Visto per il controllo di regolarità contabile Sichtvermerk für die Buchhaltungskontrolle			Per la Direttrice dell'Ufficio Bilancio e Appalti Für die Leiterin des Amtes für Haushalt und Vergaben IL VICESEGRETARIO GENERALE/DER VIZEGENERALSEKRETÄR
Capitolo/Kapitel	Esercizio/Finanzjahr	Trento, Trient	

CONSIGLIO REGIONALE DEL TRENTINO-ALTO ADIGE

REGIONALRAT TRENTINO-SÜDTIROL

DELIBERAZIONE DELL'UFFICIO DI PRESIDENZA

BESCHLUSS DES PRÄSIDIUMS

N. 9/2023

Nr. 9/2023

SEDUTA DEL

SITZUNG VOM

14.02.2023

Presidente	***Josef Noggler***	***Präsident***
Vicepresidente vicario	***Roberto Paccher***	***Stellv. Vizepräsident***
Vicepresidente	***Luca Guglielmi***	***Vizepräsident***
Segretaria questora	***Paula Bacher***	***Präsidialsekretärin***
Segretario questore	***Devid Moranduzzo***	***Präsidialsekretär***
Assiste il Segretario generale del Consiglio regionale	***MMag. Jürgen Rella***	***Im Beisein des Generalsekretärs des Regionalrates***
Assenti:		***Abwesend:***
Segretario questore	***(giust.) Marco Galateo (entsch.)***	***Präsidialsekretär***

L'Ufficio di Presidenza delibera sul seguente OGGETTO:	**Das Präsidium beschließt zu nachstehendem GEGENSTAND:**
Prescrizioni generali in tema di protezione dei dati personali del Consiglio regionale	**Allgemeine Datenschutzbestimmungen des Regionalrats**

DELIBERAZIONE N. 9/2023

L'UFFICIO DI PRESIDENZA DEL CONSIGLIO REGIONALE

Visto il Regolamento Generale sulla Protezione dei Dati del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito GDPR) che ha introdotto un nuovo assetto normativo in materia di privacy e nuovi adempimenti per le Pubbliche Amministrazioni;

Dato atto che con Decreto legislativo 10 agosto 2018, n. 101 è stato adeguato il Decreto legislativo 30 giugno 2003, 196 – Codice in materia di protezione dei dati personali - alle disposizioni del GDPR;

Considerato che con il GDPR viene recepito nell'ordinamento giuridico italiano il "principio di accountability" (di responsabilizzazione), che impone alle Pubbliche Amministrazioni titolari del trattamento dei dati personali di mettere in atto misure tecniche e organizzative, riesaminate e aggiornate qualora necessario, adeguate per garantire che il trattamento è effettuato conformemente al GDPR;

Atteso che, per perseguire le finalità del principio di responsabilizzazione, di cui all'alinea precedente, il capo IV del GDPR prevede le seguenti tre figure: il titolare del trattamento, il responsabile del trattamento ed il responsabile della protezione dei dati (RPD);

Dato atto che il Consiglio regionale è il Titolare del trattamento dei dati personali riferibili all'esercizio delle funzioni istituzionali attribuite dall'ordinamento statutario;

Dato atto che con Deliberazione dell'Ufficio di Presidenza 21 febbraio 2022, n. 7 il Consiglio regionale ha deciso di avvalersi, per gli anni 2022 e 2023, del servizio di Responsabile della Protezione dei Dati (RPD) e di consulenza in materia di privacy affidato dalla Giunta regionale, anche nell'interesse del Consiglio regionale, al Consorzio dei Comuni Trentini per lo svolgimento delle funzioni ed i compiti del Responsabile della protezione dei dati personali

BESCHLUSS Nr. 9/2023

DAS PRÄSIDIUM DES REGIONALRATS -

Nach Einsicht in die Datenschutz-Grundverordnung des europäischen Parlaments und des Rates vom 27. April 2016 (nachfolgend GDPR), die neue Gesetzesbestimmungen auf dem Sachgebiet des Datenschutzes und neue Formalitäten für öffentliche Körperschaften eingeführt hat;

Zur Kenntnis genommen, dass das gesetzesvertretende Dekret Nr. 196 vom 30. Juni 2003 (Datenschutzkodex) durch das gesetzesvertretende Dekret Nr. 101 vom 10. August 2018 an die Bestimmungen der GDPR angepasst wurde;

Festgestellt, dass der „Grundsatz der Accountability" (d.h. der Rechenschaftspflicht) mittels der GDPR in die italienische Rechtsordnung aufgenommen wird und dass dadurch die öffentlichen Körperschaften als Verantwortliche für die Datenverarbeitung angehalten sind, adäquate technisch-organisatorische Maßnahmen zur Gewährleistung einer GDPR-konformen Datenverarbeitung umzusetzen und diese bei Bedarf zu überprüfen und zu aktualisieren;

Festgehalten, dass das Kapitel IV der GDPR zum Zweck der Umsetzung des im vorigen Absatz erwähnten Grundsatzes der Rechenschaftspflicht drei Akteure bestimmt, und zwar den Verantwortlichen der Datenverarbeitung, den Auftragsverarbeiter und den Datenschutzbeauftragten (DSB);

Festgestellt, dass der Regionalrat der Verantwortliche für die Verarbeitung personenbezogener Daten im Rahmen der ihm durch das Statut übertragenen amtlichen Aufgaben ist;

Festgestellt, dass der Regionalrat mit Präsidiumsbeschluss Nr. 7 vom 21. Februar 2022 beschlossen hat, für die Jahre 2022 und 2023 den Dienst des Datenschutzbeauftragten (DSB) und der datenschutzrechtlichen Beratung wahrzunehmen, den die Regionalregierung auch im Interesse des Regionalrates an das Trentiner Gemeindenkonsortium für die Erfüllung der Funktionen und der Aufgaben als Datenschutzbeauftragten (DSB) vergeben hat;

(RPD);

Dato atto che l'art. 29 del GDPR dispone che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento";*

Kundgetan, dass Artikel 29 der GDPR Folgendes verfügt: „*Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten*";

Preso atto che l'art. 30 del GDPR disciplina in capo al Titolare del trattamento la tenuta di un registro finalizzato alla mappatura di tutte le attività di trattamento svolte sotto la propria responsabilità;

Zur Kenntnis genommen, dass gemäß Artikel 30 der GDPR der Verantwortliche für die Datenverarbeitung angehalten ist, ein Verzeichnis für die Erfassung aller unter seiner Amtsgewalt durchgeführten Verarbeitungstätigkeiten zu führen;

Dato atto che il Registro dei trattamenti del Consiglio regionale è stato adottato ai sensi del GDPR, come risulta dalla nota prot. CRTAA n. 1138 del 19 marzo 2019;

Kundgetan, dass das Verzeichnis der Datenverarbeitungen des Regionalrates im Sinne der GDPR eingeführt wurde, wie dies aus dem Schreiben Prot. Nr. 1138 RegRat vom 19. März 2019 hervorgeht;

Visto l'articolo 32 del GDPR, che richiama le misure tecniche e organizzative che il Titolare del trattamento è tenuto ad adottare per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento;

Nach Einsicht in den Artikel 32 der GDPR, der auf die technisch-organisatorischen Maßnahmen hinweist, die der Verantwortliche für die Datenverarbeitung einleiten muss, damit unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung ein risikoadäquater Sicherheitsstandard gewährleistet wird;

Visto l'articolo 33 del GDPR, che tratta del caso di violazione dei dati personali e disciplina i conseguenti compiti informativi richiesti al titolare del trattamento nei confronti dell'autorità di controllo competente (c.d. procedura di "data breach");

Nach Einsicht in den Artikel 33 der GDPR, der vom Fall einer Verletzung personenbezogener Daten handelt und die damit zusammenhängende Meldepflicht des Verantwortlichen für die Datenverarbeitung gegenüber der Aufsichtsbehörde regelt (sog. „Data-Breach-Verfahren");

Dato atto che il Registro dei trattamenti di cui all'articolo 30 del GDPR è stato aggiornato in coerenza con il nuovo Regolamento della struttura organizzativa del Consiglio regionale, approvato con propria deliberazione 24 marzo 2022, n. 15, e con le attribuzioni degli uffici in esso previste;

Festgehalten, dass das Verzeichnis der Verarbeitungen laut Artikel 30 der GDPR entsprechend der mit eigenem Beschluss Nr. 15 vom 24. März 2022 genehmigten neuen Verordnung betreffend die Verwaltungsstruktur des Regionalrates und den darin vorgesehenen Zuständigkeitsbereichen der Ämter aktualisiert wurde;

Ritenuto di ridefinire la procedura di "data breach", ai sensi dell'articolo 33 del GDPR sopracitato, secondo il testo allegato alla presente deliberazione e costituente sua parte integrante e sostanziale;

In der Ansicht, das „Data-Breach-Verfahren", von dem Artikel 33 der GDPR handelt, im Sinne der Anlage, die integralen und wesentlichen Bestandteil des vorliegenden Beschlusses bildet, neu festzulegen;

Ritenuto, altresì, di far seguire al nuovo Regolamento della struttura organizzativa del Consiglio regionale la ricognizione delle prescrizioni e delle istruzioni generali in tema di trattamento dei dati personali e delle misure di sicurezza dei dati, come allegate alla presente deliberazione;

Visto l'articolo 5 del Regolamento interno;

Ad unanimità di voti legalmente espressi;

d e l i b e r a

1. per le motivazioni in premessa, di adottare i seguenti allegati alla presente deliberazione, costituenti sua parte integrante e sostanziale:
- l'allegato 1) "*Prescrizioni generali in tema di protezione dei dati personali"*;
- l'allegato 2) "*Procedura di segnalazione per le violazioni di dati personali (data breach)*";
- l'allegato 3) "*Misure di sicurezza dei dati*" .

2. di riservarsi l'adozione di ulteriori misure tecniche e organizzative per la sicurezza dei dati personali.

3. di trasmettere la presente deliberazione al RPD, Responsabile della Protezione dei Dati.

In der Ansicht, auf die Verordnung betreffend die Verwaltungsstruktur des Regionalrates die diesem Beschluss beigefügte Übersicht der Vorschriften und allgemeinen Anweisungen in Sachen Datenverarbeitung und der Datensicherheitsbestimmungen folgen zu lassen;

Nach Einsicht in den Artikel 5 der Geschäftsordnung;

Mit gesetzmäßig zum Ausdruck gebrachter Stimmeneinhelligkeit -

b e s c h l i e ß t

1. Aus den in den Prämissen dargelegten Gründen die folgenden Anlagen zum vorliegenden Beschluss zu billigen, die integrierenden und wesentlichen Bestandteil desselben bilden:
- Anlage 1) „*Allgemeine Datenschutzbestimmungen*";
- Anlage 2) „*Meldeverfahren bei Datenschutzverletzungen (Data Breach)*";
- Anlage 3) „*Datensicherheitsbestimmungen*".

2. sich vorzubehalten, zusätzliche technische und organisatorische Datenschutzbestimmungen zu erlassen;

3. vorliegenden Beschluss an den Datenschutzbeauftragten (DSB) weiterzuleiten.

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 ai sensi dell'art. 29 e ss. del D.lgs. 2.7.2010, n. 104;

b) ricorso straordinario al Presidente della Repubblica da parte di chi vi abbia interesse entro 120 giorni ai sensi del DPR 24.11.1971, n. 1199.

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, innerhalb von 60 Tagen im Sinne des Art. 29 ff. des GvD vom 2. Juli 2010, Nr. 104 einzulegen ist;

b) außerordentlicher Rekurs an den Präsidenten der Republik, der von Personen, die ein rechtliches Interesse daran haben, innerhalb 120 Tagen im Sinne des DPR vom 24. November 1971, Nr. 1199 einzulegen ist.

IL PRESIDENTE/DER PRÄSIDENT
- Josef Noggler -
firmato-gezeichnet

IL SEGRETARIO GENERALE/DER GENERALSEKRETÄR
- MMag. Jürgen Rella -
firmato-gezeichnet

Allegato 1

Prescrizioni generali in tema di protezione dei dati personali

1. Le prescrizioni contenute nel presente documento e nel documento al medesimo allegato devono essere considerate quale livello minimo per il puntuale adempimento degli obblighi previsti dal d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, e dal Regolamento generale (UE) 2016/679 sulla protezione dei dati personali (RPD, di seguito Regolamento o GDPR).

2. Il Consiglio regionale è il Titolare del trattamento dei dati personali finalizzati all'esercizio delle funzioni istituzionali attribuite dall'ordinamento. Per espletare le funzioni istituzionali connesse alla titolarità dei dati operano, nell'ambito delle rispettive competenze, il Presidente del Consiglio regionale e l'Ufficio di presidenza. Rientra nella responsabilità del Titolare:

a) assicurare costantemente di aver messo in atto le misure tecniche ed organizzative adeguate conformi al Regolamento, dimostrandolo e documentandolo (principio di accountability art. 24.1 GDPR) anche sotto il profilo dell'efficacia delle misure intraprese;

b) notificare all'Autorità di controllo (il Garante italiano per la protezione dei dati) la violazione di dati personali (personal data breach) entro 72 ore dal momento in cui ne è venuto a conoscenza (art. 33 GDPR);

c) notificare agli interessati al trattamento di dati personali la violazione, solo nel caso in cui questa sia suscettibile di presentare un rischio elevato per i loro diritti e le libertà (art. 34 GDPR).

3. Ai sensi dell'art. 2-quaterdecies Codice Privacy (d.lgs. n. 196/2003, novellato dal d.lgs. n. 101/2018), il Titolare può delegare compiti e funzioni a persone fisiche che operano sotto la sua autorità e che, a tal fine, dovranno essere espressamente designati. Conseguentemente, il Segretario generale e il Vicesegretario generale, ciascuno per i trattamenti che siano riconducibili allo loro esclusiva competenza, sono designati, previa istruzione, all'esercizio dei compiti e delle funzioni inerenti la protezione dei dati personali.

4. Ai sensi dell'art. 37, par. 1, lett. a), del GDPR, che impone l'obbligo per il Titolare ed il Responsabile del trattamento dei personali, "quando il trattamento è effettuato da un'autorità pubblica (…)", di designare il Responsabile dei dati personali (RPD), il Consorzio dei

Comuni di Trento, sino alla scadenza dell'incarico, e successivamente gli altri soggetti che saranno individuati per l'esercizio delle medesime funzioni, sono i soggetti designati Responsabili dei dati personali (RDP) del Consiglio regionale e curano per il medesimo il servizio di Responsabile della Protezione dei dati (RPD) e di consulenza in materia di privacy.

5. Esclusi gli ambiti di competenza degli organi istituzionali, per i quali provvede il Titolare, ai Dirigenti/Responsabili del trattamento dei dati è demandato, per conto del Titolare, il compito di nominare, quali Responsabili esterni del trattamento, tutti i soggetti esterni che collaborano con il Consiglio regionale per l'esercizio delle funzioni istituzionali ad essi attribuiti e che non siano persone fisiche. I soggetti esterni che collaborano con il Consiglio regionale per l'esercizio delle proprie funzioni istituzionali e che siano persone fisiche sono nominati Responsabili esterni del trattamento dal Dirigente/Responsabile del trattamento solo dopo aver individuato il ruolo ritenuto più idoneo, posto che gli stessi possono essere nominati, in alternativa, anche incaricati esterni del trattamento. Ad integrazione delle attribuzioni in tema di nomina dei Responsabili esterni, i dirigenti/Responsabili del trattamento impartiscono ai medesimi le istruzioni relative al predetto ruolo.

6. Spetta ai Dirigenti/responsabili del trattamento designare le Persone autorizzate al trattamento dei dati avvalendosi della facoltà di cui articolo 4, n. 10, del GDPR, che permette di autorizzare al trattamento i dipendenti del Consiglio regionale in ragione dell'appartenenza alle rispettive strutture e/o uffici. I Dirigenti/Responsabili del trattamento possono fare riferimento nell'atto di autorizzazione a tutte le informazioni contenute nel registro delle attività di trattamento, di cui al successivo punto 12). In applicazione dei principi di semplificazione ed economicità, i Dirigenti/Responsabili del trattamento sono tenuti ad inserire nel registro delle attività i nominativi delle Persone autorizzate in corrispondenza ai trattamenti di loro pertinenza. In conseguenza, le Persone autorizzate al trattamento potranno trattare esclusivamente i dati di pertinenza dell'ufficio di appartenenza e quelli ulteriori eventualmente attribuiti. Nel caso di passaggio o trasferimento, anche temporaneo, ad altra struttura/ufficio, la persona autorizzata perde i privilegi di accesso ai dati personali attribuiti all'ufficio di provenienza.

7. Alle Persone autorizzate al trattamento sono impartite le istruzioni generali, indicate in allegato alle presenti Prescrizioni, che rappresentano l'ambito del trattamento consentito. Ad opera dei Dirigenti/Responsabili del trattamento, il contenuto delle istruzioni potrà essere periodicamente integrato ed aggiornato, anche con eventuali e più specifiche prescrizioni, quando lo richieda la peculiarità dei trattamenti svolti nell'ambito delle strutture di appartenenza.

8. Ai Dirigenti/responsabili dei trattamenti è attribuito il compito di individuare nell'ambito delle strutture di rispettiva competenza i collaboratori (c.d. Referenti privacy) chiamati ad occuparsi anche di protezione dei dati personali, i quali sono chiamati a coordinarsi con i Dirigenti/Responsabili del trattamento.

9. Ove non già disposto, i Dirigenti/Responsabili del trattamento sono incaricati di provvedere, nell'ambito delle strutture di competenza, alla nomina dell'Amministratore dei sistemi informativi non gestiti da Informatica Trentina s.p.a..

10. I Dirigenti/responsabili del trattamento sono incaricati, per conto del Titolare e sulla base di quanto disposto dall'articolo 29, commi 2 e 5, del d.lgs. n. 196/2003, di vigilare sull'osservanza delle misure di sicurezza e sulle istruzioni fornite dal Titolare.

11. L'Ufficio competente in materia di informatica è incaricato, per conto del Titolare, del compito di svolgere i controlli miranti a garantire l'applicazione delle misure di sicurezza informatica previste all'articolo 32, paragrafo 1, del GDPR. Il medesimo Ufficio può avvalersi, ove necessario, di soggetti esterni. In tale caso, l'Ufficio è tenuto ad accertare che l'applicazione delle misure di sicurezza informatica sia realizzata puntualmente. Allo stesso Ufficio è demandato il compito di individuare le istruzioni operative ad integrazione, specificazione e chiarimento delle disposizioni contenute nel documento allegato alle presenti prescrizioni.

12. I Dirigenti del Consiglio regionale dovranno provvedere al censimento dei trattamenti dei dati personali in atto e delle banche dati in uso nell'ambito degli uffici consiliari, inserendo tali informazioni nel registro delle attività di trattamento. Ogni singolo ufficio dovrà tenere costantemente aggiornato il predetto registro secondo modalità tecnico-operative condivise con l'ufficio competente in materia di informatica.

Allegato A

Istruzioni generali impartite dal Titolare

Definizioni:

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile mediante riferimento a qualsiasi altra informazione disponibile.

Dato particolare: i dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

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.

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

Autorizzati al trattamento: le persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, a prescindere dalla funzione svolta all'interno dell'Ateneo.

Postazione di lavoro: l'insieme degli strumenti informatici e non messi a disposizione dal datore di lavoro per rendere la prestazione lavorativa, sia in sede sia in mobilità (ad es. archivi, armadi, cassettiere, scrivanie, computer, stampanti, fax, telefoni cellulari di proprietà dell'Ateneo, ecc.).

La presente comunicazione è rivolta a tutti gli incaricati del trattamento dei dati ed è impartita ai sensi dell'articolo 29 del GDPR, il quale stabilisce che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non* ***è istruito*** *in tal senso dal Titolare del trattamento".*

1. Il soggetto autorizzato al trattamento deve aver accesso ai soli dati personali la cui conoscenza è strettamente necessaria ad adempiere alle funzioni e ai compiti a lui assegnati.

2. Il soggetto autorizzato al trattamento deve controllare e custodire gli atti e i documenti contenenti i dati personali per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento. Gli stessi non devono essere lasciati incustoditi in assenza del soggetto autorizzato.

3. Durante le operazioni di trattamento al soggetto autorizzato al trattamento compete la conservazione degli atti e dei documenti a lui affidati. Al termine delle operazioni di trattamento, questi ultimi devono essere archiviati, conservati al chiuso e protetti da serratura. Nel caso di atti o documenti elettronici, vanno chiusi gli applicativi o le cartelle informatiche utilizzate per il loro prelievo.

4. In caso di trattamento di dati sensibili o di dati giudiziari, il soggetto autorizzato al trattamento deve controllare e custodire gli atti e i documenti a lui affidati, in maniera tale che ad essi non accedano persone prive di autorizzazione. Al termine delle operazioni affidate, il soggetto autorizzato al trattamento provvede ai sensi del punto 3.

5. I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento dei dati sensibili e/o dei dati giudiziari devono essere conservati e custoditi in modo tale da escluderne l'accesso ai soggetti non autorizzati.

6. Nelle operazioni di trattamento, si devono ridurre al minimo i rischi di distruzione e di perdita dei dati.

7. Per l'effettuazione di operazioni di trattamento mediante l'ausilio di strumenti elettronici o automatizzati si devono utilizzare le modalità di accesso fornite dai Dirigenti/Responsabili del trattamento attraverso l'Amministratore dei sistemi informativi e si devono custodire i dati trattati con la dovuta riservatezza.

8. Nei casi in cui è prevista l'utilizzazione di codici identificativi e/o di parole chiave di accesso, l'addetto al trattamento deve modificare tali credenziali alle scadenze previste, rispettando le prescrizioni fornite dall'Amministratore dei sistemi informativi.

9. Non è consentito lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. Del pari, non è consentito lasciare incustoditi e accessibili atti e documenti contenenti dati personali, compresi quelli riconducibili a particolari categorie (art. 9 del Regolamento GDPR) e quelli relativi a condanne penali e reati (art. 10 del Regolamento GDPR).

10. È fatto divieto di trasmettere a terzi informazioni circa i dati personali trattati o comunque appresi in occasione dell'espletamento della propria attività. La comunicazione e la diffusione è ammessa soltanto se funzionale allo svolgimento dei compiti affidati o in forza di obblighi normativi, comunque previa autorizzazione del Responsabile del trattamento.

In caso di rapporti con un soggetto interessato, si deve accertare che allo stesso sia consegnata l'informativa sul trattamento dei suoi dati personali, completa in tutte le sue parti.

11. Nel caso in cui, per lo svolgimento delle attività e dei compiti affidati, è doveroso accertare l'identità dell'interessato, ma senza alcuna necessità di mantenere copia del documento identificativo del medesimo, è sufficiente limitarsi alla verifica del documento.

12. La postazione di lavoro deve essere configurata in modo che sia impostato l'avvio automatico dello screensaver ("salvaschermo") dopo al massimo 15 minuti di inattività del Personal Computer. È facoltà degli Autorizzati, qualora lo ritengano necessario od opportuno in ragione dei dati che stanno trattando, stabilire un intervallo temporale minore.

Anlage 1

Allgemeine Datenschutzbestimmungen

1. Die in diesem Schreiben und in der Anlage enthaltenen Bestimmungen sind als Mindeststandard für die rechtmäßige Erfüllung der Verpflichtungen laut dem gesetzesvertretenden Dekret Nr. 196 vom 30. Juni 2003, abgeändert durch das gesetzesvertretende Dekret Nr. 101 vom 10. August 2018, und der Datenschutz-Grundverordnung (EU) 2016/679 (im Folgenden Verordnung oder GDPR) zu betrachten.

2. Der Regionalrat ist der Verantwortliche für die Verarbeitung personenbezogener Daten zwecks Ausübung der gesetzlich vorgesehenen institutionellen Aufgaben. Der Präsident des Regionalrats und das Präsidium sind im Rahmen ihrer jeweiligen Zuständigkeiten mit der Durchführung der institutionellen Aufgaben im Zusammenhang mit dem Eigentum an den Daten betraut. Es obliegt dem Verantwortlichen:

a) sich laufend zu vergewissern, dass geeignete technische und organisatorische Maßnahmen im Einklang mit der Verordnung umgesetzt werden, was auch im Hinblick auf die Wirksamkeit der getroffenen Maßnahmen nachzuweisen und zu dokumentieren ist (Grundsatz der Rechenschaftspflicht, Art. 24.1 GDPR);

b) der Aufsichtsbehörde (d.h. der italienischen Datenschutzbehörde) Verletzungen personenbezogener Daten (personal data breach) binnen 72 Stunden nach deren Bekanntwerden zu melden (Art. 33 GDPR);

c) die betroffenen Personen erst dann von der Verletzung personenbezogener Daten in Kenntnis zu setzen, wenn ein hohes Risiko für ihre Rechte und Freiheiten besteht (Art. 34 GDPR).

3. Im Sinne von Art. 2-quaterdecies der Datenschutzverordnung (gvD Nr. 196/2003 abg. durch gvD Nr. 101/2018) darf der Verantwortliche Aufgaben und Funktion an natürliche Personen delegieren, die unter seiner Amtsgewalt handeln, wobei diese Personen zu diesem Zweck ausdrücklich zu bestimmen sind. Dementsprechend werden der Generalsekretär und der Vizegeneralsekretär jeweils für Verarbeitungen, die in ihre ausschließlichen Zuständigkeitsbereiche fallen, nach erfolgter Anweisung mit der Wahrnehmung der Aufgaben und Funktionen im Zusammenhang mit dem Datenschutz betraut.

4. Im Sinne von Art. 37, Abs. 1, Buchstabe a) der GDPR, der dem Verantwortlichen und dem Auftragsverarbeiter die Pflicht vorschreibt, einen Datenschutzbeauftragten (DSB) zu benennen, wenn „die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt

wird“, werden bis zum Ablauf des Auftrags das Trentiner Gemeindekonsortium und danach die anderen mit denselben Aufgaben betrauten Rechtssubjekte als Datenschutzbeauftragte (DSB) des Regionalrats bestimmt; diese erbringen in dessen Auftrag den Dienst des Datenschutzbeauftragten (DSB) und die entsprechende datenschutzrechtliche Beratung.

5. Mit Ausnahme der Zuständigkeitsbereiche der institutionellen Organe, für die der Verantwortliche sorgt, sind die Führungskräfte/Auftragsverarbeiter im Auftrag des Verantwortlichen mit der Aufgabe betraut, alle externen Rechtssubjekte, die mit dem Regionalrat bei der Ausübung der ihm zugewiesenen institutionellen Aufgaben zusammenarbeiten und die keine natürlichen Personen sind, als externe Auftragsverarbeiter zu bestimmen. Externe Rechtssubjekte, die mit dem Regionalrat bei der Ausübung seiner institutionellen Aufgaben zusammenarbeiten und natürliche Personen sind, werden von der Führungskraft/vom Auftragsverarbeiter nur dann als externe Auftragsverarbeiter bestimmt, nachdem die für sie am besten geeignete Rolle festgelegt worden ist, zumal sie alternativ auch als externe beauftragte Verarbeiter bestimmt werden können. Zusätzlich zu den Befugnissen zu deren Bestimmung erteilen die Führungskräfte/Auftragsverarbeiter den externen Auftragsverarbeitern Anweisungen in Bezug auf die vorgenannte Aufgabe.

6. Kraft der in Artikel 4, Absatz 10 der GDPR vorgesehenen Befugnis, die mit der Datenverarbeitung zu betrauenden Personen zu bestimmen, obliegt es den Führungskräften/Auftragsverarbeitern, die Bediensteten des Regionalrats aufgrund ihrer Zugehörigkeit zu den jeweiligen Einrichtungen bzw. Ämtern zur Datenverarbeitung zu ermächtigen. Die Führungskräfte/Auftragsverarbeiter können im Ermächtigungsschreiben auf alle Informationen verweisen, die im Verzeichnis der Verarbeitungstätigkeiten (siehe Punkt 12) erfasst sind. In Anwendung der Grundsätze der Vereinfachung und der Kosteneffizienz sind die Führungskräfte/Auftragsverarbeiter verpflichtet, im Verzeichnis der Verarbeitungstätigkeiten die Namen der zur Verarbeitung Ermächtigten neben den ihnen zugewiesenen Verarbeitungen zu vermerken. Folglich dürfen die zur Verarbeitung Ermächtigten nur die Daten verarbeiten, die in die Zuständigkeit des Amts fallen, dem sie angehören, sowie weitere Daten, die ihnen gegebenenfalls zugewiesen werden. Im Falle eines auch nur vorübergehenden Wechsels oder einer Versetzung in eine andere Einrichtung oder in ein anderes Amt kommen die zur Verarbeitung Ermächtigten um die Zugriffsrechte auf die personenbezogenen Daten, die dem Herkunftsamt zugewiesen sind.

7. Den zur Verarbeitung Ermächtigten werden die im Anhang zu den vorliegenden Datenschutzbestimmungen aufgeführten allgemeinen Anweisungen erteilt, die den zulässigen Verarbeitungsbereich darstellen. Die Führungskräfte/Auftragsverarbeiter können den Inhalt der Anweisungen regelmäßig aktualisieren und gegebenenfalls auch um spezifischere Vorschriften ergänzen, wenn besondere Arten der Verarbeitung bei den eigenen Einrichtungen dies erfordern.

8. Die Führungskräfte/Auftragsverarbeiter haben die Aufgabe, in den ihnen unterstellten Einrichtungen die Bediensteten zu bestimmen, die sich als sog. Datenschutzreferenten auch mit dem Datenschutz befassen und sich hierfür mit den Führungskräften/Auftragsverarbeitern koordinieren müssen.

9. Falls dies nicht bereits erfolgt ist, haben die Führungskräfte/Auftragsverarbeiter die Aufgabe, in den ihnen unterstellten Einrichtungen einen Administrator für die Informationssysteme zu bestimmen, die nicht von der Firma Informatica Trentina AG betrieben werden.

10. Die Führungskräfte/Auftragsverarbeiter haben die Aufgabe, im Auftrag der Verantwortlichen auf der Grundlage der Bestimmungen von Artikel 29, Absätze 2 und 5 des gvD Nr. 196/2003 die Einhaltung der vom Verantwortlichen erteilten Sicherheitsbestimmungen und Anweisungen zu überwachen.

11. Das Amt für Informatik hat die Aufgabe, im Auftrag der Verantwortlichen Kontrollen durchzuführen, damit die Umsetzung der IT-Sicherheitsbestimmungen laut Artikel 32, Absatz 1 der GDPR gewährleistet wird. Dasselbe Amt kann bei Bedarf auf externe Stellen zurückgreifen. In diesem Fall muss das Amt sicherstellen, dass die IT-Sicherheitsbestimmungen vorschriftsmäßig angewandt werden. Demselben Amt wird die Aufgabe übertragen, operative Anweisungen zur Ergänzung, Präzisierung und Klärung der Vorschriften aus der Anlage zu den vorliegenden Bestimmungen festzulegen.

12. Die Führungskräfte des Regionalrates müssen eine Bestandsaufnahme der laufenden Verarbeitungen personenbezogener Daten und der bei den Regionalratsämtern verwendeten Datenbanken vornehmen und diese Informationen ins Verzeichnis der Verarbeitungstätigkeiten eintragen. Die einzelnen Ämter müssen das genannte Verzeichnis gemäß den mit dem Informatik-Amt abgestimmten technisch-operativen Modalitäten laufend aktualisieren.

Anlage A

Allgemeine Anweisungen des Verantwortlichen

Begriffsbestimmungen:

Personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder anhand jeglicher anderen verfügbaren Information identifizierbare natürliche Person beziehen.

Besondere Daten: personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer Person.

Verarbeitung: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten.

Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Zur Datenverarbeitung Ermächtigte: natürliche Personen, die unabhängig von der eigenen Funktion innerhalb der Körperschaft unter der direkten Amtsgewalt des Verantwortlichen bzw. des Auftragsverarbeiters zur Verarbeitung von Daten ermächtigt sind.

Arbeitsplatz: die Gesamtheit der elektronischen und nichtelektronischen Hilfsmittel, die vom Arbeitgeber für die Erbringung von Arbeitsleistungen vor Ort sowie unterwegs bereitgestellt werden (wie etwa Archive, Schränke, Schubladen, Schreibtische, PCs, Drucker, Faxgeräte, Mobiltelefone im Eigentum der Körperschaft usw.).

Die vorliegende Mitteilung richtet sich an alle zur Verarbeitung Ermächtigten und erfolgt im Sinne von Artikel 29 der GDPR, der Folgendes verfügt: „*Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten*“.

1. Die zur Datenverarbeitung Ermächtigten haben Zugang ausschließlich zu jenen personenbezogenen Daten, deren Kenntnis zur Erfüllung der ihnen übertragenen Funktionen und Aufgaben unbedingt erforderlich ist.

2. Die zur Datenverarbeitung Ermächtigten müssen die Unterlagen und Dokumente, die personenbezogenen Daten enthalten, während des gesamten für die Durchführung der

Verarbeitung erforderlichen Zeitraums in Verwahrung nehmen und überwachen. Dieselben Dokumente dürfen in Abwesenheit der Ermächtigten nicht unbeaufsichtigt bleiben.

3. Während der Verarbeitungsvorgänge sind die zur Verarbeitung Ermächtigten für die Aufbewahrung der ihnen anvertrauten Unterlagen und Dokumente verantwortlich. Nach Beendigung der Vorgänge müssen die Unterlagen und Dokumente im Archiv gelagert und in geschlossenen, vorzugsweise mit Schlössern versehenen Boxen aufbewahrt werden. Handelt es sich um elektronische Unterlagen oder Dokumente müssen die Anwendungen oder Computerordner, die man für deren Abruf verwendet hat, geschlossen werden.

4. Im Falle der Verarbeitung sensibler oder gerichtlicher Daten müssen die zur Verarbeitung Ermächtigten die ihnen zugeteilten Unterlagen und Dokumente überwachen und verwahren, damit Unbefugte keinen Zugriff darauf haben. Nach Beendigung der Vorgänge gehen die zur Verarbeitung Ermächtigten gemäß Punkt 3 vor.

5. Nichtelektronische Datenträger, die Informationen über die Verarbeitung sensibler bzw. gerichtlicher Daten abbilden, müssen so aufbewahrt werden, dass der Zugriff durch Unbefugte ausgeschlossen ist.

6. Bei der Verarbeitung müssen die Risiken der Vernichtung und des Verlusts von Daten minimiert werden.

7. Bei der Durchführung von Verarbeitungen mithilfe elektronischer oder automatisierter Verfahren sind die von den Führungskräften/Auftragsverarbeitern durch die Vermittlung des Administrators der Informationssysteme bereitgestellten Zugriffsmodalitäten anzuwenden; die verarbeiteten Daten müssen mit der gebotenen Vertraulichkeit aufbewahrt werden.

8. Wenn die Verwendung von Identifizierungscodes bzw. Kennwörtern vorgesehen ist, muss der Datenverarbeiter dieselben zu den vorgeschriebenen Fristen unter Einhaltung der Anweisungen des Administrators der Informationssysteme ändern.

9. Während eines Verarbeitungsvorgangs darf ein elektronisches Gerät nicht unbeaufsichtigt bzw. zugänglich gelassen werden. Das Gleiche gilt für Unterlagen und Dokumente, die personenbezogene Daten enthalten, einschließlich derjenigen, die den besonderen Kategorien zugeordnet werden können (Art. 9 der GDPR) oder sich auf strafrechtliche Verurteilungen und Straftaten beziehen (Art. 10 der GDPR).

10. Die Weitergabe an Dritte von Informationen über die verarbeiteten oder bei der Ausübung der Tätigkeit wie auch immer eingesehenen personenbezogenen Daten ist untersagt. Die Übermittlung und Verbreitung sind nur dann zulässig, wenn sie entweder für die Erfüllung der übertragenen Aufgaben zweckmäßig oder gesetzlich vorgeschrieben sind; in jedem Fall erfolgen sie vorbehaltlich der Ermächtigung durch den Auftragsverarbeiter.

Im Falle von Beziehungen zu einer betroffenen Person muss sichergestellt werden, dass dieser die vollständige Datenschutzerklärung ausgehändigt wird.

11. Falls für die Durchführung der übertragenen Tätigkeiten und Aufgaben die Identität der betroffenen Person festgestellt, aber keine Kopie von deren Personalausweis eingeholt werden muss, genügt die Überprüfung des Personalausweises.

12. Der Computerarbeitsplatz muss so konfiguriert sein, dass der Bildschirmschoner („Screensaver“) spätestens nach fünf Minuten Inaktivität automatisch gestartet wird. Es liegt im Ermessen der zur Verarbeitung Ermächtigten, eine kürzere Aktivierungszeit einzustellen, wenn sie dies aufgrund der von ihnen verarbeiteten Daten für notwendig oder angemessen halten.

CONSIGLIO REGIONALE
DELLA REGIONE AUTONOMA
TRENTINO-ALTO ADIGE

REGIONALRAT
DER AUTONOMEN REGION
TRENTINO-SÜDTIROL

Allegato 2

PROCEDURA DI SEGNALAZIONE PER LE VIOLAZIONI DI DATI PERSONALI (DATA BREACH)

Definizione di data breach

Il "data breach" è 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.

Alcuni possibili esempi sono l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati; - il furto o la perdita di dispositivi informatici contenenti dati personali; - la deliberata alterazione di dati personali; - l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.; - la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità; la divulgazione non autorizzata dei dati personali.

Contenuto dell'obbligo

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo senza giustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dai motivi del ritardo.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

La notifica deve contenere i seguenti elementi fondamentali:

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

- descrizione delle probabili conseguenze della violazione dei dati personali;

- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Il titolare del trattamento è tenuto a documentare qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto delle prescrizioni normative.

La violazione dei dati personali deve essere prontamente comunicata all'interessato dal titolare del trattamento quando è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La comunicazione deve essere resa con un linguaggio semplice e chiaro atto a far comprendere la natura della violazione dei dati personali e deve contenere almeno le informazioni e le misure necessarie a descrivere le probabili conseguenze e le misure adottate per porre rimedio alla violazione.

Non è richiesta la comunicazione all'interessato solamente qualora il titolare del trattamento abbia messo in atto le misure tecniche e organizzative adeguate di protezione oppure abbia adottato successivamente misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati.

È altresì possibile procedere ad una comunicazione pubblica o ad una misura simile, tramite la quale gli interessati sono informati con analoga efficacia, se la comunicazione agli interessati richieda sforzi sproporzionati.

Procedura

Schema delle diverse fasi da osservare da parte dei dipendenti e/o collaboratori, consulenti e fornitori che vengono a conoscenza di un'ipotesi di violazione dei dati personali nel contesto dell'attività lavorativa o professionale per conto del Consiglio Regionale Trentino-Alto Adige/Südtirol.

Fase	***Attività***	***Chi***	***A chi***	***Quando***	***Come***
1	**Rilevazione e segnalazione di violazione dei dati**	Tutto il personale, collaboratori, fornitori	Al Segretario Generale del Consiglio regionale, in qualità di responsabile del trattamento dei dati o al Vicesegretario Generale del Consiglio regionale, in caso di assenza o impedimento del primo, che attiva la procedura	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, di persona, e-mail)

Fase	*Attività*	*Chi*	*A chi*	*Quando*	*Come*
2	**Raccolta informazioni sulla violazione**	Il Segretario Generale del Consiglio regionale o il Vicesegretario Generale del Consiglio regionale, in caso di assenza o impedimento del primo, insieme ai soggetti coinvolti nella violazione		Appena ricevuta la comunicazione	Raccogliendo informazioni dai soggetti coinvolti nella segnalazione e nel trattamento dei dati violati

3	**Comunicazione della violazione dati**	Il Segretario Generale del Consiglio regionale o il Vicesegretario Generale del Consiglio regionale, in caso di assenza o impedimento del primo	Al Responsabile della protezione dei dati (RPD)	Appena ottenute informazioni di base sulla violazione	Utilizzando le vie più brevi o la mail del RPD
Fase	***Attività***	***Chi***	***A chi***	***Quando***	***Come***
4	**Valutazione d'impatto**	RPD, soggetti coinvolti		Appena ricevuta la comunicazione	Utilizzando le metodologie standard
5	**Individuazione delle azioni correttive**	RPD, soggetti coinvolti		Appena terminata la valutazione d'impatto	Analizzando i risultati della valutazione d'impatto

6	**Comunicazione delle valutazioni effettuate e delle azioni da intraprendere**	RPD, Segretario Generale del Consiglio regionale o Vicesegretario Generale del Consiglio regionale, in caso di assenza o impedimento del primo	Al Titolare		Tramite una relazione
Fase	***Attività***	***Chi***	***A chi***	***Quando***	***Come***
7	**Notifica della violazione**	Titolare	Al Garante	Entro 72 ore dalla rilevazione	Mediante la modulistica predisposta dal Garante
8	**Comunicazione agli interessati coinvolti**	Titolare	Alle persone fisiche i cui dati sono stati violati	Nei termini indicati nella valutazione d'impatto	Comunicazione diretta alle singole persone o mediante pubblicazione in sito a loro accessibile delle eventuali conseguenze della violazione sulle categorie di persone fisiche interessate

CONSIGLIO REGIONALE
DELLA REGIONE AUTONOMA
TRENTINO-ALTO ADIGE

REGIONALRAT
DER AUTONOMEN REGION
TRENTINO-SÜDTIROL

Anlage 2

MELDEVERFAHREN
BEI DATENSCHUTZVERLETZUNGEN
(DATA BREACH)

DEFINITION VON DATA BREACH

Ein „Data Breach" (Datenschutzverletzung) ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Eine Verletzung kann die Vertrautlichkeit, Integrität oder Verfügbarkeit von personenbezogenen Daten beeinträchtigen.

Einige mögliche Beispiele sind der Zugang zu oder die Erhebung von personenbezogenen Daten von Seiten unbefugter Dritter; der Diebstahl oder der Verlust der Datenträger, auf denen personenbezogene Daten abgespeichert sind; die absichtliche Veränderung der personenbezogenen Daten; die Unmöglichkeit des Datenzugriffs, durch ein zufälliges Ereignis oder aufgrund externer Angriffe, Viren, Malware usw.; der Verlust oder die Vernichtung der personenbezogenen Daten aufgrund von Unfällen, unerwünschten Ereignissen, Bränden oder anderen Naturkatastrophen; die unbefugte Verbreitung von personenbezogenen Daten.

INHALT DER MELDEPFLICHT

Der Verantwortliche meldet der Aufsichtsbehörde eine Verletzung des Schutzes personenbezogener Daten unverzüglich, wenn machbar, innerhalb von 72 Stunden, nachdem ihm die Verletzung bekannt wurde, es sei denn, die Verletzung des Schutzes personenbezogener Daten hat voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge. Erfolgt die Meldung gegenüber der Aufsichtsbehörde nicht innerhalb 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Sofern und soweit es nicht möglich ist, die Informationen gleichzeitig bereitzustellen, können sie ohne unangemessene weitere Verzögerung nach und nach bereitgestellt werden.

Die Meldung muss nachstehende Grundangaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, wenn möglich, unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen sowie der Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;

- eine Beschreibung der von dem Verantwortlichen getroffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Begrenzung ihrer möglichen nachteiligen Folgen.

Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich der Umstände der Verletzung des Schutzes personenbezogener Daten, ihrer Folgen und der getroffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Gesetzesvorschriften ermöglichen.

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung. In der Nachricht an die betroffene Person ist in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und sie muss mindestens die Informationen und Maßnahmen zur Beschreibung der möglichen Folgen und der ergriffenen Abhilfemaßnahmen enthalten.

Die Nachricht an die betroffene Person ist nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Schutzmaßnahmen getroffen hat oder der Verantwortliche durch Folgemaßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen voraussichtlich nicht eintritt.

Sofern die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden ist, werden die betroffenen Personen durch eine öffentliche Bekanntmachung oder auf ähnlich wirksame Weise informiert.

VERFAHREN

Vorlage für die seitens der Bediensteten und/oder Mitarbeiter, Berater oder Lieferanten einzuhaltenden Schritte, welchen im Rahmen ihrer Arbeit oder beruflichen Tätigkeit im Auftrag des Regionalrates von Trentino-Südtirol eine mögliche Verletzung des Schutzes personenbezogener Daten bekannt wird.

Schritt	***Tätigkeit***	***Wer***	***Wem***	***Wann***	***Wie***
1	**Feststellung und Meldung einer Datenschutzverletzung**	Alle Bediensteten, Mitarbeiter, Lieferanten	Dem Generalsekretär des Regionalrates oder – im Falle seiner Abwesenheit oder Verhinderung – dem Vizegeneralsekretär des Regionalrates in ihrer Eigenschaft als Auftragsverarbeiter zwecks Einleitung des Verfahrens	Sobald die Verletzung bekannt wird	Auf kürzestem Weg (Telefon, persönliches Gespräch, E-Mail)

Schritt	*Tätigkeit*	*Wer*	*Wem*	*Wann*	*Wie*
2	**Einholen von Informationen über die Datenschutzverletzung**	Der Generalsekretär des Regionalrates oder – im Falle seiner Abwesenheit oder Verhinderung – der Vizegeneralsekretär des Regionalrates zusammen mit den an der Feststellung der Verletzung beteiligten Personen		Unmittelbar nach Erhalt der Meldung	Einholen von Informationen bei den an der Meldung und an der Verarbeitung der verletzten Daten beteiligten Personen
3	**Meldung einer Datenschutzverletzung**	Der Generalsekretär des Regionalrates oder – im Falle seiner Abwesenheit oder Verhinderung – der Vizegeneralsekretär des Regionalrates	Dem Datenschutzbeauftragten (DSB)	Sobald die wichtigsten Informationen über die Verletzung vorliegen	Auf kürzestem Weg oder durch die E-Mail des DSB

Schritt	*Tätigkeit*	*Wer*	*Wem*	*Wann*	*Wie*
4	**Datenschutz-Folgeabschätzung**	DSB, beteiligte Personen		Unmittelbar nach Erhalt der Meldung	Standardisierte Vorgehensweisen
5	**Festlegung von Korrekturmaßnahmen**	DSB, beteiligte Personen		Sobald die Datenschutz-Folgeabschätzung abgeschlossen ist	Analyse der Ergebnisse der Datenschutz-Folgeabschätzung
6	**Mitteilung der durchgeführten Überprüfungen und der zu ergreifenden Maßnahmen**	DSB, Generalsekretär des Regionalrates oder – im Falle seiner Abwesenheit oder Verhinderung – Vizegeneralsekretär des Regionalrates	Dem Verantwortlichen		Bericht

Schritt	*Tätigkeit*	*Wer*	*Wem*	*Wann*	*Wie*
7	**Meldung der Datenschutzverletzung**	Verantwortlicher	Der Aufsichtsbehörde	Binnen 72 Stunden ab Bekanntwerden	Anhand der von der Datenschutzbehörde erstellten Vordrucke
8	**Benachrichtigung der betroffenen Personen**	Verantwortlicher	Den von der Datenschutzverletzung betroffenen Personen	Innerhalb der in der Datenschutz-Folgeabschätzung angeführten Fristen	Direkte Benachrichtigung der einzelnen betroffenen Personen oder Veröffentlichung auf einer ihnen zugänglichen Webseite der möglichen Folgen der Datenschutzverletzung für die Kategorien betroffener natürlicher Personen

Allegato 3

Misure di sicurezza dei dati

Al fine di contrastare la vulnerabilità dei dati, a mente del d.lgs. 07 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e delle conseguenti Linee guida AGID, sono previste le seguenti misure di sicurezza dei dati.

Autenticazione e autorizzazione degli utenti

La gestione degli accessi ai dati presuppone la loro accessibilità unicamente agli utenti che ne hanno necessità per lo svolgimento delle proprie mansioni lavorative. A tale scopo è prevista la preventiva autorizzazione e l'autenticazione, mediante assegnazione di nome utente e password temporanea, del personale interessato.

L'autorizzazione riguarda tanto i dati cartacei quanto quelli informatici.

L'autenticazione è riferita ai soli dati informatici e presuppone che ciascun utente all'interno di un sistema informatico sia dotato di un proprio account individuale utile all'identificazione del soggetto autorizzato a trattare i dati. Tale passaggio è compiuto previa registrazione dei dipendenti nel controller di dominio con l'assegnazione dell'utente a specifiche categorie di dati accessibili. Il controller di dominio rilascia automaticamente una serie di servizi, come, ad esempio, l'applicazione dei criteri di sicurezza, l'autenticazione e l'accesso alle risorse.

La condivisione delle credenziali di autenticazione tra più soggetti anche legittimati all'accesso ai sistemi non risponde ad alcun requisito di sicurezza, motivo per il quale deve intendersi espressamente vietata.

Aggiornamento delle applicazioni

L'utilizzo di applicazioni richiede che le stesse siano aggiornate e non obsolete. Il continuo aggiornamento delle applicazioni costituisce una misura di sicurezza idonea a correggere vulnerabilità di volta in volta rese note e corrette dagli sviluppatori.

Le applicazioni fornite dal Consiglio regionale al momento della creazione dell'account sono di regola aggiornate automaticamente dal Consiglio regionale.

Le altre applicazioni fornite a taluni dipendenti in collegamento con le funzioni da esercitare devono essere aggiornate, per il tramite dell'amministratore di sistema, quando le stesse segnalino la richiesta di aggiornamento. L'utilizzo di applicazioni non aggiornate, per le quali il sistema ha richiesto l'aggiornamento, costituisce violazione delle misure di sicurezza.

È prevista una procedura di sorveglianza, demandata, rispettivamente, all'amministratore di sistema, per le applicazioni fornite alla generalità dei dipendenti, e all'utilizzatore, per le

applicazioni fornite solo a taluni dipendenti. Tale procedura prevede un periodico controllo sul regolare e corretto funzionamento delle applicazioni in dotazione finalizzata alla verifica di eventuali aggiornamenti e/o all'installazioni di patch di sicurezza.

La protezione dei dati trasmessi a terzi

Il dato trasmesso a terzi può essere intercettato e subire una violazione di riservatezza.
I dati cartacei devono essere trattati e conservati in modo tale da evitarne la divulgazione e l'accessibilità ai soggetti, anche dipendenti, non autorizzati.
Relativamente ai dati informatici, la maggior parte delle comunicazioni via Internet avviene tramite modalità criptate, con protocollo *https*; tuttavia esistono ancora servizi che non prevedono la cifratura dei dati, ad esempio il protocollo *http* (internet), il quale non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato.
Il Garante, con provvedimento del 23 gennaio 2020, ha stabilito che "*il mancato utilizzo di strumenti di crittografia per il trasporto dei dati si pone in contrasto con l'articolo 32 del Regolamento*" del GDPR. La medesima raccomandazione si applica anche all'utilizzo delle e-mail istituzionali. Pertanto, l'utilizzo di protocolli di cifratura, come il protocollo TLS e la cifratura end-to-end delle email in trasmissione, adottati dal Consiglio regionale, costituisce misura di sicurezza adeguata ai sensi dell'articolo 32 del GDPR.
Per la sicurezza dei dati trasmessi a terzi mediante il protocollo informatico (Pitre) è previsto, in conformità a quanto previsto dall'articolo 32 del G.D.P.R., l'utilizzo di strumenti di crittografia per il trasporto dei dati.

La protezione di dati e sistemi

Per la protezione dei dati cartacei, gli stessi, nel tempo in cui non sono utilizzati, sono conservati al chiuso. I dati archiviati sono conservati in appositi armadi chiusi, muniti di serratura, sottoposti alla sorveglianza degli uffici competenti e disponibili solo al personale autorizzato.
In ambito informatico i principali parametri di sicurezza dei dati sono, a mente del d.lgs. 07 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale) e delle conseguenti Linee Guida AGID, la riservatezza, l'integrità e la disponibilità che richiedono, rispettivamente, di:

- consentire l'accesso ai dati ai soli soggetti autorizzati e/o preposti (riservatezza);
- evitare che i dati possano essere modificati, cancellati, resi illeggibili, attaccati da virus (integrità);
- garantire un corretto e funzionale accesso ai dati accessibili mantenendo il corretto funzionamento del sistema informatico (disponibilità).

Per assicurare il rispetto dei parametri descritti, l'amministratore di sistema verifica sistematicamente l'integrità dei sistemi e monitora in modo pro-attivo qualsiasi irregolarità. Per impedire l'alterazione diretta o indiretta delle informazioni, sia da parte di utenti non autorizzati, sia a causa di eventi accidentali, è prescritto l'utilizzo di software di contrasto ai virus e ai malware informatici. Il Consiglio regionale, per il tramite dell'amministratore di sistema e in collaborazione con i singoli dipendenti, aggiorna periodicamente tali software,

fatti salvi i casi di oggettiva impossibilità. La medesima prescrizione è applicata ai sistemi operativi e agli applicativi utilizzati per il trattamento dei dati.

Procedure di continuità operativa

La continuità operativa è essenzialmente il risultato di un processo organizzativo che comprende tecnologie informatiche rispondenti a precise caratteristiche di robustezza.

Le Linee guida di AGID in materia di continuità operativa non prevedono misure tecniche predefinite, rimettendo alle amministrazioni la scelta ottimale delle soluzioni da adottare sulla base delle esigenze di continuità in termini di risorse da proteggere.

Per il Consiglio regionale, la continuità operativa è assicurata mediante un sistema di copie di riserva dei dati e dei sistemi in uso. In particolare, questi ultimi sono protetti da eventuali incidenti o violazioni di dati tramite applicazione di una procedura di ripristino degli stessi da effettuarsi in tempo reale rispetto al momento della conoscenza o comunque nel più breve tempo possibile. In via ordinaria, è previsto il backup giornaliero dei dati e dei sistemi.

Anlage 3

Datensicherheitsbestimmungen

Um die Anfälligkeit der Daten zu bekämpfen, werden in Übereinstimmung mit dem gesetzesvertretenden Dekret Nr. 82 vom 7. März 2005 (Kodex der digitalen Verwaltung) und den daraus folgenden AGID-Richtlinien nachstehende Datensicherheitsbestimmungen eingeführt.

Benutzerauthentifizierung und -autorisierung

Die Verwaltung der Datenzugriffe setzt voraus, dass nur die Benutzer Zugang zu den Daten haben, die sie zur Erfüllung ihrer Arbeitsaufgaben benötigen. Zu diesem Zweck ist die vorherige Autorisierung und Authentifizierung des betroffenen Personals durch die Zuteilung eines Benutzernamens und eines temporären Passworts erforderlich.
Die Autorisierung betrifft sowohl Daten in Papierform als auch elektronische.
Die Authentifizierung bezieht sich nur auf elektronische Daten und setzt voraus, dass jeder Benutzer innerhalb eines IT-Systems über ein eigenes individuelles Konto verfügt, das zur Identifizierung der zur Verarbeitung ermächtigten Person dient. Dies geschieht nach der Registrierung der Mitarbeiter im Domänencontroller mit der Zuordnung des Benutzers zu bestimmten Kategorien von zugänglichen Daten. Der Domänencontroller stellt automatisch eine Reihe von Diensten bereit wie z. B. die Anwendung von Sicherheitsrichtlinien, die Authentifizierung und den Zugang zu Ressourcen.
Die gemeinsame Nutzung von Authentifizierungsdaten durch mehrere auch zugriffsberechtigte Personen entspricht nicht den Sicherheitsanforderungen und ist daher ausdrücklich verboten.

Aktualisierung der Anwendungen

Die Nutzung von Anwendungen erfordert, dass sie aktualisiert werden, damit sie nicht veralten. Die regelmäßige Aktualisierung der Anwendungen stellt eine angemessene Sicherheitsmaßnahme dar, um Schwachstellen zu beheben, die von Zeit zu Zeit von den Entwicklern bekannt gegeben und korrigiert werden.
Anwendungen, die vom Regionalrat bei der Einrichtung eines Kontos zur Verfügung gestellt werden, werden normalerweise automatisch vom Regionalrat selbst aktualisiert.
Andere Anwendungen, die bestimmten Mitarbeitern im Zusammenhang mit den auszuübenden Funktionen zur Verfügung gestellt werden, müssen über den Systemadministrator aktualisiert werden, wenn eine Aktualisierungsaufforderung aufscheint.
Die Verwendung nicht aktualisierter Anwendungen, für die das System eine Aktualisierung angefordert hat, stellt einen Verstoß gegen die Sicherheitsmaßnahmen dar.

Es gibt ein Überwachungsverfahren, das für die allen Mitarbeitern zur Verfügung gestellten Anwendungen dem Systemadministrator und für die einzelnen Mitarbeitern zur Verfügung gestellten Anwendungen dem Benutzer übertragen wird. Dieses Verfahren sieht eine regelmäßige Überprüfung der ordnungsgemäßen und einwandfreien Funktionsweise der bereitgestellten Anwendungen vor, mit dem Ziel, etwaige Updates bzw. die Installierung von Sicherheitspatches zu überprüfen.

Schutz von an Dritte übermittelten Daten

An Dritte übermittelte Daten können abgefangen werden und eine Verletzung der Vertraulichkeit zur Folge haben.

Daten in Papierform müssen so verarbeitet und aufbewahrt werden, dass der Zugriff und die Verbreitung durch Unbefugte, einschließlich unbefugter Bediensteten, verhindert werden.

Was die elektronischen Daten betrifft, so erfolgt die Kommunikation über das Internet größtenteils verschlüsselt mit dem *https*-Protokoll. Es gibt jedoch immer noch Dienste, die keine Datenverschlüsselung vorsehen wie z. B. das *http*-Protokoll (Internet), das keine sichere Kommunikation sowohl in Bezug auf die Vertraulichkeit und Integrität der ausgetauschten Daten als auch auf die Authentizität der angezeigten Webseite gewährleistet.

Mit einer Maßnahme vom 23. Januar 2020 hat die Aufsichtsbehörde bestimmt, dass „die Nichtverwendung von Verschlüsselungsinstrumenten für die Datenübertragung gegen Artikel 32 der Datenschutz-Grundverordnung verstößt“. Das gilt gleichermaßen für die Verwendung von institutionellen E-Mail-Adressen. Daher stellt die Verwendung von Verschlüsselungsprotokollen wie dem TLS-Protokoll und der Ende-zu-Ende-Verschlüsselung für die Übertragung von E-Mails, die der Regionalrat eingeführt hat, eine angemessene Sicherheitsmaßnahme im Sinne von Artikel 32 der Datenschutz-Grundverordnung dar.

Für die Sicherheit von Daten, die über das elektronische Protokoll (Pitre) an Dritte übermittelt werden, ist gemäß Artikel 32 der GDPR die Verwendung von Verschlüsselungsinstrumenten für die Datenübertragung vorgesehen.

Schutz von Daten und Systemen

Zum Schutz von Daten in Papierform werden diese in geschlossenen Räumen aufbewahrt, wenn sie nicht benutzt werden. Die archivierten Daten werden in speziellen abschließbaren, mit einem Schloss versehenen Aktenschränken aufbewahrt, die von den zuständigen Stellen überwacht werden und nur für befugtes Personal zugänglich sind.

Gemäß dem gesetzesvertretenden Dekret Nr. 82 vom 7. März 2005 (Kodex der digitalen Verwaltung) und den nachfolgenden AGID-Richtlinien stellen die Vertraulichkeit, die Integrität und die Verfügbarkeit die wichtigsten Parameter für die Datensicherheit im IT-Bereich dar. Dadurch soll Folgendes gewährleistet werden:

- dass nur ermächtigte bzw. befugte Personen Zugriff auf die Daten haben (Vertraulichkeit);
- dass verhindert wird, dass die Daten verändert, gelöscht, unlesbar gemacht oder von Viren befallen werden (Integrität);

- dass ein korrekter und funktioneller Datenzugang und gleichzeitig das ordnungsgemäße Funktionieren des Computersystems sichergestellt werden (Verfügbarkeit).

Um die Einhaltung der beschriebenen Parameter zu gewährleisten, überprüft der Systemadministrator systematisch die Integrität der Systeme und überwacht proaktiv etwaige Unregelmäßigkeiten. Um die direkte oder indirekte Veränderung von Informationen durch unbefugte Benutzer oder durch zufällige Ereignisse zu verhindern, ist der Einsatz von Software zur Bekämpfung von Computerviren und Malware vorgeschrieben. Der Regionalrat lässt durch den Systemadministrator und in Zusammenarbeit mit den einzelnen Mitarbeitern diese Software regelmäßig aktualisieren, außer dies ist objektiv unmöglich. Die gleiche Anweisung gilt für die Betriebssysteme und Anwendungen, die für die Datenverarbeitung verwendet werden.

Betriebskontinuitätsverfahren

Die Betriebskontinuität ist im Wesentlichen das Ergebnis eines organisatorischen Prozesses, der IT-Werkzeug umfasst, das genauen Anforderungen der Widerstandsfähigkeit Genüge tut. Die AGID-Leitlinien zur Betriebskontinuität sehen keine vordefinierten technischen Maßnahmen vor, so dass es den Körperschaften überlassen bleibt, die optimale Lösung auf der Grundlage des Kontinuitätsbedarfs in Bezug auf die zu schützenden Ressourcen zu bestimmen.

Für den Regionalrat wird die Betriebskontinuität durch ein System von Sicherungskopien der verwendeten Daten und Systeme gewährleistet. Letztere werden insbesondere durch die Anwendung eines Datenwiederherstellungsverfahrens, das in Echtzeit zum Zeitpunkt der Kenntnisnahme oder auf jeden Fall so schnell wie möglich durchgeführt wird, vor möglichen Zwischenfällen oder Datenverletzungen geschützt. Im Regelfall wird täglich ein Backup der Daten und Systeme erstellt.