REGIONE AUTONOMA TRENTINO-ALTO ADIGE/SÜDTIROL

GIUNTA REGIONALE

AUTONOME REGION TRENTINO-SÜDTIROL

REGIONALREGIERUNG

Estratto del verbale della seduta del

Auszug aus dem Protokoll der Sitzung vom

4.12.2024

DELIBERAZIONE N.

BESCHLUSS Nr.

232

Oggetto:

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

Betreff:

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

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:

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

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;

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;

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, nonchè 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;

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;

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;

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;

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.

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;

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

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;

Stellungnahme zu dem von der Region ausgearbeiteten Verfahren abgegeben hat, da es den geltenden Datenschutzbestimmungen entspricht.

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";

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;

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."

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";

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";

Aufgrund des Beschlusses der Regionalregierung vom 8. Mai 2019, Nr. 63 „Neufestlegung der Staffelung 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";

Vista la deliberazione della Giunta regionale 28 agosto 2024, n. 157 "Determinazioni in merito agli incarichi di preposizione alle strutture dirigenziali";

Aufgrund des Beschlusses der Regionalregierung vom 28. August 2024, Nr. 157 „Entscheidungen bezüglich der Aufträge zur Leitung der Führungsstrukturen";

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";

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";

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";

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 gesetzesvertretenden 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;

Tagen ab Veröffentlichung dieses Beschlusses im Sinne des Art. 29 des gesetzesvertretenden Dekrets vom 2. Juli 2010, Nr. 104 einzulegen ist;

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.

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.

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).

PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Documento approvato con Deliberazione di Giunta regionale n. …. di data …….		
Revisione	Data	Motivo
1^		Revisione complessiva della prima redazione della procedura approvata con deliberazione n. 193 del 2019

INDICE

1 Premessa introduttiva

L'amministrazione regionale, quale Titolare del Trattamento dei dati ai sensi del Regolamento europeo 2016/679 (da qui in avanti GDPR), è tenuta a garantire la sicurezza dei dati personali trattati nell'ambito delle proprie attività e ad agire prontamente in caso di violazione dei dati stessi, secondo le indicazioni fornite dal Garante. L'amministrazione regionale pertanto istituisce e mette in atto procedure idonee a rilevare e limitare tempestivamente gli effetti di una violazione, o di una potenziale violazione di dati, al fine di valutare il rischio per le persone fisiche e stabilire se sia necessario o meno procedere alla notifica della violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario e secondo gli schemi previsti dal Garante.

2 Definizione di una violazione di dati

Secondo il Garante della privacy[1], si definisce *Data Breach* "una 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". Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali raccolti e catalogati presso l'amministrazione regionale per le quotidiane attività lavorative (database).
Di seguito riportiamo per maggior comprensione della definizione di *Data Breach* alcune fattispecie di eventi che possono manifestarsi, al fine di mettere tutti i collaboratori nelle condizioni di identificarlo rapidamente, e quindi di renderli maggiormente consapevoli di come le violazioni di dati possano verificarsi in molti modi diversi, e senza alcun indugio:
- furto o smarrimento di beni di proprietà dell'amministrazione regionale e/o di dispositivi informatici (laptop, smartphone, tablet) sui quali i dati memorizzati possono essere facilmente accessibili se non protetti adeguatamente. Ricordiamo a tal fine le indicazioni già a suo tempo stabilite e contenute "Disciplinare per l'utilizzo dei dispositivi elettronici della Regione Autonoma Trentino-Alto Adige/Südtirol"[2]

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati, anche in maniera illegale, ai sistemi informatici, mediante, ad esempio, attacchi ai dati conservati in maniera diversa (ransomware, injection, mail di phishing). Rientra in questa fattispecie anche l'accesso fisico non autorizzato agli uffici regionali di terze persone con lo scopo di furto di documenti cartacei, hard disk o altri dispositivi di memorizzazione contenenti dati sensibili.

- la deliberata alterazione di dati personali da parte dei collaboratori, ma anche un uso improprio dei dati personali da parte dei dipendenti per scopi personali o finalità estranee all'attività regionale.
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;

[1] https://www.garanteprivacy.it/data-breach
[2] Approvato con deliberazione della Giunta regionale n. 237 del 31.10.2019

- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità. Un fattore che può portare a questo può essere l'utilizzo di password deboli o comuni per account online, che rende più facile per gli hacker accedere a tali account. Una volta ottenuta l'accesso a un account, gli hacker possono rubare informazioni personali, finanziarie o aziendali.
- la divulgazione non autorizzata dei dati personali, da intendersi come errore accidentale da parte di uno dei soggetti che trattano dati personali (es invio di una e-mail contenente dati personali ad un destinatario errato). Gli errori umani, come inviare un'email al destinatario sbagliato, caricare file sensibili su un server pubblico o dimenticare di proteggere con password i documenti, possono portare a violazioni di dati.

- errata valutazione delle misure di sicurezza poste in essere, ovvero un'analisi inaccurata o insufficiente dei rischi e delle contromisure necessarie per proteggere un sistema, una rete, un'organizzazione o una persona da minacce e vulnerabilità, che possono avere conseguenze gravi, portando quindi a incidenti di sicurezza, perdite finanziarie, danni alla reputazione e violazioni legali o regolamentari. A titolo esemplificativo questo può essere l'utilizzo di un software non aggiornato che può lasciare i sistemi vulnerabili agli attacchi. Gli hacker possono sfruttare le vulnerabilità note nei sistemi operativi, nelle applicazioni e nei plugin per ottenere accesso non autorizzato ai dati.

3 *Scopo*

Il presente documento contiene le indicazioni, le responsabilità e le azioni da attuare per la gestione della procedura da attivare in caso di possibile violazione dei dati personali, in osservanza agli obblighi relativi alla notifica all'Autorità Garante per la protezione dei dati personali e alla comunicazione all'interessato, secondo quanto prescritto agli articoli 33 e 34 del Regolamento europeo n. 679 del 2016.
Tutti i soggetti, che in virtù di un rapporto di qualsiasi natura con l'amministrazione regionale trattano dati personali, devono essere informati e osservare la presente Procedura, che viene messa in consultazione nella libreria M:\Comune\Privacy, nonché trasmessa a tutto il personale dell'amministrazione regionale attraverso il sistema documentale Pi.Tre.
La presente procedura, proposta dal Referente privacy della Regione, viene portata a conoscenza anche agli Uffici del Giudice di Pace del Trentino-Alto Adige e agli Uffici giudiziari del distretto della Corte d'Appello di Trento, solamente per la parte di dati personali non riferiti alle attribuzioni giurisdizionali. Questo perché gli Uffici del Giudice di Pace del Trentino-Alto Adige e gli Uffici giudiziari del distretto della Corte d'Appello di Trento sono riconosciuti titolari singolarmente dei trattamenti di dati personali per quanto riguarda le rispettive attribuzioni giurisdizionali (deliberazione n. 193 di data 3 settembre 2019).

4 *Aggiornamento*

La presente procedura aggiorna le indicazioni contenute nella deliberazione della Giunta regionale n. 193/2019, introducendo il modello di comunicazione con RPD (allegato 1) e il Registro delle violazioni dei dati (allegato 2) e il modello di comunicazione al Referente Data Breach di potenziale violazione dei dati personali (allegato 3).

5 *Definizioni*

Le seguenti definizioni dei termini utilizzati in questo documento sono tratte dall'articolo 4 del Regolamento europeo n. 679 del 2016:

«**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;
«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;
«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 in formato elettronico e/o cartaceo;
«**Responsabile della Protezione dei Dati**»: soggetto individuato dall'Ente ai sensi dell'art. 37 del GDPR, con competenze specifiche in materia di protezione dei dati personali, incaricato, ai sensi dell'art. 39 del GDPR, dei seguenti compiti:
a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35
d) cooperare con l'autorità di controllo; e
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

«Autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del GDPR dell'UE.

6 *Organizzazione delle attività di gestione dell'evento violazione dei dati personali*

La Giunta regionale, con deliberazioni n. 193/2019 e ha disposto quanto segue:

- ha individuato la/il Segretaria/o generale, o, in caso di assenza o impedimento, la/il Vicesegretaria/o generale della Giunta regionale - in ragione delle attribuzioni determinate dal Decreto del Presidente della Regione del 7 dicembre 2022, n. 27: *"Regolamento concernente la "Determinazione delle attribuzioni delle strutture organizzative regionali e delle loro articolazioni",* quale Referente privacy e Responsabile della comunicazione dell'eventuale violazione di dati personali *data breach;*
- ha individuato i designati incaricati a trattare dati personali dell'amministrazione regionale;
- ha approvato lo schema di procedura per la gestione della violazione di dati personali –data breach.

Il Titolare del trattamento è tenuto a documentare qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, mediante la compilazione del Registro, coadiuvato dal Referente Data Breach.

7 *Gestione delle attività conseguenti ad una possibile violazione di dati personali*

La fase di identificazione di una violazione di dati personali ha l'obiettivo di rilevare un potenziale data breach. Non appena si concretizza la possibilità di essere in presenza di un *data breach* (anche potenziale), devono essere svolti i seguenti adempimenti con il fine ultimo di produrre la comunicazione ex art. 33- ed eventualmente ex art. 34 – da trasmettere al Garante.
Il soggetto[3] che, a diverso titolo o in quanto autorizzato al trattamento di dati personali di cui è titolare l'amministrazione regionale, viene a conoscenza di una possibile violazione dei dati personali, deve immediatamente segnalare l'evento al Referente Privacy dell'amministrazione regionale e al Referente data breach[4], fornendo loro la massima collaborazione. La modalità di comunicazione dell'episodio, è estremamente cruciale ed il segnalatore deve utilizzare – **prioritariamente** – una comunicazione scritta indirizzata al Referente Data Breach, trasmessa per e-mail o con consegna a mano, contenente una spiegazione sintetica e precisa della violazione dei dati accaduta, indicando, ove possibile, data e ora della scoperta della violazione, natura e portata della violazione, tipologia di dati compromessi, numero approssimativo di individui e database coinvolti, potenziali impatti derivanti e rischi identificati o identificabili (allegato 3).
In via secondaria sono ammesse anche comunicazioni orali, fatte di persona oppure mediante telefonata.
Qualora la potenziale violazione dei dati personali riguardi dati trattati da un responsabile esterno, incaricato ex. art. 28, sarà dovere dello stesso darne comunicazione all'amministrazione regionale, per il tramite dell'ufficio con cui ha intrattenuto i rapporti, al fine di dare avvio della procedura a seguire.
Si evidenzia che la mancata segnalazione dell'evento, potenziale o meno, che ha dato origine al Data Breach, comporta a diverso titolo responsabilità a carico del soggetto che ne è a conoscenza.
Il Referente Data Breach, una volta che ha ricevuto la comunicazione di data breach, deve:

[3] Si precisa che oltre al personale dipendente, ai collaboratori e ai fornitori, sono tenuti a segnalare la violazione tutti i soggetti che, a diverso titolo, prestano servizio presso l'amministrazione regionale, compresi, a titolo esemplificativo, stagisti, tirocinanti, studenti partecipanti ad alternanza scuola lavoro, volontari e lavoratori con contratti di somministrazione.
[4] All'interno dell'amministrazione regionale, il Referente interno privacy e il referente data breach sono coincidenti nella stessa figura

- effettuare delle verifiche interne, volte a validare o meno la presunta violazione. A tale scopo, il Garante ha ideato e messo disposizione un apposito **strumento di autovalutazione (self assessment)** che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza[5].
- in consultazione e collaborazione con l'amministratore di sistema, adottare le misure di sicurezza informatiche e/o organizzative per porre rimedio o attenuare i possibili effetti negativi della violazione dei dati personali e, contestualmente, informare immediatamente il Responsabile della Protezione dei Dati per una valutazione condivisa;
- condurre e documentare un'indagine corretta e imparziale sull'evento (aspetti organizzativi, informatici, legali, ecc.) attraverso la compilazione del "Modello di potenziale violazione di dati personali" al Responsabile Protezione Dati" (allegato 1);
- riferire i risultati dell'indagine inviando il modello al Responsabile della Protezione dei Dati e al Titolare del trattamento.

Il Responsabile della Protezione dei Dati, ricevuti i risultati dell'indagine (allegato 1), analizza l'accaduto e formula un parere in merito all'evento, esprimendo la propria valutazione, non vincolante, se lo stesso configuri una violazione dei dati personali che possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche.
Si precisa che, come previsto dal considerando 85 del GDPR, a partire dal momento in cui il Titolare del trattamento dei dati viene a conoscenza dell'evento di data breach, decorrono le 72 ore previste dal Regolamento per la gestione degli adempimenti connessi alle violazioni accertate. In questa fase, per ogni violazione dei dati personali, devono essere identificate le opportune misure tecniche e organizzative da adottare, al fine di ridurre i relativi effetti e ridurre la probabilità di impatto e ricorrenza. Le misure di mitigazione dovranno essere adeguate alla natura dei dati personali e concertate con il DPO.
Qualora l'episodio occorso non sia configurabile come una violazione di dati, ovvero non rappresenti un rischio per i diritti e le libertà delle persone fisiche, non è necessaria da parte dell'amministrazione regionale la notifica della violazione all'Autorità Garante, pur rimanendo immutato l'obbligo di censire l'evento all'interno del Registro delle violazioni.
Nel riquadro seguente si ricordano le misure di sicurezza attualmente in vigore presso l'amministrazione regionale.

(tratto dal Manuale di gestione del protocollo)
MISURE DI SICUREZZA

ACCESSO AL SISTEMA
L'accesso al sistema informatico è consentito esclusivamente agli **utenti abilitati**, previa **univoca identificazione** e **autentificazione**.

Gli utenti del sistema, appartenenti a specifiche UOR, hanno autorizzazioni di accesso differenziate in base alle loro competenze e alle tipologie di operazioni stabilite dall'ufficio di appartenenza. 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 da remoto mediante collegamento attraverso la rete VPN.

Il sistema P.I.Tre. prevede la disconnessione automatica dall'applicazione dopo 20 minuti di inattività. È impossibile accedere a sessioni multiple su postazioni differenti con la stessa UserID.

[5] Lo strumento posto a disposizione del Garante è raggiungibile al link https://servizi.gpdp.it/databreach/s/

Il/la Dirigente competente in materia di privacy individua le modalità organizzative per garantire un livello di sicurezza 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 P.I.Tre., sulla base delle competenze e dei compiti istituzionali svolti.

PIANO DI SICUREZZA INFORMATICA

Il sistema informatico di protocollazione P.I.Tre. è un servizio erogato dalla società *in house* della Regione e degli altri enti federati, accreditati all'uso di P.i.Tre., denominata Trentino Digitale S.p.A. E' stata nominata responsabile esterno del trattamento dei dati, in conformità all'articolo 28 del Regolamento UE 679/2016. Per quanto attiene gli aspetti di sicurezza nelle componenti infrastrutturali e logiche del sistema informatico di protocollazione, la stesura del piano per la sicurezza è di competenza della medesima società. A Trentino Digitale S.p.A. spetta l'onere di provvedere al backup del sistema completo (front end, back end, database).

8 *Notifica della violazione dei dati personali all'Autorità Garante*

Il Titolare, tenuto conto del parere formulato dal Responsabile della Protezione dei Dati, e dalle valutazioni fatte congiuntamente dal Referente Data Breach/Referente Privacy dell'amministrazione regionale, se ritiene accertata la violazione dei dati personali e che la stessa possa comportare un probabile rischio per i diritti e le libertà delle persone fisiche, notifica tale violazione all'Autorità Garante avvalendosi del "Modello comunicazione violazione all'Autorità Garante, seguendo la procedura telematica https://servizi.gpdp.it/databreach/s/ . La notifica deve essere effettuata senza ingiustificato ritardo dall'accertamento dell'evento e, ove possibile, entro 72 ore dall'accertamento dello stesso con le modalità e i contenuti previsti dall'art. 33 del Regolamento europeo n. 679 del 2016.
Il parere espresso dal RPD non ha carattere né obbligatorio né vincolante: il Titolare dei dati può procedere a notificare la violazione al Garante ogni qualvolta lo ritenga opportuno, motivando le sue valutazioni.

9 *Comunicazione della violazione dei dati personali agli interessati*

Il Titolare, accertata la violazione dei dati personali e ritenendo che la stessa possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche coinvolte, oltre alla notifica di cui al punto 6, può ritenere opportuno procedere a comunicare tale violazione agli interessati, come previsto dall'art. 34 del Regolamento europeo n. 679 del 2016.
Il Referente interno privacy/Referente Data Breach dovrà pertanto:

- entro 15 giorni dalla presa d'atto dell'evento, in concerto con l'RPD, provvedere a comunicare la violazione agli interessati;
- se possibile, effettuare una comunicazione a mezzo e-mail individualmente, oppure mediante pubblicazione sul sito istituzionale di avviso informante delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate.

La comunicazione all'interessato, come espressamente indicato dall'art. 34 del Regolamento Europeo, deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le seguenti informazioni:

- una descrizione della natura della violazione
- il nome e i dati di contatto del RPD
- una descrizione delle probabili conseguenze della violazione

- una descrizione delle misure adottate o di cui si propone l'adozione da parte dell'amministrazione regionale per porre rimedio alla violazione e per limitare i possibili effetti negativi.

Si rimanda quindi all'art. 34, par. 3 del Regolamento per i casi in cui non è prevista la comunicazione all'interessato. Si precisa tuttavia che qualora il Titolare di concerto con il Referente data breach/Referente privacy decida di non fare alcuna comunicazione della violazione dei dati personali agli interessati, deve darne adeguata nota all'interno del registro delle violazioni.

10 *Compilazione del Registro delle violazioni dei dati personali*

Il Titolare, avvalendosi del Referente Data Breach, documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio nel Registro delle violazioni dei dati personali (allegato 2).
Tale documento è tenuto e implementato dal Referente Data Breach e consente all'autorità di controllo di verificare il rispetto dall'art. 33 del Regolamento europeo n. 679 del 2016.
Viene inoltre prevista la creazione, all'interno del sistema di gestione documentale del protocollo P.i.Tre, di un repertorio collegato alla tipologia documentale "Data breach" al fine di agevolare la ricerca e la catalogazione della comunicazione degli eventi o dei potenziali eventi di data breach, effettuata utilizzando il modello di comunicazione al Referente Data Breach di potenziale violazione dei dati personali (allegato 3).
Operativamente quindi ogni qualvolta che verrà aggiornato il file excell del "Registro delle violazioni dei dati Regione Autonoma Trentino-Alto Adige/Südtirol" (allegato 2) lo stesso dovrà essere archiviato e repertoriato all'interno del sistema di gestione documentale nel nodo 6.4, anno per anno, in un fascicolo avente come intestazione "Registro delle violazioni dei dati personali – data breach anno 2024". All'interno del fascicolo troveranno quindi archiviazione:

- Potenziale violazione di dati personali Modello di comunicazione al Responsabile della Protezione dei Dati (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).

Allegato 1)

POTENZIALE VIOLAZIONE DI DATI PERSONALI
MODELLO DI COMUNICAZIONE AL RESPONSABILE DELLA PROTEZIONE DEI DATI

Ente	Regione Autonoma Trentino-Alto Adige/Südtirol		
Referente Privacy	La/il Segretaria/o generale		
Telefono	0461/201111	**Email**	giunta@pec.regione.taa.it

Breve descrizione della violazione dei dati personali

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca di dati?

Il _____

Tra il _____ e il _____
In un tempo non ancora determinato
È possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio: tipo di violazione

Lettura (presumibilmente i dati non sono stati copiati)
Copia (i dati sono ancora presenti sui sistemi del titolare)
Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
Furto (i dati non sono più sui sistemi del titolare e non li ha l'autore della violazione)
Altro _____

Dispositivo o strumento oggetto della violazione

Computer
Rete
Dispositivo mobile
File o parte di un file
Strumento di backup
Documento cartaceo
Software _____
Servizio informatico _____
Altro _____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

Numero _____ di persone
Circa _____ persone
Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

Dati anagrafici/codice fiscale

Dati di accesso e di identificazione (*username, password, customer ID, altro*)
Dati relativi a minori
Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale
Dati personali idonei a rivelare lo stato di salute e la vita sessuale
Dati giudiziari
Copia per immagine su supporto informatico di documenti analogici
Ancora sconosciuto
Altro _____

Fornitori o soggetti esterni coinvolti

Misure tecniche, informatiche e organizzative applicate ai dati oggetto di violazione

Luogo e data _____

Firma _____

Allegato 2)

Registro delle violazioni dei dati Regione Autonoma Trentino-Alto Adige/Südtirol								
NR.	**Data accadimento**	**Data comunicazione al referente interno**	**Breve descrizione evento**	**Servizio/Ufficio competente al trattamento**	**Coinvolgimento RPD: SI/NO**	**Azioni / Misure adottate**	**Notifica al Garante SI/NO e data**	**Comunicazione agli interessati SI/NO e data**
1								
2								
3								
4								
5								
6								

Allegato 3)

MODELLO DI COMUNICAZIONE AL REFERENTE DATA BREACH DI POTENZIALE VIOLAZIONE DI DATI PERSONALI

Il sottoscritto			
In qualità di			
Telefono		**Email**	

Comunica che il giorno _____ alle ore _____ ha scoperto la seguente violazione di dati personali.

Breve descrizione della violazione dei dati personali

Denominazione della/e banca/banche dati oggetto di data breach:

- ✓ _____
- ✓ _____
- ✓ _____
- ✓ _____
- ✓ _____
- ✓ _____

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Tipo di violazione

Lettura (presumibilmente i dati non sono stati copiati)
Copia (i dati sono ancora presenti sui sistemi del titolare)
Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
Furto (i dati non sono più sui sistemi del titolare e non li ha l'autore della violazione)
Altro _____

Dispositivo o strumento oggetto della violazione

Computer
Rete
Dispositivo mobile
File o parte di un file
Strumento di backup
Documento cartaceo
Software _____
Servizio informatico _____
Altro _____

Che tipo di dati sono oggetto di violazione?

Dati anagrafici/codice fiscale
Dati di accesso e di identificazione (*username, password, customer ID, altro*)
Dati relativi a minori
Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico, o sindacale
Dati personali idonei a rivelare lo stato di salute e la vita sessuale
Dati giudiziari
Copia per immagine su supporto informatico di documenti analogici
Ancora sconosciuto
Altro _____

Fornitori o soggetti esterni coinvolti

Luogo e data _____

Firma _____

Via Gazzoletti,2
38122 TRENTO – TRIENT – TRËNT
☎ 0461 201111

@ urp@regione.taa.it
pec: protocollo@pec.regione.taa.it
☎ 800-356552
www.regione.taa.it
C.F. / St.-Nr.: 80003690221

Piazza Università, 3 – 39100 BOLZANO
Universitätsplatz 3 – 39100 BOZEN
Plaza Università 3 – 39100 BULSAN
☎ 0471 322111