Comune di Bolzano
Stadtgemeinde Bozen

Il Sindaco

Der Bürgermeister

Decreto n. 16/S/2018 del 10.07.2018

Dekret Nr. 16/S/2018 vom 10.07.2018

OGGETTO:
Linee guida per le procedure di adeguamento al GDPR 2016/679

Misura n. 10, lettere f), g), h) del Piano delle azioni in adeguamento al GDPR

Decreto sindacale 17.05.2018, n.7/S/2018

GEGENSTAND:
Verfahrensleitlinien für die Anpassung an die DSGVO 2016/679

Maßnahme Nr. 10, Buchst. f), g) und h) des Aktionsplans zur Anpassung an die DSGVO

Dekret des Bürgermeisters Nr. 7/S/2018 vom 17.05.2018

IL SINDACO

Premesso che il piano delle azioni in adeguamento al GDPR 2016/679 d.d. 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali – di seguito denominato GDPR -, nonchè alla libera circolazione di tali dati approvato dal titolare con decreto sindacale d.d. 17.05.2018, n. 7/S/2018 prevede al punto 10 tra le priorità l'individuazione delle procedure attraverso cui realizzare ed aggiornare il registro delle attività di trattamento, valutazioni d'impatto sulla protezione dei dati, rilevazioni delle violazioni dei dati ed analisi e gestione dei rischi per la protezione dei dati attraverso l'adozione di linee guida";

Zu den Prioritäten des vom Verantwortlichen mit Dekret des Bürgermeisters Nr. 7/S/2018 vom 17.05.2018 genehmigten Aktionsplans zur Anpassung an die "*DSGVO 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*" - im Folgenden kurz DSGVO genannt - zählt unter Ziffer 10 die Festlegung von Leitlinien für die Erstellung und Aktualisierung des Verzeichnisses der Verarbeitungstätigkeiten und der Datenschutz-Folgenabschätzung, für die Ermittlung von Datenschutzverletzungen sowie für die Risikobewertung und das Risikomanagement im Bereich des Datenschutzes.

atteso che le stesse vanno redatte tenendo conto della politica organizzativa della protezione dei dati personali approvata con Decreto sindacale d.d 17.05.2018, n. 8;

Bei der Ausarbeitung dieser Leitlinien ist die Aufbauorganisation in Bezug auf den Schutz der personenbezogenen Daten zu beachten, die mit Dekret des Bürgermeisters Nr. 8 vom 17.05.2018 genehmigt wurde.

considerato che conformare l'attività comunale ai principi di responsabilizzazione, di protezione dei dati fin dalla progettazione e per impostazione predefinita (cosiddetta privacy by design e by default) ai fini della corretta, trasparente e sicura gestione degli stessi

Eine korrekte, transparente und sichere Datenverwaltung nach den Grundsätzen der Rechenschaftspflicht und des Datenschutzes durch Technik ("*data protection by design*") bzw. durch datenschutzfreundliche Voreinstellungen ("*data protection by default*")

comporta, tra l'altro, la necessità di definire modalità procedurali certe ed omogenee;

erfordert u. a. die Festlegung eindeutiger und einheitlicher Verfahrensabläufe.

considerato che l'alto livello di criticità espresso della violazione dei dati personali, di seguito denominata data breach, impone che tempi di intervento e figure coinvolte siano predefinite senza margini di equivoco;

Die Verletzung des Schutzes personenbezogener Daten - im Folgenden auch "Data Breach" genannt - ist ein in hohem Maße kritischer Vorgang, der nach eindeutigen, vorab geregelten Reaktionszeiten und Zuständigkeiten verlangt.

considerato l'obiettivo primario di valorizzazione di procedure interne codificate, diffuse ed applicate;

Oberstes Ziel der Verwaltung ist es daher, standardisierte und allgemeingültige interne Verfahrensabläufe festzulegen und diese konkret umzusetzen.

vista la necessità di documentare le scelte del titolare del trattamento dei dati in relazione alle misure assunte a garanzia della conformità dei trattamenti ai sensi degli artt. 5, paragrafo 2 e 24, paragrafo 1 del GDPR 2016/679;

Nach Art. 5 Abs. 2 und Art. 24 Abs. 1 der DSGVO 2016/679 muss der Verantwortliche für die Datenverarbeitung den Nachweis erbringen, dass die von ihm ergriffenen Maßnahmen eine Verarbeitungstätigkeit im Einklang mit der Verordnung gewährleisten.

dato atto che tra le competenze ascritte all'Ufficio Organizzazione e Formazione da regolamento organico e di organizzazione approvato nel testo vigente con deliberazione del Consiglio comunale 29.01.2015, n. 8 rientra "l'attuazione della normativa sul trattamento dei dati personali";

Laut der mit Gemeinderatsbeschluss Nr. 8 vom 29.01.2015 genehmigten Personal- und Organisationsordnung i.g.F. fällt "die Umsetzung der Datenschutzbestimmungen" in den Zuständigkeitsbereich des Amtes für Organisation und Weiterbildung.

visto il Piano esecutivo di gestione approvato dalla Giunta comunale con deliberazione 29.01.2018, n. 30, con particolare riferimento agli obiettivi "attuazione di nuovi adempimenti a carattere generale previsti dal nuovo GDPR in materia di privacy";

Der mit Stadtratsbeschluss Nr. 30 vom 29.01.2018 genehmigte Haushaltsvollzugsplan enthält als Zielsetzung die "Umsetzung der neuen von der DSGVO in Sachen Datenschutz vorgesehenen allgemeinen Maßnahmen".

visto l'art. 24, paragrafo 1 del GDPR, che individua tra le competenze del titolare la messa in atto di "misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente" al GDPR;

Gemäß Art. 24 Absatz 1 der DSGVO setzt der Verantwortliche für die Datenverarbeitung "geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt."

Atteso che il Sindaco, in qualità di legale rappresentante dell'Ente, è titolare del trattamento dei dati ai sensi dell'art. 5 del GDPR 2016/679;

Verantwortlicher für die Datenverarbeitung im Sinne von Art. 5 der DSGVO 2016/679 ist der Bürgermeister als gesetzlicher Vertreter dieser Körperschaft.

atteso che il presente atto è stato proposto dal responsabile del procedimento nominato con determinazione dirigenziale 5107 d.d. 16.06.2015

Das vorliegende Dokument wurde von dem mit Verfügung des leitenden Beamten Nr. 5107 vom 16.06.2015 ernannten Verfahrensverantwortlichen vorgeschlagen.

Comune di Bolzano
Stadtgemeinde Bozen

Tutto ciò premesso, in qualità di titolare del trattamento dei dati

Dies vorausgeschickt,
verfügt der Bürgermeister
als Verantwortlicher für die Datenverarbeitung

decreta

Folgendes:

di approvare le allegate linee guida per le procedure di adeguamento del GDPR 2016/679, in applicazione dal 25.05.2018;

Die Verfahrensleitlinien für die Anpassung an die am 25.05.2018 in Kraft getretene DSGVO 2016/679 werden genehmigt.

di incaricare l'Ufficio Organizzazione e formazione di promuoverne adeguata conoscenza.

Das Amt für Organisation und Weiterbildung wird beauftragt, für eine angemessene Bekanntgabe dieses Beschlusses zu sorgen.

La dirigente competente/Die zuständige Amtsdirektorin
Dr. Cristina Caravaggi
f.to digitalmente/digital gez.

.

IL SINDACO
DER BÜRGERMEISTER
dott. Renzo CARAMASCHI
f.to digitalmente/digital gez.

Copia da inviare a:
Segreteria Generale
Direzione generale
Ufficio Organizzazione
Ufficio Informatica e telecomunicazioni
Direttori di Ripartizione, Direttori d'Ufficio e Responsabili di Servizio
e per loro tramite ai responsabili esterni già designati
RPD

Folgende Stellen erhalten eine Kopie dieses Dokuments:
Generalsekretariat
Generaldirektion
Organisationsamt
Amt für Informatik und Telekommunikation
Abteilungs- und Amtdirektorinnen und –direktoren, Dienststellenleiter und über diese die bereits benannten externen Auftragsverarbeiter/-innen
VDS

LINEE GUIDA PER LE PROCEDURE DI ADEGUAMENTO AL GDPR 2016/679

CAPO I
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Art. 1
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DEL TITOLARE

1. I responsabili interni redigono, ciascuno per la propria struttura organizzativa, il registro delle attività di trattamento del titolare implementando il SW appositamente predisposto, accedendovi con le proprie credenziali, avvalendosi, se richiesto, del supporto del privacy manager.
2. Nel corso della redazione il privacy manager può rilevare eventuali incongruenze e segnalarle al responsabile interno per le correzioni o integrazioni che questi riterrà opportuno adottare.
3. Alla data concordata per l'estrazione dei dati, l'inserimento è considerato definitivo ed il registro redatto.
4. La prima estrazione dei dati inseriti è avvenuta il 25.05.2018.
5. Il responsabile interno competente in materia di protezione dei dati personali è delegato a sottoscrivere digitalmente e conservare il registro, risultante dall'estrazione dall'apposito applicativo dei dati e delle informazioni inserite con firma elettronica dai singoli responsabili interni.
6. Ogni qualvolta si verifichino cambiamenti nelle situazioni di diritto o di fatto che comportino una modifica del registro, il responsabile interno della struttura organizzativa segnala la circostanza al privacy manager, che coordina le operazioni di sottoscrizione e conservazione della modifica.
7. Almeno annualmente il privacy manager invita i responsabili interni a verificare l'attualità del registro dei trattamenti.

Art. 2
REGISTRI DELLE ATTIVITA' DI TRATTAMENTO IN QUALITA' DI RESPONSABILE ESTERNO

1. Il responsabile interno della struttura organizzativa che svolge trattamenti di dati personali in qualità di responsabile esterno di soggetti terzi, redige l'apposito registro, avvalendosi, se richiesto, del supporto del privacy manager, che coordina le operazioni di sottoscrizione e conservazione del registro.
2. Ogni qualvolta si verifichino cambiamenti nelle situazioni di diritto o di fatto che comportino una modifica del registro, il responsabile interno della struttura organizzativa segnala la circostanza al privacy manager, che coordina le operazioni di sottoscrizione da parte del responsabile interno interessato e di conservazione della modifica.

Art. 3
REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DEI RESPONSABILI ESTERNI

1. Il responsabile interno della struttura che si avvale di responsabili esterni del trattamento di dati personali richiede al responsabile esterno la consegna dell'apposito registro delle categorie delle attività di trattamento. Il privacy manager cura la conservazione di quanto trasmesso dal responsabile esterno.
2. Il responsabile interno della struttura organizzativa che si avvale di responsabili esterni del trattamento di dati personali invita almeno annualmente i responsabili esterni a

confermare l'attualità del registro delle categorie delle attività di trattamenti trasmesso al Comune di Bolzano.

Art. 4

RESPONSABILI ESTERNI COMUNI A PIÙ RIPARTIZIONI

Nel caso in cui il soggetto terzo da nominare quale responsabile esterno ai sensi dell'art. 28 del GDPR 2016/679 tratti dati personali per conto di più strutture apicali, la nomina, in deroga a quanto previsto dall'art. 8 del decreto sindacale n. 8/S/2018 del 17.05.2018 è effettuata dal titolare del trattamento.

CAPO II
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (PIA)

Art. 5

PROCEDURA DELLA PIA

1. Nelle ipotesi di cui all'art. 35 del GDPR, il responsabile interno, direttamente o su proposta del privacy manager, chiede a quest'ultimo la convocazione gruppo di lavoro "advisory board" composta dal responsabile della protezione dei dati, dal direttore della struttura competente in materia di protezione dei dati personali, dal privacy manager, dal responsabile interno ICT, eventualmente integrato dagli specialisti della sicurezza ICT che questi indicherà coinvolti in relazione alle specifiche competenze, dal responsabile interno richiedente e da altri membri che si ritiene opportuno convocare.
2. All'ordine del giorno del lavori è posta la relazione preliminare "PIA" redatta dal responsabile interno avvalendosi del software appositamente messo a disposizione.
3. Il verbale dei lavori si conclude con lo schema di PIA, che il responsabile interno può sottoscrivere digitalmente o modificare motivatamente e sottoscrivere digitalmente.
4. La PIA sottoscritta dal responsabile interno è inviata al privacy manager, che ne cura la conservazione e la trasmissione al responsabile della protezione dati per gli eventuali adempimenti relativi alla consultazione preventiva del Garante per la protezione dei dati personali.
5. I trattamenti di dati personali assoggettati a PIA si effettuano previo conforme nulla osta del responsabile della protezione dei dati personali.
6. Con il nulla osta il responsabile della protezione dei dati personali comunica al privacy manager l'insussistenza dei presupposti per la consultazione preventiva del Garante per la protezione dei dati personali, o gli esiti dell'avvenuta consultazione.
7. L'acquisto e la progettazione di un software che possono comportare rilevanti attività di trattamento di dati personali sono sempre soggetti a PIA.

Art. 6

PIA RELATIVE A TRATTAMENTI DI DATI PERSONALI DEI RESPONSABILI ESTERNI

1. Il responsabile interno che intende affidare all'esterno servizi o incarichi che comportano rilevanti attività di trattamento di dati personali per conto del Comune di Bolzano e che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche attiva preventivamente la procedura di cui all'art. 5.
2. La PIA, o l'esito della consultazione preventiva del Garante per la protezione dei dati personali, fa parte delle condizioni del contratto di affidamento del servizio o dell'incarico, ed è inserita nel relativo bando.

3. In attesa delle clausole contrattuali tipo di cui ai paragrafi 7 e 8 dell'art. 28 del GDPR, tramite il privacy manager, il responsabile della protezione dei dati è consultato ai fini della stesura di clausole concernenti il trattamento di dati personali effettuato dai responsabili esterni.
4. Le clausole possono prevedere e disciplinare attività di audit di seconda parte, sia rispetto alle misure di sicurezza organizzative, che tecniche.

Art 7
NORMA TRANSITORIA RELATIVA A PIA NEI CONTRATTI IN ESECUZIONE O ALTRI RAPPORTI GIURIDICI IN ESSERE.

1. Il responsabile interno cui fanno capo contratti già in esecuzione o altre tipologie di rapporti giuridici in essere in virtù dei quali viene eseguito esternamente il trattamento di dati personali per conto del Comune di Bolzano il responsabile interno competente integra l'atto giuridico in essere con un atto di nomina a responsabile esterno e gli la documentazione a garanzia della conformità dei trattamenti a GDPR.
2. Per i contratti di fornitura e assistenza di software, anche acquistati e/o gestiti da altre strutture, è competente il responsabile interno della struttura che si occupa di informatica e telecomunicazioni.
3. La documentazione di cui al comma 1 è sottoposta, tramite il privacy manager, al parere del responsabile della protezione dei dati personali.
4. Quando gli esiti del parere del responsabile della protezione dei dati personali comportano variazioni delle condizioni contrattuali, il responsabile interno attiva tempestivamente le necessarie procedure.

CAPO III
VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Art. 8
PROCEDURA IN CASO DI DATA BREACH

1. Nell'attuazione delle procedure normate dagli artt. 33 e 34 del GDPR, dalle Linee guida approvate dal WP29 il 06.02.2018, e dal Provvedimento d.d. 02.07.2015 n. 393 del Garante per la protezione dei dati personali, in quanto compatibile, opera l'apposito gruppo di lavoro "advisory board" di cui al precedente l'art. 5, integrato dai responsabili interni cui fanno capo i dati violati o le banche dati violate.
2. Ogni responsabile interno del settore che viene a conoscenza o attua una potenziale violazione dei dati personali, ovvero una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati personali trasmessi, conservati o comunque trattati – ai sensi dell'art. 33 del GDPR 2016/679 deve immediatamente comunicarlo all'apposita casella di posta "*gruppoprivacy@comune.bolzano.it*, e nel caso in cui il servizio di posta non risultasse funzionante, adottare senza indugio ulteriore modalità comunicativa idonea ed adeguata alla gravità dell'evento che si è verificato.
3. Ai fini di cui al comma precedente, il responsabile interno ICT predispone un servizio tecnico di reperibilità che garantisca l'immediata analisi degli eventi che gli competono e l'immediata predisposizione di ogni misura informatica atta a contenere i rischi per i diritti e le libertà delle persone fisiche e per la conservazione dei dati.
4. L'advisory board si riunisce, anche attraverso modalità telematiche, al più tardi entro 24 ore dalla conoscenza dell'evento, analizza le informazioni, e predispone, se trattasi di un data breach, un verbale contenente tutti i dati necessari alla registrazione dello stesso ed all'eventuale notifica al Garante per la protezione dei dati personali.

5. Il Sindaco, il Direttore generale, il Segretario generale e il Direttore della struttura competente in materia di protezione dei dati personali sono immediatamente informati dell'evento.
6. Nelle ipotesi in cui sia necessaria la comunicazione all'interessato della violazione dei dati personali, l'advisory board potrà essere integrato del responsabile della comunicazione istituzionale.
7. Il privacy manager provvede alla registrazione dei data breach e di ogni provvedimento adottato in conseguenza.
8. Gli eventi relativi al data center sono gestiti dal responsabile interno ICT attraverso apposito sistema di registrazione, fermo restando l'obbligo di tempestiva trasmissione al privacy manager dei relativi report.

Art. 9
PROCEDURA IN CASO DI DATA BREACH PRESSO UN RESPONSABILE ESTERNO

1. Il responsabile esterno segnala il data breach al Comune di Bolzano, e per suo tramite al responsabile della protezione dei dati, immediatamente dopo averne avuto conoscenza, e si adopera con ogni mezzo per contenere i rischi per i diritti e la libertà degli interessati.
2. Il responsabile della protezione dei dati del Comune di Bolzano assicura cooperazione al responsabile esterno nella gestione del data breach.
3. All'individuazione ed attuazione degli interventi tempestivi ed adeguati può contribuire il gruppo di lavoro del Comune di Bolzano, se convocato.
4. La disciplina del data breach è disciplinata nell'atto di nomina a responsabile esterno.

CAPO IV
ANALISI DEI RISCHI

Art. 10
ANALISI DEI RISCHI

1. L'analisi dei rischi è effettuata rispetto ad ogni trattamento di dati personali eseguito dal Comune di Bolzano.
2. In sede di prima applicazione è effettuata dal responsabile della protezione dei dati in stretta collaborazione con i responsabili interni, anche ai fini della sua validazione e dell'individuazione delle eventuali misure di sicurezza tecnico-organizzative da adottare. In sede di riesame è effettuata dai responsabili interni, se richiesto, con il supporto del privacy manager.
3. L'analisi va effettuata in relazione ad ogni nuovo trattamento, come pure ogni qualvolta si verifichino cambiamenti nelle situazioni di diritto o di fatto che comportino una modifica dei trattamenti dei dati personali.
4. L'analisi dei rischi comporta l'individuazione di misure di gestione del rischio, la cui effettiva implementazione è monitorata.
5. L'analisi dei rischi è sempre documentata e trasmessa al privacy manager per la conservazione.

Art. 11
AUDIT

1. Il privacy manager progetta ed esegue attività di audit col criterio di conformità al Sistema di gestione della privacy, allo scopo di monitorare l'efficacia delle misure di adeguamento al GDPR e migliorare l'efficienza degli strumenti organizzativi.

VERFAHRENSLEITLINIEN FÜR DIE ANPASSUNG AN DIE DSGVO 2016/679

ABSCHNITT 1
VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Art. 1
VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN DES VERANTWORTLICHEN FÜR DEN DATENSCHUTZ

1. Der interne Verarbeitungsbeauftragte erstellt für seine Organisationseinheit das Verzeichnis der Verarbeitungstätigkeiten des Verantwortlichen für den Datenschutz unter Verwendung der dafür vorgesehenen Software und seiner persönlichen Zugangsdaten. Sofern erforderlich, greift er auf die Unterstützung des Privacy Managers zurück.
2. Stellt der Privacy Manager fest, dass es beim Erstellen des Verzeichnisses Unstimmigkeiten gibt, teilt er dies dem internen Beauftragten mit, damit dieser die für notwendig befundenen Korrekturen oder Ergänzungen vornehmen kann.
3. Mit der geplanten Datenextraktion gilt die Eingabe als endgültig und das Verzeichnis als erstellt.
4. Die Daten wurden erstmals am 25.05.2018 extrahiert.
5. Dem für den Bereich Datenschutz zuständigen internen Beauftragten wird die Befugnis übertragen, das Verzeichnis, das durch die Extraktion der Daten und Informationen, die von den internen Beauftragten mit ihrer digitalen Unterschrift eingespeist wurden, erstellt wird, digital zu unterzeichnen und aufzubewahren.
6. Der interne Beauftragte der jeweiligen Organisationseinheit meldet jede Änderung der Rechts- und Sachlage, die Änderungen am Verzeichnis nach sich zieht, an den Privacy Manager, der die Abläufe für die Unterzeichnung und Aufbewahrung der Änderung koordiniert.
7. Mindestens einmal jährlich fordert der Privacy Manager die internen Beauftragten auf zu prüfen, ob das Verzeichnis der Verarbeitungstätigkeiten noch auf dem aktuellen Stand ist.

Art. 2
VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN IN FÄLLEN, IN DENEN DIE STADTVERWALTUNG AUFTRAGSVERARBEITER (EXTERNER BEAUFTRAGTER) IST

1. Der interne Beauftragte der Organisationseinheit, der personenbezogene Daten als Auftragsverarbeiter (externer Beauftragter) für Dritte verarbeitet, erstellt das entsprechende Verzeichnis und greift dabei, sofern erforderlich, auf die Unterstützung des Privacy Managers zurück, der alle Maßnahmen in Hinblick auf die Unterzeichnung und Aufbewahrung des Registers koordiniert.
2. Der interne Beauftragte der jeweiligen Organisationseinheit meldet jede Änderung der Rechts- und Sachlage, die Änderungen am Verzeichnis nach sich zieht, an den Privacy Manager, der die Abläufe in Hinblick auf die Unterzeichnung durch den internen Beauftragten und auf die Aufbewahrung der Änderung koordiniert.

Art. 3
VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN DES AUFTRAGSVERARBEITERS (EXTERNER BEAUFTRAGTER)

1. Der interne Beauftragte der Organisationseinheit, die für die Verarbeitung der personenbezogenen Daten die Dienste externer Auftragsverarbeiter in Anspruch nimmt, verlangt vom externen Auftragsverarbeiter die Aushändigung des Verzeichnisses der Kategorien von Verarbeitungstätigkeiten. Die vom externen Auftragsverarbeiter weitergeleiteten Unterlagen werden vom Privacy Manager aufbewahrt.
2. Der interne Beauftragte der Organisationseinheit, die für die Verarbeitung der personenbezogenen Daten die Dienste externer Auftragsverarbeiter in Anspruch nimmt, fordert die externen Auftragsverarbeiter mindestens einmal jährlich auf zu bestätigen, dass das Verzeichnis der Kategorien von Verarbeitungstätigkeiten, das sie der Stadtgemeinde Bozen ausgehändigt haben, auf dem aktuellen Stand ist.

Art. 4

ABTEILUNGSÜBERGREIFENDE NUTZUNG EXTERNER AUFTRAGSVERARBEITER

Verarbeitet ein Dritter als externer Auftragsverarbeiter nach Art. 28 der DSGVO 2016/679 personenbezogene Daten für mehrere Abteilungen, obliegt die Ernennung ungeachtet der Bestimmungen in Art. 8 des Dekrets des Bürgermeisters Nr. 8/S/2018 vom 17.05.2018 dem Verantwortlichen für die Datenverarbeitung.

ABSCHNITT 2
DATENSCHUTZ-FOLGENABSCHÄTZUNG
(PIA)

Art. 5
ABLAUF DER DATENSCHUTZ-FOLGENABSCHÄTZUNG

1. Bei Vorliegen eines Sachverhalts nach Art. 35 der DSGVO beruft der Privacy Manager auf Antrag des internen Beauftragten oder auf eigene Initiative eine Arbeitsgruppe ein ("Advisory Board"), an der der Datenschutzbeauftragte, der Privacy Manager, der Leiter der für den Datenschutz zuständigen Organisationseinheit, der interne ICT-Beauftragten, der gegebenenfalls durch die ICT-Sicherheitsexperten unterstützt wird, der betroffene interne Beauftragte und alle weiteren Personen, deren Präsenz für notwendig befunden wird, teilnehmen.
2. Im Rahmen dieser Sitzung behandelt die Arbeitsgruppe die vom internen Beauftragten mit der einschlägigen Software erstellte Vorab-Folgenabschätzung.
3. Das Ergebnis der im Zuge der Sitzung durchgeführten Datenschutz-Folgeabschätzung wird dem Sitzungsprotokoll als Anlage beigefügt und vom internen Beauftragten elektronisch unterschrieben oder zunächst mit begründeten Änderungen versehen und anschließend elektronisch unterschrieben.
4. Die vom internen Beauftragten unterschriebene Datenschutz-Folgenabschätzung wird dem Privacy Manager übersandt. Dieser verwahrt den Bericht und leitet diesen an den Datenschutzbeauftragten weiter, damit erforderlichenfalls die entsprechenden Schritte für eine vorherige Konsultation der Aufsichtsbehörde eingeleitet werden können.
5. Erst nach einer entsprechenden Freigabe durch den Datenschutzbeauftragten können personenbezogene Daten, die einer Datentschutz-Folgeabschätzung unterzogen wurden, verarbeitet werden.
6. In der Freigabeerklärung unterrichtet der Datenschutzbeauftragte den Privacy Manager darüber, dass eine vorherige Konsultation der Aufsichtsbehörde nicht erforderlich ist bzw., welche Vorgaben die Aufsichtsbehörde gemacht hat.

7. Für die Beschaffung und Entwicklung von Software, die eine umfangreiche Verarbeitung von persönlichen Daten nach sich ziehen kann, ist immer eine Datenschutz-Folgenabschätzung vorzunehmen.

Art. 6
DATENSCHUTZ-FOLGENABSCHÄTZUNGEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN DURCH EXTERNE AUFTRAGSVERARBEITER

1. Der interne Beauftragte, der Dienstleistungen oder Aufträge, die mit einer umfangreichen Verarbeitung von personenbezogenen Daten für die Stadtgemeinde Bozen einhergehen und ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mitsichbringen könnten, an externe Auftragsverarbeiter vergibt, leitet präventiv das Verfahren nach Art. 5 ein.
2. Das Ergebnis der Datenschutz-Folgenabschätzung bzw. der Vorab-Konsultation der Datenschutz-Aufsichtsbehörde ist Teil der Vertragsbedingungen bei Vergabeverfahren bzw. Beauftragung und in die Ausschreibungsunterlagen aufzunehmen.
3. Solange keine Standardvertragsklauseln nach Art. 28 Artikel 7 und 8 der DSGVO vorliegen, ist für die Formulierung der Vertragsklauseln zur Verarbeitung der personenbezogenen Daten durch externe Auftragsverarbeiter der Datenschutzbeauftragte über den Privacy Manager hinzuzuziehen.
4. Die Vertragsklauseln können außerdem Vorgaben und Regelungen hinsichtlich der Überprüfung der organisatorischen und technischen Schutzmaßnahmen durch einen Prüfer (Audit) enthalten.

Art. 7
ÜBERGANGSBESTIMMUNG ZUR DATENSCHUTZ-FOLGENABSCHÄTZUNG BEI LAUFENDEN VERTRÄGEN ODER ANDEREN BESTEHENDEN RECHTVERHÄLTNISSEN.

1. Bei bereits laufenden Verträgen oder anderen bestehenden RechtsverhältNissen, aufgrund deren die Verarbeitung personenbezogener Daten für die Stadtgemeinde Bozen durch externe Auftragsverarbeiter erfolgt, ergänzt der zuständige Beauftragte den bestehenden Rechtsakt mit dem der Auftragsverarbeiter bennant wird. Außerdem fordert er vom diesem die Aushändigung von Unterlagen, die hinreichend Garantien dafür bieten, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt.
2. Die Zuständigkeit für Software-Lieferverträge und -Supportverträge obliegt immer dem internen Beauftragten der Informatik- und Telekommunikationseinheit, auch wenn die Beschaffung und/oder Verwaltung der Software durch eine andere Organisationseinheit erfolgt.
3. Der Privacy Manager unterbreitet die Unterlagen nach Absatz 1 dem Datenschutzbeauftragten für die Erstellung eines Gutachtens.
4. Ergibt sich aufgrund des Gutachtens des Datenschutzbeauftragten die Notwendigkeit, die Vertragsbedingungen abzuändern, leitet der interne Beauftragte unverzüglich die notwendigen Schritte ein.

ABSCHNITT 3
VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN (DATA BREACH)

Art. 8
VORGEHENSWEISE IM FALLE EINES DATA BREACH

1. Die Durchführung der Verfahren, die in Art. 33 und 34 der DSGVO, in den am 06.02.2018 von der Artikel-29-Datenschutzgruppe genehmigten Leitlinien und in der

Vorschrift Nr. 393 der Aufsichtsbehörde vom 02.07.2015, sofern kompatibel, geregelt sind, obliegt der eigenen Arbeitsgruppe ("Advisory Board") bestehend aus den Mitgliedern laut Art. 5 und aus den internen Beauftragten, in deren Bereich der Schutz der Daten oder Datenbanken verletzt wurde.

2. Erlangt der interne Beauftragte des jeweiligen Fachbereichs Kenntnis von einer möglichen Verletzung des Schutzes von personenbezogenen Daten bzw. von einer 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, oder hat er diese Verletzung selbst verursacht, hat er dies nach Art. 33 der DSGVO 2016/679 unverzüglich zu melden. Dafür sendet er eine Nachricht an die E-Mail-Adresse *"gruppoprivacy@gemeinde.bolzano.it"* Funktioniert der E-Mail-Versand nicht, ist unverzüglich ein anderes geeignetes und der Schwere des Vorfalls angemessenes Kommunikationsmittel zu verwenden.
3. Zum Zwecke der Durchführung der in Absatz 1 vorgesehenen Maßnahmen gewährleistet der interne ICT-Beauftragte einen technischen Bereitschaftsdienst, der sicherstellt, dass die Vorfälle, die in seine Zuständigkeit fallen, umgehend untersucht und umgehend alle informationstechnischen Maßnahmen ergriffen werden, die geeignet sind, die Risiken für die Rechte und Freiheiten natürlicher Personen und für die Aufbewahrung der Daten einzudämmen.
4. Das Advisory Board kommt binnen höchstens 24 Stunden, nachdem ihm die Verletzung bekannt wurde, gegebenenfalls auch auf telematischem Wege zusammen, um die Sachlage zu analysieren. Wird eine Datenschutzverletzung (Data Breach) festgestellt, fertigt das Advisory Board eine Niederschrift an, die alle für die Erfassung der Datenschutzverletzung und für eine etwaige Meldung an die Datenschutz-Aufsichtsbehörde notwendigen Daten enthält.
5. Der Bürgermeister, der Generaldirektor, der Generalsekretär und der Direktor der für den Bereich Datenschutz zuständigen Organisationseinheit werden unverzüglich über die Datenschutzverletzung unterrichtet.
6. Für den Fall, dass dem Betroffenen die Verletzung des Schutzes der personenbezogenen Daten mitgeteilt werden muss, kann das Advisory Board den Verantwortlichen für die institutionelle Kommunikation hinzuziehen.
7. Der Privacy Manager erfasst die Verletzung des Datenschutzes und alle infolgedessen ergriffenen Maßnahmen.
8. Vorfälle, die das Data Center betreffen, werden vom internen ICT-Beauftragten über ein entsprechendes Erfassungssystem abgewickelt. Der ICT-Beauftragte ist verpflichtet, dem Privacy Manager die entsprechenden Berichte zukommen zu lassen.

Art. 8
VORGEHENSWEISE BEI EINER VERLETZUNG DES SCHUTZES PERSONENBEZOGENER DATEN DURCH EINEN AUFTRAGSVERARBEITER (EXTERNER BEAUFTRAGTER)

1. Der externe Auftragsverarbeiter unterrichtet die Stadtgemeinde Bozen - und diese den Datenschutzbeauftragten - über die Verletzung, unmittelbar nachdem ihm die Verletzung bekannt wurde, und ergreift alle Maßnahmen, die geeignet sind, um die Risiken für die Rechte und die Freiheit der Betroffenen einzudämmen.
2. Der Datenschutzbeauftragte der Stadtgemeinde Bozen sichert dem externen Auftragsverarbeiter die volle Unterstützung bei der Handhabung der Datenschutzverletzung zu.
3. Die Arbeitsgruppe der Stadtgemeinde Bozen kann, sofern sie einberufen wird, an der Festlegung und Umsetzung geeigneter Sofortmaßnahmen mitwirken.
4. Das Data-Breach-Verfahren ist in dem Rechtsakt mit dem der Auftragsverarbeiter bennant wird, geregelt.

ABSCHNITT 4
RISIKOBEWERTUNG

Art. 9
RISIKOBEWERTUNG

1. Bei jeder Verarbeitung personenbezogener Daten durch die Stadtgemeinde Bozen wird eine Risikobewertung vorgenommen.
2. Die Erstbewertung wird vom Datenschutzbeauftragten in enger Abstimmung mit den internen Beautragten vorgenommen, auch um eine Datenvalidierung vorzunehmen und gegebenenfalls die notwendigen technischen und organisatorischen Schutzmaßnahmen festzulegen. Die Überprüfung der Risikobewertung erfolgt durch die internen Beauftragten, sofern erforderlich mit Unterstützung des Privacy Managers.
3. Risikobewertungen werden bei neuen Verarbeitungssituationen vorgenommen und grundsätzlich immer dann, wenn eine geänderte Rechts- oder Sachlage zu Änderungen bei der Verarbeitung der personenbezogenen Daten führt.
4. Im Zuge der Risikobewertung werden auch Maßnahmen zur Handhabung des Risikos getroffen. Die Umsetzung dieser Maßnahmen wird entsprechend überwacht.
5. Die Risikobewertung wird immer dokumentiert und zur Verwahrung an den Privacy Manager weitergeleitet.

Art. 10
AUDIT

1. Es obliegt dem Privacy Manager, Überprüfungen (Audits) hinsichtlich der Einhaltung des Datenschutzmanagementsystem zu planen und durchzuführen, um auf diese Weise die Wirksamkeit der DSGVO-Anpassungsmaßnahmen zu überwachen und die Effizienz der organisatorischen Instrumente zu verbessern.