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

31.10.2019

DELIBERAZIONE N.

BESCHLUSS Nr.

237

Oggetto:

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

Betreff:

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:

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

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;

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;

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;

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;

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;

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;

Visto l'art. 13 "Formazione informatica dei dipendenti pubblici" del D.Lgs. 7 marzo 2005, n. 82 e s.m.;

Aufgrund des Art. 13 („Digitale Ausbildung der öffentlichen Bediensteten") des GvD vom 7. März 2005, Nr. 82 i.d.g.F.;

Viste le "Linee guida per posta elettronica e internet" del Garante della privacy del 1 marzo 2007;

Nach Einsichtnahme in die von der Datenschutzbehörde erlassenen „Richtlinien für die Nutzung der elektronischen Post und von Internet" vom 1. März 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

Aufgrund der von der Datenschutzbehörde erlassenen „Sicherheitsmaßnahmen" zum Datenschutz (insbesondere der allgemeinen Maßnahme vom 27. November 2008

2008 riguardante gli Amministratori di Sistema);

betreffend die Systemverwalter);

Visto il Contratto collettivo 1.12.2008 e s. m.;

Aufgrund des Tarifvertrags vom 1.12.2008 i.d.g.F.;

Visto il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016;

Aufgrund der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 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;

Aufgrund des Rundschreibens der Agenzia per l'Italia Digitale vom 18. April 2017, Nr. 2/2017 „ICT-Mindestsicherheitsmaßnahmen für die öffentlichen Verwaltungen";

Visto il Decreto Legislativo 10 agosto 2018, n. 101;

Aufgrund des gesetzesvertretenden Dekrets vom 10. August 2018, Nr. 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.;

Aufgrund des zwischen der Regionalverwaltung und der Gesellschaft Südtiroler Informatik AG unterzeichneten Vertrags vom 20. Dezember 2018, Rep. Nr. 392;

Vista la deliberazione della Giunta Regionale del 3 settembre 2019 n. 193;

Aufgrund des Beschlusses der Regionalregierung vom 3. September 2019, Nr. 193;

Ad unanimità di voti legalmente espressi,

delibera

beschließt die Regionalregierung

mit Einhelligkeit gesetzmäßig abgegebener Stimmen,

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;

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;

di disporre che il Discplinare 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;

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;

zu verfügen, dass diese Anweisungen von allen Nutzern der Geräte zu befolgen sind;

di dare atto che le prescrizioni contenute nell' allegato A potranno essere aggiornate alla luce dell'esperienza e dell'innovazione tecnologica.

zu bestätigen, dass die Inhalte der Anlage A im Lichte der gesammelten Erfahrung und der technischen Innovation aktualisiert werden können.

Letto, confermato e sottoscritto.

Gelesen, bestätigt und unterzeichnet

IL PRESIDENTE

DER PRÄSIDENT

Arno Kompatscher
firmato digitalmente / digital signiert

IL SEGRETARIO GENERALE
DELLA GIUNTA REGIONALE

DER GENERALSEKRETÄR
DER REGIONALREGIERUNG

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 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

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 (GPDR).

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 removibili 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 removibili 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 dispostivi 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 anteponendo 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

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, idem 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, Nutzername 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 zurückführbare 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

Entfernbare 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.

Entfernbare 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. „TrueCript“) 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 Mitarbeiten, 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.