del tipo **nome.cognome@legal.propriodominio.it**.

Il gestore del dominio del Cliente (provider/maintainer) deve configurare i server DNS in modo che la posta del dominio certificato venga indirizzata correttamente verso i server InfoCert. Il mantenimento del reindirizzamento nel tempo è un prerequisito necessario per il corretto funzionamento delle caselle di Posta Elettronica Certificata InfoCert e rimane sotto la responsabilità del provider/maintainer del Cliente.

Ad avvenuto completamento di tali attività InfoCert provvederà a:

- Inserire i domini configurati nei sistemi InfoCert
- pubblicare i domini nell'Indice CNIPA (come previsto dalla Normativa)
- attivare le caselle di Posta Certificata, all'interno del nuovo Dominio personalizzato.

All'interno del dominio personalizzato (interno o esterno) il Cliente potrà richiedere/acquistare un numero indefinito di caselle di Posta Elettronica Certificata.

Eventuali variazioni del nome del sottodominio (interno o esterno) comporterà il riacquisto di tutte le caselle già attive sul vecchio sottodominio (a meno di cessazione delle stesse).

Archivio di Sicurezza

E' il servizio di salvataggio - backup - automatico e sicuro dei messaggi, dei loro allegati e delle ricevute.

Il servizio viene offerto in modalità remota: i messaggi archiviati sono depositati presso i Data Center di InfoCert.

Il Cliente attraverso Webmail può configurare/modificare nel tempo le diverse opzioni di salvataggio e la combinazione dei messaggi da salvare.

Tramite specifiche funzioni, l'utente può effettuare una ricerca dei messaggi archiviati utilizzando un'ampia serie di parametri: dalla ricerca nei singoli campi (o una combinazione degli stessi) alla ricerca testuale sull'intero messaggio.

I messaggi archiviati possono eventualmente anche essere cancellati dall'utente.

Al raggiungimento della soglia di Archivio di Sicurezza assegnata, viene comunicato al Cliente l'impossibilità di archiviare ulteriori messaggi, fermo restando la possibilità di acquistare, secondo le tariffe in vigore al momento, ulteriore spazio di Archivio.

Notifica SMS

Il servizio controlla quotidianamente, ad un'ora prestabilita dal Cliente, la presenza di messaggi di posta certificata non letti e, in caso positivo, invia un messaggio SMS di notifica della ricezione al numero di cellulare indicato dal Cliente.

Si fa presente che il servizio non controlla le ricevute e i messaggi di posta non certificata.

Il servizio prevede non più un messaggio di notifica al giorno, per un massimo di 365 messaggi annui.

Utente	Matricola	Cognome	Nome	Codice fiscale	Recapito telefonico	e-mail	nome utente di dominio	Note:
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								



**Regione Autonoma
Trentino-Alto Adige/Südtirol**

**Region Autonoma
Trentin-Südtirol**

**Autonome Region
Trentino-Südtirol**

Struttura

Ufficio _____

Tel: 0461 20

e-mail: _____@regione.taa.it

pec: _____@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Alla c.a.

Ufficio Informatica e digitalizzazione

Oggetto: richiesta di abilitazione/disabilitazione ad operare sul sito web

A partire dalla data di _____, si richiede di adeguare il profilo informatico di operatività nel sito istituzionale del seguente collaboratore:

NOMINATIVO		CODICE FISCALE	

in servizio presso:

STRUTTURA	Scegliere la struttura	UFFICIO	Scegliere l'Ufficio

e secondo le seguenti indicazioni:

SEZIONE DI EDITOR	ABILITAZIONE	DISABILITAZIONE
Amministrazione		
Inserimento/modifica utenti amministrazione		
Amministrazione Trasparente		
Documenti e dati (Atti amministrativi)		
Novità		
Servizi		

OPERATORE DIGITALE*	BACKOFFICE	SERVIZIO	ABILITAZIONE	DISABILITAZIONE

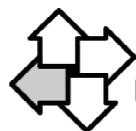
**elencare il tipo di servizio di backoffice a cui si intende abilitare/disabilitare il collaboratore (ad esempio: richiesta di comando presso l'amministrazione regionale, richiesta di esposizione temporanea di un'opera d'arte, autorizzazione all'iscrizione all'albo dei sindaci emeriti)*

IL/LA DIRIGENTE

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

____/____



La/Il sottoscritta/o (nome e cognome) _____ appartenente alla struttura organizzativa (Ripartizione, ufficio, agenzia...) Ripartizione _____ - Ufficio _____, in qualità di soggetto abilitante (ovvero, soggetto autorizzato a richiedere l'abilitazione o la revoca dell'accesso per altri utenti) e per conto del Titolare del trattamento dei dati personali ai sensi del D.Lgs 196/2003 (Codice Privacy) e s.m.i. e del Regolamento (UE) 2016/679,

autorizza i collaboratori:

Utente AD	Nome	Cognome	Struttura di appartenenza	Email	Telefono
rataa\				@regione.taa.it	0461/201
rataa\				@regione.taa.it	0461/201
rataa\				@regione.taa.it	0461/201
rataa\				@regione.taa.it	0461/201
rataa\				@regione.taa.it	0461/201
rataa\				@regione.taa.it	0461/201

ad accedere ai dati presenti nel documento Qlik (nome del documento Qlik). Consultazione capienza fondi capitoli

L'accesso consente di visualizzare, scaricare ed esportare i dati ed i documenti.

L'accesso ai dati viene concesso in visione:

- ☒ totale
- ☐ parziale (indicare quali dati sono concessi in visione, per esempio ripartizione). Immettere testo.

La/Il sottoscritta/o revocherà il diritto d'accesso, e lo comunicherà prontamente utilizzando il modulo di revoca, al ricorrere di uno dei seguenti motivi: revoca dell'incarico, trasferimento, pensionamento, ecc.

Data: _____

Soggetto abilitante
IL/LA DIRIGENTE

firmato digitalmente

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D. Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).


**Regione Autonoma
Trentino-Alto Adige/Südtirol**
**Region Autonoma
Trentin-Südtirol**
**Autonome Region
Trentino-Südtirol**

Segreteria generale
Generalsekretariat
Ufficio affari generali
Amt für allgemeine Angelegenheiten
☎ 0461 201323
@ affgen@regione.taa.it
pec: affgen@pec.regione.taa.it

Ripartizione III - Minoranze linguistiche, integrazione europea e Giudici di Pace
Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte
☎ 0461 201406 ☎ 0471 322122
@ ripmin@regione.taa.it
pec: ripmin@pec.regione.taa.it

Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i files allegati alla medesima.

Protokollnummer und Registrierungsdatum sind dem Dokument als Metadaten zugeordnet (Dekret des Präsidenten des Ministerrates vom 3.12.2013, Art. 20). Gegenstand der zertifizierten E-Mail bzw. beigefügte Dateien überprüfen.



Spettabili
Giudici di pace coordinatori

An die koordinierenden
Friedensrichterinnen und Friedensrichter

e, p.c.
Spettabile
Responsabile della protezione dei dati
della Regione autonoma Trentino-Alto
Adige/Südtirol

u. z. K.
An den
Datenschutzbeauftragten
der Autonomen Region Trentino-Südtirol

consorzio@pec.comunitrentini.it

consorzio@pec.comunitrentini.it

Oggetto: Disposizioni organizzative in materia di privacy.

Con deliberazione n. 193 di data 3 settembre 2019 la Giunta regionale ha individuato gli Uffici del Giudice di Pace, per quanto riguarda le rispettive attribuzioni giurisdizionali, quali titolari singolarmente del trattamento dei dati personali. Sulla base di tale determinazione, ai Giudici di pace coordinatori è lasciata piena autonomia nell'individuare le finalità e le modalità del trattamento dei dati personali, nel rispetto delle direttive fornite dal

Betreff: Organisatorische Bestimmungen in Sachen Datenschutz

Mit Beschluss der Regionalregierung vom 3. September 2019, Nr. 193 wurden die einzelnen Friedensgerichte als Verantwortliche für die Verarbeitung personenbezogener Daten in Zusammenhang mit den jeweiligen Gerichtsbefugnissen bestimmt. Aufgrund dieses Beschlusses können die koordinierenden Friedensrichter und Friedensrichterinnen unter Beachtung der Richtlinien des Justizministeriums, das für

Ministero della Giustizia, quale titolare del trattamento dei dati relativi all'attività giudiziaria.

Con successiva comunicazione a firma del Segretario generale (prot. 23830/2022), si è provveduto a semplificare gli adempimenti di competenza di ogni Ripartizione in materia di privacy.

Tenuto altresì conto che l'esercizio dell'attività giurisdizionale è strettamente connessa all'utilizzo di strumenti informatici e telematici gestiti dalla Regione, risulta necessario procedere ad armonizzare tra loro gli adempimenti in materia di privacy in capo alla Regione.

Di seguito si illustrano gli adempimenti necessari con le indicazioni operative.

1. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Il Registro delle attività di trattamento deve essere redatto ai sensi dell'art. 30 del Regolamento (UE) n. 679/2016 e deve essere mantenuto costantemente aggiornato ai fini dell'esibizione all'Autorità Garante in caso di ispezione. L'aggiornamento del Registro deve essere effettuato ogni qualvolta negli Uffici del Giudice di pace si realizzino i seguenti eventi:

- nuove assunzioni di collaboratori;
- cessazioni di collaboratori;
- attribuzione o rimozione di diverse abilitazioni (pec, cartelle informatiche, utilizzo e accesso a banche dati).

Preso atto che sul server di conservazione dei dati, di proprietà della Regione ed accessibile dagli operatori della giustizia, è

die Verarbeitung der Daten in Zusammenhang mit der Gerichtstätigkeit verantwortlich ist, die Zwecke und die Modalitäten der Verarbeitung personenbezogener Daten vollkommen selbstständig bestimmen.

Mit einem späteren Schreiben des Generalsekretärs (Prot. Nr. 23830/2022) wurden die Amtshandlungen in Sachen Datenschutz, für die jede Abteilung zuständig ist, vereinfacht.

In Anbetracht der Tatsache, dass die Ausübung der Rechtsprechungstätigkeit mit dem Einsatz von IT- und Telematikinstrumenten, die von der Region verwaltet werden, einhergeht, müssen die der Region obliegenden Amtshandlungen in Sachen Datenschutz vereinheitlicht werden.

Nachstehend werden die notwendigen Amtshandlungen samt Anweisungen dargelegt.

1. VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Das Verzeichnis der Verarbeitungstätigkeiten ist gemäß Artikel 30 der Verordnung (EU) Nr. 679/2016 zu erstellen und ständig auf dem neuesten Stand zu halten, damit es der Datenschutzbehörde im Falle einer Kontrolle vorgelegt werden kann. Dieses Verzeichnis ist immer dann zu aktualisieren, wenn in den Friedensgerichten folgende Ereignisse eintreten:

- wenn neue Mitarbeiter eingestellt werden;
- wenn Mitarbeiter aus dem Dienst ausscheiden;
- wenn die verschiedenen Zugriffsberechtigungen (PEC, Netzordner, Verwendung von und Zugriff auf Datenbanken) erteilt oder widerrufen

prevista la memorizzazione di dati relativi sia l'attività tipicamente giurisdizionale effettuata dai Giudici di Pace e dai loro collaboratori, sia di dati legati all'attività amministrativa (come ad esempio la gestione del fascicolo del personale), per quest'ultima tipologia di trattamenti di dati è necessario procedere alla rilevazione degli stessi all'interno di uno specifico Registro delle attività di trattamento dei dati (art. 30 Regolamento UE n. 679/2016).

Ogni ufficio del Giudice di pace dovrà quindi procedere ad elaborare il proprio Registro delle attività di trattamento dei dati personali secondo il modello allegato, per la parte attinente alle autorizzazioni concesse ed alla gestione amministrativa del personale, ponendo particolare attenzione a mantenere costantemente aggiornati i nominativi dei collaboratori incaricati.

Il documento, firmato dal Giudice coordinatore, va trasmesso alla Ripartizione III Minoranze linguistiche, integrazione europea e Giudici di pace (Ufficio giudici di pace e giustizia riparativa) mediante pec (giudicidipace@pec.regione.taa.it).

Si ribadisce inoltre che la conservazione diligente e accurata di questa documentazione è fondamentale al fine di dimostrare, in caso di eventuale ispezione da parte dell'autorità del Garante, il rispetto di quanto previsto dalla disciplina in materia di privacy. Si ricorda inoltre che i documenti vanno classificati, all'interno del gestionale Pi.Tre, con il nodo di titolario **6.4. Protezione dei dati personali**.

werden.

Da auf dem Server für die Datenspeicherung im Eigentum der Region, auf den die Mitarbeiter der Gerichtsämter Zugriff haben, sowohl die Daten betreffend die von den Friedensrichtern und ihren Mitarbeitern ausgeübte Rechtsprechungstätigkeit als auch die Daten betreffend die Verwaltungstätigkeit (z. B. die Verwaltung der Personalakten) gespeichert werden, muss die letztgenannte Kategorie von Datenverarbeitung in einem spezifischen Verzeichnis der Verarbeitungstätigkeiten (Art. 30 der Verordnung (EU) Nr. 679/2016) erfasst werden.

Jedes Friedensgericht muss demnach sein eigenes Verzeichnis der Verarbeitungstätigkeiten in Bezug auf die erteilten Zugriffsberechtigungen und die Verwaltung des Personals gemäß dem beiliegenden Vordruck erstellen und besonders darauf achten, die Namen der mit der Datenverarbeitung beauftragten Mitarbeiter stets auf dem neusten Stand zu halten.

Das vom koordinierenden Friedensrichter unterzeichnete Dokument ist mittels zertifizierter E-Mail (PEC) an die Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte (Amt für Friedensgerichte und Wiedergutmachungsjustiz) zu übermitteln (giudicidipace@pec.regione.taa.it).

Es wird erneut darauf hingewiesen, dass die genaue und sorgfältige Aufbewahrung dieser Unterlagen sehr wichtig ist, um im Falle einer Kontrolle der Datenschutzbehörde die Einhaltung der Datenschutzbestimmungen nachweisen zu können. Es wird ferner daran erinnert, dass

diese Dokumente im Pi.Tre-System unter dem Untertitel 6.4. *Protezione dei dati personali* zu klassifizieren sind.

2. AUTORIZZAZIONE AL **TRATTAMENTO DEI DATI.**

Alla luce di quanto esposto nel punto 1, deve essere rilasciata agli incaricati una lettera di incarico al trattamento dei dati firmata digitalmente dalla Dirigente della Ripartizione III Minoranze linguistiche, integrazione europea e Giudici di pace, che autorizza il collaboratore per la parte di trattamento di dati limitatamente alle attività di competenza della Regione.

La lettera di incarico dovrà poi essere conservata nel sistema di archiviazione e conservazione digitale Pi.Tre, all'interno del nodo di titolario 6.4. *Protezione dei dati personali*, ed esibita in caso di eventuale controllo da parte dell'autorità Garante. La Ripartizione III Minoranze linguistiche, integrazione europea e ai Giudici di pace, provvederà ad individuare una modalità operativa congiunta di raccolta e conservazione delle lettere.

3. RICHIESTA ABILITAZIONI/ **DISABILITAZIONI A CARTELLE ED** **APPLICATIVI.**

La richiesta di autorizzazione all'abilitazione e disabilitazione a cartelle ed applicativi, i cui modelli sono allegati alla presente, deve essere firmata dal Giudice coordinatore e

2. ERMÄCHTIGUNG ZUR **DATENVERARBEITUNG**

Im Hinblick auf die Ausführungen unter Z. 1 muss den mit der Datenverarbeitung beauftragten Personen ein von der Leiterin der Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte digital signiertes Schreiben mit dem Auftrag zur Verarbeitung personenbezogener Daten ausgestellt werden, das den jeweiligen Mitarbeiter zur Datenverarbeitung ermächtigt, und zwar beschränkt auf den Teil der in den Zuständigkeitsbereich der Region fallenden Tätigkeiten.

Das Schreiben mit der Auftragserteilung ist danach im digitalen Archivierungs- und Aufbewahrungssystem Pi.Tre unter dem Untertitel 6.4. *Protezione dei dati personali* aufzubewahren und bei einer eventuellen Kontrolle der Datenschutzbehörde vorzuzeigen. Die Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte wird eine einheitlich anzuwendende Modalität für die Sammlung und Aufbewahrung dieser Schreiben festlegen.

3. ANTRAG AUF ERTEILUNG BZW. **WIDERRUF DER** **ZUGRIFFSBERECHTIGUNG FÜR** **ORDNER UND** **ANWENDUNGSPROGRAMME**

Der Antrag auf Erteilung bzw. auf Widerruf der Zugriffsberichtigung für Ordner und Anwendungsprogramme (die entsprechenden Vordrucke liegen diesem

trasmissa alla Ripartizione III Minoranze linguistiche, integrazione europea e Giudici di pace (**Ufficio giudici di pace e giustizia riparativa**) con le modalità sopra descritte che, successivamente, provvederà come di prassi ad inoltrarle all'Ufficio informatica e digitalizzazione.

È importante procedere, ove se ne rilevi la necessità (a titolo esemplificativo per cambio di ruolo, di competenze o d'ufficio), a rimuovere le autorizzazioni concesse al fine di disabilitare l'accesso ad applicativi e cartelle. A tal fine, vanno compilati i relativi modelli.

Anche in questo caso, la Ripartizione III Minoranze linguistiche, Integrazione europea e ai Giudici di pace provvederà ad individuare una modalità operativa congiunta di raccolta e conservazione delle richieste di abilitazioni inoltrate, che dovranno essere raccolte all'interno del nodo di titolario 6.4. *Protezione dei dati personali*.

4. ULTERIORI NOTE

Si ribadisce infine, che la presente circolare è applicabile al Trattamento di dati di carattere esclusivamente amministrativo e **non** al trattamento di dati legati alla tipica attività giurisdizionale.

Pertanto, per quanto riguarda gli applicativi messi a disposizione da parte del Ministero della Giustizia si rimanda alle indicazioni fornite dal Ministero stesso.

Cordiali saluti.

Rundschreiben bei) ist vom koordinierenden Friedensrichter zu unterzeichnen und der Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte (**Amt für Friedensgerichte und Wiedergutmachungsjustiz**) auf dem oben beschriebenen Weg zu übermitteln, das diesen sodann ordnungsgemäß an das Amt für Informatik und Digitalisierung weiterleiten wird.

Es ist wichtig, gegebenenfalls (z. B. bei Änderungen der Rolle, der Zuständigkeiten oder des Amtes der betreffenden Person) die zuvor erteilten Ermächtigungen zu widerrufen, um den Zugriff auf bestimmte Anwendungsprogramme und Ordner zu sperren. Zu diesem Zweck sind die entsprechenden Vordrucke auszufüllen.

Auch in diesem Fall wird die Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte eine einheitlich anzuwendende Modalität für die Sammlung und Aufbewahrung der übermittelten Anträge auf Zugriffsberechtigung festlegen, die ebenfalls unter dem Untertitel 6.4. *Protezione dei dati personali* zu klassifizieren sind.

4. ABSCHLIESSENDE BEMERKUNGEN

Es wird schließlich darauf hingewiesen, dass dieses Rundschreiben ausschließlich für die Verarbeitung verwaltungstechnischer Daten gilt, jedoch **nicht** für die Verarbeitung von Daten betreffend die eigentliche Rechtsprechungstätigkeit.

Demzufolge wird – was die vom Justizministerium zur Verfügung gestellten Anwendungsprogramme anbelangt – auf die von diesem Ministerium erteilten Anweisungen verwiesen.

Mit freundlichen Grüßen

**IL SEGRETARIO GENERALE/
DER GENERALSEKRETÄR**

Michael Mayr
firmato digitalmente/
digital signiert

**LA DIRIGENTE DELLA RIPARTIZIONE III /
DIE LEITERIN DER ABTEILUNG III**

Eva Maria Kofler
firmato digitalmente/
digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Schreiben in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (Art. 3-bis des GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

Allegati/Anlagen:

- modelli:

- Modello Registro dei trattamenti
- Modello lettera di incarico al trattamento dei dati
- Modulo richiesta abilitazione e disabilitazione utenze-casella PEC
- Modulo richiesta abilitazione e disabilitazione cartelle e stampanti

- Vordrucke:

- Vordruck Verzeichnis der Verarbeitungstätigkeiten
- Vordruck Schreiben zur Erteilung des Auftrags zur Datenverarbeitung
- Vordruck Antrag auf Erteilung bzw. Widerruf der Zugriffsberichtigung für zertifiziertes E-Mail-Postfach (PEC)
- Vordruck Antrag auf Erteilung bzw. Widerruf der Zugriffsberechtigung für Ordner und Drucker



Estratto del verbale della seduta del

26.5.2021

Auszug aus dem Protokoll der Sitzung
vom

DELIBERAZIONE N.

BESCHLUSS Nr.

91

Oggetto:

Betreff:

Determinazione delle competenze da riservare alla Giunta, alle Dirigenti ed ai Dirigenti, alle Direttrici ed ai Direttori degli Uffici.

Festlegung der der Regionalregierung, den Führungskräften und den Amtsdirektorinnen/Amtsleitern vorbehaltenen Zuständigkeiten

Arno Kompatscher	Presidente/ Präsident	presente/anwesend
Maurizio Fugatti	Vice Presidente sostituto del Presidente / Vizepräsident-Stellvertreter des Präsidenten	presente/anwesend
Waltraud Deeg	Vice Presidente / Vizepräsidentin	presente/anwesend
Lorenzo Ossanna	Assessore / Assessor	presente/anwesend
Giorgio Leonardi	Assessore / Assessor	presente/anwesend
Manfred Vallazza	Assessore / Assessor	presente/anwesend
Michael Mayr	Segretario generale della Giunta regionale Generalsekretär der Regionalregierung	presente/anwesend

Su proposta del Presidente Arno Kompatscher

Auf Vorschlag des Präsidenten Arno Kompatscher

Segreteria generale

Generalsekretariat

Ufficio Affari generali

Amt für allgemeine Angelegenheiten

In riferimento all'oggetto la Giunta regionale ha discusso e deliberato quanto segue:

Vista la legge regionale 21 luglio 2000, n. 3 concernente "Norme urgenti in materia di personale", in particolare l'articolo 1-bis, aggiunto dall'articolo 2 comma 1 della legge regionale 17 maggio 2011, n. 4 concernente l'indirizzo politico-amministrativo della Giunta regionale, che dispone come segue:

"1. La Giunta regionale definisce l'indirizzo politico-amministrativo e verifica la rispondenza dei risultati della gestione amministrativa alle direttive generali impartite.

2. A tal fine, periodicamente e comunque ogni anno, dopo l'approvazione della legge di bilancio o dell'autorizzazione all'esercizio provvisorio del bilancio:

a) definisce gli obiettivi da perseguire ed i programmi da attuare, indica le priorità ed emana le conseguenti direttive generali per l'azione amministrativa e per la gestione;

b) assegna a ciascuna struttura organizzativa una quota parte del bilancio dell'amministrazione, commisurata alle risorse finanziarie e in relazione agli obiettivi ed ai programmi da attuare.";

Visto l'art. 14, comma 1, della legge regionale 9 novembre 1983, n. 15 e s.m., ai sensi del quale il direttore "Provvede alla firma degli atti connessi all'attività dell'ufficio, salvo quelli che per spesa o tipologia sono riservati con atto a contenuto generale alle funzioni del dirigente";

Vista la propria deliberazione n. 149 del 10 agosto 2018, mediante la quale i Dirigenti di

Die Regionalregierung hat über die oben genannte Angelegenheit beraten und Folgendes beschlossen:

Aufgrund des Regionalgesetzes vom 21. Juli 2000, Nr. 3 „Dringende Bestimmungen auf dem Sachgebiet des Personalwesens“, insbesondere des durch Art. 2 Abs. 1 des Regionalgesetzes vom 17. Mai 2011, Nr. 4 eingefügten Art. 1-*bis*, der die politisch-administrativen Richtlinien der Regionalregierung betrifft und Folgendes besagt:

„(1) Der Regionalausschuss legt die politisch-administrativen Richtlinien fest und überprüft die Übereinstimmung der Ergebnisse der Verwaltungstätigkeit mit den erteilten allgemeinen Richtlinien.

(2) Zu diesem Zweck nimmt der Regionalausschuss regelmäßig und auf jeden Fall alljährlich nach Genehmigung des Haushaltsgesetzes oder der Ermächtigung zur vorläufigen Haushaltsgebarung Nachstehendes vor:

a) Er legt die Zielsetzungen und die Programme fest, gibt die Prioritäten an und erlässt die entsprechenden allgemeinen Richtlinien für das Verwaltungshandeln und die Verwaltungsorganisation;

b) er weist jeder Organisationseinheit einen Teil der Haushaltsmittel der Verwaltung zu, der nach den verfügbaren Finanzressourcen sowie den jeweiligen Zielsetzungen und Programmen bemessen wird.“;

Aufgrund des Art. 14 Abs. 1 des Regionalgesetzes vom 9. November 1983, Nr. 5 i.d.g.F., laut dem der Amtsdirektor die mit der Tätigkeit des Amtes zusammenhängenden Akten unterzeichnet, mit Ausnahme derjenigen, die aufgrund der verbundenen Kosten oder ihrer Art dem Leiter mit einem Akt allgemeinen Inhalts vorbehalten sind;

Aufgrund des Beschlusses der Regionalregierung vom 10. August 2018, Nr. 149, mit dem

Ripartizione o Struttura equiparata sono stati autorizzati a conferire o meno ai propri Direttori e Sostituti l'adozione dei provvedimenti di liquidazione delle spese inferiori ad € 20.000,00.- Iva esclusa e ritenuto di confermarne il contenuto;

Richiamata la propria deliberazione n. 152 del 27 giugno 2019 recante "Determinazione delle competenze da riservare alla Giunta, alle Dirigenti ed ai Dirigenti, alle Direttrici ed ai Direttori degli Uffici" e ritenuto opportuno aggiornare il contenuto al fine di rendere più snella l'attività amministrativa;

Vista la propria deliberazione n. 16 del 25 febbraio 2021 recante "Determinazioni in merito all'adozione dei provvedimenti in materia di personale e ritenuto di confermarne il contenuto";

Ritenuto opportuno disporre che le Direttrici ed i Direttori degli Uffici e loro Sostitute/i (in caso di assenza o impedimento delle Direttrici/dei Direttori), previa delega scritta della/del Dirigente della Ripartizione nella quale gli Uffici sono incardinati, possano provvedere all'adozione di provvedimenti che comportino impegni di spesa entro il limite di € 10.000,00.- Iva esclusa, allo scopo di semplificare le procedure di adozione dei provvedimenti medesimi;

Ad unanimità di voti legalmente espressi,

delibera

1) di riservare alla Giunta le seguenti competenze:

- a) adozione dei regolamenti,
- b) atti generali, atti di programmazione, di indirizzo e di collaborazione

die Leiterinnen/Leiter der Abteilungen und der gleichgestellten Organisationsstrukturen ermächtigt wurden, die ihnen unterstellten Amtsdirektorinnen/Amtsdirektoren und deren Stellvertreterinnen/Stellvertreter eventuell zum Erlass der Maßnahmen betreffend die Auszahlung von Ausgaben unter 20.000,00-Euro ohne MWSt. zu beauftragen, und nach Dafürhalten, den Inhalt dieses Beschlusses zu bestätigen;

Nach Verweis auf den Beschluss der Regionalregierung vom 27. Juni 2019, Nr. 152 „Festlegung der der Regionalregierung, den Führungskräften und den Amtsdirektorinnen/Amtsdirektoren vorbehaltenen Zuständigkeiten“ und nach Dafürhalten, den Inhalt dieses Beschlusses zu aktualisieren, um die Verwaltungstätigkeit agiler zu gestalten;

Aufgrund des Beschlusses vom 25. Februar 2021, Nr. 16 „Entscheidungen zum Erlass der Maßnahmen betreffend das Personal“ und nach Dafürhalten, den Inhalt dieses Beschlusses zu bestätigen;

Nach Dafürhalten, die Möglichkeit vorzusehen, dass die Amtsdirektorinnen/Amtsdirektoren und deren Stellvertreterinnen/Stellvertreter (bei Abwesenheit oder Verhinderung der Amtsdirektorinnen/Amtsdirektoren) mit schriftlicher Vollmacht der Leiterin/des Leiters ihrer Abteilung Maßnahmen zur Zweckbindung von Mitteln für Ausgaben bis zu 10.000,00- Euro ohne MWSt. erlassen, um die diesbezüglichen Verfahren zu vereinfachen;

beschließt die Regionalregierung

mit Einhelligkeit gesetzmäßig abgegebener Stimmen,

1. der Regionalregierung folgende Zuständigkeiten vorzubehalten:

- a) Erlass der Verordnungen
- b) allgemeine Maßnahmen, Programmierungs- und Ausrichtungsakte, Maßnah-

istituzionale,

- c) nomina di organismi regionali, ad eccezione della nomina di commissioni interne che non comportano spese, designazione o indicazione di rappresentanti della Regione in enti o società a partecipazione regionale,
- d) promozione o resistenza alle liti avanti l'autorità giudiziaria compresa la nomina dei difensori,
- e) spese relative agli organi istituzionali,
- f) assegnazione dalla Regione, di risorse finanziarie alle Province autonome per lo svolgimento delle funzioni delegate,
- g) conferimento di incarichi di consulenza e di collaborazione, ad eccezione degli affidamenti di incarichi per la formazione del personale regionale;
- h) servizio di informazione dell'attività regionale,
- i) acquisizione e disposizione di beni immobili patrimoniali,
- j) realizzazione di iniziative dirette regionali in materia di integrazione europea, minoranze e aiuti umanitari,
- k) assegnazione di finanziamenti e contributi di qualsiasi natura ad enti e associazioni,
- l) assunzione di anticipazioni di cassa,
- m) prestazione di garanzie,
- n) partecipazioni in società, sottoscrizioni di azioni e di obbligazioni,
- o) atti previsti da specifiche norme, riservati alla Giunta regionale,
- p) atti di impegno di spesa relativi alle competenze sopra indicate, esclusi quelli relativi alla precedente lettera c), limitatamente ai gettoni di presenza e alle spese di viaggio ed esclusi quelli relativi alla lettera d),
- q) ulteriori atti individuati dalla Giunta;

men betreffend die institutionelle Zusammenarbeit

- c) Ernennung von regionalen Einrichtungen mit Ausnahme der Ernennung von mit keinen Ausgaben verbundenen internen Kommissionen, Namhaftmachung oder Bestimmung von Vertretern der Region in Körperschaften oder Gesellschaften mit regionaler Beteiligung
- d) Erhebung von oder Einlassung auf Klagen vor Gericht und Ernennung der Verteidiger
- e) Ausgaben betreffend die institutionellen Organe
- f) Zuweisung seitens der Region von finanziellen Mitteln an die Autonomen Provinzen für die übertragenen Befugnisse
- g) Erteilung von Beratungs- und Arbeitsaufträgen, mit Ausnahme der Aufträge zur Weiterbildung des Personals der Region
- h) Informationsdienst über die Tätigkeit der Region
- i) Ankauf von unbeweglichen Vermögensgütern und Verfügungen über dieselben
- j) Verwirklichung von direkten Initiativen der Region in Sachen europäische Integration, Minderheiten und humanitäre Hilfe
- k) Gewährung von Finanzierungen und Beiträge jedweder Art an Körperschaften und Vereinigungen
- l) Kassenvorschüsse
- m) Bürgschaftsleistungen
- n) Beteiligungen an Gesellschaften sowie Zeichnung von Aktien und Schuldverschreibungen
- o) in besonderen Bestimmungen vorgesehene und der Regionalregierung vorbehaltene Akte
- p) Akte betreffend die Zweckbindung von Mitteln für obgenannte Zuständigkeiten, mit Ausnahme jener laut Buchst. c), beschränkt auf die Sitzungsgelder und die Reisekosten, und jener laut Buchst. d)
- q) sonstige von der Regionalregierung vorgesehene Akte;

2) di riservare ai Dirigenti responsabili delle strutture organizzative l'adozione di tutti gli atti non di competenza della Giunta.

3) di autorizzare le Dirigenti ed i Dirigenti di Ripartizione o struttura equiparata a conferire, mediante delega scritta, alle Direttrici ed ai Direttori degli Uffici e loro Sostitute/i (in caso di assenza o impedimento delle Direttrici/dei Direttori), l'adozione di provvedimenti che comportino impegni di spesa entro il limite di € 10.000,00.- Iva esclusa;

4) dalla data di adozione del presente provvedimento cessa di avere efficacia la propria deliberazione n. 152 del 27 giugno 2019.

Contro il presente provvedimento sono ammessi alternativamente i seguenti ricorsi:

- Ricorso giurisdizionale al T.R.G.A. di Trento da parte di chi vi abbia interesse, entro 60 giorni, ai sensi dell'art. 29 e ss. del D.lgs 2 luglio 2012, n. 104;
- Ricorso straordinario al Presidente della Repubblica da parte di chi vi abbia interesse, entro 120 giorni, ai sensi dell'art. 8 del D. P.R. 24 novembre 1971,

Letto, confermato e sottoscritto.

IL PRESIDENTE

DER PRÄSIDENT

Arno Kompatscher

firmato digitalmente / digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa

2. den verantwortlichen Leiterinnen/Leitern der Organisationsstrukturen den Erlass sämtlicher nicht in die Zuständigkeit der Regionalregierung fallenden Akte vorzubehalten;

3. die Leiterinnen/Leiter der Abteilungen und der gleichgestellten Organisationsstrukturen zu ermächtigen, die Amtsdirektorinnen/Amtsdirektoren und deren Stellvertreterinnen/Stellvertreter (bei Abwesenheit oder Verhinderung der Amtsdirektorinnen/Amtsdirektoren) mit schriftlicher Vollmacht zum Erlass von Maßnahmen betreffend die Zweckbindung von Mitteln für Ausgaben bis zu 10.000,00- Euro ohne MWSt. zu beauftragen;

4. Ab dem Datum der Genehmigung dieser Maßnahme ist der Beschluss der Regionalregierung vom 27. Juni 2019, Nr. 152 nicht mehr gültig.

Gegen diese Maßnahme können alternativ nachstehende Rekurse eingelegt werden:

- Rekurs beim Regionalen Verwaltungsgericht Trient, der von den Personen, die ein rechtliches Interesse daran haben, innerhalb von 60 Tagen im Sinne des Art. 29 ff. des GvD vom 02.07.12, Nr. 104 einzulegen ist;
- außerordentlicher Rekurs an den Präsidenten der Republik, der von Personen, die ein rechtliches Interesse daran haben, innerhalb 120 Tagen im Sinne des Art. 8 des DPR vom 24. November 1971, Nr. 8 einzulegen ist.

Gelesen, bestätigt und unterzeichnet

IL SEGRETARIO GENERALE
DELLA GIUNTA REGIONALE

DER GENERALSEKRETÄR
DER REGIONALREGIERUNG

Michael Mayr

firmato digitalmente / digital signiert

Falls dieses Dokument in Papierform übermittelt wird, stellt es die für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei

Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario
sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des
Namens der unterzeichnenden Person ersetzt deren eigenhändige
Unterschrift (Art. 3 des GvD Nr. 39/1993).



Trento, 10 luglio 2019
WM/GF/fd

Ai Segretari
Ai Referenti privacy
degli Enti aderenti al
Servizio privacy - RPD

OGGETTO: Servizio privacy RPD – Chiarimenti sulla figura dei contitolari del trattamento e modello di accordo di contitolarità.

Con riferimento ai compiti e alle funzioni che il Consorzio dei Comuni Trentini si è impegnato a svolgere nell'ambito dell'erogazione del servizio in oggetto e, segnatamente, per quanto concerne la "Verifica della sussistenza di servizi in contitolarità" di cui all'Attività integrata di supporto ed elaborazione dei documenti, con la presente si intende fornire dei chiarimenti circa la figura dei contitolari del trattamento oltre che fornire un fac-simile di accordo di contitolarità da personalizzare e adottare.

Il Regolamento europeo 679/2016 disciplina la contitolarità del trattamento all'art. 26, ai sensi del quale presupposto perché sussista un rapporto di contitolarità è che i titolari del trattamento **determinino congiuntamente finalità e mezzi del trattamento**.

La norma prescrive che i titolari di trattamento devono valutare nell'ambito della propria attività la sussistenza di situazioni di contitolarità del trattamento e nel caso stipulare un accordo avente valenza giuridica nel quale definire specificamente le funzioni e i compiti svolti da ogni contitolare, anche con riferimento all'ambito di responsabilità, della sicurezza e dell'esercizio dei diritti degli interessati.

Come anticipato in occasione degli incontri dello Staff privacy RPD presso la vostra sede così come nei momenti informativi organizzati dallo scrivente Servizio, nell'ambito del piano di lavoro attivato per l'adeguamento alle disposizioni del Regolamento n. 679/2016 la tematica della contitolarità ha necessitato di approfondimenti puntuali e dedicati. Di seguito si rendicontano gli esiti delle analisi fatte su due casi (tra i più frequenti) tra quelli che ci sono stati sottoposti dagli aderenti al servizio.

Gestione associata tra comuni

L'esercizio delle funzioni istituzionali dei Comuni in forma associata, come previsto dalla legge di riforma istituzionale, configura per quanto attiene il trattamento dei dati personali effettuato nell'esercizio di tali funzioni la sussistenza di un rapporto di contitolarità. Come previsto dall'articolo 26 del GDPR 679/2016, i titolari del trattamento (nel caso i Comuni) devono determinare mediante



un accordo interno le rispettive responsabilità e compiti in merito a che il trattamento dei dati personali avvenga in conformità alla vigente normativa in materia. A tal fine:

- nella convenzione che disciplina la gestione associata dei servizi (nella gran parte dei casi già approvata e sottoscritta) si sarebbe dovuto introdurre un articolo che chiariva che gli enti associati sono contitolari dei trattamenti in relazione ai servizi gestiti in forma associata. L'articolo avrebbe dovuto far rinvio per l'individuazione delle rispettive responsabilità e compiti in materia all'accordo interno di cui all'art. 26 del Regolamento europeo 679/2016.

-pur in mancanza di un articolo ad hoc nella convenzione della gestione associata, quel che rileva è che di certo tra i Comuni che esercitano le funzioni in forma associata sussiste un rapporto di contitolarità. Si ritiene quindi necessario che tra gli enti interessati sia formato e sottoscritto un accordo di contitolarità nelle cui premesse si faccia riferimento alla gestione associata in essere tra i comuni, citando la convenzione quali rapporto e atto amministrativo a fondamento. Si può prevedere la stipula di un unico accordo di contitolarità per i diversi servizi in gestione associata purchè sia dia puntuale contenuto alle diverse clausole in ragione dell'effettivo riparto delle responsabilità e dei compiti tra i comuni e l'ente capofila in materia di gestione dei dati personali. Si farà riferimento e si definirà per esempio la questione organizzativa, della sicurezza, dei diritti degli interessati, del processo di data breach, ecc.

Sistema interbibliotecario trentino

Esiste un rapporto di contitolarità tra Enti Locali, PaT e gli altri soggetti aderenti al Sistema Interbibliotecario Trentino in merito al trattamento dei dati degli utenti del SBT). Il Servizio privacy RPD e il Servizio attività culturali della Provincia autonoma di Trento hanno condiviso un contratto di contitolarità che verrà comunicato e illustrato dalla PaT.

Il supporto all'analisi di casi di contitolarità sarà oggetto anche della prossima visita dello staff privacy RPD sul territorio che è programmata per il prossimo autunno.

Per l'analisi di un caso specifico e l'accompagnamento nella personalizzazione dell'accordo è comunque possibile rivolgersi alla dott.ssa Federica Dallaporta all'Ufficio Segreteria dell'Area Innovazione (tel: 0461 1920717 – email: serviziordpd@comunitrentini.it).

Cordiali saluti.

Il Responsabile
dell'Area Innovazione
Walter Merler

firmato digitalmente



SERVIZIO RESPONSABILE DELLA PROTEZIONE DEI DATI

L'INTESTAZIONE VA SOSTITUITA CON LOGO E RIFERIMENTI DELL'ENTE

Oggetto: Accordo di contitolarità ai sensi dell'art. 26 del Regolamento UE 2016/679

TRA

COMUNE DI _____

E

L'art. 26 del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR) prevede che, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento.

I contitolari del trattamento determinano, in modo trasparente, mediante un accordo interno:

- le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato;
- le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 GDPR.

L'accordo può prevedere la designazione di un punto di contatto per gli interessati, fermo restando che l'interessato può esercitare i propri diritti ai sensi del GDPR nei confronti di e verso ciascun titolare del trattamento.

Non è necessario l'accordo interno nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti.

In data _____ il Comune di _____ e [NOMINATIVO/I CONTITOLARE/I], hanno stipulato il contratto/la convenzione/ il progetto [INDICARE RIFERIMENTI] avente ad [OGGETTO].

Per l'esecuzione del contratto/convenzione/progetto le parti, in qualità di contitolari del trattamento, ai sensi dell'art. 26 del Regolamento UE 2016/679, provvedono al necessario e pertinente trattamento di dati personali.

Per l'esecuzione del contratto/convenzione/progetto le parti, in qualità di contitolari del trattamento, ai sensi dell'art. 26 del Regolamento UE 2016/679 hanno congiuntamente determinato le seguenti finalità e mezzi del trattamento:

- Finalità di trattamento [INSERIRE FINALITÀ]
- Tipologia di trattamento [INSERIRE TIPOLOGIA COME DA REGISTRO DEI TRATTAMENTI]

- Tipo di dati trattati: [INSERIRE CATEGORIA DI DATI COME DA REGISTRO DEI TRATTAMENTI]
- Categorie di interessati: [INSERIRE CATEGORIE DI INTERESSATI COME DA REGISTRO DEI TRATTAMENTI]
- Strumenti hardware e software: [INSERIRE INFORMAZIONI CARATTERIZZANTI]

Altri elementi di rilievo:

Tutto ciò premesso

le parti individuano le rispettive responsabilità e compiti

RIPARTIZIONE DEI RUOLI E DEI COMPITI

In relazione alla specifica natura del rapporto derivante dal contratto/convenzione/progetto, alle rispettive prestazioni e, fermo il diritto dell'interessato di esercitare i suoi diritti nei confronti di ciascun titolare, ai sensi dell'art. 26 del Regolamento UE 2016/679, si conviene la seguente ripartizione di responsabilità e di compiti.

Trattamenti dei dati personali

I contitolari attestano che i dati sono trattati nel rispetto di quanto previsto dal Regolamento europeo 679/2016, dal D.Lgs. 196/2003 e dalla normativa vigente in materia.

EVENTUALE RIPARTIZIONE DELLE SPECIFICHE OPERAZIONI DI TRATTAMENTO:

RACCOLTA

COMUNICAZIONE

ELABORAZIONE

TRASFERIMENTO DATI EXTRA UE

Autorizzati e designati al trattamento e responsabili del trattamento

Il Comune/La Comunità _____ è autorizzata a nominare i designati al trattamento.

Il Comune/La Comunità _____ è autorizzata a nominare i responsabili del trattamento. Il Comune/La Comunità _____ è autorizzata ad individuare per tutti i contitolari, secondo idonee modalità, i soggetti autorizzati al trattamento.

Il Comune/La Comunità _____ ha l'obbligo di impartire le disposizioni organizzative e operative e fornire soggetti autorizzati le istruzioni per il corretto, lecito, pertinente e sicuro trattamento dei dati, eseguendo gli opportuni controlli

Il Comune/La Comunità _____ ha l'obbligo di fornire agli autorizzati l'adeguata formazione in materia.

Informativa ai sensi dell'art. 13 e dell'art. 14 del Regolamento europeo 679/2016

Il Comune/La Comunità _____ ha l'obbligo di curare, ai sensi degli artt. 13 e 14 Regolamento UE 2016/679, l'informativa agli interessati, predisponendo la modulistica e altre forme idonee di informazione.

Assistenza/esercizio dei diritti dell'interessato

Il Comune/La Comunità _____ ha l'obbligo di adottare misure tecniche e organizzative adeguate al fine di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del Regolamento europeo 2016/679.

Il Comune/La Comunità _____ ha l'obbligo di individuare il punto di contatto per gli interessati presso _____

Rapporti con l'Autorità di controllo e l'Autorità giudiziaria

Il Comune/La Comunità _____ ha l'obbligo di curare i rapporti con l'Autorità di controllo e l'Autorità giudiziaria, informando tempestivamente gli altri titolari in caso di ispezioni e contestazioni.

Misure di sicurezza tecniche

Il Comune/La Comunità _____ ha l'obbligo di adottare tutte le misure tecniche e organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento UE 2016/679.

Oppure indicare la ripartizione dei compiti tra i titolari

Es. gestione degli strumenti informatici

Gestione degli archivi cartacei

Gestione del sito web

Gestione degli accorgimenti relativi alle attribuzioni degli Amministratori di sistema.

Ogni titolare provvede alla formazione e tenuta del proprio registro dei trattamenti in cui annota e evidenzia i trattamenti in contitolarità.

Ogni titolare ha l'obbligo di designare un responsabile della protezione dei dati, se previsto dall'art. 37 del Regolamento UE 2016/679 e di comunicarne il nominativo e riferimento agli altri titolari oppure riportare elenco dei responsabili della protezione dei dati;

Valutazione dei rischi e valutazione d'impatto privacy

Il Comune/La Comunità _____ ha l'obbligo di predisporre e aggiornare la valutazione dei rischi e la valutazione di impatto del trattamento sui diritti e sulle libertà delle persone e comunque documentare le scelte effettuate in materia di trattamento dei dati personali.

Gestione data breach

Il Comune/La Comunità _____ ha l'obbligo di informare gli altri titolari di ogni violazione dei dati personali che abbia ad oggetto i trattamenti in contitolarità.

Il Comune/La Comunità _____ ha l'obbligo, se ricorre il caso, di effettuare nei termini e modi previsti dalla normativa la notificazione all'Autorità di controllo e/o la comunicazione agli interessati della violazione dei dati personali.

ALTRO

RESPONSABILITA'

In ragione e alla luce della suddetta ripartizione dei ruoli e dei compiti, ne consegue l'assunzione di responsabilità in via esclusiva per le violazioni, purché il danno causato o la violazione commessa sia di esclusiva conseguenze del comportamento, anche omissivo, della parte.

Pertanto, fermo il disposto dell'art. 82 del Regolamento europeo 679/2016, ciascuna delle parti manleva l'altro per ogni risarcimento del danno dalla stessa provocato ovvero per l'applicazione di sanzioni amministrative derivanti da una violazione normativa.

DURATA

L'accordo ha durata per _____

Luogo _____, data _____

Firma delle parti



Consorzio dei
Comuni Trentini

Trento, 2 dicembre 2020
GF/fd/ed

Ai segretari
Ai Referenti privacy
degli Enti aderenti al Servizio
privacy RPD

interoperabilità PITRE/PEC

OGGETTO: Servizio privacy RPD – Adempimenti attuativi dell'accordo di contitolarità del Sistema Bibliotecario Trentino

Siamo con la presente a trasmettere la circolare relativa all'argomento di cui all'oggetto.
Ricordiamo che gli uffici del Consorzio sono a disposizione per ogni chiarimento che dovesse rendersi necessario.
Cordiali saluti.

Firmato
Il Direttore generale
dott. Marco Riccadonna

Firmato
Il Presidente
dott. Paride Gianmoena



PIAO

ALLEGATO n. 1

Sottosezione 2.3.

Rischi corruttivi e trasparenza

Trasparenza dell'azione amministrativa – Piano operativo, integrato con le seguenti tre tabelle recanti: a) l'elenco degli obblighi di pubblicazione della sezione "Bandi di gare e contratti" (Allegato 9 AL PNA 2022); b) gli atti e i documenti da pubblicare in "Bandi di gara e contratti" – All. 1 Delibera ANAC 264 del 20.6.2023, come modificato con Delibera ANAC 601 del 19.12.2023 Contratti con bandi e avvisi pubblicati dopo il 1° gennaio 2024; c) l'elenco degli obblighi di pubblicazione della sezione "Bandi di gara e contratti" relativi alla fase di aggiudicazione e di esecuzione, comprese le modifiche ai contratti e le varianti in corso d'opera. Delibera ANAC n. 582 del 13.12.2023 e delibera ANAC n. 605 DEL 19.12.2023 – Contratti con bandi e avvisi pubblicati prima o dopo il 1° luglio 2023 ma non ancora conclusi alla data del 31 dicembre 2023

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
Disposizioni generali	Piano triennale per la prevenzione della corruzione e della trasparenza	Applicazione ai sensi dell'art. 1, c. 1, lett. a), L.R. n. 10/2014	Art. 10, c. 8, lett. a), d.lgs. n. 33/2013	Piano triennale per la prevenzione della corruzione e della trasparenza (PTPCT)	Piano triennale per la prevenzione della corruzione e della trasparenza e suoi allegati, le misure integrative di prevenzione della corruzione individuate ai sensi dell'articolo 1, comma 2-bis della legge n. 190 del 2012, (MOG 231) (link alla sotto-sezione Altri contenuti/Anticorruzione)	Annuale	Entro 10 giorni dall'adozione	Responsabile della Prevenzione della corruzione e della trasparenza	Ripartizione II - Enti locali, previdenza e competenze ordinamentali	Annuale Responsabile della Prevenzione della corruzione e della trasparenza
	Atti generali		Art. 12, c. 1, d.lgs. n. 33/2013	Riferimenti normativi su organizzazione e attività	Riferimenti normativi con i relativi link alle norme di legge statale pubblicate nella banca dati "Normativa" che regolano l'istituzione, l'organizzazione e l'attività delle pubbliche amministrazioni	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro tre mesi decorrenti dalla formazione dell'atto	Tutte le strutture	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
				Atti amministrativi generali	Direttive, circolari, programmi, istruzioni e ogni atto che dispone in generale sulla organizzazione, sulle funzioni, sugli obiettivi, sui procedimenti, ovvero nei quali si determina l'interpretazione di norme giuridiche che riguardano o dettano disposizioni per l'applicazione di esse	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Tutte le strutture	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
				Documenti di programmazione strategico-gestionale	<i>Direttive Presidente e Assessori - documento di programmazione, obiettivi strategici in materia di prevenzione della corruzione e trasparenza</i> Linee programmatiche di mandato, obiettivi alla dirigenza, Obiettivi strategici in materia di prevenzione della corruzione	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 12, c. 2, d.lgs. n. 33/2013	Statuti e leggi regionali	Estremi e testi ufficiali aggiornati degli Statuti e delle norme di legge regionali, che regolano le funzioni, l'organizzazione e lo svolgimento delle attività di competenza dell'amministrazione	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Tutte le strutture	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 55, c. 2, d.lgs. n. 165/2001 Art. 12, c. 1, d.lgs. n. 33/2013	Codice disciplinare e codice di condotta	Codice disciplinare, recante l'indicazione delle infrazioni del codice disciplinare e relative sanzioni (pubblicazione on line in alternativa all'affissione in luogo accessibile a tutti - art. 7, l. n. 300/1970) Codice di condotta inteso quale codice di comportamento	Tempestivo		Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
	Oneri informativi per cittadini e imprese	L'articolo non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10	Art. 12, c. 1-bis, d.lgs. n. 33/2013	Scadenzario obblighi amministrativi	Scadenzario con l'indicazione delle date di efficacia dei nuovi obblighi amministrativi a carico di cittadini e imprese introdotti dalle amministrazioni secondo le modalità definite con DPCM 8 novembre 2013	Tempestivo				
Organizzazione	Titolari di incarichi politici, di amministrazione, di direzione o di governo		Art. 13, c. 1, lett. a), d.lgs. n. 33/2013		Organi di indirizzo politico e di amministrazione e gestione, con l'indicazione delle rispettive competenze	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 30 giorni dalla nomina	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 14, c. 1, lett. a), d.lgs. n. 33/2013	Titolari di incarichi politici di cui all'art. 14, co. 1, del dlgs n. 33/2013	Atto di nomina o di proclamazione, con l'indicazione della durata dell'incarico o del mandato elettivo	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 3 mesi dalla nomina	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 14, c. 1, lett. b), d.lgs. n. 33/2013	(da pubblicare in tabella)	Curriculum vitae	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	I dati sono pubblicati limitatamente alla parte di competenza della Regione. Per alcuni dati comuni all'Amministrazione regionale e a quella provinciale, la Regione predispone un link al sito della Provincia autonoma di Trento e a quello della Provincia autonoma di Bolzano.	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 14, c. 1, lett. c), d.lgs. n. 33/2013		Compensi di qualsiasi natura connessi all'assunzione della carica	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 3 mesi dalla nomina	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
					Importi di viaggi di servizio e missioni pagati con fondi pubblici	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Semestrale (entro 15 giorni dalla scadenza di ciascun semestre)	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
			Art. 14, c. 1, lett. d), d.lgs. n. 33/2013		Dati relativi all'assunzione di altre cariche, presso enti pubblici o privati, e relativi compensi a qualsiasi titolo corrisposti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	I dati sono pubblicati limitatamente alla parte di competenza della	Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. e), d.lgs. n. 33/2013		Altri eventuali incarichi con oneri a carico della finanza pubblica e indicazione dei compensi spettanti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Regione. Per alcuni dati comuni all'Amministrazione regionale e a quella provinciale, la Regione predispone un link al sito della Provincia autonoma di Trento e a quello della Provincia autonoma di Bolzano.	Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 2, c. 1, punto 1, l. n. 441/1982		1) dichiarazione concernente diritti reali su beni immobili e su beni mobili iscritti in pubblici registri, fiduciarie di imprese, azioni di società, quote di partecipazione a società, esercizio di funzioni di amministratore o di sindaco di società, con l'apposizione della formula «sul mio onore affermo che la dichiarazione corrisponde al vero» [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)] e riferita al momento dell'assunzione dell'incarico]	Publicazione una sola volta, entro 3 mesi dalla elezione o dalla nomina; i dati sono pubblicati fino alla cessazione del mandato o dell'incarico.		Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 2, c. 1, punto 2, l. n. 441/1982		2) copia dell'ultima dichiarazione dei redditi soggetti all'imposta sui redditi delle persone fisiche (Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (dando eventualmente evidenza del mancato consenso)) NB: è necessario limitare, con appositi accorgimenti a cura dell'interessato o della amministrazione, la pubblicazione dei dati sensibili.	Publicazione una sola volta, entro 3 mesi dalla elezione o dalla nomina; i dati sono pubblicati per tre anni dalla cessazione del mandato o dell'incarico		Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 2, c. 1, punto 3, l. n. 441/1982		3) dichiarazione concernente le spese sostenute e le obbligazioni assunte per la propaganda elettorale ovvero attestazione di essersi avvalsi esclusivamente di materiali e di mezzi propagandistici predisposti e messi a disposizione dal partito o dalla formazione politica della cui lista il soggetto ha fatto parte, con l'apposizione della formula «sul mio onore affermo che la dichiarazione corrisponde al vero» (con allegate copie delle dichiarazioni relative a finanziamenti e contributi per un importo che nell'anno supera 5.000 €)	Publicazione una sola volta, entro 3 mesi dalla elezione o dalla nomina; i dati sono pubblicati per tre anni dalla cessazione del mandato o dell'incarico		Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 3, l. n. 441/1982		4) attestazione concernente le variazioni della situazione patrimoniale intervenute nell'anno precedente e copia della dichiarazione dei redditi [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)]	Annuale		Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. a), d.lgs. n. 33/2013	Cessati dall'incarico (documentazione da pubblicare sul sito web)	Atto di nomina, con l'indicazione della durata dell'incarico	I dati sono pubblicati per i tre anni successivi dalla cessazione del mandato o dell'incarico dei soggetti, eccetto i dati relativi alla situazione patrimoniale che rimangono pubblicati sino alla cessazione.		Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. b), d.lgs. n. 33/2013		Curriculum vitae	Nessun obbligo di aggiornamento		Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. c), d.lgs. n. 33/2013		Compensi di qualsiasi natura connessi all'assunzione della carica			Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
					Importi di viaggi di servizio e missioni pagati con fondi pubblici			Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. d), d.lgs. n. 33/2013		Dati relativi all'assunzione di altre cariche, presso enti pubblici o privati, e relativi compensi a qualsiasi titolo corrisposti			Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 14, c. 1, lett. e), d.lgs. n. 33/2013		Altri eventuali incarichi con oneri a carico della finanza pubblica e indicazione dei compensi spettanti			Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 2, c. 1, punto 2, l. n. 441/1982		1) copie delle dichiarazioni dei redditi riferiti al periodo dell'incarico; 2) copia della dichiarazione dei redditi successiva al termine dell'incarico o carica, entro un mese dalla scadenza del termine di legge per la presentazione della dichiarazione (Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)) (NB: è necessario limitare, con appositi accorgimenti a cura dell'interessato o della amministrazione, la pubblicazione dei dati sensibili)			Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 2, c. 1, punto 3, l. n. 441/1982		3) dichiarazione concernente le spese sostenute e le obbligazioni assunte per la propaganda elettorale ovvero attestazione di essersi avvalsi esclusivamente di materiali e di mezzi propagandistici predisposti e messi a disposizione dal partito o dalla formazione politica della cui lista il soggetto ha fatto parte con riferimento al periodo dell'incarico (con allegati copie delle dichiarazioni relative a finanziamenti e contributi per un importo che nell'anno superi 5.000 €)			Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 4, l. n. 441/1982		4) dichiarazione concernente le variazioni della situazione patrimoniale intervenute dopo l'ultima attestazione (Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso))			Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
	Sanzioni per mancata comunicazione dei dati		Art. 47, c. 1, d.lgs. n. 33/2013	Sanzioni per mancata o incompleta comunicazione dei dati da parte dei titolari di incarichi politici, di amministrazione, di direzione o di governo	Provvedimenti sanzionatori a carico del responsabile della mancata o incompleta comunicazione dei dati di cui all'articolo 14, concernenti la situazione patrimoniale complessiva del titolare dell'incarico al momento dell'assunzione della carica, la titolarità di imprese, le partecipazioni azionarie proprie nonché tutti i compensi cui dà diritto l'assunzione della carica	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dall'adozione del provvedimento	Sanzione trasmessa da ANAC al Responsabile della Prevenzione della corruzione e della trasparenza	Ripartizione II - Enti locali, previdenza e competenze ordinarie	Semestrale (30 aprile-31 ottobre) Ripartizione II - Enti locali, previdenza e competenze ordinarie
	Rendiconti gruppi consiliari regionali/provinciali		Art. 28, c. 1, d.lgs. n. 33/2013	Rendiconti gruppi consiliari regionali/provinciali	Rendiconti di esercizio annuale dei gruppi consiliari regionali e provinciali, con evidenza delle risorse trasferite o assegnate a ciascun gruppo, con indicazione del titolo di trasferimento e dell'impiego delle risorse utilizzate	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		La pubblicazione dei dati relativi ai rendiconti dei gruppi consiliari regionali/provinciali è di competenza del rispettivo Consiglio regionale/provinciale. L'amministrazione regionale predispone un link per accedere ai suddetti dati.		
				Atti degli organi di controllo	Atti e relazioni degli organi di controllo	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		La pubblicazione dei dati relativi ai rendiconti dei gruppi consiliari regionali/provinciali è di competenza del rispettivo Consiglio regionale/provinciale. L'amministrazione regionale predispone un link per accedere ai suddetti dati.		
	Articolazione degli uffici		Art. 13, c. 1, lett. b), d.lgs. n. 33/2013	Articolazione degli uffici	Indicazione delle competenze di ciascun ufficio, anche di livello dirigenziale non generale, i nomi dei dirigenti responsabili dei singoli uffici	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	entro 20 giorni dall'eventuale aggiornamento	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio gestione giuridica del personale	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
			Art. 13, c. 1, lett. c), d.lgs. n. 33/2013	Organigramma (da pubblicare sotto forma di organigramma, in modo tale che a ciascun ufficio sia assegnato un link ad una pagina contenente tutte le informazioni previste dalla norma)	Illustrazione in forma semplificata, ai fini della piena accessibilità e comprensibilità dei dati, dell'organizzazione dell'amministrazione, mediante l'organigramma o analoghe rappresentazioni grafiche	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio gestione giuridica del personale	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
			Art. 13, c. 1, lett. b), d.lgs. n. 33/2013		Nomi dei dirigenti responsabili dei singoli uffici	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio gestione giuridica del personale	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
	Telefono e posta elettronica		Art. 13, c. 1, lett. d), d.lgs. n. 33/2013	Telefono e posta elettronica	Elenco completo dei numeri di telefono e delle caselle di posta elettronica istituzionali e delle caselle di posta elettronica certificata dedicate, cui il cittadino possa rivolgersi per qualsiasi richiesta inerente i compiti istituzionali	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	entro 20 giorni dall'eventuale aggiornamento	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio gestione giuridica del personale	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
Consulenti e collaboratori	Titolari di incarichi di collaborazione o consulenza		Art. 15, c. 2, d.lgs. n. 33/2013	Consulenti e collaboratori (da pubblicare in tabelle)	Esistenti degli atti di conferimento di incarichi di collaborazione o di consulenza a soggetti esterni a qualsiasi titolo (compresi quelli affidati con contratto di collaborazione coordinata e continuativa) con indicazione dei soggetti percettori, della ragione dell'incarico e dell'ammontare erogato	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Alfatto del conferimento dell'incarico (e comunque entro tre mesi dal conferimento)	Le strutture che conferiscono l'incarico	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
					Per ciascun titolare di incarico:					

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
		In forza dell' art. 1, comma 1, lett. d), della L.R. n. 10/2014, trova applicazione la normativa provinciale in materia (- art. 39 undecies L.P. di Trento n. 23/1990)	Art. 15, c. 1, lett. b), d.lgs. n. 33/2013,		1) curriculum vitae, redatto in conformità al vigente modello europeo	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Atto del conferimento dell'incarico (e comunque entro tre mesi dal conferimento)	Le strutture che conferiscono l'incarico	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 15, c. 1, lett. c), d.lgs. n. 33/2013		2) dati relativi allo svolgimento di incarichi o alla titolarità di cariche in enti di diritto privato regolati o finanziati dalla pubblica amministrazione o allo svolgimento di attività professionali	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Atto del conferimento dell'incarico (e comunque entro tre mesi dal conferimento)	Le strutture che conferiscono l'incarico	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 15, c. 1, lett. d), d.lgs. n. 33/2013		3) compensi comunque denominati, relativi al rapporto di lavoro, di consulenza o di collaborazione (compensi quali affidati con contratto di collaborazione coordinata e continuativa), con specifica evidenza delle eventuali componenti variabili o legate alla valutazione del risultato	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Atto del conferimento dell'incarico (e comunque entro tre mesi dal conferimento)	Le strutture che conferiscono l'incarico	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 15, c. 2, d.lgs. n. 33/2013 Art. 53, c. 14, d.lgs. n. 165/2001		Tabelle relative agli elenchi dei consulenti con indicazione di oggetto, durata e compenso dell'incarico (comunicate alla Funzione pubblica)	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Atto del conferimento dell'incarico (e comunque entro tre mesi dal conferimento)	Le strutture che conferiscono l'incarico	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 53, c. 14, d.lgs. n. 165/2001		Attestazione dell'avvenuta verifica dell'insussistenza di situazioni, anche potenziali, di conflitto di interesse	Tempestivo	Atto del conferimento dell'incarico (e comunque entro tre mesi dal conferimento)	Le strutture che conferiscono l'incarico	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
Personale	Titolari di incarichi dirigenziali amministrativi di vertice			Incari amministrativi di vertice (da pubblicare in tabelle)	Per ciascun titolare di incarico:					
			Art. 14, c. 1, lett. a) e c. 1-bis, d.lgs. n. 33/2013		Atto di conferimento, con l'indicazione della durata dell'incarico	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. b) e c. 1-bis, d.lgs. n. 33/2013		Curriculum vitae, redatto in conformità al vigente modello europeo	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. c) e c. 1-bis, d.lgs. n. 33/2013		Compensi di qualsiasi natura connessi all'assunzione dell'incarico (con specifica evidenza delle eventuali componenti variabili o legate alla valutazione del risultato)	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
					Importi di viaggi di servizio e missioni pagati con fondi pubblici	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Semestrale (entro 15 giorni dalla scadenza di ciascun semestre)	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. d) e c. 1-bis, d.lgs. n. 33/2013		Dati relativi all'assunzione di altre cariche, presso enti pubblici o privati, e relativi compensi a qualsiasi titolo corrisposti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. e) e c. 1-bis, d.lgs. n. 33/2013		Altri eventuali incarichi con oneri a carico della finanza pubblica e indicazione dei compensi spettanti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. f) e c. 1-bis, d.lgs. n. 33/2013 Art. 2, c. 1, punto 1, L. n. 441/1982		1) dichiarazione concernente diritti reali su beni immobili e su beni mobili iscritti in pubblici registri, titolarità di imprese, azioni di società, quote di partecipazione a società, esercizio di funzioni di amministratore o di sindaco di società, con l'apposizione della formula «sul mio onore affermo che la dichiarazione corrisponde al vero» [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso) e riferita al momento dell'assunzione dell'incarico]	Pubblicazione una sola volta, entro 3 mesi dalla nomina; i dati sono pubblicati fino alla cessazione dell'incarico		Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
			Art. 14, c. 1, lett. f) e c. 1-bis, d.lgs. n. 33/2013 Art. 2, c. 1, punto 2.1.1 n. 441/1982		2) copia dell'ultima dichiarazione dei redditi soggetti all'imposta sui redditi delle persone fisiche [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)] (NB: è necessario limitare, con appositi accorgimenti a cura dell'interessato o della amministrazione, la pubblicazione dei dati sensibili)	Pubblicazione una sola volta, entro 3 mesi dalla nomina; i dati sono pubblicati fino alla cessazione dell'incarico		Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. f) e c. 1-bis, d.lgs. n. 33/2013 Art. 3, l. n. 441/1982		3) attestazione concernente le variazioni della situazione patrimoniale intervenute nell'anno precedente e copia della dichiarazione dei redditi [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)]	Pubblicazione annuale; i dati sulla situazione patrimoniale sono pubblicati fino alla cessazione del mandato o dell'incarico mentre la dichiarazione dei redditi per i tre anni successivi alla cessazione	Entro 1 mese dalla scadenza del termine di legge per la presentazione della dichiarazione	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 20, c. 3, d.lgs. n. 39/2013		Dichiarazione sulla insussistenza di una delle cause di inconfirmità dell'incarico	Tempestivo (art. 20, c. 1, d.lgs. n. 39/2013)	All'atto del conferimento dell'incarico	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 20, c. 3, d.lgs. n. 39/2013		Dichiarazione sulla insussistenza di una delle cause di incompatibilità al conferimento dell'incarico	Annuale (art. 20, c. 2, d.lgs. n. 39/2013)	Entro il 15/03	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1-ter, secondo periodo, d.lgs. n. 33/2013		Ammontare complessivo degli emolumenti percepiti a carico della finanza pubblica	Annuale (non oltre il 30 marzo)	Non oltre il 30 marzo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
	Titolari di incarichi dirigenziali (dirigenti non generali)			Incarichi dirigenziali, a qualsiasi titolo conferiti, ivi inclusi quelli conferiti discrezionalmente dall'organo di indirizzo politico senza procedere pubbliche di selezione e titolari di posizione organizzativa con funzioni dirigenziali	Per ciascun titolare di incarico: Atto di conferimento, con l'indicazione della durata dell'incarico	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. b) e c. 1-bis, d.lgs. n. 33/2013	(da pubblicare in tabelle che distinguono le seguenti situazioni: dirigenti, dirigenti individuati discrezionalmente, titolari di posizione organizzativa con funzioni dirigenziali)	Curriculum vitae, redatto in conformità al vigente modello europeo	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. c) e c. 1-bis, d.lgs. n. 33/2013		Compensi di qualsiasi natura connessi all'assunzione dell'incarico (con specifica evidenza delle eventuali componenti variabili o legate alla valutazione del risultato)	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
					Importi di viaggi di servizio e missioni pagati con fondi pubblici	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Semestrale (entro 15 giorni dalla scadenza di ciascun semestre)	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. d) e c. 1-bis, d.lgs. n. 33/2013		Dati relativi all'assunzione di altre cariche, presso enti pubblici o privati, e relativi compensi a qualsiasi titolo corrisposti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. e) e c. 1-bis, d.lgs. n. 33/2013		Altri eventuali incarichi con oneri a carico della finanza pubblica e indicazione dei compensi spettanti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Pubblicazione entro tre mesi dalla nomina e aggiornamento tempestivo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. f) e c. 1-bis, d.lgs. n. 33/2013 Art. 2, c. 1, punto 1.1.1 n. 441/1982		1) dichiarazione concernente diritti reali su beni immobili e su beni mobili iscritti in pubblici registri, titolarità di imprese, azioni di società, quote di partecipazione a società, esercizio di funzioni di amministratore o di sindaco di società, con l'apposizione della formula «sul mio onore affermo che la dichiarazione corrisponde al vero» [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)] e riferita al momento dell'assunzione dell'incarico	Pubblicazione una sola volta, entro 3 mesi dalla nomina; i dati sono pubblicati fino alla cessazione dell'incarico		Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
			Art. 14, c. 1, lett. f) e c. 1-bis, d.lgs. n. 33/2013 Art. 2, c. 1, punto 2.1 n. 441/1982		2) copia dell'ultima dichiarazione dei redditi soggetti all'imposta sui redditi delle persone fisiche [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)] (NB: è necessario limitare, con appositi accorgimenti a cura dell'interessato o della amministrazione, la pubblicazione dei dati sensibili)	Pubblicazione una sola volta, entro 3 mesi dalla nomina; i dati sono pubblicati fino alla cessazione dell'incarico		Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. f) e c. 1-bis, d.lgs. n. 33/2013 Art. 3, l. n. 441/1982		3) attestazione concernente le variazioni della situazione patrimoniale intervenute nell'anno precedente e copia della dichiarazione dei redditi [Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)]	Pubblicazione annuale; i dati sulla situazione patrimoniale sono pubblicati fino alla cessazione del mandato o dell'incarico mentre la dichiarazione dei redditi per i tre anni successivi alla cessazione	Entro 1 mese dalla scadenza del termine di legge per la presentazione della dichiarazione	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 20, c. 3, d.lgs. n. 39/2013		Dichiarazione sulla inossistenza di una delle cause di inconfidenzialità dell'incarico	Tempestivo (art. 20, c. 1, d.lgs. n. 39/2013)	Allatto del conferimento dell'incarico	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 20, c. 3, d.lgs. n. 39/2013		Dichiarazione sulla inossistenza di una delle cause di incompatibilità al conferimento dell'incarico	Annuale (art. 20, c. 2, d.lgs. n. 39/2013)	Entro il 15/03	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1-ter, secondo periodo, d.lgs. n. 33/2013		Ammontare complessivo degli emolumenti percepiti a carico della finanza pubblica	Annuale (non oltre il 30 marzo)	Non oltre il 30 marzo	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 19, c. 1-bis, d.lgs. n. 165/2001	Posi di funzione disponibili	Numero e tipologia dei posti di funzione che si rendono disponibili nella dotazione organica e relativi criteri di scelta	Tempestivo				
	Dirigenti cessati		Art. 14, c. 1, lett. a), d.lgs. n. 33/2013	Dirigenti cessati dal rapporto di lavoro (documentazione da pubblicare sul sito web)	Atto di nomina, con indicazione della durata dell'incarico	Nessuno	I dati sono pubblicati per i tre anni successivi dalla cessazione del mandato o dell'incarico dei soggetti, eccetto i dati relativi alla situazione patrimoniale che rimangono pubblicati sino alla cessazione. Nessun obbligo di aggiornamento	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. b), d.lgs. n. 33/2013		Curriculum vitae	Nessuno	-	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. c), d.lgs. n. 33/2013		Compensi di qualsiasi natura connessi all'assunzione della carica	Nessuno	-	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
					Importi di viaggi di servizio e missioni pagati con fondi pubblici	Nessuno	-	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. d), d.lgs. n. 33/2013		Dati relativi all'assunzione di altre cariche, presso enti pubblici o privati, e relativi compensi a qualsiasi titolo corrisposti	Nessuno	-	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. e), d.lgs. n. 33/2013		Altri eventuali incarichi con oneri a carico della finanza pubblica e indicazione dei compensi spettanti	Nessuno	-	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 2, c. 1, punto 2, l. n. 441/1982		1) copie delle dichiarazioni dei redditi riferiti al periodo dell'incarico; 2) copia della dichiarazione dei redditi successiva al termine dell'incarico o carica, entro un mese dalla scadenza del termine di legge per la presentazione della dichiarazione (Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso)) (NB: è necessario limitare, con appositi accorgimenti) a cura dell'interessato o della amministrazione, la pubblicazione dei dati sensibili)	Nessuno	I dati sono pubblicati per i tre anni successivi dalla cessazione del mandato o dell'incarico dei soggetti, eccetto i dati relativi alla situazione patrimoniale che rimangono pubblicati sino alla cessazione. Nessun obbligo di aggiornamento	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 14, c. 1, lett. f), d.lgs. n. 33/2013 Art. 4, l. n. 441/1982		3) dichiarazione concernente le variazioni della situazione patrimoniale intervenute dopo l'ultima attestazione (Per il soggetto, il coniuge non separato e i parenti entro il secondo grado, ove gli stessi vi consentano (NB: dando eventualmente evidenza del mancato consenso))	Nessuno (va presentata una sola volta entro 3 mesi dalla cessazione dell'incarico).		Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
	Sanzioni per mancata comunicazione dei dati		Art. 47, c. 1, d.lgs. n. 33/2013	Sanzioni per mancata o incompleta comunicazione dei dati da parte dei titolari di incarichi dirigenziali	Provvedimenti sanzionatori a carico del responsabile della mancata o incompleta comunicazione dei dati di cui all'articolo 14, concernenti la situazione patrimoniale complessiva del titolare dell'incarico al momento dell'assunzione della carica, la titolarità di imprese, le partecipazioni azionarie proprie nonché tutti i compensi cui dà diritto l'assunzione della carica	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dall'adozione del provvedimento	ANAC	Ripartizione II - Enti locali, previdenza e competenze ordinamentali	Annuale Ripartizione II - Enti locali, previdenza e competenze ordinamentali
	Posizioni organizzative	Art. 1 c. 1, lett. c) LR n. 10/2014	Art. 14, c. 1-quinquies, d.lgs. n. 33/2013	Posizioni organizzative	Curricula dei titolari di posizioni organizzative redatti in conformità al vigente modello europeo	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dalla nomina o dalla variazione del dato	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
	Dotazione organica		Art. 16, c. 1, d.lgs. n. 33/2013	Conto annuale del personale	Conto annuale del personale e relative spese sostenute, nell'ambito del quale sono rappresentati i dati relativi alla dotazione organica e al personale effettivamente in servizio e al relativo costo, con indicazione della distribuzione tra le diverse qualifiche e aree professionali, con particolare riguardo al personale assegnato agli uffici di diretta collaborazione con gli organi di indirizzo politico	Annuale (art. 16, c. 1, d.lgs. n. 33/2013)	Entro 1 mese dall'invio del conto annuale	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 16, c. 2, d.lgs. n. 33/2013	Costo personale tempo indeterminato	Costo complessivo del personale a tempo indeterminato in servizio, articolato per aree professionali, con particolare riguardo al personale assegnato agli uffici di diretta collaborazione con gli organi di indirizzo politico	Annuale (art. 16, c. 2, d.lgs. n. 33/2013)	Entro 1 mese dall'invio del conto annuale	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
	Personale non a tempo indeterminato		Art. 17, c. 1, d.lgs. n. 33/2013	Personale non a tempo indeterminato (da pubblicare in tabelle)	Personale con rapporto di lavoro non a tempo indeterminato, nel complesso il personale assegnato agli uffici di diretta collaborazione con gli organi di indirizzo politico	Annuale (art. 17, c. 1, d.lgs. n. 33/2013)	Entro 1 mese dall'invio del conto annuale	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
			Art. 17, c. 2, d.lgs. n. 33/2013	Costo del personale non a tempo indeterminato (da pubblicare in tabelle)	Costo complessivo del personale con rapporto di lavoro non a tempo indeterminato, con particolare riguardo al personale assegnato agli uffici di diretta collaborazione con gli organi di indirizzo politico	Trimestrale (art. 17, c. 2, d.lgs. n. 33/2013)	Entro 15 giorni dalla trasmissione dei dati stabilita al 30 aprile - 31 luglio - 31 ottobre - 31 gennaio	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
	Tassi di assenza		Art. 16, c. 3, d.lgs. n. 33/2013	Tassi di assenza trimestrali (da pubblicare in tabelle)	Tassi di assenza del personale distinti per uffici di livello dirigenziale	Trimestrale (art. 16, c. 3, d.lgs. n. 33/2013)	entro 15 giorni dalla scadenza di ciascun trimestre	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
	Incarichi conferiti e autorizzati ai dipendenti (dirigenti e non dirigenti)		Art. 18, d.lgs. n. 33/2013 Art. 53, c. 14, d.lgs. n. 165/2001	Incarichi conferiti e autorizzati ai dipendenti (dirigenti e non dirigenti) (da pubblicare in tabelle)	Elenco degli incarichi conferiti o autorizzati a ciascun dipendente (dirigente e non dirigente), con l'indicazione dell'oggetto, della durata e del compenso spettante per ogni incarico	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dall'approvazione dell'autorizzazione	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio gestione giuridica del personale	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
	Contrattazione collettiva		Art. 21, c. 1, d.lgs. n. 33/2013 Art. 47, c. 8, d.lgs. n. 166/2001	Contrattazione collettiva	Riferimenti necessari per la consultazione dei contratti e accordi collettivi nazionali ed eventuali interpretazioni autentiche	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dalla predisposizione dell'atto	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
	Contrattazione integrativa		Art. 21, c. 2, d.lgs. n. 33/2013	Contratti integrativi	Contratti integrativi stipulati, con la relazione tecnico-finanziaria e quella illustrativa, certificate dagli organi di controllo (collegio dei revisori dei conti, collegio sindacale, uffici centrali di bilancio o analoghi organi previsti dai rispettivi ordinamenti)	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dalla predisposizione dell'atto	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
			Art. 21, c. 2, d.lgs. n. 33/2013 Art. 55, c. 4, d.lgs. n. 150/2009	Costi contratti integrativi	Specifiche informazioni sui costi della contrattazione integrativa, certificate dagli organi di controllo interno, trasmesse al Ministero dell'Economia e delle finanze, che predispone, allo scopo, uno specifico modello di rilevazione, d'intesa con la Corte dei conti e con la Presidenza del Consiglio dei Ministri - Dipartimento della funzione pubblica	Annuale (art. 55, c. 4, d.lgs. n. 150/2009)	Entro 20 giorni dalla predisposizione dell'atto	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
	OVV		Art. 10, c. 8, lett. c), d.lgs. n. 33/2013	OVV (equiparato al nucleo di valutazione)	Nominativi	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 15 gg. dall'approvazione della delibera	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 10, c. 8, lett. c), d.lgs. n. 33/2013	(da pubblicare in tabelle)	Curricula	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 15 gg. dall'approvazione della delibera	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Par. 14.2, delib. CIVIT n. 12/2013		Compensi	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 15 gg. dall'approvazione della delibera	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
Bandi di concorso			Art. 19, d.lgs. n. 33/2013	Bandi di concorso (da pubblicare in tabelle)	Bandi di concorso per il reclutamento, a qualsiasi titolo, di personale presso l'amministrazione nonché i criteri di valutazione della Commissione, le tracce delle prove scritte e le graduatorie finali, aggiornate con l'eventuale scorrimento degli idonei non vincitori	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 5 giorni dall'approvazione	Segreteria generale – Ufficio gestione giuridica del personale	Segreteria generale – Ufficio gestione giuridica del personale	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio gestione giuridica del personale
Performance	Sistema di misurazione e valutazione della Performance	L'articolo non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10	Par. 1, delib. CIVIT n. 104/2010	Sistema di misurazione e valutazione della Performance	Sistema di misurazione e valutazione della Performance (art. 7, d.lgs. n. 150/2009)	Tempestivo				
	Piano della Performance	Applicazione parziale ai sensi dell'art. 1, c. 1, lett. f), L.R. n. 10/2014	Art. 10, c. 8, lett. b), d.lgs. n. 33/2013 L.R. 21/7/2000, n. 3 e s.m. art. 1	(Piano della performance) Piano degli obiettivi	(Piano della Performance (art. 10, d.lgs. 150/2009)) Piano degli obiettivi (Deliberazione giunta regionale n. 93 7/5/2014)	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dall'approvazione	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
	Relazione sulla Performance	L'articolo non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10		Relazione sulla Performance	Relazione sulla Performance (art. 10, d.lgs. 150/2009)	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
	Ammontare complessivo dei premi	Applicazione parziale ai sensi dell'art. 1, c. 1, lett. f), L.R. n. 10/2014	Art. 20, c. 1, d.lgs. n. 33/2013	Ammontare complessivo dei premi (da pubblicare in tabelle)	Ammontare complessivo dei premi collegati al merito	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 1 mese dall'invio del conto annuale	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
					Ammontare dei premi effettivamente distribuiti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
	Dati relativi ai premi	Applicazione parziale ai sensi dell'art. 1, c. 1, lett. f), L.R. n. 10/2014	Art. 20, c. 2, d.lgs. n. 33/2013	Dati relativi ai premi (da pubblicare in tabelle)	Entità del premio mediamente conseguibile dal personale dirigenziale e non dirigenziale	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dalla deliberazione in ordine ai premi	Segreteria generale – Ufficio gestione economica del personale	Segreteria generale – Ufficio sviluppo del personale e servizio ispettivo	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio sviluppo e servizio ispettivo
					Distribuzione del trattamento accessorio, in forma aggregata, al fine di dare conto del livello di selettività utilizzato nella distribuzione dei premi e degli incentivi	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *											
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile	
					Grado di differenziazione dell'utilizzo della premialità sia per i dirigenti sia per i dipendenti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)					
Enti controllati	Enti pubblici vigilati		Art. 22, c. 1, lett. a), d.lgs. n. 33/2013	Enti pubblici vigilati (da pubblicare in tabelle)	Elenco degli enti pubblici, comunque denominati, istituti, vigilati e finanziati dall'amministrazione ovvero per i quali l'amministrazione abbia il potere di nomina degli amministratori dell'ente, con l'indicazione delle funzioni attribuite e delle attività svolte in favore dell'amministrazione o delle attività di servizio pubblico affidate	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)	Entro luglio	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					Per ciascuno degli enti:						
			Art. 22, c. 2, d.lgs. n. 33/2013		1) ragione sociale	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					2) misura dell'eventuale partecipazione dell'amministrazione	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					3) durata dell'impegno	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					4) onere complessivo a qualsiasi titolo gravante per l'anno sul bilancio dell'amministrazione	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					5) numero dei rappresentanti dell'amministrazione negli organi di governo e trattamento economico complessivo a ciascuno di essi spettante (con l'esclusione dei rimborsi per vitto e alloggio)	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					6) risultati di bilancio degli ultimi tre esercizi finanziari	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					7) incarichi di amministratore dell'ente e relativo trattamento economico complessivo (con l'esclusione dei rimborsi per vitto e alloggio)	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
			Art. 20, c. 3, d.lgs. n. 39/2013		Dichiarazione sulla insussistenza di una delle cause di inconferibilità dell'incarico (link al sito dell'ente)	Tempestivo (art. 20, c. 1, d.lgs. n. 39/2013)	entro 30 giorni dal conferimento	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
			Art. 20, c. 3, d.lgs. n. 39/2013		Dichiarazione sulla insussistenza di una delle cause di incompatibilità al conferimento dell'incarico (link al sito dell'ente)	Annuale (art. 20, c. 2, d.lgs. n. 39/2013)	Entro marzo	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
			Art. 22, c. 3, d.lgs. n. 33/2013		Collegamento con i siti istituzionali degli enti pubblici vigilati	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)	Entro luglio	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
Società partecipate	Società partecipate		Art. 22, c. 1, lett. b), d.lgs. n. 33/2013	Dati società partecipate (da pubblicare in tabelle)	Elenco delle società di cui l'amministrazione detiene direttamente quote di partecipazione anche minoritaria, con l'indicazione dell'entità, delle funzioni attribuite e delle attività svolte in favore dell'amministrazione o delle attività di servizio pubblico affidate, ad esclusione delle società partecipate da amministrazioni pubbliche, con azioni quotate in mercati regolamentati italiani o di altri paesi dell'Unione europea, e loro controllate. (art. 22, c. 6, d.lgs. n. 33/2013)	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)	Entro luglio	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					Per ciascuna delle società:						
			Art. 22, c. 2, d.lgs. n. 33/2013		1) ragione sociale	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					2) misura dell'eventuale partecipazione dell'amministrazione	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					3) durata dell'impegno	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					4) onere complessivo a qualsiasi titolo gravante per l'anno sul bilancio dell'amministrazione	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
					5) numero dei rappresentanti dell'amministrazione negli organi di governo e trattamento economico complessivo a ciascuno di essi spettante	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *																
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile						
			Art. 20, c. 3, d.lgs. n. 39/2013		6) risultati di bilancio degli ultimi tre esercizi finanziari	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali						
					7) incarichi di amministratore della società e relativo trattamento economico complessivo	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali						
					Dichiarazione sulla insussistenza di una delle cause di inconferibilità dell'incarico (<u>link al sito dell'ente</u>)	Tempestivo (art. 20, c. 1, d.lgs. n. 39/2013)	entro 30 giorni dal conferimento	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali						
					Dichiarazione sulla insussistenza di una delle cause di incompatibilità al conferimento dell'incarico (<u>link al sito dell'ente</u>)	Annuale (art. 20, c. 2, d.lgs. n. 39/2013)	Entro marzo	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali						
					Collegamento con i siti istituzionali delle società partecipate	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)	entro luglio	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali						
					Provvedimenti in materia di costituzione di società a partecipazione pubblica, acquisto di partecipazioni in società già costituite, gestione delle partecipazioni pubbliche, alienazione di partecipazioni sociali, quotazione di società a controllo pubblico in mercati regolamentati e razionalizzazione periodica delle partecipazioni pubbliche, previsti dal decreto legislativo adottato ai sensi dell'articolo 18 della legge 7 agosto 2015, n. 124 (art. 20 d.lgs 175/2016) e della L.R. 16/2016	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali						
			Art. 19, c. 7, d.lgs. n. 175/2016			Provvedimenti con cui le amministrazioni pubbliche sociali fissano obiettivi specifici, annuali e pluriennali, sul complesso delle spese di funzionamento, ivi comprese quelle per il personale, delle società controllate	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali					
						Provvedimenti con cui le società a controllo pubblico garantiscono il concreto perseguimento degli obiettivi specifici, annuali e pluriennali, sul complesso delle spese di funzionamento	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali					
						Enti di diritto privato controllati	Art. 22, c. 1, lett. c), d.lgs. n. 33/2013	Enti di diritto privato controllati (da pubblicare in tabelle)	Elenco degli enti di diritto privato, comunque denominati, in controllo dell'amministrazione, con indicazione delle funzioni attribuite e delle attività svolte in favore dell'amministrazione o delle attività di servizio pubblico affidate	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)	Entro luglio	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali		
							Art. 22, c. 2, d.lgs. n. 33/2013			Per ciascuno degli enti:						
										1) ragione sociale	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali	
2) misura dell'eventuale partecipazione dell'amministrazione	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali											
3) durata dell'impegno	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali											
4) onere complessivo a qualsiasi titolo gravante per l'anno sul bilancio dell'amministrazione	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali											
5) numero dei rappresentanti dell'amministrazione negli organi di governo e trattamento economico complessivo a ciascuno di essi spettante	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali											
	Art. 20, c. 3, d.lgs. n. 39/2013			6) risultati di bilancio degli ultimi tre esercizi finanziari	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali							
				7) incarichi di amministratore dell'ente e relativo trattamento economico complessivo	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali							
				Dichiarazione sulla insussistenza di una delle cause di inconferibilità dell'incarico (<u>link al sito dell'ente</u>)	Tempestivo (art. 20, c. 1, d.lgs. n. 39/2013)		Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali							
				Dichiarazione sulla insussistenza di una delle cause di incompatibilità al conferimento dell'incarico (<u>link al sito dell'ente</u>)	Annuale (art. 20, c. 2, d.lgs. n. 39/2013)	Entro marzo	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali							
				Collegamento con i siti istituzionali degli enti di diritto privato controllati	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)	Entro luglio	Segreteria generale – Ufficio affari generali	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali							

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
	Rappresentazione grafica		Art. 22, c. 1, lett. d), d.lgs. n. 33/2013	Rappresentazione grafica	Una o più rappresentazioni grafiche che evidenziano i rapporti tra l'amministrazione e gli enti pubblici vigilati, le società partecipate, gli enti di diritto privato controllati	Annuale (art. 22, c. 1, d.lgs. n. 33/2013)	Entro luglio	Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
Attività e procedimenti	Tipologie di procedimento	L'articolo non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10 L'amministrazione rende comunque disponibili dati riferiti alla propria attività	Art. 35, c. 1, lett. a), d.lgs. n. 33/2013	Tipologie di procedimento (da pubblicare in tabelle)	Per ciascuna tipologia di procedimento: 1) breve descrizione del procedimento con indicazione di tutti i riferimenti normativi utili	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. b), d.lgs. n. 33/2013		2) unità organizzative responsabili dell'istruttoria	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. c), d.lgs. n. 33/2013		3) l'ufficio del procedimento, unitamente ai recapiti telefonici e alla casella di posta elettronica istituzionale	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. c), d.lgs. n. 33/2013		4) ove diverso, l'ufficio competente all'adozione del provvedimento finale, con l'indicazione del nome del responsabile dell'ufficio unitamente ai rispettivi recapiti telefonici e alla casella di posta elettronica istituzionale	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. c), d.lgs. n. 33/2013		5) modalità con le quali gli interessati possono ottenere le informazioni relative ai procedimenti in corso che li riguardano	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. f), d.lgs. n. 33/2013		6) termine fissato in sede di disciplina normativa del procedimento per la conclusione con l'adozione di un provvedimento espresso e ogni altro termine procedimentale rilevante	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. g), d.lgs. n. 33/2013		7) procedimenti per i quali il provvedimento dell'amministrazione può essere sostituito da una dichiarazione dell'interessato ovvero il procedimento può concludersi con il silenzio-assenso dell'amministrazione	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 25, c. 1, lett. b), d.lgs. n. 33/2013		8) strumenti di tutela amministrativa e giurisdizionale, riconosciuti dalla legge in favore dell'interessato, nel corso del procedimento nei confronti del provvedimento finale ovvero nei casi di adozione del provvedimento oltre il termine predeterminato per la sua conclusione e i modi per attivarli	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. i), d.lgs. n. 33/2013		9) link di accesso al servizio on line, ove sia già disponibile in rete, o tempi previsti per la sua attivazione	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. f), d.lgs. n. 33/2013		10) modalità per l'effettuazione dei pagamenti eventualmente necessari, con i codici IBAN identificativi del conto di pagamento, ovvero di imputazione del versamento in Tesoreria, tramite i quali i soggetti versanti possono effettuare i pagamenti mediante bonifico bancario o postale, ovvero gli identificativi del conto corrente postale sul quale i soggetti versanti possono effettuare i pagamenti mediante bollettino postale, nonché i codici identificativi del pagamento da indicare obbligatoriamente per il versamento	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. m), d.lgs. n. 33/2013		11) nome del soggetto a cui è attribuito, in caso di inerzia, il potere sostitutivo, nonché modalità per attivare tale potere, con indicazione dei recapiti telefonici e delle caselle di posta elettronica istituzionale	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. d), d.lgs. n. 33/2013		Per i procedimenti ad istanza di parte: 1) atti e documenti da allegare all'istanza e modulistica necessaria, compresi i fac-simile per le autocertificazioni	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 35, c. 1, lett. d), d.lgs. n. 33/2013 e Art. 1, c. 29, L. 190/2012		2) uffici ai quali rivolgersi per informazioni, orari e modalità di accesso con indicazione degli indirizzi, recapiti telefonici e caselle di posta elettronica istituzionale a cui presentare le istanze	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
	Dichiarazioni sostitutive e acquisizione d'ufficio dei dati	L'articolo non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10	Art. 35, c. 3, d.lgs. n. 33/2013	Recapiti dell'ufficio responsabile	Recapiti telefonici e casella di posta elettronica istituzionale dell'ufficio responsabile per le attività volte a gestire, garantire e verificare la trasmissione dei dati o l'accesso diretto degli stessi da parte delle amministrazioni precedenti all'acquisizione d'ufficio dei dati e allo svolgimento dei controlli sulle dichiarazioni sostitutive	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
Provvedimenti	Provvedimenti organi indirizzo politico	Applicazione parziale ai sensi dell'art. 1, c. 1, lett. g) e h), L.R. n. 10/2014 e Pubblicazione ai sensi della L.r. 8/2012	Art. 23, c. 1, d.lgs. n. 33/2013 /Art. 1, co. 16 della l. n. 190/2012	Provvedimenti organi indirizzo politico	Elenco dei provvedimenti, con particolare riferimento ai provvedimenti finali dei procedimenti di scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta (link alla sotto-sezione "bandi di gara e contratti"); accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche.	Tempestivo	Entro 5 giorni dall'adozione e per un periodo di 5 anni decorrente dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione	Tutte le strutture	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
	Provvedimenti dirigenti amministrativi		Art. 23, c. 1, d.lgs. n. 33/2013 /Art. 1, co. 16 della l. n. 190/2012	Provvedimenti dirigenti amministrativi	Elenco dei provvedimenti, con particolare riferimento ai provvedimenti finali dei procedimenti di scelta del contraente per l'affidamento di lavori, forniture e servizi, anche con riferimento alla modalità di selezione prescelta (link alla sotto-sezione "bandi di gara e contratti"); accordi stipulati dall'amministrazione con soggetti privati o con altre amministrazioni pubbliche.	Tempestivo		Tutte le strutture	Tutte le strutture	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali e tutte le strutture
Bandi di gara e contratti										
Si rinvia ai documenti dedicati alla trasparenza nella materia dei Bandi di gara e contratti										
Sovvenzioni, contributi, sussidi, vantaggi economici	Criteri e modalità	In forza dell'articolo 1, comma 1, lett. i), della L.R. n. 10/2014, in luogo degli articoli 26 e 27 del decreto si applica l'articolo 7 della legge regionale 13 dicembre 2012, n. 8 e successive modificazioni come modificato da ultimo dal presente articolo.	Art. 26, c. 1, d.lgs. n. 33/2013	Criteri e modalità	Atti con i quali sono determinati i criteri e le modalità cui le amministrazioni devono attenersi per la concessione di sovvenzioni, contributi, sussidi ed ausili finanziari e l'attribuzione di vantaggi economici di qualunque genere a persone ed enti pubblici e privati	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dall'approvazione dell'atto o dalla pubblicazione sul Bollettino Ufficiale	Tutte le strutture che adottano fatto	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
	Atti di concessione		Art. 26, c. 2, d.lgs. n. 33/2013	Atti di concessione	Dati dei provvedimenti di concessione di sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e comunque di vantaggi economici di qualunque genere a persone ed enti pubblici e privati di importo superiore a mille euro	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)	all'atto dell'approvazione	Tutte le strutture che adottano fatto	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 27, c. 1, lett. a), d.lgs. n. 33/2013		Per ciascun atto: 1) nome dell'impresa o dell'ente e i rispettivi dati fiscali o il nome di altro soggetto beneficiario	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)	all'atto dell'approvazione	Tutte le strutture che adottano fatto	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 27, c. 1, lett. b), d.lgs. n. 33/2013		2) importo del vantaggio economico corrisposto	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)	all'atto dell'approvazione	Tutte le strutture che adottano fatto	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 27, c. 1, lett. c), d.lgs. n. 33/2013		3) norma o titolo a base dell'attribuzione	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)	all'atto dell'approvazione	Tutte le strutture che adottano fatto	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 27, c. 1, lett. d), d.lgs. n. 33/2013		4) ufficio e funzionario o dirigente responsabile del relativo procedimento amministrativo	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)	all'atto dell'approvazione	Tutte le strutture che adottano fatto	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 27, c. 1, lett. e), d.lgs. n. 33/2013		5) modalità seguita per l'individuazione del beneficiario	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)	all'atto dell'approvazione	Tutte le strutture che adottano fatto	Segreteria generale – Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale – Ufficio affari generali
			Art. 27, c. 1, lett. f), d.lgs. n. 33/2013		6) link al progetto selezionato	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)				
			Art. 27, c. 1, lett. g), d.lgs. n. 33/2013		7) link al curriculum vitae del soggetto incaricato	Tempestivo (art. 26, c. 3, d.lgs. n. 33/2013)				
			Art. 27, c. 2, d.lgs. n. 33/2013		Elenco (in formato tabellare aperto) dei soggetti beneficiari degli atti di concessione di sovvenzioni, contributi, sussidi ed ausili finanziari alle imprese e di attribuzione di vantaggi economici di qualunque genere a persone ed enti pubblici e privati di importo superiore a mille euro	Annuale (art. 27, c. 2, d.lgs. n. 33/2013)				
Bilanci	Bilancio preventivo e consuntivo	Applicazione parziale ai sensi dell'art. 1, c. 1, lett. g) e h), L.R. n. 10/2014	Art. 29, c. 1, d.lgs. n. 33/2013 /Art. 5, c. 1, d.p.c.m. 26 aprile 2011	Bilancio preventivo	Documenti e allegati del bilancio preventivo, nonché dati relativi al bilancio di previsione di ciascun anno in forma sintetica, aggregata e semplificata, anche con il ricorso a rappresentazioni grafiche) Bilancio finanziario gestionale di previsione di ciascun anno e relative variazioni. Documento tecnico di accompagnamento del bilancio di previsione e relative variazioni.	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 10 giorni dall'approvazione	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Semestrale (30 aprile-31 ottobre) Ripartizione I – Ufficio bilancio e controllo contabile
			Art. 29, c. 1-bis, d.lgs. n. 33/2013 e d.p.c.m. 29 aprile 2016		Dati relativi alle entrate e alla spesa dei bilanci preventivi in formato tabellare aperto in modo da consentire l'esportazione, il trattamento e il riutilizzo.					

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
			Art. 29, c. 1, d.lgs. n. 33/2013 Art. 5, c. 1, d.p.c.m. 26 aprile 2011	Bilancio consuntivo	(Documenti e allegati del bilancio consuntivo, nonché dati relativi al bilancio consuntivo di ciascun anno in forma sintetica, aggregata e semplificata, anche con il ricorso a rappresentazioni grafiche) Rendiconto generale di ciascun anno	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 10 giorni dall'approvazione	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Semestrale (30 aprile-31 ottobre) Ripartizione I – Ufficio bilancio e controllo contabile
			Art. 29, c. 1-bis, d.lgs. n. 33/2013 e d.p.c.m. 29 aprile 2016		Dati relativi alle entrate e alle spese dei bilanci consuntivi in formato tabellare aperto in modo da consentire l'esportazione, il trattamento e il riutilizzo.					
	Piano degli indicatori e dei risultati attesi di bilancio	L'articolo 29 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10	Art. 29, c. 2, d.lgs. n. 33/2013 Art. 19 e 22 del dlgs n. 91/2011 - Art. 18-bis del dlgs n. 118/2011	Piano degli indicatori e dei risultati attesi di bilancio	<i>(Piano degli indicatori e risultati attesi di bilancio, con l'integrazione delle risultanze osservate in termini di raggiungimento dei risultati attesi e le motivazioni degli eventuali accostamenti e gli aggiornamenti in corrispondenza di ogni nuovo esercizio di bilancio, sia tramite la specificazione di nuovi obiettivi e indicatori, sia attraverso l'aggiornamento dei valori obiettivo e la soppressione di obiettivi già raggiunti oppure di oggetti di ripianificazione)</i> Piano degli indicatori e risultati attesi di bilancio	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 10 giorni dall'approvazione	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Semestrale (30 aprile-31 ottobre) Ripartizione I – Ufficio bilancio e controllo contabile
Beni immobili e gestione patrimonio	Patrimonio immobiliare		Art. 30, d.lgs. n. 33/2013	Patrimonio immobiliare	Informazioni identificative degli immobili posseduti e detenuti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Ripartizione IV Risorse strumentali - Ufficio patrimonio	Ripartizione IV Risorse strumentali - Ufficio patrimonio	Semestrale (30 aprile-31 ottobre) Ripartizione IV – Risorse strumentali - Ufficio patrimonio
	Canoni di locazione o affitto		Art. 30, d.lgs. n. 33/2013	Canoni di locazione o affitto	Canoni di locazione o di affitto versati o percepiti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)		Ripartizione IV Risorse strumentali - Ufficio patrimonio	Ripartizione IV Risorse strumentali - Ufficio patrimonio	Semestrale (30 aprile-31 ottobre) Ripartizione IV – Risorse strumentali - Ufficio patrimonio
Controlli e rilievi sull'amministrazione	Organismi indipendenti di valutazione, nuclei di valutazione o altri organismi con funzioni analoghe		Art. 31, d.lgs. n. 33/2013	Atti degli Organismi indipendenti di valutazione, nuclei di valutazione o altri organismi con funzioni analoghe	Attestazione dell'OIV o di altra struttura analoga nell'assolvimento degli obblighi di pubblicazione	Annuale e in relazione a delibere A.N.AC.	Entro 20 giorni dal ricevimento dell'atto	Organismo indipendente di valutazione, Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
					Documento dell'OIV di validazione della Relazione sulla Performance (art. 14, c. 4, lett. c), d.lgs. n. 150/2009)					
					Relazione dell'OIV sul funzionamento complessivo del Sistema di valutazione, trasparenza e integrità dei controlli interni (art. 14, c. 4, lett. a), d.lgs. n. 150/2009)					
					Altri atti degli organismi indipendenti di valutazione, nuclei di valutazione o altri organismi con funzioni analoghe, procedendo all'indicazione in forma anonima dei dati personali eventualmente presenti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dal ricevimento dell'atto	Organismo indipendente di valutazione, Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
	Organi di revisione amministrativa e contabile	Corte dei conti		Rilievi Corte dei conti	Relazioni degli organi di revisione amministrativa e contabile al bilancio di previsione o budget, alle relative variazioni e al conto consuntivo o bilancio di esercizio	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dal ricevimento dell'atto	Ripartizione I - Risorse finanziarie	Ripartizione I - Risorse finanziarie	Semestrale (30 aprile-31 ottobre) Ripartizione I - Risorse finanziarie
					Tutti i rilievi della Corte dei conti ancorchè non recupri riguardanti l'organizzazione e l'attività delle amministrazioni stesse e dei loro uffici	Tempestivo (ex art. 8, d.lgs. n. 33/2013)	Entro 20 giorni dal ricevimento dell'atto	Segreteria generale - Ufficio affari generali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
Servizi erogati	Carta dei servizi e standard di qualità	L'articolo 32 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10 L'amministrazione rende comunque disponibili dati riferiti alla propria attività	Art. 32, c. 1, d.lgs. n. 33/2013	Carta dei servizi e standard di qualità	Carta dei servizi o documento contenente gli standard di qualità dei servizi pubblici	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
	Class action		Art. 1, c. 2, d.lgs. n. 198/2009	Class action	Notizia del ricorso in giudizio proposto dai titolari di interessi giuridicamente rilevanti ed omogenei nei confronti delle amministrazioni e dei concessionari di servizio pubblico al fine di ripristinare il corretto svolgimento della funzione o la corretta erogazione di un servizio	Tempestivo	Entro 15 dall'avvenuta notifica	Tutte le strutture	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
			Art. 4, c. 2, d.lgs. n. 198/2009		Sentenza di definizione del giudizio	Tempestivo	Entro 15 giorni dalla sentenza	Tutte le strutture	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
			Art. 4, c. 6, d.lgs. n. 198/2009		Misure adottate in ottemperanza alla sentenza	Tempestivo	Entro 15 giorni dall'adozione delle misure	Tutte le strutture	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
	Costi contabilizzati	L'articolo 32 e l'articolo 41 del D.Lgs. 33/2013 non trova applicazione ai sensi della LR n. 10/2014	Art. 32, c. 2, lett. a), d.lgs. n. 33/2013 Art. 10, c. 5, d.lgs. n. 33/2013	Costi contabilizzati (da pubblicare in tabelle)	Costi contabilizzati dei servizi erogati agli utenti, sia finali che intermedi e il relativo andamento nel tempo	Annuale (art. 10, c. 5, d.lgs. n. 33/2013)				
	Liste di attesa	L'articolo 32 e l'articolo 41 del D.Lgs. 33/2013 non trova applicazione ai sensi della LR n. 10/2015	Art. 41, c. 6, d.lgs. n. 33/2013	Liste di attesa (obbligo di pubblicazione a carico di enti, aziende e strutture pubbliche e private che erogano prestazioni per conto del servizio sanitario) (da pubblicare in tabelle)	Criteri di formazione delle liste di attesa, tempi di attesa previsti e tempi medi effettivi di attesa per ciascuna tipologia di prestazione erogata	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
	Servizi in rete		Art. 7 co. 3 d.lgs. 82/2005	Risultati delle indagini sulla soddisfazione da parte degli utenti rispetto alla qualità dei servizi in rete e statistiche di utilizzo dei servizi in rete	Risultati delle rilevazioni sulla soddisfazione da parte degli utenti rispetto alla qualità dei servizi in rete resi all'utente, anche in termini di fruibilità, accessibilità e tempestività, statistiche di utilizzo dei servizi in rete.	Tempestivo		Ripartizione IV Risorse strumentali	Segreteria generale - Ufficio affari generali	Semestrale (30 aprile-31 ottobre) Segreteria generale - Ufficio affari generali
	Dati sui pagamenti		Art. 4-bis, c. 2, d.lgs. n. 33/2013	Dati sui pagamenti (da pubblicare in tabelle)	Dati sui propri pagamenti in relazione alla tipologia di spesa sostenuta, all'ambito temporale di riferimento e ai beneficiari	Trimestrale	15 aprile / 15 luglio / 15 ottobre / 15 gennaio	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile	Semestrale (30 aprile-31 ottobre) Ripartizione I Risorse finanziarie - Ufficio bilancio e controllo contabile
	Dati sui pagamenti del servizio sanitario nazionale		Art. 41, c. 1-bis, d.lgs. n. 33/2013	Dati sui pagamenti in forma sintetica e aggregata (da pubblicare in tabelle)	Dati relativi a tutte le spese e a tutti i pagamenti effettuati, distinti per tipologia di lavoro, bene o servizio in relazione alla tipologia di spesa sostenuta, all'ambito temporale di riferimento e ai beneficiari					
	Indicatore di tempestività dei pagamenti		Art. 33, d.lgs. n. 33/2013	Indicatore di tempestività dei pagamenti	Indicatore dei tempi medi di pagamento relativi agli acquisti di beni, servizi, prestazioni professionali e forniture (indicatore annuale di tempestività dei pagamenti)	Annuale (art. 33, c. 1, d.lgs. n. 33/2013)	entro il 31 marzo	Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria	Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria	Semestrale (30 aprile-31 ottobre) Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria
					Indicatore trimestrale di tempestività dei pagamenti	Trimestrale (art. 33, c. 1, d.lgs. n. 33/2013)	entro 15 giorni dalla scadenza di ciascun trimestre	Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria	Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria	Semestrale (30 aprile-31 ottobre) Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria
				Ammontare complessivo dei debiti	Ammontare complessivo dei debiti e il numero delle imprese creditrici	Annuale (art. 33, c. 1, d.lgs. n. 33/2013)	entro 15 giorni dall'elaborazione delle informazioni	Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria	Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria	Semestrale (30 aprile-31 ottobre) Ripartizione I Risorse finanziarie - Ufficio programmazione finanziaria
	IBAN e pagamenti informatici	L'articolo 36 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10. L'amministrazione rende comunque disponibili le informazioni	Art. 36, d.lgs. n. 33/2013 Art. 5, c. 1, d.lgs. n. 82/2005	IBAN e pagamenti informatici	Nelle richieste di pagamento: i codici IBAN identificativi del conto di pagamento, ovvero di imputazione del versamento in Tesoreria, tramite i quali i soggetti versanti possono effettuare i pagamenti mediante bonifico bancario o postale, ovvero gli identificativi del conto corrente postale sul quale i soggetti versanti possono effettuare i pagamenti mediante bollettino postale, nonché i codici identificativi del pagamento da indicare obbligatoriamente per il versamento					
Opere pubbliche	Nuclei di valutazione e verifica degli investimenti pubblici	L'articolo 38 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10.	Art. 38, c. 1, d.lgs. n. 33/2013	Informazioni relative ai nuclei di valutazione e verifica degli investimenti pubblici (art. 1, l. n. 144/1999)	Informazioni relative ai nuclei di valutazione e verifica degli investimenti pubblici, incluse le funzioni e i compiti specifici ad essi attribuiti, le procedure e i criteri di individuazione dei componenti e i loro nominativi (obbligo previsto per le amministrazioni centrali e regionali)	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
	Atti di programmazione delle opere pubbliche		Art. 38, c. 2 e 2-bis d.lgs. n. 33/2013 Art. 21 co.7 d.lgs. n. 50/2016 Art. 29 d.lgs. n. 50/2016	Atti di programmazione delle opere pubbliche	Atti di programmazione delle opere pubbliche (link alla sotto-sezione "bandi di gara e contratti"). A titolo esemplificativo: - Programma triennale dei lavori pubblici, nonché i relativi aggiornamenti annuali, ai sensi art. 21 d.lgs. n. 50/2016 - Documento pluriennale di pianificazione ai sensi dell'art. 2 del d.lgs. n. 228/2011, (per i Ministeri)	Tempestivo (art.8, c. 1, d.lgs. n. 33/2013)				

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
	Tempi costi e indicatori di realizzazione delle opere pubbliche		Art. 38, c. 2, d.lgs. n. 33/2013	Tempi, costi unitari e indicatori di realizzazione delle opere pubbliche in corso o completate.	Informazioni relative ai tempi e agli indicatori di realizzazione delle opere pubbliche in corso o completate	Tempestivo (art. 38, c. 1, d.lgs. n. 33/2013)				
			Art. 38, c. 2, d.lgs. n. 33/2013	(da pubblicare in tabelle, sulla base dello schema tipo redatto dal Ministero dell'economia e della finanza d'intesa con l'Autorità nazionale anticorruzione)	Informazioni relative ai costi unitari di realizzazione delle opere pubbliche in corso o completate	Tempestivo (art. 38, c. 1, d.lgs. n. 33/2013)				
Pianificazione e governo del territorio		L'articolo 39 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10. Ai sensi dell'art. 8 dello Statuto la materia è di competenza delle Province autonome di Trento e di Bolzano	Art. 39, c. 1, lett. a), d.lgs. n. 33/2013	Pianificazione e governo del territorio (da pubblicare in tabelle)	Atti di governo del territorio quali, tra gli altri, piani territoriali, piani di confinamento, piani paesistici, strumenti urbanistici, generali e di attuazione, nonché le loro varianti	Tempestivo (art. 39, c. 1, d.lgs. n. 33/2013)				
			Art. 39, c. 2, d.lgs. n. 33/2013		Documentazione relativa a ciascun procedimento di presentazione e approvazione delle proposte di trasformazione urbanistica di iniziativa privata o pubblica in variante allo strumento urbanistico generale comunque denominato vigente nonché delle proposte di trasformazione urbanistica di iniziativa privata o pubblica in attuazione dello strumento urbanistico generale vigente che comportino premialità edificatorie a fronte dell'impegno dei privati alla realizzazione di opere di urbanizzazione extra oneri o della cessione di aree o volumetrie per finalità di pubblico interesse	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
Informazioni ambientali		L'articolo 40 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10. Ai sensi dell'art. 8 dello Statuto la materia è di competenza delle Province autonome di Trento e di Bolzano	Art. 40, c. 2, d.lgs. n. 33/2013	Informazioni ambientali	Informazioni ambientali che le amministrazioni detengono ai fini delle proprie attività istituzionali:	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
				Stato dell'ambiente	1) Stato degli elementi dell'ambiente, quali l'aria, l'atmosfera, l'acqua, il suolo, il territorio, i siti naturali, compresi gli igrotopi, le zone costiere e marine, la diversità biologica ed i suoi elementi costitutivi, compresi gli organismi geneticamente modificati, e, inoltre, le interazioni tra questi elementi	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
				Fattori inquinanti	2) Fattori quali le sostanze, l'energia, il rumore, le radiazioni od i rifiuti, anche quelli radioattivi, le emissioni, gli scarichi ed altri rilasci, nell'ambiente, che incidono o possono incidere sugli elementi dell'ambiente	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
				Misure incidenti sull'ambiente e relative analisi di impatto	3) Misure, anche amministrative, quali le politiche, le disposizioni legislative, i piani, i programmi, gli accordi ambientali e ogni altro atto, anche di natura amministrativa, nonché le attività che incidono o possono incidere sugli elementi e sui fattori dell'ambiente ed analisi costi-benefici ed altre analisi ed ipotesi economiche usate nell'ambito delle stesse	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
				Misure a protezione dell'ambiente e relative analisi di impatto	4) Misure o attività finalizzate a proteggere i suddetti elementi ed analisi costi-benefici ed altre analisi ed ipotesi economiche usate nell'ambito delle stesse	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
				Relazioni sull'attuazione della legislazione	5) Relazioni sull'attuazione della legislazione ambientale	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
				Stato della salute e della sicurezza umana	6) Stato della salute e della sicurezza umana, compresa la contaminazione della catena alimentare, le condizioni della vita umana, il paesaggio, i siti e gli edifici d'interesse culturale, per quanto influenzabili dallo stato degli elementi dell'ambiente, attraverso tali elementi, da qualsiasi fattore	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
				Relazione sullo stato dell'ambiente del Ministero dell'Ambiente e della tutela del territorio	Relazione sullo stato dell'ambiente redatta dal Ministero dell'Ambiente e della tutela del territorio	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				

SEZIONE "AMMINISTRAZIONE TRASPARENTE" - ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE *										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
Strutture sanitarie private accreditate		L'articolo 41 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10. Ai sensi dell'art. 8 dello Statuto la materia è di competenza delle Province autonome di Trento e di Bolzano	Art. 41, c. 4, d.lgs. n. 33/2013	Strutture sanitarie private accreditate	Elenco delle strutture sanitarie private accreditate	Annuale (art. 41, c. 4, d.lgs. n. 33/2013)				
				(da pubblicare in tabelle)	Accordi intercorsi con le strutture private accreditate	Annuale (art. 41, c. 4, d.lgs. n. 33/2013)				
Interventi straordinari e di emergenza		L'articolo 42 del D.Lgs. 33/2013 non trova applicazione ai sensi della legge regionale 29/10/2014, n. 10.	Art. 42, c. 1, lett. a), d.lgs. n. 33/2013	Interventi straordinari e di emergenza (da pubblicare in tabelle)	Provvedimenti adottati concernenti gli interventi straordinari e di emergenza che comportano deroghe alla legislazione vigente, con indicazione esplicita delle norme di legge eventualmente derogate e dei motivi della deroga, nonché con indicazione di eventuali atti amministrativi o giurisdizionali intervenuti	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
					Termini temporali eventualmente fissati per l'esercizio dei poteri di adozione dei provvedimenti straordinari	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
			Art. 42, c. 1, lett. c), d.lgs. n. 33/2013		Costo previsto degli interventi e costo effettivo sostenuto dall'amministrazione	Tempestivo (ex art. 8, d.lgs. n. 33/2013)				
Altri contenuti	Prevenzione della Corruzione	Applicazione parziale ai sensi dell'art. 1, c. 1, lett. b), L.R. n. 10/2014		Piano triennale per la prevenzione della corruzione e della trasparenza	Piano triennale per la prevenzione della corruzione e della trasparenza e suoi allegati, le misure integrative di prevenzione della corruzione individuate ai sensi dell'articolo 1, comma 2-bis della legge n. 190 del 2012, (MOG 231)	Annuale	entro 10 giorni dall'approvazione del provvedimento	Responsabile della Prevenzione della corruzione e della trasparenza	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Responsabile della Prevenzione della corruzione e della trasparenza
			Art. 43, c. 1, d.lgs. n. 33/2013	Responsabile della prevenzione della corruzione e della trasparenza	Responsabile della prevenzione della corruzione e della trasparenza	Tempestivo	entro 10 giorni dall'approvazione del provvedimento	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali
				Regolamenti per la prevenzione e la repressione della corruzione e dell'illegalità	Regolamenti per la prevenzione e la repressione della corruzione e dell'illegalità (laddove adottati)	Tempestivo	entro 10 giorni dall'approvazione del provvedimento	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali
			Art. 1, c. 14, l. n. 190/2012	Riduzione del Responsabile della prevenzione della corruzione e della trasparenza	Riduzione del Responsabile della prevenzione della corruzione recante i risultati dell'attività svolta (entro il 15 dicembre di ogni anno)	Annuale (ex art. 1, c. 14, l. n. 190/2012)	Entro 10 giorni dall'adozione	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali
			Art. 1, c. 3, l. n. 190/2012	Provvedimenti adottati dall'A.N.AC. ed atti di adeguamento a tali provvedimenti	Provvedimenti adottati dall'A.N.AC. ed atti di adeguamento a tali provvedimenti in materia di vigilanza e controllo sull'anticorruzione	Tempestivo	Entro 10 giorni dall'adozione	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali
			Art. 18, c. 5, d.lgs. n. 39/2013	Atti di accertamento delle violazioni	Atti di accertamento delle violazioni delle disposizioni di cui al d.lgs. n. 39/2013	Tempestivo	Entro 10 giorni dalla ricezione dell'atto	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali
Altri contenuti	Accesso civico	Applicazione parziale ai sensi dell'art. 1, c. 1, lett. b), L.R. n. 10/2014	Art. 5, c. 1, d.lgs. n. 33/2013	Accesso civico "semplice" concernente dati, documenti e informazioni soggetti a pubblicazione obbligatoria	Nome del Responsabile della prevenzione della corruzione e della trasparenza cui è presentata la richiesta di accesso civico, nonché modalità per l'esercizio di tale diritto, con indicazione dei recapiti telefonici e delle caselle di posta elettronica istituzionale	Tempestivo	all'atto della variazione della ricezione dell'atto	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali
			Art. 5, c. 2 e comma 7, d.lgs. n. 33/2013	Accesso civico "generalizzato" concernente dati e documenti ulteriori, e relativo riesame	Nomi Uffici competenti cui presentare la richiesta di accesso civico, nonché modalità per l'esercizio di tale diritto, e relativo riesame, con indicazione dei recapiti telefonici e delle caselle di posta elettronica istituzionale	Tempestivo	all'atto della variazione	Tutte le strutture	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali
			Linee guida Anac FOIA (del. 13/09/2016)	Registro degli accessi	Elenco delle richieste di accesso (atti, civico e generalizzato) con indicazione dell'oggetto e della data della richiesta nonché del relativo esito con la data della decisione	Semestrale	entro 30 giorni dalla scadenza di ciascun semestre	Tutte le strutture	Ripartizione II - Enti locali, prevenzione e competenze ordinamentali	Annuale Ripartizione II - Enti locali, prevenzione e competenze ordinamentali

Note
Gli adempimenti evidenziati in grigio non si applicano alla Regione autonoma Trentino-Alto Adige/Südtirol.

ALLEGATO 9 AL P.M.A. 2022 ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE DELLA SEZIONE "AMMINISTRAZIONE TRASPARENTE" SOTTO SEZIONE 1 "LIVELLO" - BANDI DI GARA E CONTRATTI										
Contratti con bandi e avvisi pubblicati prima o dopo il 1° luglio 2023 ed esecuzione conclusa entro il 31 dicembre 2023										
Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
	LA Regione applica in materia di appalti la disciplina provinciale ai sensi dell'art. 2 della legge regionale n. 2 del 2009 e s.m. La pubblicazione avviene tramite link alla banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del comma 3 disposto dall'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4 bis della legge provinciale di Trento n. 2 del 2016.		Art. 1, c. 32, l. n. 190/2012 Art. 37, c. 1, lett. a) d.lgs. n. 33/2013; Art. 4 del d. Anac n. 39/2016	Dati previsti dall'articolo 1, comma 35, della legge 9 novembre 2012, n. 195: informazioni sulle singole procedure	Codice Identificativo Gara (CIG)/SmartCIG, struttura proponente, oggetto del bando, procedura di scelta del contraente, elenco degli operatori invitati a presentare offerte/numero di offerenti che hanno partecipato al procedimento, aggiudicatario, importo di aggiudicazione, tempi di completamento dell'opera servizio o fornitura, importo delle somme liquidate	Tempestivo	all'atto dell'indizione della procedura	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			Art. 1, c. 32, l. n. 190/2012 Art. 37, c. 1, lett. a) d.lgs. n. 33/2013; Art. 4 del d. Anac n. 39/2016	(da pubblicare secondo le "Specifiche tecniche per la pubblicazione dei dati ai sensi dell'art. 1, comma 35, della Legge n. 19/2012", adottate secondo quanto indicato nella delle Anac 39/2016)	Tabelle riassuntive rese liberamente scaricabili in un formato digitale standard aperto con informazioni sui contratti relative all'anno precedente (nello specifico: Codice Identificativo Gara (CIG)/SmartCIG, struttura proponente, oggetto del bando, procedura di scelta del contraente, elenco degli operatori invitati a presentare offerte/numero di offerenti che hanno partecipato al procedimento, aggiudicatario, importo di aggiudicazione, tempi di completamento dell'opera servizio o fornitura, importo delle somme liquidate)	Annuale (art. 1, c. 32, l. n. 190/2012)		norma abrogata dal d.lgs. n. 96/2023 (comunicato ANAC del 05.01.2024)		
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013; Art. 21, c. 7, e 29, c. 1, d.lgs. n. 50/2016; D.M. MIT 14/2018, art. 5, comma 4 e 10 e art. 7, comma 4 e 10	Atti relativi alla programmazione di lavori, opere, servizi e forniture	Programma biennale degli acquisti di beni e servizi, programma triennale dei lavori pubblici e relativi aggiornamenti annuali Comunicazione della mancata redazione del programma triennale dei lavori pubblici per assenza di lavori o comunicazione della mancata redazione del programma biennale degli acquisti di beni e servizi per assenza di acquisti (D.M. MIT 14/2018, art. 5, co. 8 e art. 7, co. 4) Modifiche al programma triennale dei lavori pubblici e al programma biennale degli acquisti di beni e servizi (D.M. MIT 14/2018, art. 5, co. 10 e art. 7, co. 10)	Tempestivo	Entro 20 giorni dall'approvazione	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato
				Atti relativi alle procedure per l'affidamento di appalti pubblici di servizi, forniture, lavori e opere, di concorsi pubblici di progettazione, di concorsi di idee e di concessioni, compresi quelli tra enti nell'ambito del settore pubblico di cui all'art. 5 del d.lgs. n. 50/2016 I dati di devono riferire a ciascuna procedura contrattuale in modo da avere una rappresentazione separata di ognuna di esse, dai primi atti alla fase di esecuzione						
Bandi di gara e contratti	LA Regione applica in materia di appalti la disciplina provinciale ai sensi dell'art. 2 della legge regionale n. 2 del 2009 e s.m. La pubblicazione avviene tramite link alla banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del comma 3 disposto dall'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4 bis della legge provinciale di Trento n. 2 del 2016.		Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016; DPCM n. 76/2018	Trasparenza nella partecipazione di portatori di interessi e dibattito pubblico	Progetti di fattibilità relativi alle grandi opere infrastrutturali e di architettura di rilevanza sociale, aventi impatto sull'ambiente, sulle città e sull'assetto del territorio, nonché gli atti della consultazione pubblica, comprensivi dei resoconti degli incontri e dei dibattiti con i portatori di interesse. I contratti e i resoconti sono pubblicati, con pari evidenza, unitamente ai documenti predisposti dall'amministrazione e relativi agli stessi lavori (art. 22, c. 1) Informazioni previste dal D.P.C.M. n. 76/2018 "Regolamento recante modalità di svolgimento, tipologie e soglie dimensionali delle opere sottoposte a dibattito pubblico"	Tempestivo	all'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Avvisi di preinformazione	SETTORI ORDINARI Avvisi di preinformazione per i settori ordinari di cui all'art. 70, co. 1, d.lgs. 50/2016 SETTORI SPECIALI Avvisi periodici indicativi per i settori speciali e di cui all'art. 127, co. 2, d.lgs. 50/2016	Tempestivo	all'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Delibera a contrarre	Delibera a contrarre o atto equivalente	Tempestivo	all'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Avvisi e bandi	SETTORI ORDINARI-SOTTOSOGGLIA Avvisi di indaggi di mercato (art. 36 c. 2 e Linea guida ANAC n. 4) Bandi ed avvisi (art. 36 c. 3) Avvisi di costituzione elenco operatori economici e pubblicazione elenco (art. 36 c. 7 e Linea guida ANAC) Determina a contrarre ex art. 36 c. 2, con riferimento alle ipotesi ex art. 36, c. 2, lettere a) e b) SETTORI ORDINARI-SOPRASOGGLIA Avvisi di preinformazione per l'indizione di una gara per procedure ristrette e procedure competitive con negoziazione (amministrazioni subcentrali) (art. 76, c. 3 e 9) Bandi ed avvisi (art. 73, c. 1 e 4) Bandi di gara o avvisi di preinformazione per appalti di servizi di cui all'allegato IX (art. 142, c. 1) Bandi di concorso per concorsi di progettazione (art. 153) Bando per i concorsi a fasi (art. 156) SETTORI SPECIALI Bando e avvisi (art. 127, c. 1) Per procedure ristrette e negoziate: Avviso periodico indicativo (art. 127, c. 3) Avviso sull'esistenza di un sistema di qualificazione (art. 128, c. 1) Bando di gara e avvisi (art. 129, c. 1)	Tempestivo	all'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			Art. 48, c. 3, d.l. 77/2021	Procedure negoziate: offerenti agli investimenti pubblici finanziati, in tutto o in parte, con le risorse previste dal PNRR e dal PNIC e dai programmi cofinanziati dai fondi strutturali dell'Unione Europea	Evidenza dell'avvio delle procedure negoziate (art. 63 e art.125) ove la S.A. vi ricorrano quando, per ragioni di estrema urgenza derivanti da circostanze imprevedibili, non immediatamente sanabili, l'applicazione dei termini, anche alternativi, previsti dalla procedura ordinaria può compromettere la realizzazione degli obiettivi o il rispetto dei tempi di attuazione di cui al PNRR nonché al PNIC e ai programmi cofinanziati dai fondi strutturali dell'Unione Europea	Tempestivo				
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Commissione giudicatrice	Composizione della commissione giudicatrice, curricula dei suoi componenti.	Tempestivo	All'atto del conferimento dell'incarico	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Avvisi relativi all'atto della procedura	SETTORI ORDINARI-SOTTOSOGGLIA Avvisi sui risultati della procedura di affidamento con l'indicazione dei soggetti invitati (art. 36, c. 2, lett. b), c), c-bis). Per le ipotesi di cui all'art. 36, c. 2, lett. b) rimane nel caso in cui è procedo ad affidamento diretto l'anno determina a contrarre ex articolo 36, c. 2 Pubblicazione finalizzata dell'avviso di aggiudicazione di cui all'art. 36, co. 2, lett. a) rimane nel caso in cui il procedo di sensi dell'art. 32, co. 2 SETTORI ORDINARI-SOPRASOGGLIA Avvisi di appalto aggiudicato (art. 36) Avvisi di aggiudicazione degli appalti di servizi di cui all'allegato IX eventualmente raggruppati su base trimestrale (art. 142, c. 3) Avvisi sui risultati del concorso di progettazione (art. 153, c. 2) SETTORI SPECIALI Avvisi relativi agli appalti aggiudicati (art. 129, c. 2 e art. 130) Avvisi di aggiudicazione degli appalti di servizi sociali e di altri servizi specifici eventualmente raggruppati su base trimestrale (art. 140, c. 3) Avvisi sui risultati del concorso di progettazione (art. 141, c. 2)	Tempestivo	all'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			d.l. 76, art. 1, co. 2, lett. b) (applicabile temporaneamente)	Avviso sui risultati della procedura di affidamento diretto (ove la determina a contrarre o atto equivalente sia adottato entro il 30.6.2023)	Per gli affidamenti diretti per lavori di importo inferiore a 150.000 euro e per servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo inferiore a 130.000 euro; pubblicazione dell'avviso sui risultati della procedura di affidamento con l'indicazione dei soggetti invitati (non obbligatorio per affidamenti inferiori ad euro 40.000)	Tempestivo	all'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			d.l. 76, art. 1, co. 1, lett. b) (applicabile temporaneamente)	Avviso di avvio della procedura e avviso sui risultati della aggiudicazione di procedure negoziate senza bando (ove la determina a contrarre o atto equivalente sia adottato entro il 30.6.2023)	Per l'affidamento di servizi e forniture, ivi compresi i servizi di ingegneria e architettura e l'attività di progettazione, di importo pari o superiore a 139.000 euro e fino alle soglie comunitarie e di lavori di importo pari o superiore a 150.000 euro e inferiore a un milione di euro; pubblicazione di un avviso che evidenzia l'avvio della procedura negoziata e di un avviso sui risultati della procedura di affidamento con l'indicazione dei soggetti invitati	Tempestivo	all'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza

Denominazione sotto-sezione livello 1 (Macrofamiglie)	Denominazione sotto-sezione 2 livello (Tipologie di dati)	Note	Riferimento normativo	Denominazione del singolo obbligo	Contenuti dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile				
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Verbal delle commissioni di gara	Verbal delle commissioni di gara (fatte salve le esigenze di riservatezza ai sensi dell'art. 53, ovvero dei documenti secretati ai sensi dell'art. 162 e nel rispetto dei limiti previsti in via generale dal d.lgs. n. 196/2003 e ss.mm.ii. in materia di dati personali).	Successivamente alla pubblicazione degli avvisi relativi agli esiti delle procedure	Affatto della pubblicazione degli avvisi	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza				
			Art. 47, c.2,3, 3, 9, d.l. 77/2021 e art. 29, co. 1, d.lgs. 50/2016	Pari opportunità e inclusione lavorativa nei contratti pubblici, nel PNRR e nel FNC	Copia dell'ultimo rapporto sulla situazione del personale maschile e femminile prodotto al momento della presentazione della domanda di partecipazione o dell'offerta da parte degli operatori economici lesisti, ai sensi dell'art. 46, del d.lgs. n. 196/2003, alla sua relazione, (operatori che occupano oltre 50 dipendenti)art. 47, c. 2, d.l. 77/2021)	Successivamente alla pubblicazione degli avvisi relativi agli esiti delle procedure								
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Contratti	Solo per gli affidamenti sopra soglia e per quelli finanziati con risorse PNRR e fondi strutturali, testo dei contratti e dei successivi accordi modificativi e/o interpretativi degli stessi (fatte salve le esigenze di riservatezza ai sensi dell'art. 53, ovvero dei documenti secretati ai sensi dell'art. 162 e nel rispetto dei limiti previsti in via generale dal d.lgs. n. 196/2003) e ss.mm.ii. in materia di dati personali).	Tempestivo	Entro 15 giorni dalla sottoscrizione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza				
			D.l. 76/2020, art. 6 Art. 29, co. 1, d.lgs. 50/2016	Collaggi consultivi tecnici	Composizione del CCT, curricula e compenso dei componenti.	Tempestivo	Affatto del conferimento dell'incarico	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza				
			Art. 47, c.2,3, 3, 9, d.l. 77/2021 e art. 29, co. 1, d.lgs. 50/2016	Pari opportunità e inclusione lavorativa nei contratti pubblici, nel PNRR e nel FNC	Relazione di genere sulla situazione del personale maschile e femminile consegnata, entro sei mesi dalla conclusione del contratto, alla S.A. dagli operatori economici che occupano un numero pari o superiore a quindici dipendenti (art. 47, c. 3, d.l. 77/2021)	Tempestivo								
			Art. 47, co. 3-bis e co. 9, d.l. 77/2021 e art. 29, co. 1, d.lgs. 50/2016		Pubblicazione da parte della S.A. della certificazione di cui all'articolo 17 della legge 12 marzo 1999, n. 68 e della relazione relativa all'assolvimento degli obblighi di cui alla medesima legge e alle eventuali sanzioni e provvedimenti disposti a carico dell'operatore economico nel termine antecedente la data di scadenza di presentazione delle offerte e consegnati alla S.A. entro sei mesi dalla conclusione del contratto (per gli operatori economici che occupano un numero pari o superiore a quindici dipendenti)	Tempestivo								
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Fase esecutiva	Fatte salve le esigenze di riservatezza ai sensi dell'art. 53, ovvero dei documenti secretati ai sensi dell'art. 162 del d.lgs. 50/2016, i provvedimenti di approvazione ed autorizzazione relativi a: - modifiche suggestive - varianti - proroghe - ritardi - quinto d'obbligo - subappalti (in caso di assenza del provvedimento di autorizzazione, pubblicazione del nominativo del subappaltatore, dell'importo e dell'oggetto del contratto di subappalto). Certificato di collaudo e regolare esecuzione Certificato di verifica conformità Accordi bonari e transazioni Atti di nomina del direttore dei lavori/direttore dell'esecuzione/componenti delle commissioni di collaudo	Tempestivo	Entro 15 giorni dall'addebi	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza				
			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Racconti della gestione finanziaria dei contratti al termine della loro esecuzione	Racconti della gestione finanziaria dei contratti al termine della loro esecuzione. Il resoconto deve contenere, per ogni singolo contratto, almeno i seguenti dati: data di inizio e conclusione dell'esecuzione, importo del contratto, importo complessivo liquidati, importo complessivo dello scadenamento, ove si sia verificato (accostamento positivo o negativo).	Annuale (entro il 31 gennaio) con riferimento agli affidamenti dell'anno precedente	Entro il 31/01	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza				
			La Regione applica in materia di discipline provinciali ai sensi dell'art. 2 della legge regionale n. 2 del 2005 e s.m. - La pubblicazione avviene tramite link alla Banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del combinato disposto dell'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4-bis della legge provinciale di Trento n. 2 del 2016.			Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Concessioni e partenariati pubblico privato	Tutti gli obblighi di pubblicazione elencati nel presente allegato sono applicabili anche ai contratti di concessione e di partenariato pubblico privato, <u>in quanto compatibili</u> , ai sensi degli artt. 29, 164, 179 del d.lgs. 50/2016. Con riferimento agli avvisi e ai bandi si richiamano inoltre: Bando di concessione, invito a presentare offerte (art. 164, c. 2, che rinvia alle disposizioni contenute nella parte I e II del d.lgs. 50/2016 anche relativamente alla modalità di pubblicazione e redazione dei bandi e degli avvisi) Nuovo invito a presentare offerte a seguito della modifica dell'ordine di importanza dei criteri di aggiudicazione (art. 173, c. 3) Nuovo bando di concessione a seguito della modifica dell'ordine di importanza dei criteri di aggiudicazione (art. 173, c. 3) Bando di gara relativo alla finanza di progetto (art. 163, c. 2) Bando di gara relativo alla locazione finanziaria di opere pubbliche e di pubblica utilità (art. 167) <u>Bando di gara relativo al contratto di disponibilità (art. 168, c. 9)</u>	Tempestivo	Affatto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza	
							Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Affidamenti diretti di lavori, servizi e forniture di somma urgenza e di protezione civile	Gli atti relativi agli affidamenti diretti di lavori, servizi e forniture di somma urgenza e di protezione civile, con specifica dell'affidatario, della modalità della scelta e delle motivazioni che non hanno consentito il ricorso alle procedure ordinarie (art. 163, c. 10)	Tempestivo	Affatto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
							Art. 37, c. 1, lett. b) d.lgs. n. 33/2013 e art. 29, c. 1, d.lgs. n. 50/2016	Affidamenti in house	Tutti gli atti connessi agli affidamenti in house in formato open data di appalti pubblici e contratti di concessione tra enti nell'ambito del settore pubblico (art. 192, c. 1 e 3)	Tempestivo	Affatto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
							Art. 90, c. 10, d.lgs. n. 50/2016	Elenchi ufficiali di operatori economici riconosciuti e certificazioni	<u>Obbligo previsto per i soli enti che gestiscono gli elenchi e per gli operatori di certificazione</u> Elenco degli operatori economici iscritti in un elenco ufficiale (art. 90, c. 10, d.lgs. n. 50/2016) Elenco degli operatori economici in possesso del certificato rilasciato dal competente organismo di certificazione (art. 90, c. 10, d.lgs. n. 50/2016)	Tempestivo	Affatto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
Art. 11, co. 2-quater, l. n. 30/2003, introdotto dall'art. 41, co. 1, d.l. n. 76/2020	Progetti di investimento pubblico	<u>Obbligo previsto per i soggetti titolari di progetti di investimento pubblico.</u> Elenco dei progetti finanziati, con indicazione del CUP, importo totale del finanziamento, le fonti finanziarie, la data di avvio del progetto e lo stato di attuazione finanziario e procedurale					Annuale	Entro il 31/01	Tutte le strutture in relazione agli affidamenti di competenza	Ripartizione IV Regione strumentali - Ufficio appalti, contratti ed economato	Annuale (30 aprile) Tutte le strutture in relazione agli affidamenti di competenza			
Nota														
Gli allegamenti evidenziati in grigio non si applicano alla Regione autonoma Trentino Alto Adige-South.														

Note
Gli allegamenti evidenziati in grigio non si applicano alla Regione autonoma Trentino Alto Adige Sudtirolo

ATTI E DOCUMENTI DA PUBBLICARE IN "AMMINISTRAZIONE TRASPARENTE" SOTTOSEZIONE "BANDI DI GARA E CONTRATTI"									
All. 1 Delibera ANAC 264 del 20.6.2023, come modificato con Delibera ANAC 601 del 19.12.2023									
Contratti con bandi e avvisi pubblicati dopo il 1° gennaio 2024									
Denominazione sotto-sezione L.14/11	ATTI E DOCUMENTI DI CARATTERE GENERALE RIFERITI A TUTTE LE PROCEDURE								
Bandi di gara e contratti	Note	Riferimento normativo	Contenuto dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile	
La Regione applica in materia di appalti la disciplina provinciale ai sensi dell'art. 2 della legge regionale n. 2 del 2000 e s.m.. La pubblicazione avviene tramite link alla banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del combinato disposto dell'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4 bis della legge provinciale di Trento n. 2 del 2016.		Art. 30, d.lgs. 36/2023 Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici	Elenco delle soluzioni tecnologiche adottate dalle SA e enti concedenti per l'automatizzazione delle proprie attività.	Una tantum con aggiornamento tempestivo in caso di modifiche	all'atto della adozione	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	
		ALLEGATO I.5 al d.lgs. 36/2023 Elementi per la programmazione dei lavori e dei servizi. Schemi tipo (art. 4, co. 3)	Avviso finalizzato ad acquisire le manifestazioni di interesse degli operatori economici in ordine ai lavori di possibile completamento di opere incomplete nonché alla gestione delle stesse NB: Ove l'avviso è pubblicato nella apposita sezione del portale web del Ministero delle infrastrutture e dei trasporti, la pubblicazione in AT è assicurata mediante link al portale MIT	Tempestivo	all'atto dell'approvazione	Tutte le strutture	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	
		ALLEGATO I.5 al d.lgs. 36/2023 Elementi per la programmazione dei lavori e dei servizi. Schemi tipo (art. 5, co. 8, art. 7, co. 4)	Comunicazione circa la mancata redazione del programma triennale dei lavori pubblici, per assenza di lavori Comunicazione circa la mancata redazione del programma triennale degli acquisti di forniture e servizi, per assenza di acquisti di forniture e servizi.	Tempestivo	entro il 31 gennaio dell'anno successivo a quello di approvazione dell'ultimo Programma	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	
		Art. 168, d.lgs. 36/2023 Procedure di gara con sistemi di qualificazione	Atti recanti norme, criteri oggettivi per il funzionamento del sistema di qualificazione, l'eventuale aggiornamento periodico dello stesso e durata, criteri soggettivi (requisiti relativi alle capacità economiche, finanziarie, tecniche e professionali) per l'iscrizione al sistema.	Tempestivo	all'atto dell'approvazione	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	
		Art. 169, d.lgs. 36/2023 Procedure di gara regolamentate Settori speciali	<u>Obbligo applicabile alle imprese pubbliche e ai soggetti titolari di diritti speciali esclusivi</u> Atti eventualmente adottati recanti l'elencazione delle condotte che costituiscono gravi illeciti professionali agli effetti degli artt. 95, co. 1, lettera e) e 98 (cause di esclusione dalla gara per gravi illeciti professionali).	Tempestivo					
		Art. 11, co. 2-quater, l. n. 3/2003, introdotto dall'art. 41, co. 1, d.l. n. 76/2020 Dati e informazioni sui progetti di investimento pubblico	<u>Obbligo previsto per i soggetti titolari di progetti di investimento pubblico.</u> Elenco annuale dei progetti finanziari, con indicazione del CUP, importo totale del finanziamento, le fonti finanziarie, la data di avvio del progetto e lo stato di attuazione finanziato e procedurale	Annuale	entro il 31 gennaio dell'anno successivo	Tutte le strutture per i progetti di competenza	Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio appalti, contratti ed economato	
	PER CIASCUNA PROCEDURA SONO PUBBLICATI I SEGUENTI ATTI E DOCUMENTI								
		Fase	Riferimento normativo	Contenuto dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
		Pubblicazione	Art. 40, co. 3 e co. 5, d.lgs. 36/2023 Dibattito pubblico (da intendersi riferito a quello facoltativo) Allegato I.6 al d.lgs. 36/2023 Dibattito pubblico obbligatorio	1) Relazione sul progetto dell'opera (art. 40, co. 3 codice e art. 5, co. 1, lett. a) e b) allegato) 2) Relazione conclusiva redatta dal responsabile del dibattito (con i contenuti specificati dall'art. 40, co. 5 codice e art. 7, co. 1 dell'allegato) 3) Documento conclusivo redatto dalla SA sulla base della relazione conclusiva del responsabile (solo per il dibattito pubblico obbligatorio) ai sensi dell'art. 7, co. 2 dell'allegato Per il dibattito pubblico obbligatorio, la pubblicazione dei documenti di cui ai nn. 2 e 3, è prevista sia per le SA sia per le amministrazioni locali interessate dall'intervento	Tempestivo	All'atto dell'approvazione	Ripartizione IV Risorse strumentali - Ufficio tecnico e manutenzione - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio tecnico e manutenzione - Ufficio appalti, contratti ed economato	Annuale Ripartizione IV Risorse strumentali - Ufficio tecnico e manutenzione - Ufficio appalti, contratti ed economato
			Art. 82, d.lgs. 36/2023 Documenti di gara Art. 85, co. 4, d.lgs. 36/2023 Pubblicazione a livello nazionale (cfr. anche l'Allegato II.7)	Documenti di gara che comprendono, almeno: - Delibera a contrarre - Bando/avviso di gara/lettera di invito - Disciplina di gara - Capitolato speciale - Condizioni contrattuali proposte	Tempestivo	All'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
		Affidamento	Art. 28, d.lgs. 36/2023 Trasparenza dei contratti pubblici	Composizione delle commissioni giudicatrici e CV dei componenti	Tempestivo	All'atto del conferimento dell'incarico	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
			Art. 47, co. 2, e 9 d.l. 77/2021, convertito con modificazioni dalla L. 108/2021 D.P.C.M. 20 giugno 2023 recante Linee guida volte a favorire le pari opportunità generazionali e di genere, nonché l'inclusione lavorativa delle persone con disabilità nei contratti riservati (art. 1, co. 8, allegato II.3, d.lgs. 36/2023)	Pari opportunità e inclusione lavorativa nei contratti pubblici, PNRR e PNC e nei contratti riservati. Copia dell'ultimo rapporto sulla situazione del personale maschile e femminile redatto dall'operatore economico, tenuto alla sua riduzione ai sensi dell'art. 46, decreto legislativo 11 aprile 2006, n. 198 (operatori economici che occupano oltre 50 dipendenti). Il documento è prodotto, a pena di esclusione, al momento della presentazione della domanda di partecipazione e dell'offerta.					

	Fase	Riferimento normativo	Contenuto dell'obbligo	Aggiornamento	Termine di scadenza per la pubblicazione	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
La Regione applica in materia di appalti la disciplina provinciale ai sensi dell'art. 2 della legge regionale n. 2 del 2000 e s.m.. La pubblicazione avviene tramite link alla banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del combinato disposto dell'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4-bis della legge provinciale di Trento n. 2 del 2016.		Art. 10, co. 5; art. 14, co. 3; art. 17, co. 2; art. 24; art. 30, co. 2; art. 31, co. 1 e 2; D.lgs. 201/2022 Riordino della disciplina dei servizi pubblici locali di rilevanza economica	Procedure di affidamento dei servizi pubblici locali: 1) deliberazione di istituzione del servizio pubblico locale (art. 10, co. 5); 2) relazione contenente la valutazione finalizzata alla scelta della modalità di gestione (art. 14, co. 3); 3) Deliberazione di affidamento del servizio a società in house (art. 17, co. 3) per affidamenti sopra soglia del servizio pubblico locale, compresi quelli nei settori del trasporto pubblico locale e dei servizi di distribuzione di energia elettrica e gas naturale; 4) contratto di servizio sottoscritto dalle parti che definisce gli obblighi di servizio pubblico e le condizioni economiche del rapporto (art. 24 e 31 co. 2); 5) relazione periodica contenente le verifiche periodiche sulla situazione gestionale (art. 30, co. 2)	Tempestivo				
	Esecutiva	Art. 215 e ss. e Al. V.2, d.lgs. 36/2023 Collegio consultivo tecnico	Composizione del Collegio consultivo tecnici (nominativi) CV dei componenti	Tempestivo	All'atto dell'approvazione dell'incarico	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
		Art. 47, co. 3, co. 3-bis, co. 9, l. 77/2021 convertito con modificazioni dalla L. 108/2021 Pari opportunità e inclusione lavorativa nei contratti pubblici PNRR e PNC e nei contratti riservati D.P.C.M. 20 giugno 2023 recante Linee guida volte a favorire le pari opportunità generazionali e di genere, nonché l'inclusione lavorativa delle persone con disabilità nei contratti riservati (art. 1, co. 8, allegato II.3, d.lgs. 36/2023)	<u>Pari opportunità e inclusione lavorativa nei contratti pubblici PNRR e PNC e nei contratti riservati.</u> 1) Relazione di genere sulla situazione del personale maschile e femminile consegnata, entro sei mesi dalla conclusione del contratto, alla stazione appaltante/ente concedente dagli operatori economici che occupano un numero pari o superiore a quindici dipendenti 2) Certificazione di cui all'art. 17 della legge 12 marzo 1999, n. 68 e della relazione relativa all'assolvimento degli obblighi di cui alla medesima legge e alle eventuali sanzioni e provvedimenti disposti a carico dell'operatore economico nel biennio antecedente la data di scadenza della presentazione delle offerte e consegnate alla stazione appaltante/ente concedente entro sei mesi dalla conclusione del contratto (per gli operatori economici che occupano un numero pari o superiore a quindici dipendenti)	Tempestivo				
	Sponsorizzazioni	Art. 134, co. 4, d.lgs. 36/2023 Contratti gratuiti e forme speciali di finanziamento	Affidamento di contratti di sponsorizzazione di lavori, servizi o forniture per importi superiori a quarantamila 40.000 euro:- 1) avviso con il quale si rende nota la ricerca di sponsor per specifici interventi, ovvero si comunica l'avvenuto ricevimento di una proposta di sponsorizzazione, con sintetica indicazione del contenuto del contratto proposto.	Tempestivo	All'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
	Procedure di somma urgenza e di protezione civile	Art. 140, d.lgs. 36/2023 Comunicato del Presidente ANAC del 19 settembre 2023	Atti e documenti relativi agli affidamenti di somma urgenza a prescindere dall'importo di affidamento. In particolare: 1) verbale di somma urgenza e provvedimento di affidamento; con specifica indicazione delle modalità della scelta e delle motivazioni che non hanno consentito il ricorso alle procedure ordinarie; 2) perizia giustificativa; 3) elenco prezzi unitari, con indicazione di quelli concordati tra le parti e di quelli dedotti da prezziari ufficiali; 4) verbale di consegna dei lavori o verbale di avvio dell'esecuzione del servizio/fornitura; 5) contratto, ove stipulato.	Tempestivo	All'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
	Finanza di progetto	Art. 193, d.lgs. 36/2023 Procedura di affidamento	Provvedimento conclusivo della procedura di valutazione della proposta del promotore relativa alla realizzazione in concessione di lavori o servizi	Tempestivo	All'atto dell'approvazione	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza

**ELENCO DEGLI OBBLIGHI DI PUBBLICAZIONE DELLA SEZIONE "AMMINISTRAZIONE TRASPARENTE" SOTTOSEZIONE 1° LIVELLO –
BANDI DI GARA E CONTRATTI, relativi alla fase di aggiudicazione e di esecuzione, comprese le modifiche ai contratti e le varianti in corso d'opera
Delibera ANAC n. 582 del 13.12.2023 e delibera ANAC n. 605 DEL 19.12.2023
Contratti con bandi e avvisi pubblicati prima o dopo il 1° luglio 2023 ma non ancora conclusi alla data del 31 dicembre 2023**

Tipologie appalti	Contenuto dell'obbligo	Note	Pubblicazione	Aggiornamento	Responsabile elaborazione e trasmissione	Responsabile pubblicazione	Monitoraggio tempistiche e responsabile
In caso di CIG acquisiti con SIMOG	Fase di aggiudicazione Fase di esecuzione dei contratti	La Regione applica in materia di appalti la disciplina provinciale ai sensi dell'art. 2 della legge regionale n. 2 del 2000 e s.m.. La pubblicazione avviene tramite link alla banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del combinato disposto dell'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4-bis della legge provinciale di Trento n. 2 del 2016.	All'atto dell'approvazione ¹	Tempestivo ²	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
	Elenco dei soggetti invitati	La Regione applica in materia di appalti la disciplina provinciale ai sensi dell'art. 2 della legge regionale n. 2 del 2000 e s.m.. La pubblicazione avviene tramite link alla banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del combinato disposto dell'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4-bis della legge provinciale di Trento n. 2 del 2016.	All'atto della approvazione	Tempestivo	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
	<i>Per tutte le fattispecie per le quali non è obbligatorio l'invio delle schede successive al perfezionamento del CIG: dati relativi all'aggiudicazione/ esito della procedura.</i>		All'atto della approvazione	Tempestivo	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza

¹ Ai sensi della delibera dell'ANAC n. 582/2023 "sono superati i termini di comunicazione di tali dati all'ANAC precedentemente fissati rispettivamente in 30 giorni per l'aggiudicazione e in 60 giorni per la fase esecutiva".

² Vedi nota n. 1.

	<i>Per tutte le fattispecie per le quali non è obbligatorio l'invio delle schede successive all'aggiudicazione:</i> - atti di nomina del direttore dei lavori/direttore dell'esecuzione/componenti della commissione di collaudo - modifica contrattuale e varianti - accordi bonari e transazioni - certificato collaudo/reg. esecuzione/verifica conformità - resoconti della gestione finanziaria dei contratti al termine della loro esecuzione	La Regione applica in materia di appalti la disciplina provinciale ai sensi dell'art. 2 della legge regionale n. 2 del 2000 e s.m.. La pubblicazione avviene tramite link alla banca dati dell'Osservatorio Provinciale dei Contratti pubblici ai sensi del combinato disposto dell'art. 3 della legge provinciale di Trento n. 19 del 2016 e dell'art. 4-bis della legge provinciale di Trento n. 2 del 2016.	All'atto della approvazione	Tempestivo	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
	<i>Per gli affidamenti in house:</i> Atti connessi agli affidamenti in house		All'atto della approvazione	Tempestivo	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
	Obblighi previsti dall'All. 1 della Delibera ANAC n. 601/2023		All'atto della approvazione	Tempestivo	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza
In caso di Smart CIG acquisiti entro il 31 dicembre 2023	Denominazione e codice fiscale dell'aggiudicatario: - importo delle somme liquidate - tempi di completamento del contratto e resoconti della gestione finanziaria al termine dell'esecuzione		All'atto della approvazione	Tempestivo	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza

Procedure di somma urgenza e protezione civile	Comunicato del Presidente dell'ANAC del 19.09.2023 e nella Delibera ANAC n. 601 del 19.12.2023: Atti e documenti relativi agli affidamenti di somma urgenza a prescindere dall'importo di affidamento. In particolare: 1) verbale di somma urgenza e provvedimento di affidamento; con specifica indicazione delle modalità della scelta e delle motivazioni che non hanno consentito il ricorso alle procedure ordinarie; 2) perizia giustificativa; 3) elenco prezzi unitari, con indicazione di quelli concordati tra le parti e di quelli dedotti da prezzi ufficiali; 4) verbale di consegna dei lavori o verbale di avvio dell'esecuzione del servizio/fornitura; 5) contratto, ove stipulato.		All'atto della approvazione	Tempestivo	Tutte le strutture in relazione agli affidamenti di competenza	Tutte le strutture in relazione agli affidamenti di competenza	Semestrale (30 aprile-31 ottobre) Tutte le strutture in relazione agli affidamenti di competenza

PIAO

ALLEGATO n. 2

Sottosezione 2.3. Rischi corruttivi e trasparenza

Circolare n. 11 del 2018 prot. n. 18085 concernente
“Gestione delle istanze di accesso civico generalizzato,
accesso civico (semplice), accesso documentale, tramite
sistema PITre e registro degli accessi civici generalizzati”
e relativi Allegati



Trento / Trient 4.09.2018 prot. n. 18085

CIRCOLARE/RUNDSCHREIBEN Nr. 11

Oggetto: gestione delle istanze di accesso civico generalizzato, accesso civico (semplice), accesso documentale, tramite il sistema P.I.Tre. e registro degli accessi civici generalizzati.

Alle Dirigenti ed ai Dirigenti di
Ripartizione e Strutture equiparate

Alle Direttrici ed ai Direttori degli Uffici

Al personale regionale
Alle Organizzazioni Sindacali

Si informa il personale regionale che è stata implementata nel sistema P.I.Tre la nuova funzionalità concernente la gestione delle diverse fasi procedurali connesse alle istanze di accesso civico generalizzato, istituto giuridico previsto dall'articolo 1, comma 1, lettera 0a) della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, concernente l'ostensibilità dei documenti detenuti dall'amministrazione, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria.

Tale nuova funzionalità introdotta nel sistema consente la gestione delle diverse fasi procedurali relative all'istanza di accesso

Betreff: Abwicklung der Anträge auf allgemeinen Bürgerzugang, auf (einfachen) Bürgerzugang sowie auf Zugang zu den Verwaltungsunterlagen über das P.I.Tre.-System und Register der allgemeinen Bürgerzugänge

An die Leiterinnen und Leiter der Abteilungen
und der gleichgestellten
Organisationsstrukturen
An die Direktorinnen und Direktoren der Ämter

An die Regionalbediensteten
An die Gewerkschaften

Es wird mitgeteilt, dass im P.I.Tre.-System eine neue Funktion implementiert wurde, welche die Abwicklung der verschiedenen Verfahrensphasen in Zusammenhang mit den Anträgen auf allgemeinen Bürgerzugang betrifft. Dieses neue Rechtsinstitut ist im Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10 – geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16 – vorgesehen und betrifft die Einsehbarkeit von bei der Verwaltung aufliegenden Dokumenten, die über die veröffentlichungspflichtigen Dokumente hinausgehen.

Mit dieser neuen Funktion können die verschiedenen Verfahrensphasen in Zusammenhang mit den Anträgen auf

civico generalizzato ovvero:

- protocollazione delle richieste;
- gestione della fase istruttoria;
- gestione della fase relativa agli eventuali rimedi giurisdizionali e non, da attivare da parte del richiedente, in caso di diniego parziale o totale dell'accesso e quindi richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) o alternativemente, ricorso al difensore civico o alternativemente ricorso al Tribunale amministrativo regionale;
- la verifica in ogni momento dello stato di avanzamento di ogni procedimento;
- la registrazione delle richieste di accesso civico generalizzato pervenute, sottoforma di "Registro degli accessi" ovvero l'estrazione automatica dei files riepilogativi delle richieste pervenute (in tre formati diversi xls, pdf, e xml) che verrà gestita dalla Segreteria generale. Ciò, in osservanza a quanto stabilito nel punto 9 delle Linee guida dell'Autorità nazionale Anticorruzione, approvate con delibera n. 1309 del 28 dicembre 2016, recanti "*Indicazioni operative, ai fini della definizione delle esclusioni e dei limiti di accesso civico di cui all'articolo 5, comma 2, del decreto legislativo n. 33 e successive modificazioni*", (si legga per la Regione TAA articolo 1, comma 1, lettera 0a) della Legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16).

allgemeinen Bürgerzugang abgewickelt werden, d. h.:

- Protokollierung der Anträge;
- Bearbeitung der Anträge;
- Phase betreffend die eventuell von der antragstellenden Person eingeleiteten Rechtsbehelfe (Antrag an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz – RPCT auf Überprüfung der Entscheidung oder Rekurs bei der Volksanwaltschaft oder Rekurs beim Regionalen Verwaltungsgericht), falls der Zugangsantrag teilweise oder ganz abgelehnt wurde;
- jederzeit mögliche Überprüfung des Stands des jeweiligen Verfahrens;
- Erfassung der eingegangenen Anträge auf allgemeinen Bürgerzugang in Form eines „Registers der Zugänge“, d. h. automatische Extraktion der Dateien der eingegangenen Anträge (in den drei Dateiformaten .xls, .pdf und .xml). Dieser Schritt wird vom Generalsekretariat durchgeführt. Dadurch wird den Bestimmungen laut Z. 9 der mit Beschluss der nationalen Antikorruptionsbehörde (ANAC) vom 28. Dezember 2016, Nr. 1309 genehmigten Richtlinien entsprochen, die Anleitungen zur Bestimmung der Fälle enthalten, in denen der Bürgerzugang laut Art. 5 Abs. 2 des gesetzesvertretenden Dekrets Nr. 33 i.d.g.F. Ausnahmen und Einschränkungen unterliegt (in Bezug auf die Region Trentino-Südtirol siehe Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember

Nelle predette linee guida, l'Autorità raccomanda infatti, la raccolta organizzata delle richieste di accesso civico generalizzato sottoforma di "Registro" il quale deve contenere l'elenco delle richieste con l'oggetto e la data, il relativo esito con la data della decisione, da pubblicare nel sito istituzionale dell'Amministrazione regionale, oscurando i dati personali eventualmente presenti.

Il Registro degli accessi, oltre ad essere funzionale per il monitoraggio che in quest'ambito l'Autorità periodicamente intende svolgere, è anche utile per l'Amministrazione, al fine di rendere note le tipologie di documenti sulle quali è stato consentito l'accesso in una ottica di sempre maggiore semplificazione delle attività.

Con l'occasione dell'introduzione della nuova funzionalità finalizzata al monitoraggio delle istanze di accesso civico generalizzato, nel fascicolo tipizzato con classificazione 6.3 accesso ai documenti amministrativi, è stata inserita un'ulteriore tipologia di registrazione degli accessi ai documenti amministrativi, ovvero l'accesso agli atti o accesso documentale (tipologia fascicolo "Accesso documentale").

Pertanto, ogni richiesta di accesso dovrà preliminarmente essere ricondotta alla propria fattispecie giuridica e conseguentemente inserita nel sistema P.I.Tre nel fascicolo 6.3 accesso ai documenti amministrativi scegliendo uno dei fascicoli corrispondenti alla tipologia individuata.

Die Antikorruptionsbehörde empfiehlt in genannten Richtlinien nämlich die organisierte Erfassung der Anträge auf allgemeinen Bürgerzugang in Form eines „Registers“, das das Verzeichnis der eingegangenen Anträge mit Gegenstand und Datum sowie Ergebnis und Datum der diesbezüglichen Entscheidung enthält und auf der offiziellen Website der Regionalverwaltung zu veröffentlichen ist, wobei eventuell vorhandene personenbezogene Daten unkenntlich zu machen sind. Der Register der Zugänge ist nicht nur für das Monitoring nützlich, das die Antikorruptionsbehörde regelmäßig in diesem Bereich durchzuführen gedenkt, sondern im Hinblick auf die Vereinfachung der Tätigkeit auch für die Verwaltung, um die Art der Dokumente bekannt zu geben, auf die der Bürgerzugang erlaubt ist.

Anlässlich der Einführung dieser neuen Funktion zum Monitoring der Anträge auf allgemeinen Bürgerzugang wurde im Faszikeltyp „6.3 accesso ai documenti amministrativi“ zur Registrierung der Dokumentenzugänge ein weiterer Zugangstyp vorgesehen, nämlich der Zugang zu den Verwaltungsunterlagen (Faszikeltyp: „*Accesso documentale*“).

Dementsprechend muss jeder Zugangsantrag vorab der jeweiligen Kategorie zugeordnet und in das jeweilige Faszikel unter 6.3 „Accesso ai documenti amministrativi“ im P.I.Tre-System eingegeben werden.

Al fine di agevolare gli uffici nello svolgimento delle attività sopra descritte, si allegano per ogni utile consultazione i seguenti documenti:

- allegato A – breve sintesi sulle disposizioni in materia di accesso;
- allegato B – modalità di gestione delle domande di accesso tramite P.I.Tre;
- Allegato C - diagramma di flusso delle attività in cui sono indicati gli attori del processo e le operazioni da compiere con riferimento all'accesso civico generalizzato;
- modello per le richieste di accesso civico generalizzato, accesso documentale e accesso civico semplice (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico" unitamente alla presente circolare);
- modello per la richiesta di riesame al Responsabile per la prevenzione della corruzione e della trasparenza (RPCT) da parte del richiedente accesso in caso di diniego totale, parziale, differimento o mancata risposta dell'accesso civico generalizzato (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico unitamente alla presente circolare);
- modello per la richiesta di riesame al Responsabile per la prevenzione della corruzione e della trasparenza (RPCT) da parte dei controinteressati in caso di opposizione all'accoglimento dell'istanza di accesso civico generalizzato (pubblicato nel sito sotto la sezione "Amministrazione trasparente – altri contenuti – Accesso civico unitamente alla presente circolare).

Um die Durchführung der oben beschriebenen Tätigkeiten zu erleichtern, werden nachstehende Unterlagen beigelegt:

- Anlage A – Übersicht über die Regelung des Zugangsrechts;
- Anlage B – Modalitäten für die Abwicklung der Zugangsanträge mittels Eingabe in das P.I.Tre-System;
- Anlage C – Flussdiagramm der Aktivitäten in Bezug auf den allgemeinen Bürgerzugang mit Angabe der Akteure und der durchzuführenden Schritte;
- Vordruck für die Anträge auf allgemeinen Bürgerzugang, Zugang zu den Verwaltungsunterlagen und einfachen Bürgerzugang (der Vordruck ist zusammen mit diesem Rundschreiben auf der offiziellen Website unter dem Bereich „Transparente Verwaltung – Sonstige Inhalte – Bürgerzugang“ veröffentlicht);
- Vordruck für den von der antragstellenden Person an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz (RPCT) zu richtenden Antrag auf Überprüfung für den Fall, dass der Antrag auf allgemeinen Bürgerzugang ganz oder teilweise abgelehnt oder der Zugang aufgeschoben oder keine Antwort erteilt wurde (der Vordruck ist zusammen mit diesem Rundschreiben auf der offiziellen Website unter dem Bereich „Transparente Verwaltung – Sonstige Inhalte – Bürgerzugang“ veröffentlicht);
- Vordruck für den von den Drittbetroffenen an den Verantwortlichen für die

Korruptionsvorbeugung und die
Transparenz (RPCT) zu richtenden
Antrag auf Überprüfung für den Fall,
dass gegen den Antrag auf allgemeinen
Bürgerzugang Einspruch erhoben
wurde (der Vordruck ist zusammen mit
diesem Rundschreiben auf der
offiziellen Website unter dem Bereich
„Transparente Verwaltung – Sonstige
Inhalte – Bürgerzugang“ veröffentlicht).

Cordiali saluti.

Mit freundlichen Grüßen

IL SEGRETARIO GENERALE
DER GENERALESEKRETÄR

Alexander Steiner

(firmato digitalmente - digital signiert)

AS/cg

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Dokument in Papierform übermittelt wird, stellt es die für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

ALLEGATO A

Breve sintesi sulle disposizioni in materia di diritto di accesso

Il diritto di accedere ai documenti detenuti dall'Amministrazione può essere esercitato mediante:

- a) **accesso agli atti (accesso documentale)** ai sensi di quanto previsto dalla legge regionale 31 luglio 1993, n. 13, e successive modificazioni, recante “*Norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*” nonché dal Regolamento di esecuzione D.P.Reg. 16 novembre 2004, n. 7/L, e successive modificazioni;
- b) **accesso civico semplice**, inteso come richiesta di pubblicazione di documenti soggetti a pubblicazione obbligatoria, laddove sia stata omessa (art. 1, comma 1, della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, - riferimento: art. 5, comma 1, del decreto legislativo n. 33 del 2013 e successive modificazioni);
- c) **accesso civico generalizzato**, inteso come diritto di accedere ai DOCUMENTI detenuti dall'Amministrazione, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria (articolo 1, comma 1, lettera 0a) della Legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, - riferimento articolo 5, comma 2, del decreto legislativo n. 33 del 2013, e successive modificazioni).

Nel caso dell'**accesso agli atti “accesso documentale”** previsto dalla legge regionale 31 luglio 1993, n. 13, e successive modificazioni, la domanda di accesso deve essere motivata da parte del richiedente per far valere una situazione giuridicamente tutelata.

L'**accesso civico semplice, “accesso civico”**, è esercitabile unicamente presso il Responsabile della prevenzione della corruzione e della trasparenza (RPCT), al fine di verificare la presunta mancata pubblicazione, nella sezione “Amministrazione Trasparente” del sito istituzionale della Regione, di documenti che, in forza della vigente normativa in materia di trasparenza (legge regionale 29 ottobre 2014, n. 10 come modificata dalla legge regionale 15 dicembre 2016, n. 16) sono oggetto di pubblicazione obbligatoria.

L'inadempimento degli obblighi di pubblicazione, rilevato a seguito della presentazione di una domanda di accesso civico semplice comporta, per il Responsabile della prevenzione della corruzione e della trasparenza, l'obbligo di effettuare una segnalazione alla struttura competente in materia di procedimenti disciplinari, al Nucleo di valutazione dei dirigenti in funzione di Organismo Indipendente di Valutazione (O.I.V.) nonché al vertice politico dell'amministrazione (art. 43, comma 5, d. lgs. n. 33 del 2013, e successive modificazioni).

L'**accesso civico generalizzato, “accesso generalizzato”**, può essere esercitato da chiunque, senza bisogno di motivazione, nel rispetto dei limiti relativi alla tutela di interessi pubblici e privati giuridicamente rilevanti (articolo 1, comma 1, lettera 0a) e seguenti della Legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16 - riferimento: articolo 5, comma 2, e art. 5-bis del decreto legislativo n. 33 del 2013, e successive modificazioni).

Il contesto normativo di riferimento è delineato inoltre, dalle Linee guida dell'Autorità nazionale Anticorruzione recanti “*Indicazioni operative ai fini della definizione delle esclusioni e dei limiti di accesso civico di cui all'articolo 5, comma 2, del decreto legislativo n. 33 e successive modificazioni*” approvate con delibera n. 1309 del 28 dicembre 2016 e dalla circolare del Dipartimento della Funzione pubblica presso la Presidenza del Consiglio dei Ministri n. 2 del 2017, alle quali si rinvia per ogni utile approfondimento.

L'accoglimento o il non accoglimento della domanda deve essere sempre motivato. In applicazione del principio della tutela preferenziale dell'interesse conoscitivo la motivazione del non accoglimento della domanda, nelle varie forme in cui esso può essere manifestato, richiede un'attenta valutazione degli interessi pubblici e privati che possono giustificare una sua limitazione. Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine dei trenta giorni, il richiedente può presentare richiesta di riesame al Responsabile della prevenzione e della corruzione e della trasparenza (articolo 5, comma 7, del decreto legislativo n. 33 del 2013, e successive modificazioni) che decide con provvedimento motivato entro il termine di venti giorni, fatte salve le sospensioni del termine qualora si ritenga necessario acquisire l'avviso del Garante per la protezione dei dati personali.

Il differimento e la limitazione all'accesso civico generalizzato nei casi non previsti dalla citata normativa vigente, costituisce **elemento di valutazione della responsabilità dirigenziale**, anche ai fini della corresponsione della retribuzione di risultato.

Istruttoria (articolo 5, commi 5 e 6, e articolo 5-bis, commi 1 e 2 del decreto legislativo n. 33 del 2013 e successive modificazioni):

Assenza di controinteressati

Riscontrata l'assenza di controinteressati cui comunicare la domanda di accesso pervenuta il procedimento si conclude con:

- risposta motivata da comunicare al richiedente nel rispetto del termine di trenta giorni dalla data di presentazione della domanda.

Presenza di controinteressati

Nel caso di presenza di controinteressati, intesi quali soggetti portatori di uno degli interessi pubblici e/o privati tutelati:

- deve essere data comunicazione agli stessi mediante raccomandata con avviso di ricevimento o per via telematica, se dal richiedente è stato fornito nella domanda di accesso un indirizzo di posta elettronica certificata (PEC);
- devono essere contestualmente sospesi i termini per la risposta fino alla scadenza dei dieci giorni concessi ai controinteressati per fare opposizione;
- dalla ricezione della comunicazione inizia a decorrere il termine di dieci giorni concesso ai controinteressati per fare opposizione: in presenza di una pluralità di controinteressati la verifica deve essere compiuta rispetto alla ricezione di ciascuna comunicazione.

Scenari possibili:

A) Nessuno dei controinteressati fa opposizione

Accertata la data della ricezione della comunicazione ai fini della verifica dell'integrale decorrenza dei dieci giorni concessi per l'opposizione, il termine per la risposta ricomincia a decorrere e il procedimento si conclude con la comunicazione dell'esito al richiedente e con la tempestiva messa a disposizione dello stesso dei documenti richiesti, con le modalità indicate nella domanda. Dell'accoglimento della domanda deve essere data comunicazione ai controinteressati non opposti.

B) Uno o più controinteressati presentano opposizione

In via pregiudiziale deve essere verificato il rispetto del termine di 10 giorni dalla ricezione delle singole comunicazioni di opposizione, pena l'inammissibilità delle stesse: dall'integrale decorso del termine di dieci giorni riprende a decorrere il termine, precedentemente sospeso, per la risposta.

A seguito della valutazione dei motivi dell'opposizione, il procedimento può concludersi:

- con l'accoglimento della domanda di accesso nonostante l'opposizione dei controinteressati;
- con il non accoglimento della domanda di accesso, qualora si ravvisi in particolare l'esigenza di tutelare uno degli interessi previsti dall'art. 5-bis, commi 1 e 2, del d.lgs. n. 33 del 2013, e successive modificazioni.

Salvi i casi di comprovata indifferibilità (art. 5, comma 6, d.lgs. n. 33 del 2013 e successive modificazioni), deve essere data comunicazione dell'accoglimento della domanda di accesso al controinteressato, indicando che si procederà a trasmettere i documenti al richiedente non prima di quindici giorni dall'avvenuta ricezione della comunicazione stessa e che, avverso l'accoglimento, lo stesso controinteressato (ai sensi di quanto previsto dall'articolo 5, comma 9, d. lgs. n. 33 del 2013, e successive modificazioni) può presentare richiesta di riesame al Responsabile della prevenzione della corruzione e della trasparenza o ricorso al Difensore civico (art. 5, commi 7, 8 e 9, d. lgs. n. 33 del 2013 e successive modificazioni). A tal riguardo, la citata circolare del Dipartimento della Funzione pubblica n. 2 del 2017 suggerisce: *"Anche al fine di evitare contestazioni, è opportuno che la comunicazione di accoglimento della richiesta di accesso (in caso di opposizione) contenga l'espressa precisazione che la trasmissione al richiedente dei dati o documenti avviene qualora, decorsi quindici giorni, non siano stati notificati all'amministrazione ricorsi o richieste di riesame sulla medesima domanda di accesso"*.

Anche in questo caso, il Responsabile della prevenzione della corruzione e della trasparenza decide motivatamente entro venti giorni dalla richiesta di riesame, fatta salva la sospensione di tale termine qualora si ritenga necessario acquisire l'avviso del Garante per la protezione dei dati personali.

Il Difensore civico invece, si pronuncia entro trenta giorni dalla presentazione del ricorso.

ANLAGE A

Übersicht über die Regelung des Zugangsrechts

Das Recht auf Zugang zu den bei der Verwaltung aufliegenden Dokumenten kann in verschiedenen Weisen ausgeübt werden:

a) Zugang zu den Verwaltungsunterlagen im Sinne des Regionalgesetzes vom 31. Juli 1993, Nr. 13 i.d.g.F. „*Bestimmungen auf dem Gebiet des Verwaltungsverfahrens und des Rechtes auf Zugang zu den Verwaltungsunterlagen*“ sowie der Durchführungsverordnung laut DPRReg. vom 16. November 2004, Nr. 7/L i.d.g.F.;

b) einfacher Bürgerzugang: Antrag auf Veröffentlichung von veröffentlichungspflichtigen Dokumenten, wenn diese unterlassen wurde (Art. 1 Abs. 1 des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16; Bezugsbestimmung: Art. 5 Abs. 1 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.);

c) allgemeiner Bürgerzugang: Recht auf Zugang zu bei der Verwaltung aufliegenden Dokumenten, die über die veröffentlichungspflichtigen hinausgehen (Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16; Bezugsbestimmung: Art. 5 Abs. 2 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.).

Der **Zugang zu den Verwaltungsunterlagen („accesso documentale“)** gemäß Regionalgesetz vom 31. Juli 1993, Nr. 13 i.d.g.F. kann beantragt werden, um eine rechtlich geschützte Situation geltend zu machen. Der Antrag muss von der ansuchenden Person entsprechend begründet werden.

Das Recht auf **einfachen Bürgerzugang („accesso civico“)** kann ausschließlich über einen Antrag an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz (RPCT) ausgeübt werden, welcher daraufhin die vermeintlich unterlassene Veröffentlichung von Dokumenten, die laut den geltenden Bestimmungen in Sachen Transparenz (Regionalgesetz vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16) veröffentlichungspflichtig sind, unter dem Bereich „Transparente Verwaltung“ der offiziellen Website der Region überprüft.

Stellt der Verantwortliche für die Korruptionsvorbeugung und die Transparenz infolge eines Antrags auf einfachen Bürgerzugang fest, dass die Veröffentlichungspflicht nicht erfüllt wurde, so muss er dies der für die Disziplinarverfahren zuständigen Struktur, dem Gremium zur Bewertung der Führungskräfte in seiner Funktion als Unabhängiges Bewertungsgremium (OIV) sowie dem politischen Führungsorgan der Verwaltung melden (Art. 43 Abs. 5 des GvD Nr. 33/2013 i.d.g.F.).

Das Recht auf **allgemeinen Bürgerzugang („accesso generalizzato“)** kann von einer jeden Person ohne Begründung innerhalb der Grenzen des Schutzes rechtlich relevanter öffentlicher und privater Interessen ausgeübt werden (Art. 1 Abs. 1 Buchst. 0a) ff. des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16; Bezugsbestimmungen: Art. 5 Abs. 2 und Art. 5-bis des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.).

Den rechtlichen Rahmen bilden ferner die mit Beschluss der Nationalen Antikorruptionsbehörde vom 28. Dezember 2016, Nr. 1309 erlassenen Richtlinien mit *Anleitungen zur Bestimmung der Fälle, in denen der Bürgerzugang laut Art. 5 Abs. 2 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F. Ausnahmen und Einschränkungen unterliegt*, sowie das Rundschreiben Nr. 2/2017 der Abteilung für das öffentliche Verwaltungswesen beim Präsidium des Ministerrats, auf die zur Vertiefung verwiesen wird.

Die Annahme bzw. Ablehnung des Antrags ist immer zu begründen. Gemäß dem Grundsatz des vorrangigen Schutzes des Informationsinteresses müssen bei der Begründung der in welcher Form auch immer bekundeten Ablehnung des Antrags die öffentlichen und privaten Interessen, die eine Einschränkung des Zugangsrechts rechtfertigen können, genau abgewogen werden.

Wird der Zugangsantrag ganz oder teilweise abgelehnt oder erfolgt keine Antwort binnen der Frist von 30 Tagen, so kann die antragstellende Person beim Verantwortlichen für die Korruptionsvorbeugung und die Transparenz einen Antrag auf Überprüfung der Entscheidung stellen (Art. 5 Abs. 7 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.). Dieser entscheidet binnen zwanzig Tagen mit begründeter Maßnahme, unbeschadet der Aussetzung dieser Frist, falls die Datenschutzbehörde angehört werden muss.

Der Aufschub und die Einschränkung des allgemeinen Bürgerzugangs in Fällen, die nicht in den oben genannten Bestimmungen vorgesehen sind, werden **bei der Bewertung der Verantwortung der Führungskraft**, u. a. auch im Hinblick auf das Ergebnisgehalt, **berücksichtigt**.

Bearbeitung (Art. 5 Abs. 5 und 6 und Art. 5-bis Abs. 1 und 2 des gesetzesvertretenden Dekrets Nr. 33/2013 i.d.g.F.):

Es sind keine Drittbetroffenen vorhanden:

Nach Feststellung des Nichtvorhandenseins von Drittbetroffenen, denen der eingegangene Zugangsantrag mitzuteilen ist, wird das Verfahren

- mit einer begründeten Antwort abgeschlossen, die der antragstellenden Person innerhalb 30 Tagen ab Einreichung des Antrags zu erteilen ist.

Es sind Drittbetroffene vorhanden:

Falls Drittbetroffene, d. h. Rechtsträger eines geschützten öffentlichen und/oder privaten Interesses, vorhanden sind, ist folgendermaßen vorzugehen:

- Die Drittbetroffenen sind per Einschreiben mit Rückschein oder auf digitalem Weg – falls die antragstellende Person im Zugangsantrag eine zertifizierte E-Mail-Adresse (PEC) angegeben hat – über den Antrag zu informieren.
- Gleichzeitig wird die Frist für die Beantwortung des Antrags bis zum Ablauf der zehntägigen Frist ausgesetzt, innerhalb deren die Drittbetroffenen Einspruch erheben können.
- Die den Drittbetroffenen gewährte zehntägige Einspruchsfrist läuft ab dem Datum, an dem sie die Mitteilung erhalten haben. Sind mehrere Drittbetroffene vorhanden, so muss zur Berechnung der Frist das Datum des Erhalts jeder einzelnen Mitteilung berücksichtigt werden.

Mögliche Szenarien:

A) Keiner der Drittbetroffenen erhebt Einspruch

Nachdem das Datum des Erhalts der Mitteilung überprüft und der vollständige Ablauf der zehntägigen Einspruchsfrist festgestellt wurde, beginnt die Frist für die Beantwortung des Antrags wieder zu laufen und das Verfahren wird abgeschlossen, indem der antragstellenden Person das Ergebnis mitgeteilt wird und ihr die beantragten Dokumente umgehend und nach den im Antrag angegebenen Modalitäten zur Verfügung gestellt werden. Die Annahme des Antrags ist den Drittbetroffenen, die keinen Einspruch erhoben haben, mitzuteilen.

B) Einer oder mehrere Drittbetroffene erheben Einspruch

Vor der Entscheidung muss überprüft werden, dass die zehntägige Frist für die Einspruchserhebung ab Erhalt der jeweiligen Mitteilungen eingehalten wurde, da ansonsten der Einspruch unzulässig ist. Wenn diese zehntägige Frist vollständig abgelaufen ist, beginnt die zuvor ausgesetzte Frist für die Beantwortung des Antrags wieder zu laufen.

Je nachdem, wie die Einspruchsgründe beurteilt werden, kann das Verfahren folgendermaßen abgeschlossen werden:

- Dem Zugangsantrag wird trotz Einspruch der Drittbetroffenen stattgegeben.
- Der Zugangsantrag wird abgelehnt, falls insbesondere der Schutz eines der im Art. 5-bis Abs. 1 und 2 des GvD Nr. 33/2013 i.d.g.F. vorgesehenen Interessen für notwendig erachtet wird.

Außer in nachweislich unaufschiebbaren Fällen (Art. 5 Abs. 6 des GvD Nr. 33/2013 i.d.g.F.) sind die Drittbetroffenen über die Annahme des Zugangsantrags zu informieren mit dem Hinweis, dass die angeforderten Dokumente an die antragstellende Person erst nach Ablauf von fünfzehn Tagen ab Erhalt der Mitteilung zugesandt werden und dass gemäß Art. 5 Abs. 9 des GvD Nr. 33/2013 i.d.g.F. die Drittbetroffenen gegen die Annahme einen Antrag auf Überprüfung der Entscheidung beim Transparenzverantwortlichen oder Rekurs bei der Volksanwaltschaft einlegen können (Art. 5 Abs. 7, 8, und 9 des GvD Nr. 33/2013 i.d.g.F.). Diesbezüglich wird im genannten Rundschreiben Nr. 2/2017 der Abteilung für das öffentliche Verwaltungswesen Nachstehendes empfohlen: „*Um im Einspruchsfall Beanstandungen zu vermeiden, sollte die Mitteilung über die Annahme des Zugangsantrags den ausdrücklichen Hinweis enthalten, dass die angeforderten Daten oder Dokumente an die antragstellende Person erst nach Ablauf von fünfzehn Tagen übermittelt werden, sofern der Verwaltung innerhalb dieser Frist kein Rekurs oder kein Antrag auf Überprüfung der Entscheidung betreffend den Zugangsantrag zugestellt wird.*“

Wird ein Antrag auf Überprüfung der Entscheidung eingereicht, so entscheidet der Verantwortliche für die Korruptionsvorbeugung und die Transparenz auch in diesem Fall binnen zwanzig Tagen ab Eingang des Antrags mit begründeter Maßnahme, unbeschadet der Aussetzung dieser Frist, falls die Datenschutzbehörde angehört werden muss.

Die Volksanwaltschaft entscheidet hingegen innerhalb von dreißig Tagen nach Einlegung des Rekurses.

ALLEGATO B

Modalità di gestione delle domande di accesso tramite inserimento in P.I.Tre

La domanda di accesso, qualunque sia la modalità scelta dal richiedente (posta elettronica o posta elettronica certificata, consegna a mano, invio tramite il servizio postale) può essere presentata alla Segreteria della Segreteria generale della Giunta e alle Segreterie delle strutture competenti per materia – Ripartizioni - che provvederanno a protocollarla immettendola nel sistema P.I. Tre.

Gli indirizzi di posta elettronica cui inviare le domande sono i seguenti:

Segreteria generale della Giunta	giunta@pec.regione.taa.it
Ripartizione I - Pianificazione e programmazione delle risorse	programmazione@pec.regione.taa.it
Ripartizione II – Enti locali, previdenza e competenze ordinamentali	ripaist@pec.regione.taa.it
Ripartizione III – Minoranze linguistiche, integrazione europea, e giudici di pace	ripmin@pec.regione.taa.it
Ripartizione IV- Gestione delle risorse umane	personale@pec.regione.taa.it
Ripartizione V- Gestione delle risorse strumentali	risorsestrumentali@pec.regione.taa.it

E' ulteriormente possibile trasmettere istanza di accesso alla casella generale di posta elettronica certificata della Regione Autonoma Trentino-Alto Adige/Südtirol regione.taa@regione.taa.legalmail.it .
Sarà cura del servizio protocollo trasmettere l'istanza all'Ufficio competente.

Gli addetti delle segreterie delle strutture competenti, sentito il dirigente, provvedono a trasmettere, per competenza, le richieste di accesso protocollate agli incaricati dell'istruttoria.

L'incaricato dell'istruttoria provvede alla creazione del "fascicolo tipizzato" secondo quanto di seguito specificato.

Come registrare le pratiche di accesso

Ogni richiesta di accesso è preliminarmente ricondotta alla propria fattispecie giuridica creando uno specifico fascicolo, con classificazione 6.3 *accesso ai documenti amministrativi*, nell'ambito delle seguenti tipologie:

1. accesso agli atti o accesso documentale (tipologia fascicolo "Accesso documentale");
2. accesso civico generalizzato e accesso civico semplice (tipologia fascicolo "Accesso generalizzato e civico");

Ciascun profilo del fascicolo, oltre ai campi comuni alle tre diverse tipologie, prevede specifici campi aggiuntivi, oggetto di compilazione nel corso della progressione del procedimento.

Per la rappresentazione del sistema di fascicolazione, relativa alle diverse tipologie di accesso, si rimanda al diagramma di flusso delle attività (**Allegato C**), in cui sono indicati gli attori del processo e le operazioni da compiere.

Nel presente allegato, sono descritti i campi tipici di ognuna delle due tipologie di fascicolo e sono riportate le indicazioni per la compilazione.

Si richiama la necessità di verificare attentamente, soprattutto nel campo *Descrizione*, che non vengano inseriti riferimenti alla sfera personale del richiedente in violazione delle vigenti disposizioni in materia di tutela della privacy.

Tipologia fascicolo: Accesso generalizzato e civico

Per la creazione del fascicolo selezionare Fascicoli, Crea nuovo fascicolo.

Scheda fascicolo

ContenutoStrutturaTrasmissioniVisibilitàEventi

RegistroRATAA☐ Privato

Codice di Classificazione*
6.3Accesso ai documenti amministrativi
Descrizione*

Caratteri disponibili 2000

Nessuna nota visibile
☐ Personale ☐ Ruolo ☒ Tutti

Caratteri disponibili 2000

Trasmissione rapida
Scegli un modello di trasmissione

Tipologia Fascicolo
Seleziona una tipologia
Accesso documentale
Accesso generalizzato e civico

Tipologia Fascicolo

Accesso generalizzato e civico

Progressivo

AOO

RATAA

Data di arrivo della domanda *

24

Nr protocollo della domanda *

Si seleziona la tipologia “Accesso generalizzato e civico” e il profilo del fascicolo viene arricchito di alcuni campi ovvero la **Data arrivo della domanda** e il **Numero di protocollo della domanda, che sono già stati assegnati dalla segreteria al momento della protocollazione e che sono da inserire nuovamente.**

Entrambi sono campi obbligatori (contrassegnati da *) e saranno compilati al momento dell’effettuazione del passo n. 3 del diagramma di flusso allegato (Allegato C).

L’indicazione della **Presenza controinteressati** sarà fatta al momento dell’effettuazione del passo n. 4 del diagramma di flusso delle attività.

Presenza controinteressati

☐ SI ☐ NO

Utilizzare il pulsante  per correggere eventuali errori di selezione.

I campi relativi all’esito del procedimento saranno compilati dall’incaricato dell’istruttoria al momento dell’effettuazione del passo n. 7 del diagramma di flusso delle attività. In dettaglio, la compilazione del campo **Esito** sarà effettuata scegliendo uno dei valori ammessi: Accoglimento, Differimento, Rifiuto parziale, Rifiuto totale.

Esito

Seleziona

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

La compilazione del campo **Motivi del rifiuto parziale, del rifiuto totale o del differimento** sarà effettuata solo se l’esito non è Accoglimento. Per facilitare la compilazione del campo sono proposte alcune motivazioni che è possibile scegliere dalle voci del menu a tendina:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Seleziona

ALTRO - Motivi del rifiuto parziale, del rifiuto totale o del differimento**Data risposta**

24

Seleziona

a protezione di uno degli interessi previsti dall'art. 5 bis, comma 1, D. lgs. n. 33 del 2013

a protezione di interessi economici e commerciali

a protezione di dati personali

divieto di divulgazione per norma di legge

dati richiesti non sono detenuti dall'Amministrazione provinciale

dati richiesti richiedono un'elaborazione a cui l'Amministrazione non è tenuta

Se il motivo non è presente nella lista, selezionare *altri motivi* e inserire una descrizione a testo libero nel campo apposito. Si evidenzia che, in ogni caso, il campo altri motivi è stato inserito solamente in via cautelativa. Prima di procedere alla sua compilazione valutare attentamente di non essere in alcuna delle ipotesi di diniego non consentito descritte dalle linee guida ANAC approvate con delibera n. 1309 del 28 dicembre 2016 o dalla circolare del Dipartimento della Funzione pubblica della Presidenza del Consiglio dei Ministri n. 2 del 2017.

Motivi del rifiuto parziale, del rifiuto totale o del differimento

altri motivi (descriverli nel campo successivo) X

Il campo **Data risposta** sarà compilato con la data di protocollo della risposta al richiedente.

Data risposta

24

Il campo **Riesame – data di presentazione della domanda** sarà compilato al momento dell'effettuazione del passo n. 14 del diagramma di flusso delle attività.

Riesame - Data di presentazione della domanda

24

Il campo **Riesame – Esito** sarà compilato al momento dell'effettuazione del passo n. 16 del diagramma di flusso, scegliendo uno dei valori ammessi: Accoglimento, Differimento, Rifiuto parziale, Rifiuto totale

Riesame - Esito

Seleziona ▼

Riesame - Esito

Seleziona ▲

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

Nel caso di Esito Differimento, Rifiuto parziale, Rifiuto totale, si richiede la compilazione del campo **Motivi del rifiuto parziale, del rifiuto totale o del differimento**. Il campo prevede testo libero:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Il campo **Riesame – Data risposta** sarà compilato con la data di protocollo della risposta al richiedente.

Riesame - Data risposta

24

Il campo **Ricorso – Data di notificazione del ricorso all'Amministrazione** sarà compilato al momento dell'effettuazione del passo n. 21 del diagramma di flusso delle attività:

Ricorso – data di notificazione del ricorso

24

Il campo **Ricorso – Esito** sarà compilato al momento dell'effettuazione del passo n. 23 del diagramma di flusso delle attività, scegliendo uno dei valori ammessi: Accoglimento, Accoglimento parziale, Non accoglimento.

Ricorso - Esito

Seleziona ▼

Ricorso - Esito

Seleziona

Accoglimento

Accoglimento parziale

Non accoglimento

Tipologia fascicolo: Accesso agli atti/ Accesso Documentale

Per la creazione del fascicolo selezionare Fascicoli, Crea nuovo fascicolo.

Scheda fascicolo

Contenuto | Struttura | Trasm. | Visibilità | Eventi

Registro RATAA Privato

Codice di Classificazione*

6.3 Accesso ai documenti amministrativi

Descrizione*

Caratteri disponibili: 2000

Nessuna nota visibile

☐ Personale ☐ Ruolo ☒ Tutti

Caratteri disponibili: 2000

Trasmissione rapida

Scegli un modello di trasmissione

Tipologia Fascicolo

Seleziona una tipologia

Accesso documentale

Accesso generalizzato e civico

Si seleziona la tipologia Accesso documentale. Il profilo del fascicolo viene arricchito di alcuni campi:

La **Data arrivo della domanda** e il **Nr protocollo della domanda**, sono campi obbligatori (contrassegnati da *) e saranno compilati al momento dell'effettuazione del passo n. 3 del diagramma di flusso delle attività (Allegato C) e sono da inserire nuovamente.

L'indicazione della **Presenza controinteressati** sarà fatta al momento dell'effettuazione del passo n. 4 del diagramma di flusso delle attività.

Presenza controinteressati

☐ SI ☐ NO



Utilizzare il pulsante per correggere eventuali errori di selezione.

I campi relativi all'esito del procedimento saranno compilati al momento dell'effettuazione del passo n. 7 del diagramma di flusso delle attività. In dettaglio, la compilazione del campo **Esito** sarà effettuata scegliendo uno dei valori ammessi: Accoglimento, Differimento, Rifiuto parziale, Rifiuto totale.

The screenshot shows a dropdown menu titled 'Esito'. The menu is open, displaying a search bar and four options: 'Accoglimento', 'Differimento', 'Rifiuto parziale', and 'Rifiuto totale'.

Nel caso di Esito Differimento, Rifiuto parziale, Rifiuto totale, si richiede la compilazione del campo a testo libero **Motivi del rifiuto parziale, del rifiuto totale o del differimento** :

The screenshot shows a text input field with the placeholder text 'Motivi del rifiuto parziale, del rifiuto totale o del differimento'.

Il campo **Data risposta** sarà compilato con la data di protocollo della risposta al richiedente.

The screenshot shows a date selection field labeled 'Data risposta'. A calendar icon is visible, and the date '24' is displayed.

Il campo **Ricorso – Data di notificazione del ricorso all'Amministrazione** sarà compilato al momento dell'effettuazione del passo n. 12 del diagramma di flusso delle attività:

The screenshot shows a date selection field labeled 'Ricorso – data di notificazione del ricorso'. A calendar icon is visible, and the date '24' is displayed.

Il campo **Ricorso – Esito** sarà compilato al momento dell'effettuazione del passo n. 14 del diagramma di flusso delle attività, scegliendo uno dei valori ammessi: Accoglimento, Accoglimento parziale, Non accoglimento.

The screenshot shows a dropdown menu labeled 'Ricorso - Esito'. The menu is closed, showing the placeholder text 'Seleziona'.

The screenshot shows the 'Ricorso - Esito' dropdown menu open. The menu displays a search bar and three options: 'Accoglimento' (highlighted in blue), 'Accoglimento parziale', and 'Non accoglimento'.

Rapporti tra Fascicoli generati nel protocollo informatico e Registro degli accessi

La protocollazione, attraverso gli specifici fascicoli creati per le diverse tipologie di accesso delle domande e dei documenti relativi alle stesse (eventuale comunicazione ai controinteressati, la risposta di opposizione all'accesso, comunicazione della struttura con

l'indicazione dei motivi del rifiuto dell'accesso, ecc.) costituisce lo strumento per generare automaticamente il Registro degli accessi. Il Registro, gestito dalla Segreteria generale, pubblicato attraverso report periodici sul sito Amministrazione trasparente, costituisce la rappresentazione delle informazioni inserite nei vari campi del protocollo documentale.

ANLAGE B

Modalitäten für die Abwicklung der Zugangsanträge mittels Eingabe in das P.I.Tre.-System

Der Zugangsantrag kann – unabhängig von der gewählten Modalität (E-Mail, zertifizierte E-Mail, persönliche Übergabe, Post) – beim Sekretariat des Generalsekretariats der Regionalregierung oder der für das jeweilige Sachgebiet zuständigen Struktur/Abteilung eingereicht werden, das ihn zur Protokollierung in das P.I.Tre.-System eingibt.

Die Anträge können an nachstehende E-Mail-Adressen gesandt werden:

Generalsekretariat der Regionalregierung	giunta@pec.regione.taa.it
Abteilung I – Planung und Programmierung der Ressourcen	programmazione@pec.regione.taa.it
Abteilung II – Örtliche Körperschaften, Vorsorge und Ordnungsbefugnisse	ripaist@pec.regione.taa.i
Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte	ripmin@pec.regione.taa.it
Abteilung IV – Verwaltung der Humanressourcen	personale@pec.regione.taa.it
Abteilung V – Verwaltung der Technischen Ressourcen	risorsestrumentali@pec.regione.taa.it

Es ist außerdem möglich, den Zugangsantrag an die allgemeine zertifizierte E-Mail-Adresse der Autonomen Region Trentino-Südtirol regione.taa@regione.taa.legalmail.it zu senden.

Der Protokolldienst leitet dann den Antrag an das zuständige Amt weiter.

Die Sekretariatsbediensteten der zuständigen Strukturen übermitteln die protokollierten Zugangsanträge nach Anhören der Abteilungsleiterin / des Abteilungsleiters je nach Zuständigkeit an die sachbearbeitende Person.

Die sachbearbeitende Person erstellt ein Klassifikationsfaszikel („fascicolo tipizzato“) gemäß den nachstehenden Anweisungen.

Die Zugangsanträge sind wie folgt zu registrieren:

Jeder Zugangsantrag muss vorab der jeweiligen Kategorie zugeordnet werden, indem ein spezifisches Faszikel im Rahmen der nachstehenden Faszikeltypen mit Klassifizierung „6.3 accesso ai documenti amministrativi“ zu erstellen ist:

1. Zugang zu den Verwaltungsunterlagen (Faszikeltyp „Accesso documentale“);
2. allgemeiner Bürgerzugang und einfacher Bürgerzugang (Faszikeltyp „Accesso generalizzato e civico“);

Jedes Faszikel enthält neben den allen zwei Typen gemeinsamen Feldern auch spezifische Zusatzfelder, die im Laufe des Verfahrens auszufüllen sind.

Die Faszikelanlegung für die verschiedenen Arten des Zugangs ist im Flussdiagramm der Aktivitäten dargestellt (**Anlage C**), auf das verwiesen wird und in dem die Akteure und die durchzuführenden Schritte angegeben sind.

Diese Anlage enthält hingegen die Beschreibung der spezifischen Felder der zwei Faszikeltypen und die Anweisungen für das Ausfüllen derselben.

Es ist sorgfältig darauf zu achten, dass – vor allem im Feld „Descrizione“ – keine Bezüge auf die Privatsphäre der antragstellenden Person eingegeben werden, was die geltenden Datenschutzbestimmungen verletzen würde.

Faszikeltyp: „Accesso generalizzato e civico“

Um ein Faszikel zu erstellen, wählt man „Fascicoli, Crea nuovo fascicolo“.

Nun wählt man den Typ „Accesso generalizzato e civico“. Es erscheinen weitere Felder: „**Data di arrivo della domanda**“ und „**Numero di protocollo della domanda**“. Diese Daten wurden bereits vom Sekretariat bei der Protokollierung zugewiesen und sind erneut einzugeben.

Beide Felder sind Pflichtfelder (mit * markiert) und werden ausgefüllt, wenn Schritt 3 des beiliegenden Flussdiagramms (Anlage C) ausgeführt wird.

Das Vorhandensein von Drittbetroffenen wird im Feld „**Presenza controinteressati**“ angegeben, wenn Schritt 4 des Flussdiagramms ausgeführt wird.



Mit der Schaltfläche können eventuelle Fehler bei der Auswahl korrigiert werden.

Die Felder betreffend den Ausgang des Verfahrens werden von der sachbearbeitenden Person ausgefüllt, wenn Schritt 7 des Flussdiagramms ausgeführt wird. Für das Feld „**Esito**“ muss eine der folgenden Optionen gewählt werden: „Accoglimento“, „Differimento“, „Rifiuto parziale“, „Rifiuto totale“.

Esito

Seleziona

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

Falls nicht die Option „Accoglimento“ gewählt wurde, muss das Feld „**Motivi del rifiuto parziale, del rifiuto totale o del differimento**“ ausgefüllt werden. Um das Ausfüllen zu erleichtern, enthält das Dropdown-Menü bereits einige Begründungsvorschläge:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Seleziona

ALTRO - Motivi del rifiuto parziale, del rifiuto totale o del differimento

Data risposta

24

Seleziona

a protezione di uno degli interessi previsti dall'art. 5 bis, comma 1, D. lgs. n. 33 del 2013

a protezione di interessi economici e commerciali

a protezione di dati personali

divieto di divulgazione per norma di legge

dati richiesti non sono detenuti dall'Amministrazione provinciale

dati richiesti richiedono un'elaborazione a cui l'Amministrazione non è tenuta

Wenn die Begründung nicht in der Liste enthalten ist, wählt man „*altri motivi*“ und beschreibt die Begründung mit freien Worten im entsprechenden Feld. Es wird darauf hingewiesen, dass das Feld „*altri motivi*“ rein vorsichtshalber eingefügt wurde. Bevor es ausgefüllt wird, sollte sorgfältig abgewogen werden, dass keiner der Fälle einer unzulässigen Ablehnung vorliegt, die in den mit Beschluss der Nationalen Antikorruptionsbehörde vom 28. Dezember 2016, Nr. 1309 erlassenen Richtlinien oder im Rundschreiben

Nr. 2/2017 der Abteilung für das öffentliche Verwaltungswesen beim Präsidium des Ministerrats beschrieben werden.

Motivi del rifiuto parziale, del rifiuto totale o del differimento

altri motivi (descriverli nel campo successivo) X ▾

Das Feld „**Data risposta**“ ist mit dem Protokollierungsdatum der Antwort an die antragstellende Person auszufüllen.

Data risposta

24

Das Feld „**Riesame – data di presentazione della domanda**“ ist auszufüllen, wenn Schritt 14 des Flussdiagramms ausgeführt wird.

Riesame - Data di presentazione della domanda

24

Das Feld „**Riesame – Esito**“ ist auszufüllen, wenn Schritt 16 des Flussdiagramms ausgeführt wird, wobei eine der folgenden Optionen zu wählen ist: „Accoglimento“, „Differimento“, „Rifiuto parziale“, „Rifiuto totale“.

Riesame - Esito

Seleziona ▾

Riesame - Esito

Seleziona ▴

🔍

Accoglimento

Differimento

Rifiuto parziale

Rifiuto totale

Falls im Feld „Esito“ die Option „Differimento“, „Rifiuto parziale“ oder „Rifiuto totale“ gewählt wird, ist das Feld „**Motivi del rifiuto parziale, del rifiuto totale o del differimento**“ auszufüllen. Es handelt sich dabei um ein offenes Textfeld:

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Das Feld „**Riesame – Data risposta**“ ist mit dem Protokollierungsdatum der Antwort an die antragstellende Person auszufüllen.

Riesame - Data risposta

24

Das Feld „**Ricorso – Data di notificazione del ricorso all'Amministrazione**“ ist auszufüllen, wenn Schritt 21 des Flussdiagramms ausgeführt wird:



The screenshot shows a form header with the text "Ricorso - Data di notificazione del ricorso giurisdizionale all'Amministrazione". Below the header is a text input field. To the right of the input field is a small red icon with the number "24" inside it.

Das Feld „**Ricorso – Esito**“ ist auszufüllen, wenn Schritt 23 des Flussdiagramms ausgeführt wird, wobei eine der folgenden Optionen zu wählen ist: „Accoglimento“, „Accoglimento parziale“, „Non accoglimento“.



The screenshot shows a dropdown menu titled "Ricorso - Esito". The menu is open, showing a search bar with the text "Seleziona" and a magnifying glass icon. Below the search bar are three options: "Accoglimento", "Accoglimento parziale", and "Non accoglimento". The "Accoglimento" option is highlighted in blue.



This is a closer view of the dropdown menu from the previous image. It shows the search bar "Seleziona" and the three options: "Accoglimento", "Accoglimento parziale", and "Non accoglimento". The "Accoglimento" option is highlighted in blue.

Faszikeltyp: „Accesso agli atti/ Accesso Documentale“

Um ein Faszikel zu erstellen, wählt man „Fascicoli, Crea nuovo fascicolo“.

Contenuto Struttura Trasm. ni Visibilità Eventi

Descrizione*

Caratteri disponibili 2000

Nessuna nota visibile

☐ Personale ☐ Ruolo ☐ RF ☒ Tutti

Caratteri disponibili 2000

Trasmissione rapida

Scegli un modello di trasmissione

Tipologia Fascicolo

Seleziona una tipologia

Accesso dei Consiglieri provinciali

Accesso documentale

Accesso generalizzato e civico

Nun wählt man den Typ „Accesso documentale“. Es erscheinen weitere Felder:

Tipologia Fascicolo Accesso documentale	
Progressivo AOO PAT	
Data di arrivo della domanda * 24	
Nr protocollo della domanda *	

Tipologia Fascicolo

Accesso documentale

Progressivo

A00

PAT

Data di arrivo della domanda *

24

Nr protocollo della domanda *

Die Felder „**Data di arrivo della domanda**“ und „**Nr protocollo della domanda**“ sind Pflichtfelder (mit * markiert) und müssen erneut eingegeben werden, wenn Schritt 3 des Flussdiagramms (Anlage C) ausgeführt wird.

Das Vorhandensein von Drittbetroffenen wird im Feld „**Presenza controinteressati**“ angegeben, wenn Schritt 4 des Flussdiagramms ausgeführt wird.

Presenza controinteressati

☐ SI ☐ NO

Mit der Schaltfläche  können eventuelle Fehler bei der Auswahl korrigiert werden.

Die Felder betreffend den Ausgang des Verfahrens werden ausgefüllt, wenn Schritt 7 des Flussdiagramms ausgeführt wird. Das Feld „**Esito**“ wird demnach ausgefüllt, indem eine der folgenden Optionen gewählt wird: „Accoglimento“, „Differimento“, „Rifiuto parziale“, „Rifiuto totale“.

Falls im Feld „Esito“ die Option „Differimento“, „Rifiuto parziale“ oder „Rifiuto totale“ gewählt wird, ist das offene Textfeld „**Motivi del rifiuto parziale, del rifiuto totale o del differimento**“ auszufüllen.

Motivi del rifiuto parziale, del rifiuto totale o del differimento

Das Feld „**Data risposta**“ ist mit dem Protokollierungsdatum der Antwort an die antragstellende Person auszufüllen.

Data risposta

24

Das Feld „**Ricorso – Data di notificazione del ricorso all'Amministrazione**“ ist auszufüllen, wenn Schritt 12 des Flussdiagramms ausgeführt wird:

Ricorso - Data di notificazione del ricorso giurisdizionale all'Amministrazione

24

Das Feld „**Ricorso – Esito**“ ist auszufüllen, wenn Schritt 14 des Flussdiagramms ausgeführt wird, wobei eine der folgenden Optionen zu wählen ist: „Accoglimento“, „Accoglimento parziale“, „Non accoglimento“.

Ricorso - Esito

Seleziona ▼

Ricorso - Esito

Seleziona

Accoglimento

Accoglimento parziale

Non accoglimento

Zusammenhang zwischen den im P.I.Tre.-System erstellten Faszikeln und dem „Register der Zugänge“

Durch die Protokollierung der Zugangsanträge und der diesbezüglichen Unterlagen (eventuelle Mitteilungen an Drittbetroffene, Antwort auf den Einspruch gegen den Zugang, Mitteilung der zuständigen Struktur mit Angabe des Ablehnungsgrunds usw.) mittels der spezifischen je nach Art des Zugangs vorgesehenen Faszikel erfolgt zugleich die automatische Erstellung des Registers der Zugänge. In diesem Register, das vom Generalsekretariat verwaltet und regelmäßig auf der Website der Region im Bereich „Transparente Verwaltung“ veröffentlicht wird, werden die in die verschiedenen Felder des Protokolls zur Dokumentenverwaltung eingegebenen Informationen dargestellt.



**REGIONE AUTONOMA TRENTINO - ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENTINO-SÜDTIROL**

RICHIESTA DI ACCESSO

☐ **Alla Segreteria¹** _____
(in caso di accesso civico generalizzato e accesso documentale);

oppure

☐ **Al Responsabile per la prevenzione della corruzione e della trasparenza della Regione Autonoma Trentino-Alto Adige/Südtirol** (in caso di accesso civico semplice);

Il sottoscritto/a

(campi obbligatori: nome, cognome e almeno un dato di recapito o contatto)

Dati anagrafici				
	nome	cognome	luogo di nascita	data di nascita

Residenza				
	indirizzo	CAP	Comune	Prov./Stato estero

1 In caso di accesso civico generalizzato e accesso documentale l'istanza va presentata alle segreterie delle Strutture competenti per materia (Ripartizioni e/o Segreteria generale della Giunta in quanto struttura equiparata).
In caso di accesso civico semplice l'istanza va presentata al Responsabile per la prevenzione della corruzione e della trasparenza, per il tramite della Segreteria generale della Giunta.

Gli indirizzi di posta elettronica cui inviare le domande sono i seguenti:

Segreteria generale della Giunta	giunta@pec.regione.taa.it
Ripartizione I - Pianificazione e programmazione delle risorse	programmazione@pec.regione.taa.it
Ripartizione II - Enti locali, previdenza e competenze ordinamentali	ripaist@pec.regione.taa.it
Ripartizione III - Minoranze linguistiche, integrazione europea, e giudici di pace	ripmin@pec.regione.taa.it
Ripartizione IV- Gestione delle risorse umane	personale@pec.regione.taa.it
Ripartizione V- Gestione delle risorse strumentali	risorsestrumentali@pec.regione.taa.it

E' ulteriormente possibile trasmettere istanze di accesso alla casella generale di posta elettronica certificata della Regione Autonoma Trentino - Alto Adige/Südtirol regione.taa@regione.taa.legalmail.it .
Sarà cura del servizio protocollo trasmettere l'istanza all'Ufficio competente

La richiesta di accesso può essere inviata con una delle seguenti modalità:

tramite posta elettronica, tramite posta elettronica certificata (PEC), tramite posta ordinaria all'indirizzo: Regione Autonoma Trentino-Alto Adige/Südtirol – Via Gazzoletti, 2 – 38122 TRENTO, tramite fax al n. 0461/201496, con consegna a mano presso la Segreteria Generale della Giunta regionale – secondo piano – Regione Autonoma Trentino – Alto Adige – Via Gazzoletti, 2 – 38122 TRENTO

Dati di contatto	@		
	indirizzo PEC/e-mail	telefono/cellulare	fax

in qualità di legale rappresentante della società/ditta/persona giuridica/ente		
	Denominazione società/ditta/persona giuridica/ente/altro (da precisare)	Dati inerenti la procura/incarico

in qualità di:	
	<i>campo facoltativo: solo per rilevazioni statistiche (a titolo meramente esemplificativo ricercatore, studente, giornalista, libero professionista, dipendente pubblico, ecc.)</i>

CHIEDE
(barrare la casella corrispondente)

☐ **accesso civico generalizzato, ai sensi dell'articolo 1, comma 1, lettera 0a) della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16 (riferimento art. 5, comma 2, decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni) per i DOCUMENTI non soggetti ad obbligo di pubblicazione in base alla normativa vigente, detenuti dalla Regione Autonoma Trentino - Alto Adige/Südtirol, e di seguito specificati:**

Documenti	
	Specificare gli elementi necessari per consentire di identificare quanto richiesto.

mediante:

- ☐ **visione**
- ☐ **rilascio in copia semplice**
- ☐ **rilascio in copia autenticata**
- ☐ **rilascio in copia autenticata in bollo (il costo delle marche da bollo è a carico del richiedente);**



☐ **accesso ai documenti amministrativi, ai sensi degli artt. 26 e seguenti della legge regionale 31 luglio 1993, n. 13, e successive modificazioni, nonché D.P.Reg. 16 novembre 2004, n. /L (riferimento: legge n. 241 del 1990, e successive modificazioni.)**

Documenti	
	Specificare gli elementi necessari per consentire di identificare quanto richiesto.

mediante:

- ☐ **visione**
- ☐ **rilascio in copia semplice**
- ☐ **rilascio in copia autenticata**
- ☐ **rilascio in copia autenticata in bollo (il costo delle marche da bollo è a carico del richiedente)**

in quanto portatore dei seguenti interessi giuridicamente rilevanti e motivi di legittimazione collegati al documento richiesto:

Motivazione	



☐ **accesso civico semplice, ai sensi dell'art. 1 della legge regionale 29 ottobre 2014, n. 10, come modificata dalla legge regionale 15 dicembre 2016, n. 16, per omessa pubblicazione obbligatoria, ai sensi della normativa regionale vigente, dei seguenti DOCUMENTI nella sezione "Amministrazione trasparente" del sito istituzionale della Regione Autonoma Trentino-Alto Adige/Südtirol:**

Documenti	
	Specificare i dati, le informazioni, i documenti di cui è stata omessa, anche parzialmente, la pubblicazione obbligatoria; nel caso in cui il richiedente ne sia a conoscenza, specificare anche la norma che impone la pubblicazione di quanto richiesto.

Tale accesso sarà assicurato tramite pubblicazione e contestuale comunicazione dell'avvenuta pubblicazione (con indicazione del collegamento ipertestuale).



Modalità di esercizio dell'accesso (indicare la modalità prescelta):

- ☐ **visione/ritiro presso la sede dell'Ufficio che detiene i documenti;**
- ☐ **invio al seguente indirizzo di posta elettronica (PEO) / posta elettronica certificata (PEC);**
- ☐ **invio per posta tramite raccomandata con avviso di ricevimento al seguente indirizzo:**

indirizzo _____ **località** _____
provincia _____ **CAP** _____ **Stato** _____;

Il sottoscritto/a, inoltre

DICHIARA

di essere informato/a che potrà essere richiesto il pagamento delle spese effettivamente sostenute e documentate per la riproduzione su supporti materiali (carta o CD)¹;

di aver preso visione dell'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento europeo n. 679/2016.

ALLEGA

copia di documento di identità o di riconoscimento (non occorre per le istanze sottoscritte con firma digitale o elettronica qualificata o con identificazione tramite SPID nonché per le istanze consegnate direttamente all'addetto dell'Ufficio e sottoscritte in sua presenza).

(luogo e data)

(firma)

¹La trasmissione telematica e la copia di file digitali su supporto fornito dal richiedente (CD o dispositivo USB) sono esenti da pagamento.



REGIONE AUTONOMA TRENINO - ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL

ZUGANGSANTRAG

☐ **An das Sekretariat¹** _____
(falls der allgemeine Bürgerzugang oder der Zugang zu den Verwaltungsunterlagen beantragt wird)

oder

☐ **An den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz der Autonomen Region Trentino-Südtirol** (falls der einfache Bürgerzugang beantragt wird)

Die/Der Unterfertigte

(Pflichtfelder: Vorname, Zuname und mindestens eine Kontaktangabe)

Personalien				
	Vorname	Zuname	Geburtsort	Geburtsdatum
Wohnsitz				
	Adresse	PLZ	Gemeinde	Provinz/ausländ. Staat
Kontakt- daten				
	E-Mail- oder zertifizierte E-Mail-Adresse		Telefon/Mobiltelefon	Fax

ERSUCHT

¹ Anträge auf allgemeinen Bürgerzugang und auf Zugang zu den Verwaltungsunterlagen sind beim Sekretariat der für das jeweilige Sachgebiet zuständigen Struktur (Abteilungen und/oder Generalsekretariat der Regionalregierung als gleichgestellte Organisationsstruktur) einzureichen.

Anträge auf einfachen Bürgerzugang sind über das Generalsekretariat der Regionalregierung an den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz zu richten.

Die Anträge können an nachstehende E-Mail-Adressen gesandt werden:

Generalsekretariat der Regionalregierung	giunta@pec.regione.taa.it
Abteilung I – Planung und Programmierung der Ressourcen	programmazione@pec.regione.taa.it
Abteilung II – Örtliche Körperschaften, Vorsorge und Ordnungsbefugnisse	ripaist@pec.regione.taa.it
Abteilung III – Sprachminderheiten, europäische Integration und Friedensgerichte	ripmin@pec.regione.taa.it
Abteilung IV – Verwaltung der Humanressourcen	personale@pec.regione.taa.it
Abteilung V – Verwaltung der technischen Ressourcen	risorsestrumentali@pec.regione.taa.it

Es ist außerdem möglich, den Zugangsantrag an die allgemeine zertifizierte E-Mail-Adresse der Autonomen Region Trentino-Südtirol regione.taa@regione.taa.legalmail.it zu senden.

Der Protokolldienst leitet dann den Antrag an das zuständige Amt weiter.

Der Zugangsantrag kann mit einer der nachstehenden Modalitäten übermittelt werden:

E-Mail; zertifizierte E-Mail; Post an die Adresse: Autonome Region Trentino-Südtirol – Via Gazzoletti 2 – 38122 TRIENT; Fax an die Nr. 0461/201496; persönliche Übergabe beim Generalsekretariat der Regionalregierung – 2. Stock – Autonome Region Trentino-Südtirol – Via Gazzoletti 2 – 38122 TRIENT.

in ihrer Eigenschaft als gesetzliche Vertreterin / in seiner Eigenschaft als gesetzlicher Vertreter der Gesellschaft/Firma/juristischen Person/Körperschaft		
	Name der Gesellschaft/Firma/juristischen Person/Körperschaft o. ä. (bitte genau angeben)	Angaben zur Vollmacht/zum Auftrag

Beschäftigung:	
	Fakultatives Feld, nur für statistische Erhebungen (z. B. Forscher/in, Student/in, Journalist/in, Freiberufler/in, öffentliche/r Bedienstete/r usw.)

(Zutreffendes ankreuzen)

☐ **um allgemeinen Bürgerzugang** im Sinne des Art. 1 Abs. 1 Buchst. 0a) des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch Regionalgesetz vom 15. Dezember 2016, Nr. 16, (Bezugsbestimmung: Art. 5 Abs. 2 des gesetzesvertretenden Dekrets vom 14. März 2013, Nr. 33 i.d.g.F) zu nachstehenden DOKUMENTEN, die aufgrund der geltenden Bestimmungen nicht veröffentlichungspflichtig sind und bei der Autonomen Region Trentino-Südtirol aufliegen

Dokumente	
	Die zur Identifizierung der beantragten Dokumente erforderlichen Daten genau angeben

durch:

- ☐ Einsichtnahme
☐ Ausstellung einer einfachen Kopie
☐ Ausstellung einer beglaubigten Kopie
☐ Ausstellung einer beglaubigten Kopie mit Stempelmarke (Die Gebühr für die Stempelmarke geht zu Lasten der antragstellenden Person)



☐ **um Zugang zu den Verwaltungsunterlagen** im Sinne des Art. 26 ff. des Regionalgesetzes vom 31. Juli 1993, Nr. 13 i.d.g.F. sowie des DPRReg. vom 16. November 2004, Nr. 7/L (Bezugsbestimmung: Gesetz Nr. 241/1990 i.d.g.F.)

Dokumente	
	Die zur Identifizierung der beantragten Dokumente erforderlichen Daten genau angeben

durch:

- ☐ Einsichtnahme

- ☐ Ausstellung einer einfachen Kopie
- ☐ Ausstellung einer beglaubigten Kopie
- ☐ Ausstellung einer beglaubigten Kopie mit Stempelmarke (Die Gebühr für die Stempelmarke geht zu Lasten der antragstellenden Person),

da in Zusammenhang mit den Dokumenten, zu denen der Zugang beantragt wird, sie/er Trägerin/Träger nachstehender rechtlich relevanter Interessen ist bzw. nachstehende Legitimierungsgründe bestehen:

Begründung	



☐ **um einfachen Bürgerzugang** im Sinne des Art. 1 des Regionalgesetzes vom 29. Oktober 2014, Nr. 10, geändert durch das Regionalgesetz vom 15. Dezember 2016, Nr. 16, da die nachstehenden im Sinne der geltenden Regionalbestimmungen der Veröffentlichungspflicht unterliegenden DOKUMENTE nicht unter dem Bereich „Transparente Verwaltung“ der offiziellen Website der Autonomen Region Trentino-Südtirol veröffentlicht wurden:

Dokumente	
	Die veröffentlichungspflichtigen Daten, Informationen, Dokumente angeben, deren Veröffentlichung – auch nur teilweise – unterlassen wurde; wenn bekannt, auch die Bestimmung angeben, in der die Veröffentlichungspflicht vorgesehen ist.

Der Zugang erfolgt durch Veröffentlichung der Dokumente und Mitteilung an die antragstellende Person über die erfolgte Veröffentlichung (mit Angabe des entsprechenden Hyperlinks).



Das Zugangsrecht wird wie folgt ausgeübt (Zutreffendes ankreuzen):

- ☐ Einsichtnahme/Abholen beim Amt, bei dem die Dokumente aufliegen
- ☐ Zusendung an die folgende E-Mail- bzw. zertifizierte E-Mail-Adresse: _____
- ☐ Zusendung mittels Einschreiben mit Rückschein an die folgende Adresse:

Straße/Platz _____ Ort _____
 Provinz _____ PLZ _____ Staat _____

Die/Der Unterfertigte

ERKLÄRT

ferner, dass sie/er darüber in Kenntnis ist, dass für die bestrittenen und nachgewiesenen Kosten für die Wiedergabe der Dokumente auf Datenträgern (Papier oder CD)¹ eine Gebühr erhoben werden kann;

dass sie/er Einsicht in die Information über die Verarbeitung der personenbezogenen Daten im Sinne des Art. 13 der EU-Verordnung Nr. 679/2016 genommen hat,

und

LEGT

eine Kopie des Personalausweises bei. (Davon wird abgesehen, wenn der Antrag digital oder in einer anderen qualifizierten Form elektronisch signiert ist oder die antragstellende Person mittels SPID identifiziert wird oder wenn der Antrag unmittelbar der/dem Bediensteten des Amtes übergeben und vor dieser/diesem unterzeichnet wird.)

(Ort und Datum)

(Unterschrift)

¹ Die digitale Übermittlung und das Kopieren von digitalen Dateien auf Datenträger (CD oder USB-Stick), die von der antragstellenden Person zur Verfügung gestellt werden, sind gebührenfrei.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL**

**RICHIESTA DI RIESAME
(per il richiedente accesso)**

Al Responsabile per la prevenzione della corruzione e della trasparenza della Regione Autonoma Trentino-Alto Adige/Südtirol

**per il tramite
della Segreteria della Segreteria generale della Giunta**

giunta@pec.regione.taa.it

e p.c.

**Al Responsabile _____
(dirigente responsabile a decidere in merito all'istanza di accesso civico generalizzato)**

Il sottoscritto/a

(campi obbligatori: nome, cognome e almeno un dato di recapito o contatto)

Dati anagrafici	_____ / ____ / ____			
	nome	cognome	luogo di nascita	data di nascita
Residenza	_____			
	indirizzo	CAP	Comune	Prov./Stato estero
Dati di contatto	_____			
	@ indirizzo PEC/e-mail	telefono/cellulare	fax	

**in riferimento all'istanza di accesso civico generalizzato presentata in data _____
prot. n. _____, con il seguente esito:**

- ☐ diniego totale dell'accesso
☐ diniego parziale dell'accesso
☐ differimento dell'accesso

**come da comunicazione a firma del Responsabile _____ prot. n. _____
del _____, inviata a mezzo _____ e ricevuto in
data _____;**

oppure

☐ è mancata dall'Ufficio la risposta nei termini previsti dalla legge,

CHIEDE

il **RIESAME dell'istanza presentata**, ai sensi dell'art. 5, comma 7, del decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni, con le seguenti motivazioni:

CHIEDE INOLTRE,

che le comunicazioni inerenti la presente richiesta di riesame siano inviate:
(barrare la modalità prescelta e compilare le parti relative)

☐ al seguente indirizzo di posta elettronica (PEO) / posta elettronica certificata (PEC);

☐ al seguente indirizzo postale;

indirizzo _____ località _____
_____ provincia _____ CAP _____ Stato _____
_____;

DICHIARA

- di essere informato/a che potrà essere richiesto il pagamento delle spese effettivamente sostenute e documentate per la riproduzione su supporti materiali dei documenti richiesti (carta o CD)¹;
- di aver preso visione dell'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del d.lgs. n. 196 del 2003.

ALLEGA

copia di documento di identità o di riconoscimento (non occorre per le istanze sottoscritte con firma digitale o elettronica qualificata o con identificazione tramite SPID nonché per le istanze consegnate direttamente all'addetto dell'Ufficio e sottoscritte in sua presenza).

(luogo e data)

(firma)

¹ La trasmissione telematica e la copia di file digitali su supporto fornito dal richiedente (CD o dispositivo USB) sono esenti da pagamento.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL**

**ANTRAG AUF ÜBERPRÜFUNG
(für die um Zugang ansuchende Person)**

**An den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz der Autonomen
Region Trentino-Südtirol**

**über
das Sekretariat des Generalsekretariats der Regionalregierung**

giunta@pec.regione.taa.it

u. z. K.

**An die Verantwortliche / An den Verantwortlichen _____
(für die Entscheidung über den Antrag auf allgemeinen Bürgerzugang verantwortliche
Führungskraft)**

Die/Der Unterfertigte

(Pflichtfelder: Vorname, Zuname und mindestens eine Kontaktangabe)

Personalien				
	Vorname	Zuname	Geburtsort	Geburtsdatum
Wohnsitz				
	Adresse	PLZ	Gemeinde	Provinz/ausländ. Staat
Kontaktdaten				
	E-Mail- oder zertifizierte E-Mail-Adresse	Telefon/Mobiltelefon	Fax	

ERSUCHT

in Bezug auf den Antrag auf allgemeinen Bürgerzugang vom _____, Prot. Nr. _____,

**der mit Mitteilung der/des Verantwortlichen _____ Prot. Nr. _____ vom _____
(die mittels _____ zugesandt und am _____
erhalten wurde) mit folgendem Ergebnis beantwortet wurde:**

- ☐ der Zugang wurde gänzlich verweigert
☐ der Zugang wurde teilweise verweigert
☐ der Zugang wurde aufgeschoben

bzw.

☐ der Antrag wurde in der gesetzlich vorgesehenen Frist vom zuständigen Amt nicht beantwortet

um **ÜBERPRÜFUNG des eingereichten Antrags** im Sinne des Art. 5 Abs. 7 des gesetzesvertretenden Dekrets vom 14. März 2013, Nr. 33 i.d.g.F. aus den nachstehenden Gründen:

Sie/Er

ERSUCHT FERNER

darum, dass die Mitteilungen in Zusammenhag mit diesem Antrag wie folgt zugesandt werden:
(Zutreffendes ankreuzen und ausfüllen)

☐ an die nachstehende E-Mail- bzw. zertifizierte E-Mail-Adresse:

☐ per Post an die nachstehende Adresse:

Straße/Platz _____ Ort _____
Provinz _____ PLZ _____ Staat _____

Die/Der Unterfertigte

ERKLÄRT

ferner, dass sie/er darüber in Kenntnis ist, dass für die bestrittenen und nachgewiesenen Kosten für die Wiedergabe der beantragten Dokumente auf Datenträgern (Papier oder CD)¹ eine Gebühr erhoben werden kann;

dass sie/er Einsicht in die Information über die Verarbeitung der personenbezogenen Daten im Sinne des Art. 13 der EU-Verordnung Nr. 679/2016 genommen hat,

und

LEGT

eine Kopie des Personalausweises bei. (Davon wird abgesehen, wenn der Antrag digital oder in einer anderen qualifizierten Form elektronisch signiert ist oder die antragstellende Person mittels SPID identifiziert wird oder wenn der Antrag unmittelbar der/dem Bediensteten des Amtes übergeben und vor dieser/diesem unterzeichnet wird.)

(Ort und Datum)

(Unterschrift)

¹ Die digitale Übermittlung und das Kopieren von digitalen Dateien auf Datenträger (CD oder USB-Stick), die von der antragstellenden Person zur Verfügung gestellt werden, sind gebührenfrei.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL**

**RICHIESTA DI RIESAME
(del controinteressato)**

Al Responsabile per la prevenzione della corruzione e della trasparenza della Regione Autonoma Trentino-Alto Adige/Südtirol

**per il tramite
della Segreteria della Segreteria generale della Giunta**

giunta@pec.regione.taa.it

e p.c.

**Al Responsabile _____
(dirigente responsabile che ha comunicato l'accoglimento dell'istanza di accesso)**

Il sottoscritto/a

(campi obbligatori: nome, cognome e almeno un dato di recapito o contatto)

Dati anagrafici	_____ / ____ / ____			
	nome	cognome	luogo di nascita	data di nascita
Residenza	_____			
	indirizzo	CAP	Comune	Prov./Stato estero
Dati di contatto	_____ @ _____			
	indirizzo PEC/e-mail	telefono/cellulare	fax	

in riferimento al non accoglimento dell'opposizione presentata in data _____ prot. n. _____ come da comunicazione a firma del Responsabile _____ prot. n. _____ del _____, inviata a mezzo _____ e ricevuto in data _____,

e dell'accoglimento dell'istanza di accesso come da comunicazione a firma del Responsabile _____ prot. n. _____ del _____, inviata a mezzo _____ e ricevuto in data _____;

CHIEDE

il RIESAME dell'opposizione e del relativo accoglimento dell'istanza di accesso, ai sensi dell'art. 5, comma 9, del decreto legislativo 14 marzo 2013, n. 33, e successive modificazioni, con le seguenti motivazioni:

CHIEDE INOLTRE,

*che le comunicazioni inerenti la presente richiesta di riesame siano inviate:
(barrare la modalità prescelta e compilare le parti relative)*

☐ *al seguente indirizzo di posta elettronica (PEO) / posta elettronica certificata (PEC);*

☐ *al seguente indirizzo postale;*

indirizzo _____ localit  _____
_____ provincia _____ CAP _____ Stato
_____;

DICHIARA

- di essere informato/a che potr  essere richiesto il pagamento delle spese effettivamente sostenute e documentate per la riproduzione su supporti materiali dei documenti richiesti (carta o CD)¹;
- di aver preso visione dell'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del d.lgs. n. 196 del 2003.

ALLEGA

copia di documento di identit  o di riconoscimento (non occorre per le istanze sottoscritte con firma digitale o elettronica qualificata o con identificazione tramite SPID nonch  per le istanze consegnate direttamente all'addetto dell'Ufficio e sottoscritte in sua presenza).

(luogo e data) (firma)

¹ La trasmissione telematica e la copia di file digitali su supporto fornito dal richiedente (CD o dispositivo USB) sono esenti da pagamento.



**REGIONE AUTONOMA TRENINO-ALTO ADIGE/SÜDTIROL
AUTONOME REGION TRENINO-SÜDTIROL**

**ANTRAG AUF ÜBERPRÜFUNG
(für Drittbetroffene)**

An den Verantwortlichen für die Korruptionsvorbeugung und die Transparenz der Autonomen Region Trentino-Südtirol

**über
das Sekretariat des Generalsekretariats der Regionalregierung**

giunta@pec.regione.taa.it

u. z. K.

**An die Verantwortliche / An den Verantwortlichen _____
(verantwortliche Führungskraft, welche die Annahme des Zugangsantrags mitgeteilt hat)**

Die/Der Unterfertigte

(Pflichtfelder: Vorname, Zuname und mindestens eine Kontaktangabe)

Personalien				
	Vorname	Zuname	Geburtsort	Geburtsdatum
Wohnsitz				
	Adresse	PLZ	Gemeinde	Provinz/ausländ. Staat
Kontaktdaten				
	@ E-Mail- oder zertifizierte E-Mail-Adresse	Telefon/Mobiltelefon	Fax	

ERSUCHT

in Bezug auf die Ablehnung des Einspruchs vom _____, Prot. Nr. _____, laut Mitteilung der/des Verantwortlichen _____ Prot. Nr. _____ vom _____ (die mittels _____ zugesandt und am _____ erhalten wurde)

sowie in Bezug auf die Annahme des Zugangsantrags laut Mitteilung der/des Verantwortlichen _____ Prot. Nr. _____ vom _____ (die mittels _____ zugesandt und am _____ erhalten wurde)

um **ÜBERPRÜFUNG des eingelegten Einspruchs und der Annahme des Zugangsantrags** im Sinne des Art. 5 Abs. 9 des gesetzesvertretenden Dekrets vom 14. März 2013, Nr. 33 i.d.g.F. aus den nachstehenden Gründen:

Sie/Er

ERSUCHT FERNER

darum, dass die Mitteilungen in Zusammenhag mit diesem Antrag wie folgt zugesandt werden:
(Zutreffendes ankreuzen und ausfüllen)

☐ an die nachstehende E-Mail- bzw. zertifizierte E-Mail-Adresse:

☐ per Post an die nachstehende Adresse:

Straße/Platz _____ Ort _____
Provinz _____ PLZ _____ Staat _____

Die/Der Unterfertigte

ERKLÄRT

ferner, dass sie/er darüber in Kenntnis ist, dass für die bestrittenen und nachgewiesenen Kosten für die Wiedergabe der beantragten Dokumente auf Datenträgern (Papier oder CD)¹ eine Gebühr erhoben werden kann;

dass sie/er Einsicht in die Information über die Verarbeitung der personenbezogenen Daten im Sinne des Art. 13 der EU-Verordnung Nr. 679/2016 genommen hat,

und

LEGT

eine Kopie des Personalausweises bei. (Davon wird abgesehen, wenn der Antrag digital oder in einer anderen qualifizierten Form elektronisch signiert ist oder die antragstellende Person mittels SPID identifiziert wird oder wenn der Antrag unmittelbar der/dem Bediensteten des Amtes übergeben und vor dieser/diesem unterzeichnet wird.)

(Ort und Datum)

(Unterschrift)

¹ Die digitale Übermittlung und das Kopieren von digitalen Dateien auf Datenträger (CD oder USB-Stick), die von der antragstellenden Person zur Verfügung gestellt werden, sind gebührenfrei.

Informativa sul trattamento dei dati personali ai sensi dell'art. 13 del Regolamento europeo n. 679/2016 connessa all'ISTANZA DI ACCESSO/RIESAME

Titolare del trattamento

Ai sensi dell'art. 13 del Regolamento (UE) n. 2016/679 – “Regolamento del Parlamento Europeo relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)” (di seguito denominato “Regolamento”), la Regione Autonoma Trentino -Alto Adige/Südtirol di seguito “Regione”, con sede via Gazzoletti n.2, Trento, in qualità di “Titolare” del trattamento dei dati personali, è tenuta a comunicare ai richiedenti accesso informazioni in merito all'utilizzo dei dati personali forniti.

Il Responsabile della protezione dei dati personali

Il Responsabile della Protezione dei Dati RPD-DPO della Regione è Il Consorzio dei comuni trentini

Telefono: 04611920717

E-mail: servizioRPD@comunitrentini.it

PEC: consorzio@pec.comunitrentini.it

Finalità e base giuridica del trattamento

Il trattamento dei dati personali viene effettuato dal Titolare, in relazione all'oggetto dell'istanza di accesso, per l'esecuzione di un compito di interesse pubblico connesso al rispetto del principio della pubblicità e della trasparenza cui soggiace l'attività dei pubblici poteri e pertanto, ai sensi dell'art. 6 comma 1 lett. e) del citato Regolamento non necessita di consenso. I dati personali sono trattati per la seguente finalità: assicurare l'esercizio del diritto di accesso.

Modalità di trattamento

I dati personali vengono trattati con sistemi informatici e/o manuali attraverso procedure adeguate a garantire la sicurezza e la riservatezza degli stessi.

Responsabili esterni del trattamento

La Regione può avvalersi di soggetti terzi per l'espletamento di attività e relativi trattamenti di dati personali di cui mantiene la titolarità. Conformemente a quanto stabilito dalla normativa, tali soggetti assicurano livelli di esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati.

La Regione formalizza istruzioni, compiti ed oneri in capo a tali soggetti terzi con la designazione degli stessi a "Responsabili del trattamento" e sottopone tali soggetti a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia.

Soggetti autorizzati al trattamento

I dati personali sono trattati da personale interno previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei dati personali.

Destinatari dei dati personali

I dati personali trattati non sono oggetto di comunicazione ad altri soggetti pubblici pubblici o privati o di diffusione.

Trasferimento dei dati personali a Paesi extra UE

I dati personali trattati non sono trasferiti al di fuori dell'Unione europea.

Periodo di conservazione

I dati personali sono conservati per il periodo strettamente necessario all'esecuzione del compito o della funzione di interesse pubblico e comunque sulla base della vigente normativa in materia di conservazione della documentazione e degli archivi della pubblica amministrazione e potrà protrarsi, nell'osservanza di tali disposizioni, anche a tempo indeterminato.

All'interessato al trattamento dei dati personali sono riconosciuti i seguenti diritti:

- richiedere la conferma dell'esistenza o meno dei dati che lo riguardano;
- ottenere la loro comunicazione in forma intelligibile;
- richiedere di conoscere le finalità e modalità del trattamento;
- ottenere la rettifica, la cancellazione, la limitazione o la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge;
- richiedere la portabilità dei dati;
- aggiornare, correggere o integrare i dati che lo riguardano;
- opporsi, per motivi legittimi, al trattamento dei dati;
- di proporre reclamo al Garante per la protezione dei dati personali.

Conferimento dei dati

Il conferimento dei dati personali è obbligatorio e necessario per le finalità sopra indicate. Il suo mancato conferimento comporterà l'impossibilità di dare corso alla richiesta di accesso.

LEGGE REGIONALE 31 LUGLIO 1993, N. 13

**Norme in materia di procedimento amministrativo e di
diritto di accesso ai documenti amministrativi^{1 2}**

CAPO I
Disposizioni generali

**Art. 1 (Ambito di applicazione della legge e finalità
dell'attività amministrativa)**

1. Le norme della presente legge si applicano all'attività amministrativa della Regione, degli enti pararegionali e degli enti pubblici per i quali la Regione è competente a dettare norme di ordinamento ai sensi dell'articolo 4, numeri 1, 2 e 8, dell'articolo 5, numeri 1 e 2 e dell'articolo 6 dello Statuto speciale per il Trentino-Alto Adige approvato con decreto del Presidente della Repubblica 31 agosto 1972, n. 670.

1 *bis*. Le norme della presente legge si applicano anche ai soggetti che gestiscono direttamente o in concessione servizi pubblici locali ai sensi dell'articolo 44 della legge regionale 4 gennaio 1993, n. 1.³

2. Gli enti di cui all'articolo 1 diversi dalla Regione curano gli adempimenti previsti dalla presente legge secondo le competenze dei rispettivi organi e strutture, quali fissate dagli ordinamenti che li concernono.

¹ In B.U. 10 agosto 1993, n. 37, suppl. ord. n. 1.

² Si veda il DPR n. 16 novembre 2004, n. 7/L *Approvazione del nuovo regolamento di esecuzione della presente legge regionale*.

³ Comma inserito dall'art. 19, comma 31, della l.r. 23 ottobre 1998, n. 10.

3. Nell'ambito della presente legge le espressioni "amministrazione" e "attività amministrativa" si riferiscono agli enti sopraindicati e alla loro attività amministrativa.

4. L'attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di massima semplicità, di efficacia e di pubblicità, secondo le modalità previste dalla presente legge e dalle altre disposizioni che disciplinano singoli procedimenti.

5. Gli atti devono essere redatti per scritto, salvo che la legge o la natura dell'atto non richiedano una forma diversa.

Art. 2 (Esercizio della discrezionalità procedimentale)

1. Il procedimento amministrativo non può essere aggravato o ritardato rispetto agli adempimenti previsti per legge o per regolamento se non per straordinarie e motivate esigenze imposte dallo svolgimento dell'istruttoria, da accertarsi e comunicarsi agli interessati da parte del responsabile del procedimento.

2. Nei procedimenti ad iniziativa di parte l'amministrazione può procedere ad attività istruttorie che non siano previste dalla legge, qualora vi sia il consenso dell'istante.

Art. 3 (Conclusione del procedimento)

1. Ove il procedimento consegua obbligatoriamente ad una istanza, ovvero debba essere iniziato d'ufficio, l'amministrazione ha il dovere di concluderlo mediante l'adozione di un provvedimento espresso.

2. L'amministrazione determina, per ciascun tipo di procedimento, il termine entro il quale esso deve concludersi,

qualora esso non sia già determinato da legge o regolamento. Tale termine decorre d'ufficio dall'inizio del procedimento o, se il procedimento è ad iniziativa di parte, dal ricevimento della domanda.

3. Sino a quando il termine non è determinato ai sensi del comma 2, esso si intende stabilito in trenta giorni.

4. Ove l'istante debba regolarizzare o integrare la domanda o la documentazione prodotta per consentire il perfezionamento dell'atto, il termine è sospeso dalla data di invio della comunicazione agli interessati fino alla data di ricevimento della documentazione richiesta.

5. Qualora fatti o atti eccezionalmente sopravvenuti incidano sullo svolgimento dell'istruttoria, il termine può essere sospeso, con provvedimento motivato, dal dirigente della struttura amministrativa competente in via principale. Tale circostanza è comunicata all'interessato contestualmente alla richiesta di acquisizione di pareri o di documenti integrativi. Il termine riprende a decorrere dalla data di ricezione dei predetti pareri o documenti.

6. Le domande e le istanze rivolte ad organo della stessa amministrazione diverso da quello competente o pervenute a struttura diversa da quella competente a riceverle, non possono essere dichiarate inammissibili per tale motivo e sono trasmesse d'ufficio all'organo o alla struttura rispettivamente competente.

7. Decorsi i termini di cui ai commi 2 e 3, sono esperibili i ricorsi previsti dalla legge.

8. Le determinazioni adottate ai sensi del comma 2 dagli organi della Regione sono pubblicate nel Bollettino Ufficiale della Regione; le altre amministrazioni curano che alle corrispondenti determinazioni sia data adeguata forma di pubblicità.

Art. 4 (Proroga dei termini per domande ed istanze)

1. In caso di calamità pubbliche, interruzioni dei servizi pubblici, impossibilità di funzionamento degli uffici o altra grave emergenza, la Giunta regionale, con propria deliberazione, può riaprire o prorogare i termini, previsti anche da legge, per la presentazione di domande, istanze o ricorsi.

Art. 5 (Motivazione dei provvedimenti)

1. Ogni provvedimento amministrativo, compresi quelli concernenti l'organizzazione amministrativa, lo svolgimento dei pubblici concorsi ed il personale, deve essere motivato.

2. La motivazione indica i presupposti di fatto e le ragioni giuridiche che hanno determinato la decisione dell'amministrazione, in relazione alle risultanze dell'istruttoria.

3. Quando il provvedimento è discrezionale, la motivazione indica, oltre ai presupposti di fatto e alle ragioni giuridiche, le valutazioni di carattere amministrativo o tecnico che hanno condotto alla decisione espressa nel provvedimento.

4. Se le ragioni della decisione risultano da altro atto dell'amministrazione richiamato dalla decisione stessa, insieme con la comunicazione di quest'ultima, deve essere indicato e reso disponibile anche l'atto a cui essa si richiama.

5. La motivazione non è richiesta per gli atti normativi e per quelli a contenuto generale.

6. Ogni provvedimento deve indicare l'autorità amministrativa ed il termine entro cui è possibile ricorrere.

Art. 6 (Accordi amministrativi)

1. In accoglimento di osservazioni e proposte presentate a norma dell'articolo 16, l'amministrazione precedente può

concludere con gli interessati, senza pregiudizio dei diritti dei terzi, e in ogni caso nel perseguimento del pubblico interesse, accordi al fine di determinare il contenuto discrezionale del provvedimento finale, ovvero, nei casi previsti dalla legge, in sostituzione di questo.

1 *bis*. Al fine di favorire la conclusione degli accordi di cui al comma 1, il responsabile del procedimento può disporre un calendario di incontri cui invita, separatamente o contestualmente, il destinatario del provvedimento ed eventuali controinteressati.⁴

2. Gli accordi di cui al presente articolo devono essere stipulati, a pena di nullità, per atto scritto, salvo che la legge disponga altrimenti. Ad essi si applicano, ove non diversamente previsto, i principi del codice civile in materia di obbligazioni e contratti, in quanto compatibili.

3. Gli accordi sostitutivi di provvedimenti sono soggetti ai medesimi controlli previsti per questi ultimi.

4. Per sopravvenuti motivi di pubblico interesse, l'amministrazione recede unilateralmente dall'accordo, salvo l'obbligo di provvedere alla liquidazione di un indennizzo in relazione agli eventuali pregiudizi verificatisi in danno del privato.

5. L'amministrazione può sempre concludere accordi con altre pubbliche amministrazioni, ai sensi e con le modalità previste dall'articolo 15 della legge 7 agosto 1990, n. 241, per disciplinare lo svolgimento in collaborazione di attività di interesse comune.

6. Gli accordi di cui al comma 1 sono sottoscritti dal titolare dell'organo competente a provvedere. Se si tratta di organo

⁴ Comma inserito dall'art. 19, comma 32 della l.r. 23 ottobre 1998, n. 10.

collegiale, sono sottoscritti dal presidente, previa deliberazione del collegio.

7. Gli accordi di cui al comma 5 sono stipulati dal legale rappresentante, previa deliberazione dell'organo competente.

8. L'amministrazione può altresì partecipare agli accordi di programma previsti dall'articolo 43 della legge regionale 4 gennaio 1993, n. 1.

9. In virtù dell'articolo 11, comma 5 della legge 7 agosto 1990, n. 241 le controversie in materia di formazione, conclusione ed esecuzione degli accordi di cui al presente articolo sono riservate alla giurisdizione esclusiva del giudice amministrativo.

Art. 7 (Erogazione di benefici economici e trasferimenti)

1. Quando non siano disposte con legge o sulla base di criteri analiticamente definiti dalla legge che li prevede, la concessione di sovvenzioni, contributi, sussidi e l'attribuzione di vantaggi economici di qualunque genere a persone ed enti pubblici e privati sono precedute dalla predeterminazione e dalla pubblicazione dei criteri e delle modalità cui l'amministrazione deve attenersi.

2. L'effettiva osservanza dei criteri e delle modalità di cui al comma 1 deve risultare dai singoli provvedimenti relativi agli interventi di cui al medesimo comma 1.

3. Gli enti e i soggetti destinatari di trasferimenti per il finanziamento di attività di gestione, da determinarsi annualmente e direttamente con legge di bilancio, presentano all'ente trasferente, entro il 31 luglio di ciascun anno, le proprie indicazioni ai fini della determinazione dei finanziamenti per l'esercizio successivo, con la specificazione degli elementi

previsionali relativi alle attività da realizzare nel medesimo esercizio.

Art. 8 (Commissione regionale per il procedimento e l'accesso ai documenti amministrativi)

1. E' istituita presso la Presidenza della Giunta regionale la commissione per l'accesso ai documenti amministrativi.

2. La commissione, costituita da esperti in materie giuridico-amministrative, è nominata con decreto del Presidente della Giunta regionale, previa deliberazione della Giunta. Essa è presieduta dal Presidente della Giunta regionale o da un Assessore da lui delegato ed è composta da:

- a) due rappresentanti della Regione, di cui uno designato dalle minoranze politiche rappresentate nel Consiglio regionale;
- b) un rappresentante designato dalle Giunte provinciali;
- c) un rappresentante designato dalle associazioni rappresentative dei comuni;
- d) un rappresentante designato dalle associazioni provinciali rappresentative delle istituzioni pubbliche di assistenza e beneficenza I.P.A.B.;
- e) un rappresentante delle camere di commercio;
- f) un professore universitario di ruolo in materie giuridico-amministrative.

Le funzioni di segretario sono svolte da un dipendente regionale appartenente ad una qualifica funzionale non inferiore alla settima, in servizio presso l'Ufficio legislativo-legale.

3. La commissione vigila affinché venga attuato il principio di piena conoscibilità dell'attività della pubblica

amministrazione con il rispetto dei limiti fissati dalla presente legge; elabora proposte per la piena attuazione della presente legge; formula i pareri richiesti dalla Giunta regionale, dalle amministrazioni comunali, dalle camere di commercio e dagli enti pararegionali in materia di procedimento amministrativo e di accesso ai documenti amministrativi; redige per gli stessi enti una relazione annuale sulla trasparenza dell'attività amministrativa che viene comunicata alla Giunta regionale, al Consiglio regionale, alle associazioni provinciali rappresentative dei comuni, alle camere di commercio e agli enti para-regionali; predispone schemi di regolamenti-tipo per l'attuazione della presente legge; propone alla Giunta regionale modifiche ai testi legislativi e regolamentari che siano utili a realizzare la più ampia garanzia del diritto di accesso di cui all'articolo 26; cura la raccolta degli atti di cui al comma 1 dell'articolo 29 adottati dai comuni e dalle I.P.A.B.

4. La commissione rimane in carica per la durata della legislatura nel corso della quale viene nominata.

5. La composizione della commissione deve adeguarsi alla consistenza dei gruppi linguistici quale risulta dall'ultimo censimento generale della popolazione ed al rapporto esistente fra la popolazione delle due Province.

6. Tutte le amministrazioni di cui all'articolo 1 sono tenute a comunicare alla commissione le informazioni e i documenti da essa richiesti, ad eccezione di quelli coperti da segreto d'ufficio.

Art. 9 (Rispetto della normativa sull'uso della lingua)

1. Le disposizioni contenute nella presente legge si applicano in ogni caso nel rispetto delle norme dello Statuto

speciale e delle relative norme di attuazione in materia di uso delle lingue negli atti della pubblica amministrazione.

CAPO II

Responsabile del procedimento

Art. 10 (Identificazione dei procedimenti)

1. L'amministrazione provvede ad identificare i procedimenti assegnati alle singole strutture organizzative.

2. A tal fine, approva e aggiorna una apposita tabella, recante l'indicazione dei procedimenti di competenza di ciascuna struttura amministrativa.

3. La tabella è posta a disposizione del pubblico, in forma aggiornata, presso ciascuna struttura amministrativa.

4. Alla tabella relativa ai procedimenti è data pubblicità ai sensi dell'articolo 3, comma 8.

Art. 11 (Responsabile del procedimento)

1. Ove non sia diversamente disposto da leggi o regolamenti, responsabile di ciascun tipo di procedimento di competenza dell'amministrazione è il responsabile della struttura amministrativa competente per la trattazione, secondo la tabella prevista dall'articolo 10.

2. Il responsabile della struttura amministrativa può assegnare la responsabilità del procedimento, di norma per tipi di procedimento, a dipendenti facenti parte della struttura amministrativa medesima.

3. Il dipendente incaricato ai sensi del comma 2 ha responsabilità piena ed esclusiva della conduzione del procedimento.

4. Tuttavia, il responsabile della struttura amministrativa può in ogni momento richiamare a sé la responsabilità del procedimento.

5. La struttura amministrativa competente e il nominativo del responsabile del procedimento sono comunicati ai soggetti di cui all'articolo 13 e, a richiesta, a chiunque vi abbia interesse.

Art. 12 (Compiti del responsabile del procedimento)

1. Il responsabile del procedimento:

- a) valuta, ai fini istruttori, le condizioni di ammissibilità, i requisiti di legittimazione ed i presupposti che siano rilevanti per l'emanazione del provvedimento;
 - b) accerta d'ufficio i fatti, disponendo il compimento degli atti all'uopo necessari, e adotta ogni misura per l'adeguato e sollecito svolgimento dell'istruttoria. In particolare, può chiedere il rilascio di dichiarazioni e la rettifica di dichiarazioni o istanze erranee o incomplete, può esperire accertamenti tecnici ed ispezioni ed ordinare esibizioni documentali;
 - c) propone l'indizione o, avendone la competenza, indice la conferenza di servizi di cui all'articolo 19;
 - d) cura i rapporti con tutti i soggetti che hanno interesse al provvedimento; cura le comunicazioni, le pubblicazioni e le notificazioni previste dalle leggi e dai regolamenti;
 - e) formula le proprie valutazioni, sigla la proposta di provvedimento e trasmette gli atti all'organo competente
-
-

per l'adozione, ovvero, qualora ne abbia la competenza, lo adotta;

- f) segue l'andamento presso le strutture organizzative competenti delle fasi del procedimento che non rientrano nella sua diretta competenza, dando impulso all'azione amministrativa per assicurarne il corretto svolgimento. In particolare, il responsabile del procedimento concorda, per tipi di procedimento o per i singoli procedimenti, con le strutture organizzative competenti nelle fasi successive, la ripartizione dei tempi a disposizione di ciascuno, sollecitandone, ove occorra, il rispetto. Per le fasi del procedimento che non rientrino nella sua diretta disponibilità, il responsabile del procedimento risponde limitatamente ai compiti previsti dalla presente lettera f .

CAPO III

Partecipazione al procedimento amministrativo

Art. 13 (Comunicazione dell'avvio del procedimento)

1. Ove non sussistano ragioni di impedimento derivanti da particolari esigenze di celerità del procedimento, l'avvio del procedimento stesso è comunicato ai soggetti nei confronti dei quali il provvedimento finale è destinato a produrre effetti diretti ed a quelli che per legge debbono intervenire.

2. Ove parimenti non sussistano le ragioni di impedimento predette, qualora da un provvedimento possa derivare un pregiudizio a soggetti individuati, o facilmente individuabili, diversi dai suoi diretti destinatari, l'amministrazione è tenuta a

comunicare loro, con le stesse modalità, l'inizio del procedimento.

3. Resta in ogni caso salva la facoltà dell'amministrazione di adottare, anche prima dell'effettuazione delle comunicazioni di cui ai commi 1 e 2, provvedimenti cautelari.

4. Nei procedimenti ad istanza di parte il responsabile del procedimento o l'autorità competente, prima della formale adozione di un provvedimento negativo, comunica tempestivamente agli interessati i motivi che ostano all'accoglimento della domanda. Entro il termine di trenta giorni dal ricevimento della comunicazione, eccezionalmente prorogabile per una sola volta, su richiesta motivata, gli interessati hanno il diritto di presentare per iscritto le loro osservazioni, eventualmente corredate da documenti. Dell'eventuale mancato accoglimento di dette osservazioni si deve dare ragione nella motivazione del provvedimento finale. Tali disposizioni non si applicano alle procedure concorsuali.

5. Nella comunicazione debbono essere indicati:

- a) l'amministrazione competente;
- b) l'oggetto del procedimento promosso;
- c) la struttura amministrativa competente per il procedimento in via principale e la persona responsabile del procedimento;
- d) l'ufficio in cui si può prendere visione degli atti;
- e) il termine entro il quale il procedimento deve essere concluso;
- f) le fasi del procedimento e i tempi ad esse necessarie, anche se riguardanti altre amministrazioni.

6. L'omissione di taluna delle comunicazioni prescritte può essere fatta valere solo dal soggetto nel cui interesse la comunicazione è prevista.

Art. 14 (Modalità della comunicazione)

1. L'amministrazione provvede a dare notizia dell'avvio del procedimento mediante comunicazione personale.

2. La comunicazione ai soggetti interessati dell'avvio del procedimento è effettuata dal responsabile dello stesso.

3. La comunicazione è effettuata mediante lettera, regolarmente protocollata in uscita. Può essere effettuata mediante raccomandata con avviso di ricevimento o notifica tramite messo comunale, quando appaia indispensabile la prova dell'avvenuto ricevimento.

4. Ove il soggetto interessato si presenti personalmente presso l'unità organizzativa competente, la comunicazione può essere consegnata a mani, con contestuale sottoscrizione del ricevimento.

5. Qualora, per il numero dei destinatari, la comunicazione personale non sia possibile o risulti particolarmente gravosa, l'amministrazione provvede a rendere noti gli elementi di cui al comma 4 dell'articolo 13 mediante forme di pubblicità idonee, di volta in volta stabilite dall'amministrazione procedente. Si procede comunque alla comunicazione personale, qualora il numero dei destinatari sia inferiore a dieci.

Art. 15 (Intervento nel procedimento)

1. I portatori di interessi pubblici o privati e i portatori d'interessi diffusi costituiti in associazioni o comitati, cui possa derivare un pregiudizio da un provvedimento, hanno facoltà di intervenire nel procedimento.

Art. 16 (Diritti di partecipazione)

1. I soggetti di cui all'articolo 13 e quelli intervenuti ai sensi dell'articolo 15 hanno diritto:

- a) di conoscere lo stato del procedimento;
- b) di prendere visione e di estrarre copia degli atti del procedimento, salvo quanto disposto dall'articolo 27;
- c) di presentare memorie scritte e documenti relativi all'oggetto del procedimento, che l'amministrazione ha il dovere di valutare ove siano pertinenti all'oggetto del procedimento;

2. Le modalità di esercizio del diritto ad avere copia degli atti di cui al punto b saranno disciplinate dagli statuti o regolamenti dei rispettivi enti.

Art. 17 (Atti a regime particolare)

1. Le disposizioni contenute nel presente capo non si applicano nei confronti dell'attività della amministrazione diretta alla emanazione di atti normativi, amministrativi generali, di programmazione, per i quali restano ferme le particolari norme che ne regolano la formazione.

2. Dette disposizioni non si applicano altresì ai procedimenti tributari, per i quali restano parimenti ferme le particolari norme che li regolano.

Art. 18 (Rapporto tra servizi)

1. Ove il dirigente di una struttura amministrativa, nell'esercizio delle proprie attribuzioni ovvero su segnalazione del responsabile del procedimento, venga a conoscenza di situazioni che ritenga possano richiedere interventi di

competenza di altre strutture, ne informa per iscritto i relativi dirigenti.

Art. 19 (Conferenza di servizi)

1. Qualora sia opportuno effettuare un esame contestuale di vari interessi pubblici coinvolti in un procedimento amministrativo, l'amministrazione procedente indice di regola una conferenza di servizi.

2. La conferenza stessa può essere indetta anche quando l'amministrazione procedente debba acquisire intese, concerti, nulla osta o assensi comunque denominati di altre amministrazioni pubbliche. In tal caso, le determinazioni concordate nella conferenza tra tutte le amministrazioni intervenute tengono luogo degli atti predetti.

3. Si considera acquisito l'assenso dell'amministrazione la quale, regolarmente convocata, non abbia partecipato alla conferenza o vi abbia partecipato tramite rappresentanti privi della competenza ad esprimerne definitivamente la volontà, salvo che essa non comunichi all'amministrazione procedente il proprio motivato dissenso entro venti giorni dalla conferenza stessa, ovvero dalla data di ricevimento della comunicazione delle determinazioni adottate, qualora queste ultime abbiano contenuto sostanzialmente diverso da quello originariamente previsto.

4. Le disposizioni di cui al comma 3 non si applicano alle amministrazioni preposte alla tutela ambientale, paesaggistico-territoriale e della salute dei cittadini.

CAPO IV
Semplificazione dell'azione amministrativa

Art. 20 (Disciplina dei pareri obbligatori)

1. Nei casi in cui debba essere obbligatoriamente sentito un organo consultivo, questo deve emettere il proprio parere entro il termine prefissato da disposizioni di legge o di regolamento o, in mancanza, non oltre sessanta giorni dal ricevimento della richiesta.

2. L'organo adito, nel caso in cui abbia rappresentato esigenze istruttorie ovvero l'impossibilità, dovuta alla natura dell'affare, di rispettare il termine generale di cui al comma 1, deve emettere il proprio parere non oltre trenta giorni dalla ricezione delle notizie o dei documenti richiesti, ovvero dalla scadenza del termine generale.

3. In caso di definitiva decorrenza del termine generale di cui al comma 1 o, ricorrendone le condizioni, dell'ulteriore termine di trenta giorni di cui al comma 2 senza che sia stato comunicato il parere, è in facoltà dell'amministrazione richiedente di procedere indipendentemente dall'acquisizione dello stesso.

4. Le disposizioni di cui ai commi 1 e 3 non si applicano in caso di pareri che debbano essere rilasciati da amministrazioni preposte alla tutela ambientale, paesaggistico-territoriale e della salute dei cittadini.

5. Qualora il parere sia favorevole, senza osservazioni, il dispositivo è comunicato telegraficamente o con mezzi telematici.

6. L'amministrazione approva procedure idonee ad assicurare che i pareri richiesti ad organi consultivi dell'amministrazione siano resi nei termini previsti.

Art. 21 (Richiesta di valutazioni tecniche ad altri organi in caso di decorrenza dei termini)

1. Ove la legge o il regolamento prevedano che per l'adozione di un provvedimento debbano essere preventivamente acquisite le valutazioni tecniche di organi od enti appositi, questi devono fornire le valutazioni anzidette entro il termine prefissato da disposizioni di legge o di regolamento o, in mancanza, non oltre sessanta giorni dal ricevimento della richiesta.

2. L'organo adito, nel caso in cui abbia rappresentato esigenze istruttorie ovvero l'impossibilità, dovuta alla natura dell'affare, di rispettare il termine generale di cui al comma 1, deve fornire le valutazioni tecniche non oltre trenta giorni dalla ricezione delle notizie o dei documenti richiesti, ovvero dalla scadenza del termine generale.

3. In caso di definitiva decorrenza del termine generale di cui al comma 1 o, ricorrendone le condizioni, dell'ulteriore termine di trenta giorni di cui al comma 2 senza che le valutazioni tecniche siano state comunicate, il responsabile del procedimento provvede a richiederle ad altri organi dell'amministrazione o ad enti pubblici che siano dotati di qualificazione e capacità tecnica equipollenti, ovvero ad istituti universitari.

4. Le disposizioni di cui ai commi 1, 2 e 3 non si applicano in caso di valutazioni che debbano essere prodotte da

amministrazioni preposte alla tutela ambientale, paesaggistico-territoriale e della salute dei cittadini.

5. Il responsabile del procedimento può tuttavia assegnare un nuovo termine, non superiore a trenta giorni, all'organismo originariamente competente, quando ciò appaia preferibile in vista della più rapida conclusione del procedimento.

Art. 22 (Misure organizzative per l'applicazione delle disposizioni di autocertificazione)

1. L'amministrazione adotta le misure organizzative idonee a garantire l'applicazione delle disposizioni in materia di autocertificazione e di presentazione di atti e documenti da parte di cittadini a pubbliche amministrazioni di cui alla legge 4 gennaio 1968, n. 15 e successive modificazioni e integrazioni.

2. Qualora l'interessato dichiara che fatti, stati e qualità sono attestati in documenti già in possesso della amministrazione o di altra pubblica amministrazione, il responsabile del procedimento provvede d'ufficio all'acquisizione dei documenti stessi o di copia di essi.

3. Parimenti sono accertati d'ufficio dal responsabile del procedimento, ferma restando la facoltà dell'interessato di provvedere personalmente, i fatti, gli stati e le qualità che l'amministrazione o altra pubblica amministrazione procedente è tenuta a certificare.

4. Il termine per la conclusione del procedimento rimane sospeso durante il periodo necessario all'acquisizione dei documenti e all'accertamento d'ufficio di cui ai commi 2 e 3, quando sia richiesta l'attività di amministrazione diversa da quella procedente. La sospensione è comunicata all'interessato.

5. E' fatto divieto all'amministrazione di esigere atti di notorietà in luogo della dichiarazione sostitutiva dell'atto di notorietà prevista dall'articolo 4 della legge 4 gennaio 1968, n. 15, quando si tratti di provare qualità personali, stati o fatti che siano a diretta conoscenza dell'interessato.

Art. 23 (Inizio di attività previa denuncia)

1. Con regolamento, da emanarsi entro novanta giorni dall'entrata in vigore della presente legge, sono determinati i casi in cui l'esercizio di un'attività privata, subordinato ad autorizzazione, licenza, abilitazione, nulla osta, permesso o altro atto di consenso comunque denominato, può essere intrapreso su denuncia di inizio dell'attività stessa da parte dell'interessato alla struttura organizzativa competente. In tali casi, spetta al servizio competente per il procedimento in via principale verificare d'ufficio la sussistenza dei presupposti e dei requisiti di legge richiesti e disporre, se ricorrono i presupposti, con provvedimento motivato, il divieto di prosecuzione dell'attività e la rimozione dei suoi effetti, salvo che, ove ciò sia possibile, l'interessato non provveda a conformare alla normativa vigente detta attività ed i suoi effetti entro il termine prefissatogli dal servizio stesso.

2. Con il regolamento di cui al comma 1 vengono indicati i casi in cui all'attività può darsi inizio immediatamente dopo la presentazione della denuncia, ovvero dopo il decorso di un termine fissato per categorie di atti, in relazione alla complessità degli accertamenti richiesti.

3. Le disposizioni del presente articolo si applicano nei casi in cui il rilascio dell'atto di assenso dell'amministrazione dipenda esclusivamente dall'accertamento dei presupposti e dei

requisiti prescritti, senza l'esperimento di prove a ciò destinate, e non sia previsto alcun limite o contingente complessivo per il rilascio dell'atto stesso.

Art. 24 (Accoglimento automatico di domande per il rilascio di autorizzazioni e licenze)

1. Con regolamento da emanarsi entro novanta giorni dall'entrata in vigore della presente legge, sono determinati i casi in cui le domande di rilascio di una autorizzazione, licenza, abilitazione, nulla osta, permesso od altro atto di consenso comunque denominato, cui sia subordinato lo svolgimento di un'attività privata, si considera accolta, qualora non venga comunicato all'interessato il provvedimento di diniego entro il termine fissato per categorie di atti, in relazione alla complessità del rispettivo procedimento, dal medesimo predetto regolamento. In tali casi, sussistendo le ragioni di pubblico interesse, il dirigente del servizio competente in via principale può annullare l'atto di assenso illegittimamente formatosi, salvo che, ove ciò sia possibile, l'interessato provveda a sanare i vizi esistenti entro il termine prefissatogli dall'amministrazione stessa.

2. Restano ferme le disposizioni attualmente vigenti che stabiliscono regole analoghe od equipollenti a quelle previste dal presente articolo.

Art. 25 (Adempimenti nei casi di denuncia o domanda da parte dell'interessato)

1. Con la denuncia o con la domanda di cui agli articoli 23 e 24 l'interessato deve dichiarare la sussistenza dei presupposti e

dei requisiti di legge richiesti. Salva la responsabilità penale di cui all'articolo 21 della legge 7 agosto 1990, n. 241 in caso di dichiarazioni mendaci o di false attestazioni, non è ammessa la conformazione dell'attività e dei suoi effetti a legge ai sensi dell'articolo 23, nè la sanatoria ai sensi dell'articolo 24.

2. Le sanzioni attualmente previste in caso di svolgimento dell'attività in carenza dell'atto di assenso dell'amministrazione o in difformità da esso si applicano anche nei riguardi di coloro i quali diano inizio all'attività ai sensi degli articoli 23 e 24 in mancanza dei requisiti richiesti o, comunque, in contrasto con la normativa vigente.

CAPO V

Accesso ai documenti amministrativi

Art. 26 (Diritto di accesso)

1. Al fine di assicurare la trasparenza dell'attività amministrativa e di favorirne lo svolgimento imparziale, è riconosciuto, a chiunque abbia interesse al procedimento, il diritto di accesso ai documenti amministrativi, secondo le modalità stabilite dalla presente legge.

2. E' considerato documento amministrativo ogni rappresentazione grafica, fotocinematografica, elettro-magnetica o di qualunque altra specie del contenuto di atti, anche interni, formati dall'amministrazione o, comunque, utilizzati ai fini dell'attività amministrativa.

3. Entro sei mesi dalla data di entrata in vigore della presente legge, l'amministrazione adotta le misure organizzative idonee a garantire l'applicazione della disposizione di cui al

comma 1, dandone comunicazione alla commissione di cui all'articolo 8.

Art. 27 (Limiti al diritto di accesso)

1. Il diritto di accesso è escluso per i documenti coperti da segreto di Stato ai sensi dell'articolo 12 della legge 24 ottobre 1977, n. 801, nonché negli altri casi di segreto o di divieto di divulgazione altrimenti previsti dall'ordinamento.

2. L'amministrazione adotta le misure organizzative idonee a dare attuazione ai regolamenti emanati in base all'articolo 24, commi 2 e 3, della legge 7 agosto 1990, n. 241.

3. Con le misure di cui al comma 2 sono stabilite norme particolari per assicurare che l'accesso ai dati raccolti mediante strumenti informatici avvenga nel rispetto delle esigenze di cui al comma 2 dell'articolo 24 della legge 7 agosto 1990, n. 241.

4. L'amministrazione individua, altresì, con le misure di cui al comma 2, le categorie di documenti dalla medesima formati o comunque rientranti nella disponibilità della stessa sottratti all'accesso per le esigenze di cui al comma 2 dell'articolo 24 della legge 7 agosto 1990, n. 241.

5. Non è comunque ammesso l'accesso agli atti preparatori nel corso della formazione dei provvedimenti di cui all'articolo 17, salvo diverse disposizioni di legge.

Art. 28 (Esercizio del diritto di accesso)

1. Il diritto di accesso si esercita mediante esame ed estrazione di copia dei documenti amministrativi, nei modi e con i limiti indicati dalla presente legge. L'esame dei documenti è gratuito. Il rilascio di copia è subordinato soltanto al rimborso

del costo di riproduzione, salve le disposizioni vigenti in materia di bollo, nonché i diritti di ricerca e di visura.

2. La richiesta di accesso ai documenti deve essere motivata. Essa deve essere rivolta all'amministrazione che ha formato il documento o che lo detiene stabilmente.

3. Il rifiuto e la limitazione dell'accesso sono opposti dal responsabile della struttura nei casi e nei limiti stabiliti dall'articolo 27 e devono essere motivati.

4. Trascorsi inutilmente venti giorni dalla richiesta, questa si intende rifiutata.

5. Contro il diniego di accesso espresso o tacito è ammesso ricorso al rispettivo organo di governo che è tenuto a pronunciarsi entro trenta giorni dalla notifica del ricorso, fermo restando quanto previsto dal comma 4 dell'articolo 25 della legge 7 agosto 1990, n. 241. Avverso la decisione espressa o tacita del rispettivo organo di governo, nonché nel caso di silenzio di cui al comma 4 è esperibile il ricorso previsto dall'articolo 25, comma 5, della legge 7 agosto 1990, n. 241.

Art. 29 (Pubblicità delle disposizioni sull'organizzazione e sulle funzioni dell'amministrazione)

1. Le amministrazioni di cui alla presente legge provvedono ad adottare adeguate forme di pubblicità per le circolari ed istruzioni organizzative, le direttive, i programmi ed ogni atto che dispone in generale sulla organizzazione, sulle funzioni, sugli obiettivi, sui procedimenti, ovvero nel quale si determina l'interpretazione di norme giuridiche.

2. L'amministrazione cura altresì la raccolta sistematica degli atti di cui al presente articolo che rimane a disposizione di chiunque vi abbia interesse.

3. Con la pubblicità di cui al comma 1, ove essa sia integrale, la libertà di accesso ai documenti indicati nel comma 1 si intende realizzata.

4. L'amministrazione regionale curerà la pubblicazione delle raccolte degli atti di cui al presente articolo adottati dai comuni e dalle I.P.A.B.

Art. 30 (Uffici per le relazioni con il pubblico)

1. Le amministrazioni pubbliche di cui all'articolo 1, al fine di garantire la piena attuazione della presente legge, individuano, nell'ambito del proprio ordinamento, uffici per le relazioni con il pubblico.

2. Gli uffici per le relazioni con il pubblico provvedono, anche mediante l'utilizzo di tecnologie informatiche:

- a) al servizio all'utenza per i diritti di partecipazione di cui al capo III della presente legge;
- b) all'informazione all'utenza relativa agli atti e allo stato dei procedimenti;
- c) alla ricerca ed analisi finalizzate alla formulazione di proposte alla propria amministrazione sugli aspetti organizzativi e logistici del rapporto con l'utenza.

3. Al fine di assicurare la conoscenza di normative, servizi e strutture, le amministrazioni pubbliche programmano ed attuano iniziative di comunicazione di pubblica utilità.

Art. 31 (Obbligo di identificazione)

1. I funzionari e dipendenti della amministrazione aventi diretto contatto con il pubblico sono tenuti ad esporre un cartello

da tavolo con il loro nome e la loro qualifica, ovvero un cartellino di riconoscimento personale ben visibile.

2. Entro novanta giorni dall'entrata in vigore della presente legge, l'amministrazione predisporrà il necessario materiale idoneo all'identificazione dei funzionari e dipendenti di cui al comma 1.

CAPO VI

Disposizioni transitorie e finali

Art. 32 (Disposizioni transitorie per la prima applicazione)

1. L'amministrazione determina il termine per i procedimenti previsti dalla legislazione vigente, ai sensi dell'articolo 3, entro centottanta giorni dall'entrata in vigore della legge.

2. La tabella recante l'indicazione dei procedimenti di competenza di ciascuna struttura organizzativa prevista dall'articolo 10 è approvata entro centottanta giorni dall'entrata in vigore della legge.

3. Le norme sul diritto di accesso ai documenti amministrativi di cui al Capo V hanno effetto dopo tre mesi dall'emanazione dei regolamenti di cui all'articolo 24, commi 2 e 3, della legge 7 agosto 1990, n. 241.

Art. 33 (Entrata in vigore)

1. La presente legge entra in vigore il trentesimo giorno successivo alla pubblicazione nel Bollettino Ufficiale della Regione.

**DECRETO DEL PRESIDENTE DELLA REGIONE
16 NOVEMBRE 2004, N. 7/L**

**Approvazione del nuovo regolamento di esecuzione della
legge regionale 31 luglio 1993, n. 13, recante norme in
materia di procedimento amministrativo e di diritto di
accesso ai documenti amministrativi¹**

**CAPO I
DISPOSIZIONI PRELIMINARI**

Articolo 1 (Ambito di applicazione e finalità)

1. Il presente regolamento disciplina i procedimenti amministrativi di competenza della Regione Trentino-Alto Adige/Südtirol nonché le modalità di esercizio e le limitazioni del diritto di accesso ai documenti amministrativi e prevede le misure organizzative per l'applicazione delle disposizioni sull'autocertificazione, al fine di attuare i principi di pubblicità, di trasparenza e semplificazione dell'attività amministrativa di cui alla legge regionale 31 luglio 1993, n. 13, di seguito denominata legge.

¹ In B.U. 7 dicembre 2004, n. 49 - suppl. n. 2.

CAPO II
PROCEDIMENTO AMMINISTRATIVO

Art. 2 (Termine per la conclusione del procedimento)

1. I procedimenti amministrativi, ad iniziativa di parte o promossi d'ufficio, si concludono con un provvedimento espresso e motivato nel termine stabilito, per ciascun tipo di procedimento, nella tabella di cui all'allegato 1, costituente parte integrante del presente regolamento che contiene altresì l'indicazione della fonte normativa del procedimento, della struttura organizzativa competente nonché del responsabile del procedimento medesimo. La tabella anzidetta è posta a disposizione del pubblico presso ogni struttura organizzativa dell'amministrazione, pubblicata nel Bollettino Ufficiale della Regione, nel sito Internet della Regione e nelle apposite bacheche situate negli uffici della Regione a Trento e Bolzano.

2. In caso di mancata inclusione del procedimento nella tabella di cui al comma 1 nonché di assenza di determinazione del termine nella normativa specifica vigente il procedimento stesso si concluderà nel termine di 30 giorni previsto dall'art. 3, comma 3, della legge.

3. I termini di cui ai commi 1 e 2 del presente articolo costituiscono termini massimi e non esonerano l'amministrazione dall'obbligo di provvedere con speditezza.

4. Ove non sia diversamente disposto, per i procedimenti di modifica di provvedimenti già emanati, si applicano i medesimi termini finali previsti per il procedimento finale.

Articolo 3 (Decorrenza del termine iniziale dei procedimenti)

1. Il termine iniziale dei procedimenti promossi d'ufficio decorre dalla data in cui si sia manifestato per l'amministrazione l'obbligo di provvedere.

2. Il termine iniziale dei procedimenti ad iniziativa di parte decorre dalla data di ricevimento della domanda o istanza. Nel caso in cui la domanda sia stata presentata ad organo o a struttura organizzativa dell'amministrazione diverso da quello competente, sarà trasmessa d'ufficio, immediatamente, a quello competente.

3. Nel caso di domande da presentarsi entro un termine prestabilito, il termine iniziale del procedimento inizia a decorrere il giorno successivo a quello di scadenza per la presentazione delle domande stesse. Nel caso in cui la domanda, da presentarsi entro un termine prestabilito, pervenga, nei termini, a organo o struttura dell'amministrazione, diverso da quello competente, non può per tale motivo essere dichiarata inammissibile e verrà trasmessa, immediatamente, all'organo o struttura competente.

4. La domanda, corredata dalla prevista documentazione, può essere presentata direttamente, mediante raccomandata con avviso di ricevimento, nonché, salvo i casi di procedimenti diversamente disciplinati, mediante fax o telematicamente. La data di ricevimento è comprovata dal timbro datario e dal protocollo apposto sulla domanda.

Articolo 4 (Durata del procedimento)

1. I termini stabiliti nella tabella di cui all'art. 2, comma 1, corrispondono alla sommatoria dei tempi necessari a ciascun

organo o struttura organizzativa dell'amministrazione per intervenire nel procedimento. I dirigenti delle strutture, i cui uffici debbano intervenire nel procedimento amministrativo, provvedono con propria circolare a stabilire, nell'ambito del termine fissato per l'emanazione dell'atto, la durata delle singole fasi di competenza di ciascun ufficio compreso nella propria struttura.

2. Per i procedimenti che prevedono l'intervento di altri soggetti pubblici o privati, estranei all'amministrazione, i termini fissati nella tabella di cui all'art. 2, comma 1, sono sospesi per il periodo che intercorre tra la data della richiesta dell'atto agli altri soggetti e il momento di acquisizione dello stesso.

Articolo 5 (Termine finale del procedimento)

1. Il termine finale è quello della data di adozione del provvedimento ovvero, nel caso di provvedimenti recettizi, della data in cui il destinatario ne riceve comunicazione. L'eventuale ulteriore fase integrativa dell'efficacia dell'atto medesimo, di competenza dell'organo di controllo, non è computata ai fini del termine di conclusione del procedimento. Dell'avvenuta trasmissione dell'atto all'organo di controllo viene data all'interessato contestuale comunicazione, indicando l'Autorità amministrativa, le modalità e i termini entro cui è possibile ricorrere.

2. In caso di osservazioni da parte dell'organo di controllo, il responsabile della struttura organizzativa competente per il procedimento è tenuto a fornire gli elementi di risposta

all'organo di controllo stesso, entro il termine di 20 giorni dalla ricezione del rilievo.

3. Qualora il termine fissato per ciascun tipo di procedimento non possa, per fatti o atti eccezionalmente sopravvenuti, essere rispettato, il responsabile del procedimento, prima della scadenza dello stesso, ne dà comunicazione agli interessati, contestualmente alla richiesta di eventuali pareri o di documentazione integrativa, indicando le ragioni del ritardo ed il nuovo termine entro il quale verrà adottato l'atto. La durata complessiva del relativo procedimento non può comunque essere superiore al doppio di quella originariamente fissata.

Articolo 6 (Acquisizione in via facoltativa di pareri e di valutazioni tecniche)

1. L'acquisizione in via facoltativa di pareri e di valutazioni tecniche di organi, uffici, amministrazioni o enti, non previsti di regola nel corso del procedimento, ha luogo con l'osservanza del termine finale del procedimento.

Articolo 7 (Domande e documentazione)

1. La domanda o istanza indirizzata all'organo o alla struttura competente e corredata dalla prescritta documentazione, indica la sussistenza dei requisiti e delle condizioni richiesti dalla normativa vigente per l'adozione del provvedimento.

2. Le strutture amministrative adottano idonea modulistica al fine di facilitare gli interessati alla presentazione di domande o istanze.

3. All'atto della presentazione della domanda o istanza è rilasciata all'interessato una ricevuta, anche mediante apposita timbratura su copia della domanda o istanza, e sono ordinariamente comunicate le indicazioni di cui all'art. 13, comma 5, della legge.

4. Per le domande o istanze inviate a mezzo del servizio postale, mediante raccomandata con avviso di ricevimento o tramite corrieri autorizzati, la ricevuta è costituita dall'avviso o rispettivamente dalla bolla di consegna sottoscritti dal ricevente.

5. Qualora la domanda risulti irregolare o la documentazione presentata sia incompleta, il responsabile del procedimento ne dà tempestiva comunicazione al richiedente, assegnando un termine massimo di 15 giorni per provvedere alla regolarizzazione od integrazione. Nei casi in cui la domanda non sia sanabile, o non venga sanata nel termine prefissato, il responsabile della struttura organizzativa competente ne dispone l'archiviazione, mediante provvedimento motivato. Il provvedimento, che deve contenere l'indicazione della normativa applicata e dei ricorsi amministrativi e giudiziari ammessi contro lo stesso, deve essere comunicato all'interessato.

6. Le strutture organizzative acquisiscono d'ufficio, anche tramite fax o con altro mezzo telematico o informatico, la documentazione accessibile, emessa o detenuta da pubbliche amministrazioni o privati. In tal caso l'attestazione della fedele riproduzione dei dati, con l'indicazione della fonte di provenienza, da parte del responsabile del procedimento, o altro impiegato incaricato, tiene luogo del documento originale.

Articolo 8 (Comunicazione del procedimento)

1. I soggetti di cui all'art. 13 della legge sono resi edotti dell'avvio del procedimento mediante comunicazione personale che deve contenere le informazioni previste dalla legge stessa. La ricevuta di cui all'art. 7, comma 3, del presente regolamento qualora contenga le predette indicazioni, equivale a tutti gli effetti a comunicazione personale dell'inizio del procedimento.

2. L'omissione, il ritardo o l'incompletezza della comunicazione può essere fatta valere dai soggetti che abbiano titolo alla comunicazione stessa, mediante segnalazione scritta al responsabile del procedimento, il quale è tenuto tempestivamente a fornire gli opportuni chiarimenti o ad adottare le misure necessarie per consentire la partecipazione nel procedimento.

Articolo 9 (Criteri e modalità di partecipazione al procedimento)

1. I soggetti che ricevono la comunicazione di avvio del procedimento, nonché i portatori di interessi pubblici o privati cui possa derivare un pregiudizio da un provvedimento, ai quali la legge riconosce la facoltà di intervenire, hanno diritto di:

- a) prendere visione degli atti del procedimento e di richiedere copie degli stessi, salvo i limiti previsti per il diritto di accesso;
- b) presentare memorie scritte e documenti;
- c) essere ascoltati, a richiesta, dal responsabile del procedimento;
- d) ricevere risposta motivata quando le memorie siano pertinenti all'oggetto del procedimento.

2. Le prerogative di cui al comma 1 possono essere esercitate anche dai portatori di interessi diffusi costituiti in associazioni o comitati, tramite i propri rappresentanti.

3. I soggetti che intervengono ai sensi del comma 1 documentano il pregiudizio che potrebbe derivare dal provvedimento conclusivo; qualora il responsabile del procedimento ritenga il pregiudizio non documentato, dichiara l'intervento inammissibile.

4. L'intervento nel procedimento deve essere promosso con atto scritto e sottoscritto dall'interessato, utilizzando a tal fine l'eventuale modulistica predisposta dall'amministrazione; deve essere indirizzato al responsabile della struttura organizzativa regionale competente e deve contenere tutti gli elementi necessari per l'individuazione del procedimento nel quale si intende intervenire, le generalità e il domicilio dell'interveniente.

5. A salvaguardia della speditezza dell'attività amministrativa, sono presi in considerazione gli atti di intervento pervenuti entro un termine pari a due terzi di quello fissato per la durata del procedimento, sempre che lo stesso non sia già concluso. La presentazione di memorie e documenti oltre il suddetto termine non può comunque determinare lo spostamento del termine finale.

CAPO III
MODALITÀ DI ESERCIZIO DEL DIRITTO DI ACCESSO
AI DOCUMENTI AMMINISTRATIVI

Art. 10 (Diritto all'accesso)

1. Il diritto di accesso ai documenti amministrativi può essere esercitato nei confronti di tutte le strutture organizzative dell'amministrazione, da soggetti privati, da amministrazioni, da associazioni e comitati portatori di interessi pubblici o diffusi, che abbiano un interesse personale e concreto, per la tutela di situazioni giuridicamente rilevanti.

2. Qualora la richiesta di accesso venga presentata dal rappresentante del soggetto legittimato all'accesso, il richiedente è tenuto ad indicare il titolo in base al quale è attribuita la rappresentanza.

3. Il diritto di accesso si esercita, con riferimento agli atti del procedimento amministrativo, anche durante il corso dello stesso, nei confronti dell'organo o struttura organizzativa che è competente a formare l'atto conclusivo o a detenerlo stabilmente.

4. Non è ammesso l'accesso agli atti preparatori nel corso della formazione degli atti normativi, amministrativi generali, di pianificazione e di programmazione, salvo diverse disposizioni di legge.

Art. 11 (Oggetto del diritto di accesso)

1. Oggetto del diritto di accesso sono i documenti amministrativi.

2. È considerato documento amministrativo ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, formati dall'amministrazione o comunque utilizzati ai fini dell'attività amministrativa.

3. Una singola richiesta di accesso può riguardare anche più documenti, fermo restando che la stessa deve essere formulata in modo da consentire all'amministrazione l'identificazione di tutti i documenti richiesti.

4. Non possono formare oggetto del diritto di accesso i documenti non definitivi e quelli non più esistenti presso le strutture organizzative dell'amministrazione. L'amministrazione, nell'indicare le ragioni dell'inesistenza del documento, indica, se ne ha conoscenza, l'ente che lo detiene.

Art. 12 (Accesso informale)

1. Il diritto di accesso si esercita in via informale mediante richiesta, anche verbale, alla struttura organizzativa competente a formare l'atto conclusivo del procedimento o a detenerlo stabilmente. Il responsabile di tale struttura è responsabile del procedimento di accesso informale.

2. L'interessato deve indicare gli estremi del documento oggetto della richiesta, ovvero gli elementi che ne consentano l'individuazione, specificare e, ove occorra, comprovare l'interesse connesso all'oggetto della richiesta, far constare la propria identità e, quando è necessario, i propri poteri rappresentativi.

3. La richiesta esaminata immediatamente e senza formalità, è accolta mediante indicazione della pubblicazione contenente il

documento, l'esibizione del documento o il rilascio di copia del medesimo.

Art. 13 (Accesso formale)

1. Qualora non sia possibile l'accoglimento immediato della richiesta in via informale, ovvero sorgano dubbi sulla legittimazione del richiedente, sulla sua identità, sui suoi poteri rappresentativi, sulla sussistenza dell'interesse alla stregua delle informazioni e della documentazione fornita o sull'accessibilità del documento, il richiedente è invitato contestualmente a presentare istanza formale contenente le indicazioni e gli elementi di cui al comma 2 dell'art. 12 del presente regolamento. Al fine di agevolare i richiedenti le strutture organizzative rendono disponibile apposita modulistica conforme al modello di cui all'allegato 2 costituente parte integrante del presente regolamento.

2. Al di fuori dei casi indicati al comma 1, il richiedente può sempre presentare richiesta formale di cui l'ufficio, su richiesta dell'interessato, è tenuto a rilasciare ricevuta.

3. La richiesta formale presentata ad organo o struttura organizzativa diversi da quelli nei cui confronti va esercitato il diritto di accesso è dai medesimi immediatamente trasmessa a quelli competenti. Di tale trasmissione è data comunicazione all'interessato.

4. Il procedimento di accesso deve concludersi nel termine di 20 giorni decorrenti dalla presentazione della richiesta all'organo o struttura organizzativa competenti. Decorso inutilmente detto termine la richiesta si intende rigettata.

5. Ove la richiesta sia irregolare o incompleta, l'amministrazione, entro 10 giorni, è tenuta a darne tempestiva comunicazione al richiedente con raccomandata con avviso di ricevimento od altro mezzo idoneo ad accertarne la ricezione. Il termine del procedimento ricomincia a decorrere dalla presentazione della richiesta perfezionata.

6. Il responsabile del procedimento di accesso formale è il responsabile della struttura organizzativa competente a formare l'atto o a detenerlo stabilmente.

Art. 14 (Esame della richiesta di accesso)

1. Esaminata la richiesta di accesso, la struttura organizzativa competente, ne dispone l'accoglimento, totale o parziale, il rifiuto o il differimento, utilizzando eventualmente nell'ipotesi di accoglimento parziale, rifiuto o differimento, i modelli di cui all'allegato 3 costituente parte integrante del presente regolamento.

2. La struttura competente nel comunicare all'interessato l'esito della richiesta indica altresì:

- a) la struttura presso cui è possibile accedere ai documenti, con la specificazione del suo orario di apertura al pubblico, in caso di accoglimento;
- b) la motivazione dell'accoglimento parziale, del diniego e del differimento dell'accesso;
- c) la data a partire dalla quale è possibile accedere ai documenti richiesti, nell'ipotesi di differimento.

3. Su richiesta dell'interessato, la documentazione può essere trasmessa allo stesso con qualunque mezzo conformemente alle

disposizioni vigenti, previo accertamento dell'avvenuto pagamento delle relative spese di cui all'art. 16.

Articolo 15 (Modalità di accesso)

1. Fatta salva la più specifica disciplina contenuta nelle misure organizzative di cui all'art. 17, il diritto di accesso si esercita secondo le modalità che seguono.

2. Il diritto di accesso può essere esercitato attraverso l'acquisita cognizione della pubblicazione contenente il documento amministrativo, la visione dei documenti, la trascrizione manuale degli stessi, l'estrazione di copia o l'esperimento congiunto di tali operazioni. Le informazioni contenute in strumenti informatici possono essere rilasciate sugli appositi supporti, ove forniti dal richiedente, ovvero mediante collegamento telematico, ove esistente e regolarmente attivato.

3. Possono essere rilasciate copie parziali dei documenti. Le copie parziali devono comprendere la prima e l'ultima pagina del documento e le pagine omesse devono essere indicate.

4. Per i documenti contenenti i dati di cui all'art. 4 comma 1 lettere d) ed e) del codice in materia di protezione dei dati personali di cui al decreto legislativo 27 giugno 2003, n. 196, relativi a soggetti terzi rispetto al richiedente, l'accesso è consentito unicamente nelle forme di cui all'art. 19 comma 2 del presente regolamento.

5. L'esame dei documenti avviene presso la competente struttura organizzativa, nelle ore di ufficio, alla presenza, ove necessaria, di personale addetto. Il tempo di visione è commisurato alla natura, alla lunghezza e alla complessità dei documenti stessi.

6. Salva comunque l'applicazione delle norme penali, è vietato asportare i documenti dal luogo presso cui sono dati in visione, contraffarli o comunque alterarli in qualsiasi modo.

7. L'esame dei documenti può essere effettuato dal richiedente, anche accompagnato da persona di sua fiducia, o da persona in possesso di atto di delega, della quale vanno specificate le generalità, che devono essere registrate in calce alla richiesta.

Articolo 16 (Tariffe)

1. L'esame dei documenti è gratuito. Fanno carico al richiedente soltanto i costi relativi all'imposta di bollo, se dovuti per legge, nonché il rimborso delle spese di riproduzione che vengono stabilite in Euro 0,20 a facciata formato A4. Il rimborso non è dovuto se l'importo è inferiore ad Euro 10,00.²

2. All'atto del pagamento degli importi suddetti è rilasciata all'interessato una ricevuta, redatta in duplice copia nella forma di cui all'allegato 4 del presente regolamento. Le somme introitate a tale titolo sono depositate mensilmente, unitamente ad una copia delle singole ricevute, all'ufficio economato che provvede al versamento al tesoriere regionale.

3. Il rimborso del costo di riproduzione non è dovuto dai consiglieri regionali qualora il rilascio di copia avvenga al fine di garantire l'espletamento della funzione ispettiva e di controllo politico-amministrativo relativa al loro mandato.

² Comma sostituito dall'art. 1, comma 1, dell'allegato al DPRReg. 20 novembre 2019, n. 83.

4. Il rilascio di pubblicazioni edite dall'amministrazione, messe a disposizione del pubblico, è gratuito.

Articolo 17 (Misure organizzative)

1. Le misure organizzative occorrenti per l'attuazione del diritto di accesso sono adottate dal dirigente della struttura organizzativa che ha formato il documento richiesto o che lo detiene stabilmente.

2. Le misure organizzative di cui al comma 1, riguardano in particolare:

- a) le modalità di compilazione delle richieste di accesso, anche mediante l'uso dell'apposito modello di cui all'allegato 2 del presente regolamento;
- b) le categorie di documenti da pubblicare secondo modalità e in luoghi accessibili a tutti e i servizi volti ad assicurare e semplificare tecniche di ricerca di documenti, in particolare con la predisposizione di indici e l'indicazione dei luoghi di consultazione;
- c) l'accesso alle informazioni contenute in strumenti informatici che vanno salvaguardate dalla distruzione o dalla perdita accidentale, nonché dalla divulgazione non autorizzata;
- d) la tenuta a disposizione di chiunque vi abbia interesse, secondo quanto previsto dall'art. 2 comma 1 del presente regolamento, delle tabelle di cui all'allegato 1.

CAPO IV
LIMITAZIONI DEL DIRITTO DI ACCESSO
AI DOCUMENTI AMMINISTRATIVI

Art. 18 (Non accoglimento della richiesta)

1. L'accoglimento parziale, il rifiuto e il differimento dell'accesso sono motivati, a cura del responsabile del procedimento di accesso, con riferimento specifico alla normativa vigente e alle circostanze di fatto per cui la richiesta non può essere accolta così come proposta.

2. L'accesso non può essere rifiutato se è sufficiente l'accoglimento parziale o il differimento.

3. Il differimento dell'accesso, non può essere reiterato, salvo che per sopraggiunte, imprevedibili e motivate esigenze.

Art. 19 (Disciplina dei casi di esclusione)

1. Fermo restando il diritto dell'interessato di accedere ai propri dati personali secondo quanto disposto dall'art. 13 della legge 31 dicembre 1996, n. 675 e successive modificazioni ed integrazioni, sono sottratti all'accesso da parte di chiunque gli atti coperti da segreto per specifica disposizione di legge o regolamento.

2. Sono sottratti all'accesso di chiunque:

- a) processi verbali delle sedute della Giunta regionale;
- b) pareri non utilizzati ai fini dell'attività amministrativa.

3. Sono accessibili solo dai diretti destinatari del provvedimento finale fermo comunque restando l'esperibilità del diritto di accesso per la cura e la difesa dei propri interessi giuridici pur eventualmente limitato alla modalità della visione degli atti o con l'adozione di accorgimenti quali la omissione dei dati sensibili o giudiziari o dei dati che consentono l'identificazione della persona:

- a) documenti contenenti dati sensibili e dati giudiziari, quali certificati del casellario giudiziale, atti contenenti indicazione del gruppo linguistico d'appartenenza o aggregazione o idonei a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose, filosofiche o di altro genere e l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere politico, sindacale, religioso e filosofico;
- b) documenti contenenti informazioni riservate su persone fornite dal Commissariato del Governo, dall'Arma dei Carabinieri e dagli organi di polizia giudiziaria all'amministrazione;
- c) documenti contenenti giudizi e valutazioni dell'amministrazione sul personale dipendente quali relazioni sul periodo di prova, rapporti informativi e verbali di ispezioni;
- d) documenti contenenti dati relativi al nucleo familiare dei dipendenti.

4. Sono accessibili solo dai diretti destinatari del provvedimento finale fermo comunque restando l'esercizio del diritto di accesso se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso, è di rango almeno pari ai diritti dell'interessato ovvero consiste in un diritto della

personalità o in un altro diritto o libertà fondamentale e inviolabile:

- documenti contenenti dati idonei a rivelare lo stato di salute e la vita sessuale quali certificati medici e documentazione medica in genere.

5. È differito al momento dell'emanazione dei provvedimenti amministrativi conclusivi dei procedimenti il diritto di accesso ai documenti seguenti:

- a) atti delle commissioni esaminatrici dei concorsi pubblici, ivi compresi gli elaborati, svolti per l'assunzione di personale da parte dell'amministrazione;
- b) atti concernenti le procedure di asta pubblica, licitazione privata, trattativa privata, appalto concorso e di confronto concorrenziale;
- c) atti dei procedimenti svolti dall'organo di disciplina dell'amministrazione nei confronti del personale.

Art. 20 (Misure tecniche di protezione dei dati informatizzati)

1. Al fine di garantire il rispetto delle norme stabilite nel presente regolamento, l'accesso ai dati e ai documenti raccolti attraverso strumenti informatici è protetto mediante l'applicazione di modalità tecniche di accesso riservato.

2. La Giunta regionale, con propria deliberazione, definisce gli specifici congegni di accesso ed individua i funzionari incaricati e responsabili dell'attivazione degli stessi, in applicazione delle disposizioni vigenti in materia di dati personali.

Art. 21 (Relazioni con il pubblico)

1. Allo scopo di facilitare il rapporto con gli utenti, l'amministrazione regionale garantisce, attraverso l'Ufficio servizi generali e rapporti con il pubblico, la piena attuazione dei diritti di informazione all'utenza relativamente agli atti e allo stato dei procedimenti ferme restando le competenze in materia di ciascun ufficio e del responsabile del procedimento.

Art. 22 (Ricorsi amministrativi)

1. Contro i provvedimenti di diniego, di differimento o di limitazione del diritto di accesso è ammesso ricorso, entro 30 giorni dal ricevimento della relativa comunicazione, alla Giunta regionale, ai sensi dell'art. 28, comma 5, della legge.

Art. 23 (Identificazione degli addetti alle funzioni)

1. Il cartello da tavolo e rispettivamente il cartellino di riconoscimento di cui all'art. 31 della legge sono predisposti secondo il modello di cui all'allegato 5 costituente parte integrante del presente regolamento.



CAPO V
MISURE ORGANIZZATIVE
PER L'APPLICAZIONE DELLE DISPOSIZIONI
SULL'AUTOCERTIFICAZIONE

Art. 24 (Dichiarazioni sostitutive)

1. Al fine della corretta ed omogenea applicazione da parte delle strutture organizzative regionali delle disposizioni di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 (Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa) l'amministrazione adotta i modelli di cui agli allegati 6, 7, 8 e 9 costituenti parte integrante del presente regolamento.

Art. 25 (Controlli)

1. Ai sensi e per gli effetti del Cap. V del DPR 28 dicembre 2000, n. 445, l'amministrazione effettua sulle dichiarazioni sostitutive presentate controlli con le modalità previste dall'art. 71.

2. In particolare l'amministrazione:

- a) effettua controlli puntuali in tutti i casi in cui sorgano fondati dubbi sulla veridicità delle dichiarazioni sostitutive;
- b) effettua ordinariamente, fatto salvo il rispetto di diverse percentuali o misure di verifica eventualmente stabilite da specifiche disposizioni di settore, controlli a campione nella percentuale del 5% delle dichiarazioni sostitutive

determinato su un arco temporale annuale, per ogni tipo di procedimento di competenza delle strutture organizzative e per quanto riguarda le seguenti strutture organizzative nella percentuale a fianco indicata in relazione ad ogni specifico procedimento in concreto svolto:

- Ufficio finanze, demanio e patrimonio 10% delle dichiarazioni sostitutive per procedura di affidamento;
- c) effettua controlli a tappeto, con verifica sistematica di tutte le dichiarazioni sostitutive rese alle strutture organizzative, in ragione della natura e delicatezza dei procedimenti.

3. Provvede alle operazioni di controllo, di cui viene redatto succinto verbale, il responsabile del procedimento in relazione al quale sono state ricevute le dichiarazioni sostitutive o il dirigente della struttura organizzativa. Il dirigente della struttura organizzativa è responsabile dell'effettivo svolgimento dei controlli, garantisce una effettiva selezione casuale del campione da assoggettare a controllo, attiva, in ragione della natura e delicatezza dei procedimenti, con provvedimento motivato eventuali modalità di controllo a tappeto con una verifica sistematica di tutte le dichiarazioni sostitutive rese e provvede a stabilire la tempistica e le modalità dei controlli.

4. I controlli vengono svolti di regola e ove possibile nel corso dell'istruttoria procedimentale prima dell'emanazione del provvedimento finale dal responsabile del procedimento.

Art. 26 (False dichiarazioni)

1. Ferme restando le conseguenze di natura penale previste a carico di chi rilascia dichiarazioni mendaci, formi o faccia uso di

atti falsi e quelle di natura amministrativa previste da specifiche disposizioni di settore, qualora dai controlli di cui all'art. 25 del presente regolamento emerga la non veridicità del contenuto della dichiarazione, l'amministrazione non concede il beneficio se l'accertamento viene effettuato prima della concessione dello stesso o dichiara la decadenza dal medesimo nel caso sia già stato concesso. All'interessato deve essere garantito secondo quanto previsto dall'art. 9 del presente regolamento la partecipazione al procedimento che nega la concessione del beneficio o dichiara la decadenza dallo stesso. Nel caso di attivazione d'ufficio del procedimento diretto a dichiarare la decadenza dal beneficio concesso deve essere altresì comunicato all'interessato l'avvio del procedimento ai sensi dell'art. 8 del presente regolamento.

Art. 27 (Irregolarità ed omissioni)

1. Ai sensi e per gli effetti dell'art. 71 del DPR 28 dicembre 2000, n. 445 qualora le dichiarazioni presentino irregolarità o omissioni rilevabili d'ufficio non contenenti falsità il responsabile del procedimento le comunica all'interessato assegnando un termine di 15 giorni per la regolarizzazione secondo quanto previsto dall'art. 7 comma 5 del presente regolamento. Nel caso di irregolarità od omissioni riscontrate dopo l'emanazione del provvedimento finale il beneficio non viene revocato.

CAPO VI
DISPOSIZIONI FINALI

Art. 28 (Abrogazione)

1. È abrogato il decreto del Presidente della Giunta regionale
13 giugno 1996, n. 7/L.

DECRETO DEL PRESIDENTE DELLA REGIONE
16 NOVEMBRE 2004, N. 7/L

Allegato 1

Struttura organizzativa competente per la trattazione:
UFFICIO PER L'INTEGRAZIONE EUROPEA E GLI AIUTI UMANITARI

Responsabile del procedimento: *(omissis)*³

Procedimento	Fonte normativa	Inizio del Procedimento	Termine del procedimento	Note
CONCESSIONE DI CONTRIBUTI PER AIUTI UMANITARI IN PAESI EXTRA-COMUNITARI AD ASSOCIAZIONI DI DIVERSE	LR 11/93	primo giorno successivo al termine per la presentazione delle domande di contributo	180 giorni	stipula della convenzione
CONCESSIONE DI FINANZIAMENTI A COMUNI, ENTI O ASSOCIAZIONI CHE SVOLGONO INIZIATIVE PER LA PROMOZIONE DELL'INTEGRAZIONE EUROPEA	LR 10/88 e s.m.	primo giorno successivo al termine per la presentazione delle domande di contributo	180 giorni	
CONCESSIONE DI PATROCINI FINANZIARI AD INIZIATIVE SVOLTE DA ISTITUZIONI, ENTI, ASSOCIAZIONI OD ALTRI ORGANISMI, RITENUTE DI PARTICOLARE IMPORTANZA PER LA REGIONE	LR 10/88 e s.m.	primo giorno successivo al termine per la presentazione delle domande di contributo	180 giorni	

³ Il responsabile del procedimento è cambiato nel tempo.

Struttura organizzativa competente per la trattazione:
UFFICIO PER I RAPPORTI CON ORGANISMI INTERREGIONALI E
MINORANZE LINGUISTICHE

Responsabile del procedimento: (*omissis*)⁴

Procedimento	Fonte normativa	Inizio del procedimento	Termine del procedimento	Note
CONCESSIONE DI FINANZIAMENTI A COMUNI, ENTI O ASSOCIAZIONI CHE SVOLGONO INIZIATIVE PER LA TUTELA DELLE MINORANZE LINGUISTICHE	LR 10/88 e s.m.	primo giorno successivo al termine per la presentazione delle domande di contributo	180 giorni	

⁴ Vedi nota n. 3.

DECRETO DEL PRESIDENTE DELLA REGIONE
16 NOVEMBRE 2004, N. 7/L

Struttura organizzativa competente per la trattazione:
UFFICIO FINANZE DEMANIO E PATRIMONIO

Responsabile del procedimento: (*omissis*)⁵

Procedimento	Fonte normativa ⁶	Inizio del procedimento	Termine del procedimento	Note
INDIZIONE E GESTIONE DIRETTA DI GARE D'APPALTO PER L'ACQUISIZIONE DI BENI E DI SERVIZI E PER L'ESECUZIONE DI LAVORI PUBBLICI	norme provinciali, nazionali e comunitarie in materia di contabilità pubblica, appalti e contratti	d'ufficio o su richiesta di altre strutture amministrative regionali	i termini di ciascuna fase del procedimento sono previsti nella normativa di volta in volta applicabile	l'Ufficio gestisce la quasi totalità delle gare d'appalto dell'Amministrazione regionale e predispone i relativi contratti
EFFETTUAZIONE RICERCHE IMMOBILIARI PER ACQUISTI DI NUOVI EDIFICI DA ADIBIRE A SEDI DI UFFICI E SERVIZI REGIONALI	norme provinciali e nazionali in materia di contabilità pubblica e contratti	su indicazione dell'Ufficio Tecnico regionale	ad avvenuta valutazione delle proposte pervenute da parte dell'Ufficio Tecnico regionale	il procedimento si conclude con l'adozione della deliberazione che individua l'edificio idoneo, alla quale segue la predisposizione del contratto di compravendita

⁵ Vedi nota n. 3.

⁶ A partire dal 31 luglio 2002 - data di entrata in vigore della legge regionale 22 luglio 2002 n. 2 "Disposizioni per l'assestamento del bilancio della Regione Trentino-Alto Adige" - l'Ufficio applica, nell'esercizio della propria attività, la normativa della Provincia Autonoma di Trento in materia di lavori pubblici, trasparenza degli appalti, attività contrattuale e amministrazione dei beni (LP 19.7.1990 n. 23 "Disciplina dell'attività contrattuale e dell'amministrazione dei beni della Provincia Autonoma di Trento" e s.m. e LP 10.9.1993 n. 26 "Norme in materia di lavori pubblici di interesse provinciale e per la trasparenza negli appalti" e s.m.).

PROCEDIMENTO AMM.VO E DELEGA DI FUNZIONI

PAGAMENTO SPESE DI FUNZIONAMENTO DEGLI UFFICI REGIONALI CENTRALI DI TRENTO E BOLZANO E DEGLI UFFICI DEL GIUDICE DI PACE	norme provinciali e nazionali in materia di contabilità pubblica	al ricevimento dei relativi documenti di spesa	ad avvenuto accertamento di regolarità della prestazione e nel rispetto dei termini di pagamento concordati	il pagamento può avvenire tramite aperture di credito a favore di funzionari delegati
PAGAMENTO FATTURE RELATIVE ALLE UTENZE TELEFONICHE, ENERGIA ELETTRICA, ACQUA E GAS PER TUTTI GLI UFFICI REGIONALI	contratti di utenza e di fornitura stipulati con i singoli gestori dei servizi	al ricevimento delle relative fatture	entro la scadenza indicata in fattura	il pagamento avviene tramite apertura di credito a favore del Direttore dell'Ufficio Economato

DECRETO DEL PRESIDENTE DELLA REGIONE
16 NOVEMBRE 2004, N. 7/L

Struttura organizzativa competente per la trattazione:
UFFICIO ENTI LOCALI

Responsabile del procedimento: (*omissis*)⁷

Procedimento	Fonte normativa	Inizio del procedimento	Termine del procedimento	Note
1) riqualificazione di sede segretariale	LR 5 marzo 1993, n. 4 art. 43	a far data dalla comunicazione del parere di competenza della Giunta provinciale	45 giorni	
2) dichiarazione su stemmi e gonfaloni comunali	DPGR 12 luglio 1984, n. 12/L Art. 4 comma 7		8 giorni	
3) concessione del titolo di borgata o di città	DPGR 27 febbraio 1995, n. 4/L Art. 7, 8, 9 e 10	dalla data della comunicazione della deliberazione della Giunta provinciale con la quale viene espresso il parere sulla domanda del comune	45 giorni	
4) modificazione del territorio, della denominazione e del capoluogo dei comuni	DPGR 27 febbraio 1995, n. 4/L Art. 44 e seguenti	dalla data della comunicazione della deliberazione della Giunta provinciale con la quale viene	300 giorni	Intero procedimento fino alla presentazione al Consiglio regionale

⁷ Vedi nota n. 3.

PROCEDIMENTO AMM.VO E DELEGA DI FUNZIONI

		espresso il parere sulla domanda del comune		del relativo disegno di legge e compresa la fase re- ferendaria
5) definizione con- troversie terri- toriali fra co- muni	DPGR 27 febbraio 1995 n. 4/L art. 49	dalla data in cui perviene l'ulti- mo parere ob- bligatorio di competenza del- la Giunta pro- vinciale	180 giorni	intero pro- cedimento fino alla pubblicazio- ne sul BUR del DPGR
6) fusione di co- muni	DPGR 27 febbraio 1995 n. 4/L artt. 42 e 43	dalla data in cui perviene l'ul- timo parere obbligatorio di competenza del- la Giunta pro- vinciale	300 giorni	intero pro- cedimento fino alla presenta- zione al Consiglio regionale del relativo disegno di legge e compresa la fase refe- rendaria
7) costituzione di nuovi comuni	DPGR 27 febbraio 1995 n. 4/L artt. 43 e 45	dalla data in cui perviene l'ultimo parere obbligatorio di competenza del- la Giunta pro- vinciale	300 giorni	intero pro- cedimento fino alla presentazio- ne del di- segno di legge a se- guito iter re- ferendario

DECRETO DEL PRESIDENTE DELLA REGIONE

16 NOVEMBRE 2004, N. 7/L

8) concessione contributi alle associazioni rappresentative dei comuni Anci, Uncem e consorzio dei comuni della Provincia di Bolzano	LR 25 novembre 1982, n. 10 LR 21 agosto 1986, n. 7	dalla data di esecutività del bilancio di previsione della Regione	120 giorni	salvo diverso termine che deve essere fissato dal regolamento ex art. 7 della LR 31 luglio 1993, n. 13

Struttura organizzativa competente per la trattazione:

UFFICIO PER I RAPPORTI CON GLI ENTI LOCALI TERRITORIALI

Responsabile del procedimento: (*omissis*)⁸

Procedimento	Fonte normativa ⁹	Inizio del procedimento	Termine del procedimento	Note
1) concessione contributi alle unioni di comuni ed ai comuni originatesi da fusione	DPGR 27 febbraio 1995 n. 4/L artt. 42, 43 e 86	dalla data di esecutività del bilancio di previsione della Regione	120 giorni	salvo diverso termine che deve essere fissato dal regolamento ex art. 7 della LR 31 luglio 1993, n. 13

⁸ Vedi nota n. 3.

⁹ A partire dal 31 luglio 2002 - data di entrata in vigore della legge regionale 22 luglio 2002 n. 2 "Disposizioni per l'assestamento del bilancio della Regione Trentino-Alto Adige" - l'Ufficio applica, nell'esercizio della propria attività, la normativa della Provincia Autonoma di Trento in materia di lavori pubblici, trasparenza degli appalti, attività contrattuale e amministrazione dei beni (LP 19.7.1990 n. 23 "Disciplina dell'attività contrattuale e dell'amministrazione dei beni della Provincia Autonoma di Trento" e s.m. e LP 10.9.1993 n. 26 "Norme in materia di lavori pubblici di interesse provinciale e per la trasparenza negli appalti" e s.m.).

Allegato 2

Alla struttura
della Regione Trentino-Alto Adige
competente a soddisfare
il diritto di accesso a documenti

Oggetto: richiesta di accesso a documenti amministrativi

Il sottoscritto _____ nato a _____
il _____ residente in _____
via _____ nella sua qualità di (specificare i
poteri rappresentativi) _____

chiede

- di prendere visione ovvero
- di prendere in esame con rilascio di copia semplice ovvero
- di prendere in esame con rilascio di copia autenticata

i sottoindicati documenti amministrativi:

per i seguenti motivi (specificare l'interesse connesso all'oggetto della richiesta):

Trento,

IL RICHIEDENTE

DECRETO DEL PRESIDENTE DELLA REGIONE
16 NOVEMBRE 2004, N. 7/L

Allegato 3

Trento,
Al richiedente

Oggetto: non accoglimento della richiesta di accesso a documenti amministrativi (ovvero accoglimento parziale o differimento dell'accesso a documenti amministrativi)

In relazione alla richiesta di accesso a documenti amministrativi avanzata dalla S.V. in data _____ si comunica il non accoglimento della medesima (ovvero l'accoglimento parziale o il differimento dell'accesso di cui alla richiesta stessa fino a _____) per i seguenti motivi:

Contro la presente decisione è ammesso ricorso alla Giunta regionale entro 30 gg. dal ricevimento della presente comunicazione ovvero ricorso al Tribunale regionale di giustizia amministrativa di Trento entro 30 gg. dalla data di ricevimento della presente comunicazione.

Distintamente.

Il responsabile
del procedimento di accesso

Allegato 4

Ufficio (a) _____

Quietanza n. _____

Il sottoscritto dichiara di avere riscosso dal sig.
_____ per n. _____ copie fotostatiche
a Euro _____ ciascuna, la somma di Euro _____

Trento, _____

Il Direttore

- (a) Indicare la struttura amministrativa competente per il diritto di accesso

Allegato 5

REGIONE AUTONOMA
TRENTINO-ALTO ADIGE

(a) _____
(b) _____
(c) _____

- (a) Nome e cognome
(b) Posizione economico-professionale
(c) Ufficio di assegnazione

Allegato 6

REGIONE AUTONOMA TRENINO-ALTO ADIGE

DICHIARAZIONE SOSTITUTIVA DI CERTIFICAZIONI

(articolo 46 DPR 28 dicembre 2000, n. 445)

Il sottoscritto _____ dichiara:

- 1) di essere nato a _____ il _____;
- 2) di essere residente in _____;
- 3) di essere cittadino _____;
- 4) di godere dei diritti civili e politici;
- 5) di essere _____ (indicare lo stato civile);
- 6) di avere il seguente stato di famiglia _____;
- 7) dà atto della propria esistenza in vita;
- 8) che il figlio di nome _____ è nato in data _____ a _____;
- 9) che _____ (indicare il rapporto di parentela) di nome _____ è deceduto in data _____ a _____;
- 10) di essere iscritto nel seguente albo registro o elenco (tenuto da una pubblica amministrazione): _____;
- 11) di appartenere al seguente ordine professionale _____;
- 12) di essere in possesso del seguente titolo di studio/qualifica professionale/titolo di specializzazione, abilitazione, formazione, aggiornamento, qualificazione tecnica: _____;
- 12a) di aver sostenuto i seguenti esami _____;
- 13) di avere la seguente situazione reddituale/economica: _____;
- 14) di aver assolto i seguenti obblighi contributivi, corrispondendo il seguente ammontare: _____;
- 15) di essere in possesso di codice fiscale n. _____ partita IVA n. _____ altri dati presenti nell'archivio dell'anagrafe tributaria: _____

- 16) di essere disoccupato/studente/pensionato; categoria di pensione_____;
- 17) di essere legale rappresentante delle seguenti persone fisiche o giuridiche/tutore/curatore e sim: _____
- 18) di essere iscritto presso le seguenti associazioni o formazioni sociali: _____
- 19) di essere nella seguente situazione in relazione all'adempimento degli obblighi militari: _____(possono essere dichiarate tutte le situazioni attestate nel foglio matricolare dello stato di servizio);
- 20) di non aver riportato condanne penali e di non essere destinatario di provvedimenti che riguardano l'applicazione di misure di sicurezza e di misure di prevenzione, di decisioni civili e di provvedimenti amministrativi iscritti nel casellario giudiziale ai sensi della vigente normativa;
- 21) di non essere a conoscenza di essere sottoposto a procedimenti penali;
- 22) di non essere l'ente destinatario di provvedimenti giudiziari che applicano le sanzioni amministrative di cui al decreto legislativo 8 giugno 2001, n. 231;
- 23) di essere a carico di_____;
- 24) di_____ (indicare qualsiasi dato contenuto nei registri dello stato civile)
- 25) di non trovarsi in stato di liquidazione o di fallimento e di non aver presentato domanda di concordato;

Il sottoscritto è consapevole che, ai sensi dell'articolo 76 del DPR 28 dicembre 2000, n. 445, per le dichiarazioni mendaci e la falsità in atti si applicano le sanzioni previste dal codice penale e dalle leggi speciali in materia.

Ai sensi di quanto disposto dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196 il sottoscritto è altresì informato che il conferimento dei dati personali contenuti nella presente dichiarazione è obbligatorio, che la stessa sarà conservata presso _____, via _____ - _____ e che gli spettano inoltre i diritti di cui all'art. 7 del suddetto decreto n. 196/2003.

(Luogo e data)_____

IL DICHIARANTE

Allegato 7

REGIONE AUTONOMA TRENTINO-ALTO ADIGE
**DICHIARAZIONE SOSTITUTIVA DELL'ATTO DI
NOTORIETÀ**

(articolo 47 DPR 28 dicembre 2000, n. 445)

Il sottoscritto _____, nato a
_____ il _____, residente a _____,

dichiara:

Il sottoscritto è consapevole che, ai sensi dell'articolo 76 del DPR 28 dicembre 2000, n. 445, per le dichiarazioni mendaci e la falsità in atti si applicano le sanzioni previste dal codice penale e dalle leggi speciali in materia.

Ai sensi di quanto disposto dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196 il sottoscritto è altresì informato che il conferimento dei dati personali contenuti nella presente dichiarazione è obbligatorio, che la stessa sarà conservata presso _____, via _____ - _____ e che gli spettano inoltre i diritti di cui all'art. 7 del suddetto decreto n. 196/2003.

(Luogo e data) _____

IL DICHIARANTE

Allegato 8

Autenticazione di copia

REGIONE AUTONOMA TRENINO-ALTO ADIGE

Ufficio (a) _____

1) Conformità dichiarata dal pubblico ufficiale dal quale è stato emesso l'originale:	La presente copia, composta di n. _____ fogli, è conforme all'originale emesso da questo Ufficio.
2) Autentica di copia del pubblico ufficiale presso il quale è depositato o conservato l'originale:	La presente copia, composta di n. _____ fogli, è copia autentica dell'originale esistente presso questo Ufficio.
3) Conformità dichiarata dal pubblico ufficiale al quale deve essere prodotto il documento:	La presente copia, composta di n. _____ fogli, è conforme all'originale esibito dal sig. _____ nato a _____ il _____ identificato (b) _____ ed è stata rilasciata previa ammonizione del predetto sulla responsabilità penale cui può andare incontro in caso di esibizione di atto falso o contenente dati non più corrispondenti a verità.

(Luogo e data) _____

(c) Il _____

(d) _____

Timbro d'ufficio

- (a) Intestazione dell'ufficio.
- (b) Estremi del documento d'identità, ovvero generalità dei due testi fidefacienti ed estremi dei loro documenti di identità, ovvero conoscenza personale.
- (c) Qualifica e, tra parentesi, nome e cognome del pubblico ufficiale che rilascia la copia autentica o conforme.
- (d) Firma per esteso del pubblico ufficiale.

DECRETO DEL PRESIDENTE DELLA REGIONE
16 NOVEMBRE 2004, N. 7/L

Allegato 9

Autenticazione di sottoscrizione
REGIONE AUTONOMA TRENINO-ALTO ADIGE
Ufficio (a) _____

Ai sensi dell'art. 21 del DPR 28 dicembre 2000, n. 445, attesto che la
sottoscrizione è stata apposta in mia presenza dal signor (b)
_____ identificato (c) _____

(Luogo e data) _____

(d) Il _____

(e) _____

Timbro d'ufficio

- (a) Identificare l'ufficio di appartenenza del pubblico ufficiale che attesta.
- (b) Indicare cognome e nome del sottoscrittore.
- (c) Indicare le modalità di identificazione: tipo ed estremi del documento di identità, ovvero generalità dei testimoni ed estremi dei loro documenti di riconoscimento, ovvero conoscenza diretta.
- (d) Indicare la qualifica e, tra parentesi, nome e cognome del pubblico ufficiale.
- (e) Firma per esteso del pubblico ufficiale.

LEGGE REGIONALE 29 OTTOBRE 2014, N. 10

Disposizioni in materia di diritto di accesso civico, pubblicità, trasparenza e diffusione di informazioni da parte della Regione e degli enti a ordinamento regionale, nonché modifiche alle leggi regionali 24 giugno 1957, n. 11 (Referendum per l'abrogazione di leggi regionali) e 16 luglio 1972, n. 15 (Norme sull'iniziativa popolare nella formazione delle leggi regionali e provinciali) e successive modificazioni, in merito ai soggetti legittimati all'autenticazione delle firme dei sottoscrittori)^{1 2}

Art. 1 (Pubblicità, trasparenza e diffusione di informazioni - Accesso civico - Amministrazione trasparente)

1. In adeguamento alla disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni individuati dalla legge 6 novembre 2012, n. 190, la Regione e gli enti ad ordinamento regionale, applicano, in relazione ai rispettivi ambiti di competenza, le disposizioni contenute nel decreto legislativo 14 marzo 2013, n. 33 (nel seguito: decreto) nel testo vigente alla data di entrata in vigore del decreto legislativo 25 maggio 2016, n. 97, ad eccezione, del comma 1-bis dell'articolo 12, dell'articolo 15, dell'articolo 29, dell'articolo 32, degli articoli da 35 a 41 e del primo periodo dell'articolo 44 e con le seguenti specificazioni:³

- 0a) allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico, nel rispetto del razionale ed efficiente funzionamento dell'azione amministrativa, l'accesso civico disciplinato dall'articolo 5, comma 2 del decreto ha ad oggetto i documenti detenuti dall'amministrazione, ulteriori rispetto a quelli oggetto di pubblicazione;⁴
- a) l'articolo 9-bis del decreto si applica limitatamente alle banche dati di cui all'Allegato B del decreto medesimo per le quali sussiste per la Regione e gli enti ad ordinamento regionale l'obbligo di trasmissione dei dati stessi;⁵
- b) non trova applicazione l'articolo 10 del decreto, ad eccezione di quanto disposto dal comma 8, lettere a) e c). Sono altresì oggetto di pubblicazione il bilancio di previsione e quello consuntivo, il piano esecutivo di gestione o analoghi atti di programmazione della gestione, nonché i piani territoriali e urbanistici e le loro varianti;⁶
- c) per i comuni della regione le disposizioni contenute nell'articolo 14, comma 1, lettera f) del decreto si applicano solo ai sindaci e agli assessori dei comuni con popolazione superiore a 50.000 abitanti, a decorrere dal primo rinnovo di ciascun consiglio comunale successivo all'entrata in vigore della presente legge. Per le Camere di Commercio, Industria, Artigianato, Turismo e Agricoltura⁷ le disposizioni contenute nell'articolo 14, comma 1, lettera f) si

¹ In B.U. 4 novembre 2014, n. 44 - Supplemento n. 1

² Titolo modificato dall'art. 1, comma 1, lett. a) della l.r. 15 dicembre 2016, n. 16.

³ Alinea modificato dall'art. 1, comma 1, lett. b) 1.1, della l.r. 15 dicembre 2016, n. 16.

⁴ Lettera inserita dall'art. 1, comma 1, lett. b) 1.2, della l.r. 15 dicembre 2016, n. 16.

⁵ Lettera sostituita dall'art. 1, comma 1, lett. b) 1.3, della l.r. 15 dicembre 2016, n. 16.

⁶ Lettera modificata dall'art. 1, comma 1, lett. b) 1.4, della l.r. 15 dicembre 2016, n. 16.

⁷ La denominazione della "Camera di Commercio, industria, artigianato e agricoltura di Bolzano" è sostituita dalla seguente: "Camera di commercio, industria, artigianato, turismo e agricoltura di Bolzano". La denominazione della "Camera di Commercio, industria, artigianato e agricoltura di Trento" è sostituita dalla seguente: "Camera di commercio, industria, artigianato, turismo e agricoltura di Trento". Nella normativa regionale ovunque ricorrano le espressioni "Camera di commercio, industria, artigianato e agricoltura" o "Camere di commercio, industria, artigianato e agricoltura" con riferimento alle camere di Bolzano e di Trento, queste espressioni sono sostituite rispettivamente con "Camera di commercio, industria, artigianato, turismo e agricoltura" e "Camere di commercio, industria, artigianato, turismo e agricoltura". (Si veda l'art. 7 della l.r. 24 luglio 2024, n. 2)

applicano solo al Presidente ed al Vicepresidente delle medesime. Trovano applicazione le disposizioni dell'articolo 14 del decreto relative ai titolari di incarichi dirigenziali e di posizioni organizzative. Per la Regione e le Camere di Commercio, Industria, Artigianato, Turismo e Agricoltura⁸, per posizioni organizzative si intendono gli incarichi di direzione d'ufficio;⁹

- d) per gli incarichi di collaborazione o consulenza trova applicazione la normativa provinciale in materia;¹⁰
- e) per i comuni della regione in luogo degli articoli 16 e 17 del decreto continua a trovare applicazione quanto disposto dall'articolo 4 della legge regionale 25 maggio 2012, n. 2. I dati relativi ai tassi di assenza del personale sono pubblicati secondo le modalità dell'articolo 16, comma 3, del decreto;¹¹
- f) in luogo di quanto disposto dall'articolo 20 del decreto vengono pubblicati i dati relativi all'ammontare complessivo dei premi collegati al merito, nonché all'entità del premio mediamente conseguito dal personale dirigenziale e non dirigenziale;
- g) l'articolo 23 del decreto si applica limitatamente al comma 1 e con esclusione della lettera b). In luogo degli elenchi dei provvedimenti possono essere comunque pubblicati i provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti. Oltre a tali provvedimenti possono essere pubblicati tutti gli altri provvedimenti adottati dagli organi di indirizzo politico e dai dirigenti, fermo restando quanto disposto dal comma 3 del presente articolo. A decorrere dal 1° gennaio 2024, gli enti locali sono comunque tenuti, decorsi i dieci giorni di pubblicazione previsti dall'articolo 183 della legge regionale 3 maggio 2018, n. 2 (Codice degli enti locali della Regione autonoma Trentino-Alto Adige), e successive modificazioni alla ripubblicazione di tutti i provvedimenti adottati dagli organi di indirizzo politico nel rispetto di quanto previsto dall'articolo 8, comma 3, del decreto e dal comma 3 del presente articolo.¹²
- h)¹³
- i) in luogo degli articoli 26 e 27 del decreto si applica l'articolo 7 della legge regionale 13 dicembre 2012, n. 8 e successive modificazioni come modificato da ultimo dal presente articolo;
- l) in materia di obblighi di pubblicazione concernenti i contratti pubblici e gli affidamenti di lavori, servizi e forniture, si applica l'articolo 37 del decreto, fatto salvo quanto disposto dalla normativa provinciale in materia;¹⁴
- m) il Responsabile per la trasparenza è nominato dall'organo esecutivo ed è individuato, di norma, in armonia con quanto disposto dal primo periodo del comma 1 dell'articolo 43 del decreto, nel responsabile per la prevenzione della corruzione;¹⁵
- n) ogni riferimento all'OIV contenuto nel decreto deve intendersi, in mancanza del medesimo, al nucleo di valutazione o all'organo che svolge analoghe funzioni;
- o) i richiami alle disposizioni dei decreti legislativi 27 ottobre 2009, n. 150 e 30 marzo 2001, n. 165 e successive modificazioni contenuti nel decreto debbono intendersi riferiti alle corrispondenti disposizioni delle leggi regionali in materia di ordinamento del personale della Regione ovvero degli enti a ordinamento regionale, ove previste, e quelli

⁸ Si veda la nota n. 7.

⁹ Lettera dapprima modificata dall'art. 8, comma 1, della l.r. 3 agosto 2015, n. 22 e, successivamente, dall'art. 1, comma 1, lett. b) 1.5, della l.r. 15 dicembre 2016, n. 16 e dall'articolo 7, comma 1 della l.r. 27 luglio 2020, n. 3.

¹⁰ Lettera modificata dall'art. 1, comma 1, lett. b), 1.6, della l.r. 15 dicembre 2016, n. 16.

¹¹ Lettera modificata dall'art. 2, comma 1, lett. a), della l.r. 24 luglio 2024, n. 2.

¹² Periodo aggiunto dall'art. 2, comma 1, della l.r. 25 luglio 2023, n. 5.

¹³ Lettera abrogata dall'art. 1, comma 1, lett. b), 1.7, della l.r. 15 dicembre 2016, n. 16.

¹⁴ Lettera modificata dall'art. 1, comma 1, lett. b), 1.8, della l.r. 15 dicembre 2016, n. 16 e successivamente sostituita dall'art. 2, comma 1, lett. b), della l.r. 24 luglio 2024, n. 2.

¹⁵ Lettera sostituita dall'art. 1, comma 1, lett. b), 1.9, della l.r. 15 dicembre 2016, n. 16.

alla legge 7 agosto 1990, n. 241 e successive modificazioni debbono intendersi riferiti alle disposizioni regionali ovvero provinciali in materia di procedimento amministrativo, ove previste.

2. Alle aziende e alle società in controllo della Regione, nonché a quelle in controllo degli enti a ordinamento regionale si applicano, in quanto compatibili le disposizioni della presente legge, salvo che la disciplina provinciale a cui le medesime devono fare riferimento non regoli diversamente la materia. Per società in controllo pubblico si intendono le società come definite dal decreto legislativo emanato in attuazione dell'articolo 18 della legge 7 agosto 2015, n. 124. Sono escluse dall'applicazione della presente legge le società quotate come definite dallo stesso decreto legislativo. Le disposizioni della presente legge trovano inoltre applicazione, in quanto compatibili, nei confronti delle associazioni, fondazioni ed enti di diritto privato comunque denominati, anche privi di personalità giuridica, degli enti pubblici a ordinamento regionale, con bilancio superiore a cinquecentomila euro, la cui attività sia finanziata in modo maggioritario per almeno due esercizi finanziari consecutivi nell'ultimo triennio dai suddetti enti pubblici e in cui la totalità dei titolari o dei componenti dell'organo d'amministrazione o di indirizzo sia designata da enti pubblici a ordinamento regionale.¹⁶

3. La pubblicazione di documenti, informazioni e dati ai sensi del presente articolo viene effettuata nel rispetto delle norme in materia di tutela della riservatezza dei dati personali. Le amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o non indispensabili ai sensi dell'articolo 7-bis, comma 4 del decreto nei termini e con le modalità compatibili con l'assetto organizzativo dell'amministrazione, tenuto conto dell'obbligo di invarianza finanziaria di cui all'articolo 51 del decreto.¹⁷

4. Rimangono salve le disposizioni legislative delle Province autonome per gli aspetti di loro competenza.

5. *(omissis)*¹⁸

6. All'articolo 7 della legge regionale 13 dicembre 2012, n. 8 sono apportate le seguenti modificazioni:

a) *(omissis)*¹⁹

b) *(omissis)*²⁰

c) *(omissis)*²¹

d) *(omissis)*²²

7. L'articolo 12 della legge regionale 5 febbraio 2013, n. 1 e successive modificazioni è abrogato.

8. La Giunta regionale, al solo fine di rendere coerenti le disposizioni di cui al presente articolo con altre disposizioni di legge regionale o di legge provinciale in materia, può con regolamento coordinare le disposizioni contenute nel presente articolo con le disposizioni regionali o provinciali medesime.

9. Gli enti, le società e le aziende di cui ai commi 1 e 2 applicano le disposizioni del presente articolo secondo le indicazioni, ove compatibili, contenute nelle intese in sede di Conferenza unificata di cui all'articolo 1, comma 61 della legge 6 novembre 2012, n. 190 e comunque entro 180 giorni dall'entrata in vigore della presente legge, salvo quanto disposto nel comma 1, lettera c) del presente articolo.

¹⁶ Comma sostituito dall'art. 1, comma 1, lett. c), della l.r. 15 dicembre 2016, n. 16.

¹⁷ Comma modificato dall'art. 1, comma 1, lett. d), della l.r. 15 dicembre 2016, n. 16.

¹⁸ Modifica il comma 2 dell'art. 7-*quinquies* della l.r. 21 luglio 2000, n. 3.

¹⁹ Modifica il comma 1 dell'art. 7 della l.r. 13 dicembre 2012, n. 8.

²⁰ Sopprime la lettera b) del comma 1 dell'art. 7 della l.r. 13 dicembre 2012, n. 8.

²¹ Modifica il comma 2 dell'art. 7 della l.r. 13 dicembre 2012, n. 8.

²² Sostituisce il comma 4 dell'art. 7 della l.r. 13 dicembre 2012, n. 8.

10. Le disposizioni del presente articolo si applicano, in quanto compatibili, anche alle forme collaborative intercomunali disciplinate dagli articoli da 41-*bis* a 42-*bis* della legge regionale 4 gennaio 1993, n. 1 e successive modificazioni.

Art. 2 (Estensione del novero dei soggetti legittimati ad effettuare autenticazioni per la presentazione di progetti di legge regionale di iniziativa popolare e di richieste di referendum abrogativo di leggi regionali)

1. *(omissis)*²³

2. *(omissis)*²⁴

Art. 3 (Entrata in vigore)

1. La presente legge entra in vigore il quindicesimo giorno successivo a quello della sua pubblicazione nel Bollettino Ufficiale della Regione.

²³ Sostituisce il comma 2 dell'art. 9 della l.r. 16 luglio 1972, n. 15.

²⁴ Modifica il comma 3 dell'art. 5 della l.r. 24 giugno 1957, n. 11.



Estratto del verbale della seduta del

Auszug aus dem Protokoll der Sitzung
vom

5.11.2020

DELIBERAZIONE N.

BESCHLUSS Nr.

155

Oggetto:

Betreff:

Approvazione del nuovo regolamento interno
delle sedute della Giunta regionale.

Genehmigung der neuen Geschäftsordnung
für die Sitzungen der Regionalregierung

Arno Kompatscher	Presidente/ Präsident	presente/anwesend
Maurizio Fugatti	Vice Presidente sostituto del Presidente / Vizepräsident-Stellvertreter des Präsidenten	presente/anwesend
Waltraud Deeg	Vice Presidente / Vizepräsidentin	presente/anwesend
Claudio Cia	Assessore / Assessor	presente/anwesend
Giorgio Leonardi	Assessore / Assessor	presente/anwesend
Manfred Vallazza	Assessore / Assessor	presente/anwesend
Michael Mayr	Segretario Generale della Giunta regionale / Generalsekretär der Regionalregierung	presente/anwesend

Su proposta del Presidente Arno Kompatscher
Segreteria Generale
Ufficio Affari Generali

Auf Vorschlag des Präsidenten Arno Kompatscher
Generalsekretariat
Amt für Allgemeine Angelegenheiten

In riferimento all'oggetto la Giunta regionale ha discusso e deliberato quanto segue:

Viste le proprie deliberazioni n. 2286 del 6 dicembre 1983 e n. 126 del 17 giugno 2015 con le quali è stato rispettivamente approvato e integrato il regolamento interno delle sedute della Giunta regionale previsto dall'articolo 3, comma 2 della L.r. 9 novembre 1983, n. 15;

Visto il testo del nuovo regolamento, allegato alla presente deliberazione, che disciplina in modo organico lo svolgimento delle sedute della Giunta e ritenuto di condividerne il contenuto;

Richiamato l'art. 43 dello Statuto speciale di autonomia sulla base del quale il Presidente della Regione emana, con suo decreto, i regolamenti deliberati dalla Giunta;

Ad unanimità di voti legalmente espressi,

delibera

- 1) di approvare il nuovo regolamento interno delle sedute della Giunta regionale nel testo allegato alla presente deliberazione di cui ne forma parte integrante e sostanziale;
- 2) di disporre che detto regolamento entri in vigore il giorno successivo alla sua pubblicazione nel Bollettino Ufficiale della Regione;
- 3) con l'entrata in vigore del presente regolamento, cessa di avere efficacia il precedente regolamento approvato con le deliberazioni n. 2286 del 6 dicembre 1983 e n. 126 del 17 giugno 2015.

Die Regionalregierung hat über die oben genannte Angelegenheit beraten und Folgendes beschlossen:

Aufgrund der Beschlüsse der Regionalregierung vom 6. Dezember 1983, Nr. 2286 und vom 17. Juni 2015, Nr. 126, mit denen die Geschäftsordnung für die Sitzungen der Regionalregierung laut Art. 3 Abs. 2 des Regionalgesetzes vom 9. November 1983, Nr. 15 genehmigt bzw. ergänzt wurde;

Nach Einsichtnahme in den diesem Beschluss beiliegenden Wortlaut der neuen Geschäftsordnung, mit der die Abwicklung der Sitzungen der Regionalregierung umfassend geregelt wird, und nach Dafürhalten, dem Inhalt zuzustimmen;

Aufgrund des Art. 43 des Sonderautonomiestatuts, laut dem der Präsident der Region mit eigenem Dekret die von der Regionalregierung beschlossenen Verordnungen erlässt;

beschließt die Regionalregierung

mit Einhelligkeit gesetzmäßig abgegebener Stimmen,

1. die neue Geschäftsordnung für die Sitzungen der Regionalregierung in dem diesem Beschluss als ergänzender und wesentlicher Bestandteil beiliegenden Wortlaut zu genehmigen;
2. zu verfügen, dass genannte Geschäftsordnung am Tag nach ihrer Veröffentlichung im Amtsblatt der Region in Kraft tritt.
3. Mit Inkrafttreten dieser Verordnung gilt die vorherige, mit den Beschlüssen der Regionalregierung vom 6. Dezember 1983, Nr. 2286 und vom 17. Juni 2015, Nr. 126 genehmigte Verordnung nicht mehr.

Contro il presente provvedimento sono ammessi alternativamente i seguenti ricorsi:

- ricorso giurisdizionale al TRGA di Trento da parte di chi vi abbia interesse entro 60 giorni ai sensi del D.lgs. 2 luglio 2010, n. 104;
- ricorso straordinario al Presidente della Repubblica da parte di chi vi abbia interesse entro 120 giorni ai sensi del DPR 24.11.1971 n. 1199.

Letto, confermato e sottoscritto.

IL PRESIDENTE

DER PRÄSIDENT

Arno Kompatscher

firmato digitalmente / digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Gegen diese Maßnahme können alternativ nachstehende Rekurse eingelegt werden:

- Rekurs beim Regionalen Verwaltungsgericht Trient, der von den Personen, die ein rechtliches Interesse daran haben, innerhalb 60 Tagen im Sinne des GvD vom 2. Juli 2010, Nr. 104 einzulegen ist;
- außerordentlicher Rekurs an den Präsidenten der Republik, der von Personen, die ein rechtliches Interesse daran haben, innerhalb 120 Tagen im Sinne des DPR vom 24. November 1971, Nr. 1199 einzulegen ist.

Gelesen, bestätigt und unterzeichnet

IL SEGRETARIO GENERALE
DELLA GIUNTA REGIONALE

DER GENERALSEKRETÄR DER
REGIONALREGIERUNG

Michael Mayr

firmato digitalmente / digital signiert

Falls dieses Dokument in Papierform übermittelt wird, stellt es die für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

REGOLAMENTO INTERNO DELLE SEDUTE DELLA GIUNTA REGIONALE

Art. 1

Oggetto del regolamento

1. Il presente regolamento disciplina le modalità di svolgimento delle sedute della Giunta regionale, ai sensi dell'articolo 3, comma 2, della legge regionale 9 novembre 1983, n. 15.

Art. 2

Convocazione della Giunta regionale

1. La Giunta regionale è convocata dal Presidente della Regione con avviso scritto da comunicarsi agli Assessori con mezzi telematici - da parte della struttura competente individuata dal Regolamento concernente la "Determinazione delle attribuzioni delle strutture organizzative regionali e delle loro articolazioni" - di norma due giorni prima di quello stabilito per la riunione.

2. In caso di urgenza la convocazione può avvenire, senza limiti temporali di preavviso, anche mediante comunicazione orale o telefonica, o altro idoneo mezzo.

3. Nella convocazione è inserito l'ordine del giorno e ogni documento utile ad illustrare gli argomenti che dovranno essere esaminati.

Art. 3

Ordine del giorno della seduta

1. L'ordine del giorno della seduta contiene l'elencazione delle proposte di provvedimenti di carattere formale da sottoporre all'approvazione della Giunta. Può contenere anche l'indicazione di comunicazioni o argomenti di carattere formale o informale sui quali il Presidente o gli Assessori intendono informare o promuovere la pronuncia della Giunta stessa.

GESCHÄFTSORDNUNG FÜR DIE SITZUNGEN DER REGIONALREGIERUNG

Art. 1

Gegenstand der Verordnung

(1) Diese Verordnung regelt im Sinne des Art. 3 Abs. 2 des Regionalgesetzes vom 9. November 1983, Nr. 15 die Abwicklung der Sitzungen der Regionalregierung.

Art. 2

Einberufung der Regionalregierung

(1) Die Regionalregierung wird vom Präsidenten der Region mit schriftlicher Mitteilung einberufen, die an die Assessoren von der zuständigen, in der Verordnung betreffend die Festsetzung der Befugnisse der Organisationsstrukturen der Region und deren Gliederungen bestimmten Struktur mit telematischen Mitteln in der Regel zwei Tage vor dem Sitzungstermin übermittelt wird.

(2) In dringenden Fällen kann die Einberufung ohne Vorankündigungsfrist auch mündlich oder telefonisch oder mit sonstigen geeigneten Mitteln erfolgen.

(3) Der Einberufung wird die Tagesordnung und jede für die Erläuterung der zu beratenden Themen nützliche Unterlage beigelegt.

Art. 3

Tagesordnung der Sitzung

(1) Die Tagesordnung der Sitzung enthält die Auflistung der formellen Maßnahmevorschläge, die der Regionalregierung zur Genehmigung unterbreitet werden. Sie kann ferner die Angabe von Mitteilungen oder Themen formellen bzw. informellen Charakters enthalten, über die der Präsident oder die Assessoren die Regionalregierung informieren oder zur Stellungnahme veranlassen möchten.

2. L'ordine del giorno è proposto e sottoscritto dal Presidente della Regione tenendo conto delle proposte pervenute da parte degli Assessori regionali.

3. In casi di necessità ed urgenza insorti dopo la predisposizione dell'ordine del giorno, il Presidente può disporre la formazione di un ordine del giorno suppletivo.

4. L'ordine del giorno è comunicato anche ai dirigenti e ai direttori degli uffici regionali a cura della struttura competente individuata dal Regolamento concernente la "Determinazione delle attribuzioni delle strutture organizzative regionali e delle loro articolazioni".

Art. 4

Poteri del Presidente

1. Il Presidente apre e chiude le riunioni della Giunta, presiede lo svolgimento delle sedute e assicura la regolarità delle riunioni e delle deliberazioni.

2. A tale scopo può sospendere o sciogliere la seduta. Tale provvedimento deve essere motivato e trascritto sul processo verbale della seduta.

3. Il Presidente può variare l'ordine dei lavori indicati nell'ordine del giorno.

Art. 5

Sedute in presenza, in modalità telematica e in modalità mista

1. Le sedute della Giunta possono svolgersi:

a) in presenza.

Si intende la riunione in cui tutti i membri sono fisicamente presenti nel luogo indicato dal Presidente nella convocazione;

b) in modalità telematica (d'ora in poi: a distanza).

Si intende la riunione nella quale tutti i componenti partecipano alla seduta a

(2) Die Tagesordnung wird vom Präsidenten der Region vorgeschlagen und unterzeichnet, wobei er die von den Regionalassessoren eingebrachten Vorschläge berücksichtigt.

(3) In Not- und Dringlichkeitsfällen, die sich nach Erstellung der Tagesordnung ergeben, kann der Präsident die Aufstellung einer Zusatztagesordnung verfügen.

(4) Die Tagesordnung wird von der zuständigen, in der Verordnung betreffend die Festsetzung der Befugnisse der Organisationsstrukturen der Region und deren Gliederungen bestimmten Struktur auch den Führungskräften und den Direktoren der Regionalämter mitgeteilt.

Art. 4

Befugnisse des Präsidenten

(1) Der Präsident eröffnet und schließt die Sitzungen der Regionalregierung, führt darin den Vorsitz und gewährleistet die Ordnungsmäßigkeit der Sitzungen und der Beschlussfassungen.

(2) Zu diesem Zweck kann er die Sitzung aussetzen oder auflösen. Eine solche Maßnahme muss begründet und in das Sitzungsprotokoll aufgenommen werden.

(3) Der Präsident kann die Reihenfolge der Tagesordnungspunkte ändern.

Art. 5

Präsenzsitzungen, telematische und gemischte Sitzungen

(1) Die Sitzungen der Regionalregierung können wie folgt abgehalten werden:

a) als Präsenzsitzung,

wenn alle Mitglieder physisch an dem vom Präsidenten in der Einberufung genannten Ort anwesend sind;

b) als telematische Sitzung (in der Folge: Fernsitzung),

wenn jedes Mitglied im Fernmodus von einem anderen Ort an der Sitzung

distanza, da un luogo diverso;

c) in modalità mista.

Si intende la riunione in cui alcuni componenti partecipano alla seduta a distanza, altri in presenza. In ogni caso deve essere presente o il Presidente o il Vice Presidente sostituto, oltre al Segretario verbalizzante.

Di regola la riunione si svolge in presenza. Le modalità "a distanza" e "mista" sono autorizzate dal Presidente in motivati casi particolari quali: urgenze, impedimenti istituzionali, motivi di sicurezza sanitaria. Il Segretario generale annota la modalità di svolgimento della seduta nel verbale.

2. La partecipazione a distanza deve avvenire secondo le modalità dettate dal presente Regolamento.

Art. 6

Numero legale

1. Per la validità delle sedute della Giunta regionale è richiesta la partecipazione della maggioranza dei suoi componenti tra cui il Presidente o il Vice Presidente sostituto.

Art. 7

Assenze dei componenti la Giunta

1. In caso di impossibilità ad intervenire alle sedute, il componente della Giunta deve tempestivamente informare il Presidente della Regione.

Art. 8

Svolgimento delle sedute

1. Le sedute della Giunta non sono pubbliche e alle stesse non possono assistere o partecipare estranei, ad eccezione dei casi individuati dal presente regolamento.

partecipa;

c) als gemischte Sitzung, wenn einige Mitglieder im Fernmodus und andere in Präsenz an der Sitzung teilnehmen. Auf jeden Fall müssen der Präsident oder der Vizepräsident/ Stellvertreter des Präsidenten sowie der schriftführende Sekretär anwesend sein.

In der Regel finden die Sitzungen als Präsenzsitzungen statt. Die Abhaltung von „Fernsitzungen“ und „gemischten Sitzungen“ wird vom Präsidenten in besonderen, begründeten Fällen wie Dringlichkeit, institutionelle Verhinderungen, Gründe des Gesundheitsschutzes bewilligt. Der Generalsekretär vermerkt die Modalität der Abhaltung der Sitzung im Sitzungsprotokoll.

(2) Die Teilnahme im Fernmodus muss gemäß den in dieser Geschäftsordnung vorgesehenen Modalitäten erfolgen.

Art. 6

Beschlussfähigkeit

(1) Die Regionalregierung ist beschlussfähig, wenn die Mehrheit ihrer Mitglieder, darunter der Präsident oder der Vizepräsident/ Stellvertreter des Präsidenten an der Sitzung teilnehmen.

Art. 7

Abwesenheiten der Mitglieder der Regionalregierung

(1) Kann ein Mitglied der Regionalregierung nicht an den Sitzungen teilnehmen, so muss er den Präsidenten der Region unverzüglich darüber informieren.

Art. 8

Abwicklung der Sitzungen

(1) Die Sitzungen der Regionalregierung sind nicht öffentlich; Außenstehende dürfen – außer in den in dieser Geschäftsordnung vorgesehenen Fällen – weder den Sitzungen beiwohnen noch daran teilnehmen.

2. In caso di assenza di un componente della Giunta, la relazione sulle relative proposte è svolta dal Presidente o da altro Assessore da quest'ultimo designato.

3. Ciascun componente, può proporre alla votazione della Giunta il rinvio o il ritiro di un argomento iscritto all'ordine del giorno.

4. In caso di necessità ed urgenza, nel corso della seduta il Presidente o il Vice Presidente sostituto possono proporre la trattazione di uno o più provvedimenti di carattere formale, non contenuti nell'ordine del giorno, da sottoporre all'approvazione della Giunta. Ciò è possibile solo nel caso in cui siano presenti tutti i componenti della Giunta regionale i quali, con giudizio unanime, dovranno autorizzare la trattazione del/i suddetto/i provvedimento/i.

5. Al termine della discussione il Presidente pone in votazione la proposta di delibera proclamandone l'esito.

Art. 9

Validità delle deliberazioni della Giunta e votazione

1. Ogni deliberazione della Giunta è valida quando i voti favorevoli prevalgono sulla sommatoria dei voti contrari e degli astenuti.

2. In caso di parità di voti la proposta si intende non approvata.

3. Qualora nominati, gli Assessori supplenti partecipano alle sedute, ma devono astenersi dalla votazione a meno che non sostituiscano gli Assessori effettivi.

4. Le votazioni avvengono per alzata di mano a meno che tre componenti la Giunta o quelli appartenenti allo stesso gruppo linguistico chiedano la votazione per scrutinio segreto. È

(2) Bei Abwesenheit eines Mitglieds der Regionalregierung berichtet der Präsident oder ein anderer vom Präsidenten bestimmter Assessor über die vom abwesenden Mitglied eingebrachten Vorschläge.

(3) Jedes Mitglied kann die Regionalregierung über die Vertagung oder die Absetzung eines Tagesordnungspunktes abstimmen lassen.

(4) In Not- und Dringlichkeitsfällen kann der Präsident oder der Vizepräsident – Stellvertreter des Präsidenten im Laufe der Sitzung die Beratung einer oder mehrerer in der Tagesordnung nicht enthaltener formeller Maßnahmen vorschlagen, die der Regionalregierung zur Genehmigung unterbreitet werden. Dies ist nur dann möglich, wenn alle Mitglieder der Regionalregierung anwesend sind, die einstimmig der Beratung genannter Maßnahme/n zustimmen müssen.

(5) Am Ende der Beratung lässt der Präsident über den Beschlussfassungsvorschlag abstimmen und verkündet sodann das Abstimmungsergebnis.

Art. 9

Gültigkeit der Beschlussfassungen der Regionalregierung und Abstimmung

(1) Eine Beschlussfassung der Regionalregierung ist gültig, wenn die Anzahl der Ja-Stimmen höher als die Summe der Nein-Stimmen und der Stimmenthaltungen ist.

(2) Bei Stimmengleichheit gilt der Vorschlag als nicht genehmigt.

(3) Sofern Ersatzassessoren ernannt wurden, nehmen diese an den Sitzungen teil; sie dürfen jedoch nicht an der Abstimmung teilnehmen, außer wenn sie einen Assessor ersetzen.

(4) Die Abstimmung erfolgt durch Handerheben, es sei denn, dass drei Mitglieder der Regionalregierung oder die Angehörigen ein und derselben

consentita la "votazione tacita ed implicita" allorché, dopo la proposta del Presidente o dell'Assessore e la discussione preliminare, i componenti dell'organo collegiale, invitati dal Presidente ad intervenire nel dibattito per esprimere il loro eventuale dissenso, non accolgono tale invito: in tal caso il silenzio dei membri del Collegio ha valore di assenso e la proposta del Presidente o dell'Assessore si intende approvata all'unanimità.

5. Nelle sedute a distanza ogni partecipante alla seduta deve esprimere il proprio voto in modo palese, peralzata di mano o nominativamente. Non è previsto il voto segreto.

6. Il voto finale che i componenti del collegio possono manifestare può essere:

a) favorevole rispetto alla proposta di deliberazione o decisione da assumersi;

b) contrario rispetto alla proposta di deliberazione o decisione da assumersi;

c) di astensione rispetto alla proposta di deliberazione o decisione da assumersi. L'astensione si intende quale espressione di un voto e come tale incide sul quorum deliberativo.

d) allontanamento fisico dalla seduta: non è espressione di un voto. Si concretizza in una mancata partecipazione al voto, da far constatare a verbale, che produce l'effetto di far abbassare il quorum necessario per la delibera.

7. La deliberazione si perfeziona con la proclamazione del risultato delle votazioni da parte del Presidente e la verbalizzazione.

Sprachgruppe die geheime Abstimmung beantragen. Die „stillschweigende und implizite Abstimmung“ ist zugelassen, wenn der Präsident nach der Vorstellung des Vorschlags durch den Präsidenten oder den Assessor und dem einleitenden Meinungsaustausch die Mitglieder der Regionalregierung auffordert, sich mit eventuellen Einwänden zu Wort zu melden, und diese der Aufforderung nicht Folge leisten: In diesem Fall gilt das Stillschweigen der Mitglieder des Gremiums als Zustimmung und der Vorschlag des Präsidenten oder des Assessors versteht sich als einstimmig genehmigt.

(5) In den Fernsitzungen muss jeder Sitzungsteilnehmer seine Stimme öffentlich, durch Handerheben oder per Namensaufruf abgeben. Es findet keine geheime Stimmabgabe statt.

(6) Bei der Schlussabstimmung können die Mitglieder des Gremiums

a) eine Ja-Stimme zum Beschlussfassungs- bzw. Entscheidungsvorschlag abgeben;

b) eine Nein-Stimme zum Beschlussfassungs- bzw. Entscheidungsvorschlag abgeben;

c) sich in Bezug auf den Beschlussfassungs- bzw. Entscheidungsvorschlag der Stimme enthalten. Die Stimmenthaltung gilt als Stimmabgabe und wirkt sich somit auf das Beschlussquorum aus;

d) sich von der Sitzung entfernen: Das gilt nicht als Stimmabgabe. Das Mitglied nimmt nicht an der Abstimmung teil und lässt dies im Sitzungsprotokoll aufnehmen. Durch die Nichtteilnahme an der Abstimmung sinkt das für die Beschlussfassung erforderliche Quorum.

(7) Die Beschlussfassung wird mit der Verkündung des Abstimmungsergebnisses durch den Präsidenten und die Aufnahme des Ergebnisses in das Sitzungsprotokoll vollendet.

Art. 10

Funzioni del Segretario generale

1. Le deliberazioni della Giunta sono adottate con l'assistenza del Segretario generale, o, in caso di assenza o impedimento, del Vice segretario generale.
2. Il Vice segretario generale può collaborare con il Segretario generale in caso di sedute di particolare complessità.
3. Il Segretario e il Vice Segretario generale viene coadiuvato, durante le sedute di Giunta, da un dipendente regionale.
4. In caso di impedimento del Segretario generale in occasione della trattazione di singoli argomenti o deliberazioni, le funzioni di segretario sono svolte temporaneamente da un Assessore designato dalla Giunta.

Art. 11

Conflitto d'interessi ed obbligo di astensione

1. In applicazione del generale principio di imparzialità e di buon andamento dell'attività amministrativa (art. 97 Costituzione), i componenti la Giunta hanno l'obbligo di astensione dalla discussione e dalla votazione di deliberazioni o decisioni nel caso in cui si trovino in conflitto d'interessi. Per l'individuazione dei casi di conflitto d'interessi si fa riferimento al codice di comportamento, per tempo vigente, applicabile al personale con qualifica di dirigente.
2. Le disposizioni di cui al comma precedente si applicano anche al Segretario generale, al Vice segretario generale e al funzionario che li coadiuva.

Art. 12

Processo verbale delle sedute

1. Di ogni seduta il Segretario generale redige

Art. 10

Aufgaben des Generalsekretärs

- (1) Die Beschlüsse der Regionalregierung werden mit dem Beistand des Generalsekretärs oder – bei dessen Abwesenheit oder Verhinderung – des Vizegeneralsekretärs gefasst.
- (2) Der Vizegeneralsekretär kann im Falle besonders komplexer Sitzungen mit dem Generalsekretär zusammenarbeiten.
- (3) Der Generalsekretär und der Vizegeneralsekretär werden während der Sitzungen der Regionalregierung von einem Bediensteten der Region unterstützt.
- (4) Bei Verhinderung des Generalsekretärs anlässlich der Beratung einzelner Themen oder Beschlüsse werden die Aufgaben des Sekretärs zeitweilig von einem von der Regionalregierung bestimmten Assessor ausgeübt.

Art. 11

Interessenkonflikt und Enthaltungspflicht

- (1) In Anwendung des allgemeinen Grundsatzes der Unparteilichkeit und der guten Führung der Verwaltungstätigkeit (Art. 97 der Verfassung) unterliegen die Mitglieder der Regionalregierung der Enthaltungspflicht bei der Beratung und Abstimmung über Beschlüsse oder Entscheidungen, bei denen ein Konflikt mit ihren persönlichen Interessen besteht. Für die Bestimmung der Fälle von Interessenkonflikt wird auf die für das Personal im Führungsrang geltenden Verhaltensregeln Bezug genommen.
- (2) Die Bestimmungen laut vorstehendem Absatz gelten auch für den Generalsekretär, den Vizegeneralsekretär und den sie unterstützenden Beamten.

Art. 12

Sitzungsprotokoll

- (1) Für jede Sitzung verfasst der

processo verbale che deve contenere: il luogo e la data di svolgimento della seduta; l'indicazione nominativa dei componenti presenti e assenti, di chi presiede e di chi svolge le funzioni di soggetto verbalizzante, del dipendente che assiste alla seduta e di eventuali altri soggetti; gli atti e le deliberazioni della Giunta, indicando per le discussioni l'oggetto e gli esiti delle stesse; l'ora di apertura e di chiusura della seduta, la sospensione dei lavori e la loro ripresa; l'eventuale scioglimento della seduta; le entrate e le uscite nel corso della seduta. Nel processo verbale si deve dare conto degli eventuali problemi tecnici che si manifestino nel corso della seduta e della votazione a distanza.

2. Il processo verbale e le deliberazioni sono firmati dal Presidente e dal Segretario generale. Sono raccolti e conservati, a cura della struttura competente individuata dal Regolamento concernente la "Determinazione delle attribuzioni delle strutture organizzative regionali e delle loro articolazioni".

3. La Giunta può deliberare che non vi sia processo verbale delle sedute programmatiche.

4. Per la consultazione del verbale si applicano le norme per il diritto di accesso ai sensi della legge regionale 31 luglio 1993, n. 13 e successive modificazioni e integrazioni, nonché il relativo Regolamento.

Art. 13

Requisiti per le riunioni a distanza

1. Le riunioni telematiche devono svolgersi in video e audio-conferenza, mediante l'utilizzo di tecnologie telematiche che permettono, al contempo:

- la percezione diretta e uditiva dei partecipanti;
- l'identificazione di ciascuno di essi;

Generalsekretär ein Sitzungsprotokoll mit folgendem Inhalt: Ort und Datum der Sitzung; Namen der anwesenden und der abwesenden Mitglieder, des Vorsitzenden und des Schriftführers sowie des Bediensteten und eventueller sonstiger Personen, die an der Sitzung teilnehmen; die Akte und die Beschlussfassungen der Regionalregierung, mit Angabe des Gegenstands und des Ergebnisses der Beratungen; Beginn und Ende der Sitzung, Unterbrechung und Wiederaufnahme der Arbeiten; eventuelle Auflösung der Sitzung; Personen, die während der Sitzung den Raum betreten oder verlassen haben. Im Sitzungsprotokoll sind auch eventuelle technische Probleme zu schildern, die sich im Laufe der Fernsitzung und der Fernabstimmung ergeben sollten.

(2) Das Sitzungsprotokoll und die Beschlüsse werden vom Präsidenten und vom Generalsekretär unterzeichnet und von der zuständigen, in der Verordnung betreffend die Festsetzung der Befugnisse der Organisationsstrukturen der Region und deren Gliederungen bestimmten Struktur gesammelt und verwahrt.

(3) Die Regionalregierung kann beschließen, dass über die programmatischen Sitzungen kein Sitzungsprotokoll geführt wird.

(4) Für die Einsichtnahme in das Sitzungsprotokoll gelten die Bestimmungen über das Recht auf Zugang zu den Verwaltungsunterlagen laut Regionalgesetz vom 31. Juli 1993, Nr. 13 i.d.g.F. und die entsprechende Verordnung.

Art. 13

Voraussetzungen für die Fernsitzungen

(1) Die telematischen Sitzungen müssen in Video- und Audiokonferenz unter Verwendung telematischer Technologien stattfinden, die gleichzeitig Folgendes ermöglichen:

- den direkten Hörempfang der Teilnehmer,
- die Identifizierung jedes einzelnen

- l'intervento nonché il diritto di voto in tempo reale sugli argomenti affrontati nella discussione.

2. Gli strumenti a distanza devono assicurare:

- la riservatezza della seduta;
- il collegamento simultaneo tra i partecipanti su un piano di parità;
- la visione degli atti della riunione e lo scambio di documenti mediante posta elettronica e/o sistemi informatici di condivisione dei file;
- la contemporaneità delle decisioni;
- la sicurezza dei dati e delle informazioni

3. Ai componenti è consentito collegarsi da qualsiasi luogo che assicura il rispetto delle prescrizioni di cui al presente regolamento, purché non pubblico, né aperto al pubblico e, in ogni caso, con l'adozione di accorgimenti tecnici che garantiscano la riservatezza della seduta (come l'uso di cuffie).

4. Nelle riunioni a distanza, ai fini della validità della seduta e delle delibere, devono essere rispettate le prescrizioni del presente articolo.

Art. 14

Partecipazione alle sedute dei dirigenti – dei capi ufficio e di soggetti esterni

1. I dirigenti regionali, i direttori degli Uffici regionali centrali e/o i dipendenti sono ammessi a partecipare alle sedute della Giunta, senza diritto di voto, su invito del Presidente, del Vice Presidente sostituto, o di un Assessore regionale, in relazione ai

Teilnehmers,

- die Wortmeldung und die Stimmabgabe in Echtzeit zu den zur Beratung stehenden Themen.

(2) Die für die Fernsitzungen eingesetzten Instrumente müssen Folgendes gewährleisten:

- die Vertraulichkeit der Sitzung
- die simultane, gleichberechtigte Verbindung zwischen den Sitzungsteilnehmern,
- die Einsichtnahme in die Sitzungsakte und den Austausch von Unterlagen mittels elektronischer Post und/oder digitaler File-Sharing-Systeme,
- die Gleichzeitigkeit der Entscheidungen,
- die Sicherheit der Daten und der Informationen.

(3) Die Teilnehmer dürfen sich von jedem Ort aus einwählen, der die Einhaltung der in dieser Verordnung enthaltenen Vorgaben gewährleistet und weder öffentlich noch der Öffentlichkeit zugänglich ist, und müssen auf jeden Fall die notwendigen technischen Vorkehrungen (z. B. die Verwendung von Kopfhörern) treffen, um die Vertraulichkeit der Sitzung zu garantieren.

(4) Bei den Fernsitzungen ist die Einhaltung der in diesem Artikel genannten Vorgaben Voraussetzung für die Gültigkeit der Sitzung und der Beschlussfassungen.

Art. 14

Teilnahme der Führungskräfte, der Amtsdirektoren und verwaltungsexterner Personen an den Sitzungen

(1) Die Führungskräfte der Region, die Direktoren der Zentralämter der Region und/oder die Bediensteten dürfen auf Einladung des Präsidenten, des Vizepräsidenten – Stellvertreters des Präsidenten oder eines Regionalassessors in

problemi in discussione.

2. I consulenti, i membri esterni di organi o organismi della Regione sono ammessi a partecipare alle sedute della Giunta regionale, su invito del Presidente o del Vice Presidente sostituto, in relazione ai problemi in discussione.

Art. 15

Pubblicità delle deliberazioni e delle decisioni

1. Alle deliberazioni della Giunta viene data pubblicità secondo le disposizioni regionali e nazionali in materia.

2. Su richiesta del Presidente o degli Assessori, viene redatto un comunicato ufficiale dei lavori della Giunta, contenente l'illustrazione delle principali decisioni e deliberazioni assunte.

Zusammenhang mit den behandelten Themen an den Sitzungen der Regionalregierung ohne Stimmrecht teilnehmen.

(2) Die Berater sowie die verwaltungsexternen Mitglieder von Organen oder Gremien der Region dürfen auf Einladung des Präsidenten oder des Vizepräsidenten – Stellvertreters des Präsidenten in Zusammenhang mit den behandelten Themen an den Sitzungen der Regionalregierung teilnehmen.

Art. 15

Bekanntmachung der Beschlussfassungen und der Entscheidungen

(1) Die Beschlussfassungen der Regionalregierung werden gemäß den einschlägigen regionalen und staatlichen Bestimmungen bekanntgemacht.

(2) Auf Antrag des Präsidenten oder der Assessoren wird eine offizielle Mitteilung über die Arbeiten der Regionalregierung verfasst, in der die wichtigsten Entscheidungen und Beschlussfassungen geschildert sind.



**Regione Autonoma
Trentino - Alto Adige/Südtirol**

**Region Autonoma
Trentino - Südtirol**

**Autonome Region
Trentino - Südtirol**

Segreteria generale
Generalsekretariat
Ufficio gestione giuridica del personale
Amt für die dienstrechtliche Verwaltung des Personals
Tel: 0461 201280 – 0461 201284
e-mail: assunzioni@regione.taa.it
Pec: assunzioni@pec.regione.taa.it



Numero di protocollo e data di registrazione associati al documento come metadato (DPCM 3.12.2013, art. 20). Verificare l'oggetto della PEC o i file allegati alla medesima.

Protokollnummer und Registrierungsdatum sind dem Dokument als Metadaten zugeordnet (Dekret des Präsidenten des Ministerrates vom 3.12.2013, Art. 20). Gegenstand der zertifizierten E-Mail bzw. beigefügte Dateien überprüfen.

CIRCOLARE/RUNDSCHREIBEN

Alle Dirigenti e ai Dirigenti di Ripartizione e strutture equiparate

An die Leiterinnen und Leiter der Abteilungen und der gleichgestellten Organisationsstrukturen

Alle Segreterie del Presidente e dei membri della Giunta

An das Sekretariat des Präsidenten
An die Sekretariate der Mitglieder der Regionalregierung

Alle Direttrici ed ai Direttori degli Uffici

An die Amtsdirektorinnen und Amtsdirektoren

Alle Giudici di Pace coordinatrici e ai Giudici di Pace coordinatori

An die koordinierenden Friedensrichterinnen und Friedensrichter

Alla Presidenza della Corte di Appello di Trento

An das Präsidium des Oberlandesgerichts Trient

Al Procuratore Generale della Repubblica di Trento

An den Generalstaatsanwalt Trient

e, p.c.

u. z. K.

Alle Camere di Commercio, Industria, Artigianato e Agricoltura Trento e Bolzano

An die Handels-, Industrie-, Handwerks- und Landwirtschaftskammern Trient und Bozen

Al Consiglio regionale

An den Regionalrat

Alle Organizzazioni sindacali

An die Gewerkschaften

OGGETTO: Disposizioni per la prestazione del lavoro in modalità agile

Si forniscono alcuni chiarimenti per la prestazione del lavoro in modalità agile a seguito della firma dell'accordo individuale con decorrenza 1. settembre 2022 o data successiva.

Si ricorda, innanzitutto, che il regolamento approvato con DPR n. 14 dd. 30 giugno 2022 prevede che la prestazione lavorativa in modalità agile possa essere svolta a giornate intere e/o a mezze giornate.

Pertanto:

- la giornata intera lavorativa prestata in modalità agile dovrà essere giustificata nel portale StartWeb attraverso il codice "SMART WORKING GIORNATA INTERA";
- la giornata lavorativa prestata metà in modalità agile (mattina o pomeriggio) e metà in presenza non potrà comunque superare la durata media dell'orario di lavoro, salvo casi eccezionali autorizzati dal/dalla proprio/a superiore gerarchico. L'entrata presso la sede di lavoro dovrà essere timbrata come di consuetudine, garantendo la propria presenza nella fascia antimeridiana o pomeridiana compatibilmente con le esigenze di servizio, tra le quali l'apertura al pubblico nonché i rapporti con i/le colleghi/e e i/le propri/e superiori.

Il restante periodo prestato in modalità agile viene giustificato timbrando all'uscita il codice 101 – SMARTWORKING a completamento della giornata lavorativa (solamente per le giornate dal lunedì al giovedì), intendendo per completamento una prestazione in modalità agile di durata significativa (ad esempio, di norma, non è possibile una prestazione in presenza pari a 6 ore e 30 minuti e *smartworking* a completamento e cioè pari a 42 minuti);

- è possibile combinare la prestazione in modalità agile con gli istituti di riduzione di orario quali ferie ad ore, banca ore, flessibilità (saldo mensile), formazione inserendo nel portale StartWeb le relative durate con i

BETREFF: Bestimmungen betreffend die Arbeitserbringung im agilen Modus

Bezüglich der Arbeitserbringung im agilen Modus nach Unterzeichnung des individuellen Abkommens ab dem 1. September 2022 oder zu einem späteren Zeitpunkt folgen nachstehend einige Klarstellungen.

Gemäß der mit DPR n. 14 vom 30. Juni 2022, Nr. 14 genehmigten Verordnung kann die Arbeitsleistung im agilen Modus ganz- oder halbtags erbracht werden.

Demnach:

- ist für den im agilen Modus geleisteten Arbeitstag im StartWeb-Portal der Code „SMART WORKING GIORNATA INTERA“ anzugeben.
- Der Arbeitstag, der zur Hälfte im agilen Modus (vormittags oder nachmittags) und zur Hälfte in Präsenz geleistet wird, darf die durchschnittliche Arbeitszeit nicht überschreiten, außer in von der/dem Vorgesetzten genehmigten Ausnahmefällen. Bei Betreten des Arbeitsplatzes ist wie üblich einzustempeln, wobei die Anwesenheit während der Vormittags- oder Nachmittagsstunden entsprechend den dienstlichen Erfordernissen, einschließlich der Öffnung für Publikumsverkehr und der Beziehungen zu Kollegen und Vorgesetzten, gewährleistet sein muss. Für die restliche im agilen Modus zu leistende Arbeitszeit ist beim Ausstempeln der Code 101 – SMARTWORKING einzugeben, um den Arbeitstag zu vervollständigen (Dies gilt nur von Montag bis Donnerstag). Unter Vervollständigung ist eine Arbeitsleistung im agilen Modus von beachtlicher Dauer zu verstehen (z. B. ist in der Regel eine Arbeitsleistung in Präsenz von 6 Stunden und 30 Minuten sowie 42 Minuten im agilen Modus zur Vervollständigung des Arbeitstages nicht möglich).
- Die Arbeitsleistung im agilen Modus kann mit sonstigen Arbeitszeitkürzungen – wie Stundenurlaub, Stundenbank, Zeitguthaben innerhalb der Gleitzeit (monatlicher Stundensaldo), Schulungen – kombiniert werden, wobei die entsprechenden Codes und die jeweilige Dauer in das StartWeb-Portal einzugeben

relativi codici giustificativi;

- i/le dipendenti a tempo parziale possono svolgere la prestazione lavorativa in modalità agile solamente a giornate intere, inserendo nel portale StartWeb il codice "SMART WORKING GIORNATA INTERA";

L'Ufficio scrivente si riserva di fornire ulteriori informazioni di natura tecnica legate all'utilizzo delle causali sul portale StartWeb.

Per ulteriori informazioni sono a disposizione la dott.ssa Giulia Foscari (Tel: 0461 201507 – giulia.foscari@regione.taa.it) e il sig. Michele Beatrice (Tel: 0461 201230 – michele.beatrice@regione.taa.it).

Cordiali saluti.

sind.

- Die Bediensteten mit Teilzeitbeschäftigung können die Arbeitsleistung im agilen Modus nur ganztags erbringen, wofür im StartWeb-Portal der Code „SMART WORKING GIORNATA INTERA“ anzugeben ist.

Das Amt für die dienstrechtliche Verwaltung des Personals behält sich vor, weitere Anweisungen betreffend die im StartWeb-Portal zu verwendenden Codes zu erteilen.

Für nähere Auskünfte stehen Frau Giulia Foscari (Tel: 0461 201507 – giulia.foscari@regione.taa.it) und Herr Michele Beatrice (Tel: 0461 201230 – michele.beatrice@regione.taa.it) zur Verfügung.

Mit freundlichen Grüßen

IL SEGRETARIO GENERALE/ DER GENERALSEKRETÄR
- dott./Dr. Michael Mayr -
firmato digitalmente/digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs. 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Falls dieses Dokument in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).

REGIONE AUTONOMA
TRENTINO-ALTO ADIGE/SÜDTIROL

GIUNTA REGIONALE



AUTONOME REGION
TRENTINO-SÜDTIROL

REGIONALREGIERUNG

Estratto del verbale della seduta del

4.12.2024

Auszug aus dem Protokoll der Sitzung
vom

DELIBERAZIONE N.

BESCHLUSS Nr.

232

Oggetto:

Betreff:

Sistema di tutela dei dati personali della Regione Autonoma Trentino-Alto Adige/Südtirol. Revisione e aggiornamento procedura data breach introdotta con deliberazione di Giunta regionale n. 193 del 3 settembre 2019

Datenschutzsystem der Autonomen Region Trentino-Südtirol: Überarbeitung und Aktualisierung des mit Beschluss der Regionalregierung vom 3. September 2019, Nr. 193 eingeführten Data-Breach-Verfahrens

Arno Kompatscher	Presidente / Präsident	presente/anwesend
Giulia Zanotelli	Vice Presidente sostituta del Presidente / Vizepräsidentin-Stellvertreterin des Präsidenten	presente/anwesend
Franz Thomas Locher	Vice Presidente / Vizepräsident	presente/anwesend
Carlo Daldoss	Assessore / Assessor	presente/anwesend
Angelo Gennaccaro	Assessore / Assessor	presente/anwesend
Luca Guglielmi	Assessore / Assessor	presente/anwesend
Gabriele Morandell	Segretaria generale della Giunta regionale / Generalsekretärin der Regionalregierung	presente/anwesend

Su proposta del Presidente Arno Kompatscher

Segreteria generale

Ufficio affari generali

Auf Vorschlag des Präsidenten Arno Kompatscher

Generalsekretariat der Regionalregierung

Amt für allgemeine Angelegenheiten

In riferimento all'oggetto la Giunta regionale ha discusso e deliberato quanto segue:

Considerata l'importanza della tutela dei dati personali trattati, nonché la necessità per l'amministrazione regionale di mantenere sempre aggiornate, e conformi alla normativa vigente in materia di protezione dei dati, (Regolamento (UE) 2016/679 – GDPR) le procedure in uso;

Atteso che con deliberazione giuntale n. 193/2019 è stato approvato lo schema di procedura per la gestione della violazione di dati personali – data breach, nonché è stata individuata, nella figura del/la Segretario/a generale il Referente privacy e Responsabile della comunicazione dell'eventuale violazione di dati personali-data breach;

Preso atto che risulta opportuno adeguare la citata procedura introdotta con deliberazione n. 193 del 3 settembre 2019 alle indicazioni fornite dal Servizio RPD del Consorzio dei Comuni Trentini;

Ritenuto che le figure e le responsabilità così come previste dalla normativa in materia di dati personali ed individuate dall'amministrazione regionale nella più volte citata deliberazione n. 193/2019 rimangono immutate, mentre con l'allegata procedura si ritiene opportuno introdurre *ex-novo*:

- *allegato 1*: modello di comunicazione con RPD;
- *allegato 2*: il Registro delle violazioni dei dati;
- *allegato 3*: modello di comunicazione al Referente Data Breach di potenziale violazione dei dati personali.

Preso atto che il servizio RPD del Consorzio dei Comuni Trentini ha ritenuto, con nota di protocollo n. 24851 del 23 settembre 2024, agli atti, di esprimere parere positivo sulla procedura individuata dalla Regione in quanto

Die Regionalregierung hat über die oben genannte Angelegenheit beraten und Folgendes beschlossen:

Angesichts der Bedeutung des Schutzes personenbezogener Daten sowie der Notwendigkeit, dass die Regionalverwaltung die anzuwendenden Verfahren stets aktualisiert und den geltenden Bestimmungen in Sachen Datenschutz (EU-Verordnung 2016/679 (DSGVO)) anpasst;

In Anbetracht der Tatsache, dass mit Beschluss der Regionalregierung Nr. 193/2019 die Vorlage für das Verfahren im Falle von Verletzungen des Schutzes personenbezogener Daten (Data Breach) genehmigt sowie der Generalsekretär/die Generalsekretärin als Datenschutzreferent/in und als Verantwortliche/r für die Mitteilung einer eventuellen Datenschutzverletzung ernannt wurde;

Nach Kenntnisnahme der Tatsache, dass das mit Beschluss vom 3. September 2019, Nr. 193 eingeführte Verfahren den vom DSB-Dienst des Trentiner Gemeindenverbandes erteilten Anweisungen anzupassen ist;

Nach Dafürhalten – unbeschadet der in den Datenschutzbestimmungen vorgesehenen und im mehrmals zitierten Beschluss Nr. 193/2019 festgelegten Rollen und Verantwortungsbereiche – durch das beiliegende Verfahren Nachstehendes neu einzuführen:

- *Anlage 1*: Vorlage für die Meldung an den Datenschutzbeauftragten;
- *Anlage 2*: Verzeichnis der Datenschutzverletzungen;
- *Anlage 3*: Vorlage für die Meldung einer potenziellen Verletzung des Schutzes personenbezogener Daten an den Data-Breach-Referenten;

Nach Kenntnisnahme der Tatsache, dass der DSB-Dienst des Trentiner Gemeindenverbandes mit dem in den Akten aufliegenden Schreiben vom 23. September 2024, Prot.-Nr. 24851 seine positive

ritenuta conforme alla normativa in materia di protezione dei dati personali;

Visto il Decreto del Presidente della Regione Autonoma Trentino-Alto Adige/Südtirol del 7 dicembre 2022 n. 27 concernente la “Determinazione delle attribuzioni delle strutture organizzative regionali e delle loro articolazioni” ai sensi dell’art. 2, comma 1, della legge regionale 21 luglio 2000, n. 3”;

Visto il Decreto del Presidente della Regione Autonoma Trentino-Alto Adige/Südtirol del 21 marzo 2024 n. 9 “Ripartizione degli affari tra i componenti della Giunta regionale e nuova collocazione delle Ripartizioni e Strutture equiparate alle dipendenze del Presidente e degli Assessori per la XVII Legislatura.”

Vista la deliberazione della Giunta regionale 8 maggio 2019, n. 63 “Rideterminazione della graduazione delle strutture organizzative/funzioni ai sensi dell’articolo 41 del contratto collettivo riguardante il personale dell’area dirigenziale della Regione Autonoma Trentino-Alto Adige e delle Camere di Commercio, Industria, Artigianato e Agricoltura di Trento e Bolzano”;

Vista la deliberazione della Giunta regionale 28 agosto 2024, n. 157 “Determinazioni in merito agli incarichi di preposizione alle strutture dirigenziali”;

Visto l’art. 6 Decreto legislativo 16 marzo 1992, n. 267 “Norme di attuazione dello statuto speciale per il Trentino-Alto Adige concernenti modifiche a norme di attuazione già emanate”;

Visto il D.lgs. 7 febbraio 2017 n. 16 “Norme di attuazione dello Statuto speciale per la Regione Trentino-Alto Adige recanti disposizioni in materia di delega di funzioni riguardanti l’attività amministrativa e organizzativa di supporto agli uffici giudiziari”;

Stellungnahme zu dem von der Region ausgearbeiteten Verfahren abgegeben hat, da es den geltenden Datenschutzbestimmungen entspricht.

Aufgrund des Dekrets des Präsidenten der Region vom 7. Dezember 2022, Nr. 27 betreffend „Festsetzung der Befugnisse der Organisationsstrukturen der Region und deren Gliederungen“ im Sinne des Art. 2 Abs. 1 des Regionalgesetzes vom 21. Juli 2000, Nr. 3;

Aufgrund des Dekrets des Präsidenten der Region vom 21. März 2024, Nr. 9 „Aufteilung der Aufgabenbereiche unter den Mitgliedern der Regionalregierung sowie Neubestimmung der Abteilungen und der gleichgestellten Organisationsstrukturen, die dem Präsidenten und den Assessoren unterstehen – 17. Legislaturperiode“;

Aufgrund des Beschlusses der Regionalregierung vom 8. Mai 2019, Nr. 63 „Neufestlegung der Staffellung der Organisationsstrukturen/Funktionen im Sinne des Art. 41 des Tarifvertrags betreffend die Führungskräfte, die bei der Autonomen Region Trentino-Südtirol und bei den Handels-, Industrie-, Handwerks- und Landwirtschaftskammern Trient und Bozen Dienst leisten“;

Aufgrund des Beschlusses der Regionalregierung vom 28. August 2024, Nr. 157 „Entscheidungen bezüglich der Aufträge zur Leitung der Führungsstrukturen“;

Aufgrund des Art. 6 des gesetzesvertretenden Dekrets vom 16. März 1992, Nr. 267 „Durchführungsbestimmungen zum Sonderstatut für Trentino-Südtirol betreffend Änderungen zu bereits erlassenen Durchführungsbestimmungen“;

Aufgrund des GvD vom 7. Februar 2017, Nr. 16 „Durchführungsbestimmungen zum Sonderstatut der Region Trentino-Südtirol für die Delegierung von Befugnissen betreffend die Verwaltungs- und Organisationstätigkeit zur Unterstützung der Gerichtsämter“;

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;

Visto il Decreto legislativo 10 agosto 2018 n. 101;

Visto lo Statuto speciale per il Trentino - Alto Adige/Südtirol;

Ad unanimità di voti legalmente espressi,

delibera

1. di approvare l'allegata "*Procedura per la gestione della violazione dei dati personali (Data Breach)*", quale parte integrante della presente deliberazione, redatta nel pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, avente l'obiettivo di introdurre:
 - il modello di comunicazione con RPD (allegato 1)
 - il Registro delle violazioni dei dati (allegato 2)
 - il modello di comunicazione al Referente Data Breach di potenziale violazione dei dati personali (allegato 3);
2. di trasmettere la presente deliberazione a tutte le strutture regionali;
3. di trasmettere la presente deliberazione al servizio RPD del Consorzio dei Comuni Trentini.

Contro il presente provvedimento sono ammessi alternativamente i seguenti ricorsi:

a) ricorso giurisdizionale al TRGA di Trento da parte di chi vi abbia interesse entro 60 giorni dalla pubblicazione della presente

Aufgrund der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016;

Aufgrund des gesetzvertretenden Dekrets vom 10. August 2018, Nr. 101;

Aufgrund des Sonderstatuts für Trentino-Südtirol;

beschließt die Regionalregierung

mit Einhelligkeit gesetzmäßig abgegebener Stimmen,

1. das beiliegende unter Beachtung der geltenden Datenschutzbestimmungen verfasste „Verfahren im Fall von Datenschutzverletzungen (Data Breach)“, das ergänzender Bestandteil dieses Beschlusses ist, zu genehmigen, mit dem Nachstehendes eingeführt wird:
 - Vorlage für die Meldung an den Datenschutzbeauftragten (Anlage 1)
 - Verzeichnis der Datenschutzverletzungen (Anlage 2)
 - Vorlage für die Meldung einer potenziellen Verletzung des Schutzes personenbezogener Daten an den Data-Breach-Referenten (Anlage 3)
2. diesen Beschluss an sämtliche Organisationsstrukturen der Region zu übermitteln;
3. diesen Beschluss dem DSB-Dienst des Trentiner Gemeindenverbandes zu übermitteln.

Gegen diese Maßnahme können alternativ nachstehende Rekurse eingelegt werden:

a) Rekurs beim Regionalen Verwaltungsgericht Trient, der von den Personen, die ein rechtliches Interesse daran haben, binnen 60

deliberazione ai sensi dell'art. 29 del decreto legislativo 2 luglio 2010 n. 104;

b) ricorso straordinario al Presidente della Repubblica da parte di chi vi abbia interesse giuridicamente rilevante entro 120 giorni dalla pubblicazione della presente deliberazione ai sensi del DPR 24 novembre 1971 n. 1199.

Letto, confermato e sottoscritto.

IL PRESIDENTE

DER PRÄSIDENT

Arno Kompatscher

firmato digitalmente / digital signiert

Questo documento, se trasmesso in forma cartacea, costituisce copia dell'originale informatico firmato digitalmente, valido a tutti gli effetti di legge, predisposto e conservato presso questa Amministrazione (D.Lgs 82/05). L'indicazione del nome del firmatario sostituisce la sua firma autografa (art. 3 D. Lgs. 39/93).

Tagen ab Veröffentlichung dieses Beschlusses im Sinne des Art. 29 des gesetzvertretenden Dekrets vom 2. Juli 2010, Nr. 104 einzulegen ist;

b) außerordentlicher Rekurs an den Präsidenten der Republik, der von Personen, die ein bedeutendes rechtliches Interesse daran haben, binnen 120 Tagen ab der Veröffentlichung dieses Beschlusses im Sinne des DPR vom 24. November 1971, Nr. 1199 einzulegen ist.

Gelesen, bestätigt und unterzeichnet

LA SEGRETARIA GENERALE
DELLA GIUNTA REGIONALE

DIE GENERALSEKRETÄRIN
DER REGIONALREGIERUNG

Gabriele Morandell

firmato digitalmente / digital signiert

Falls dieses Dokument in Papierform übermittelt wird, stellt es eine für alle gesetzlichen Wirkungen gültige Kopie des elektronischen digital signierten Originals dar, das von dieser Verwaltung erstellt und bei derselben aufbewahrt wird (GvD Nr. 82/2005). Die Angabe des Namens der unterzeichnenden Person ersetzt deren eigenhändige Unterschrift (Art. 3 des GvD Nr. 39/1993).