Bearbeitet von / redatto da:
Cristina Motti

An den Generalsekretär des Landes
An die Ressortdirektorinnen und -direktoren
An die Abteilungsdirektorinnen und -direktoren
An die Bereichsdirektorinnen und -direktoren
An die Amtsdirektorinnen und -direktoren

Al Segretario generale della Provincia
Alle direttrici e ai direttori di dipartimento
Alle direttrici e ai direttori di ripartizione
Alle direttrici e ai direttori d'area
Alle direttrici e ai direttori d'ufficio

und zur Kenntnis:
An den Landeshauptmann
An die Landesrätinnen und Landesräte

e per conoscenza:
Al Presidente della Provincia
Alle Assessore e agli Assessori provinciali

An die Prüfstelle des Landes
An den Generaldirektor der Informatik AG
An den DSB der Landesverwaltung

Al Nucleo di valutazione della Provincia
Al Direttore generale di Informatica Alto Adige
Al DPO dell'Amministrazione provinciale

Rundschreiben des Generaldirektors Nr. 5 vom 05.04.2023

Circolare del Direttore generale n. 5 del 05.04.2023

Ergänzende operative Anweisungen für die Anwendung der neuen europäischen Grundverordnung zum Thema Schutz von personenbezogenen Daten

Istruzioni operative integrative in merito agli adempimenti previsti dalla normativa vigente in materia di protezione dei dati

Sehr geehrte Damen und Herren,

es sind fast 5 Jahre vergangen, seitdem die Grundverordnung (EU) 2016/679 des Europäischen Parlaments und des Rates "*zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG*" (Datenschutz-Grundverordnung "DSGVO") **am 25. Mai 2018** in jedem Mitgliedstaat der EU unmittelbar anwendbar wurde.

Mit **Rundschreiben Nr. 4 vom 23.Mai 2018** hatte der Generaldirektor alle Direktoren und Direktorinnen der Organisationseinheiten des Landes, als mit der Verarbeitung betrauten Personen (ehemalige interne Auftragsverarbeiter), in den unter ihrer Zuständigkeit fallenden Bereiche, darauf aufmerksam gemacht, dass es ihre Pflicht war, in Einklang mit den erteilten Anweisungen, die Vorgaben der Grundverordnung umzusetzen und diese Umsetzung nachzuweisen (Rechenschaftspflicht).

Gentili Signore e Signori,

sono trascorsi quasi 5 anni da quando **il 25 maggio 2018** il Regolamento del Parlamento europeo e del Consiglio 2016/679 "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*" (Regolamento generale sulla protezione dei dati "GDPR") è divenuto direttamente applicabile.

Con **la circolare n. 4 del 23 maggio 2018** il Direttore generale aveva richiamato l'attenzione di tutti i direttori e le direttrici delle strutture organizzative in indirizzo, preposti al trattamento dei dati personali (ex responsabili interni del trattamento) nelle materie che fossero riconducibili alla loro esclusiva competenza sul fatto che incombeva su di loro l'obbligo di attuare e dimostrare l'attuazione degli adempimenti previsti dal regolamento in conformità alle istruzioni rese (principio di responsabilizzazione).

In der Zwischenzeit, ist **am 19. September 2018,** das gesetzesvertretende Dekret vom 10. August 2018 in Kraft getreten, welches die Vorschriften des gesetzesvertretenden Dekrets 196/2003 "Datenschutzkodex" (in der Folge, "Datenschutz-kodex") an die DSGVO angepasst hat.

Auf Grund dieser Prämissen werden jene Aufgabe hervorgehoben, die sich im Laufe dieser Zeit am meisten weiterentwickelt haben und diejenigen, die nach wie vor, die dringendsten und verbindlichsten Maßnahmen darstellen, um den Anpassungsprozess an die Vorgaben der EU-Bestimmungen zu vollenden, und gleichzeitig einige operative Anweisungen zu geben.

1. Übermittlung der Daten ins Ausland

1.1 Erklärungen

Während die Übermittlung der personenbezogenen Daten innerhalb der EU immer zulässig ist, sind für die Übermittlung in Länder außerhalb der EU besondere Garantien für den Schutz der personenbezogenen Daten notwendig, insbesondere nach dem Urteil des Gerichtshofs der EU vom 16. Juli 2020, Data Protection Commissioner/Facebook Ireland Limited gegen Maximilian Schrems, C-311/18 (Urteil Schrems 2). Dieses Urteil hat den Privacy Shield, d. h. den vorherigen Angemessenheitsbeschluss zugunsten der USA, für ungültig erklärt und damit die rechtlichen Grundlagen und die Rechtmäßigkeit der Übermittlung personenbezogener Daten aus europäischen Staaten in die USA in Frage gestellt, mit der Begründung, dass die US-amerikanischen Rechtsvorschriften nicht in der Lage sind, ein dem Europäischen Wirtschaftsraums im Wesentlichen gleichwertiges Schutzniveau zu gewährleisten, weil sie "*aufgrund des Vorrangs, der dort der nationalen Sicherheit eingeräumt wird, einen Eingriff in die Grundrechte der Personen, deren Daten in dieses Drittland übermittelt werden, ermöglichen würden*".
Diese besonderen Garantien bestehen aus:

- einem Angemessenheitsbeschluss der EU-Kommission,
- vertraglichen Garantien gemäß Artikel 46 der Verordnung (wie beispielsweise Standard-vertragsklauseln die von der Kommission mit der Entscheidung 2021/914/EU vom 4. Juni 2021 oder einer nationalen Datenschutz-behörde erlassenen wurden unbeschadet der Einführung zusätzlicher organisatorischer und technischer Sicherheitsmaßnahmen durch die Verantwortlichen für die Daten-verarbeitung und deren Auftragsverarbeiter.
-

Nel frattempo, il **19 settembre 2018** è entrato in vigore il D.lgs. 10 agosto 2018 che reca le disposizioni per l'adeguamento del D.lgs. 196/2003 “Codice in materia di protezione dei dati personali” (di seguito “Codice privacy”) al GDPR.

Sulla base di tali premesse, si procederà ad evidenziare le tematiche che hanno subito le maggiori evoluzioni nel corso del tempo e quelle che ancora costituiscono le iniziative più urgenti e cogenti al fine di poter ultimare il processo di adeguamento alle prescrizioni della normativa europea, fornendo, al contempo, alcune istruzioni operative

1. Trasferimento di dati all’estero

1.1 Spiegazioni

Mentre il trasferimento di dati personali all’interno dell’area UE è sempre ammesso, in caso di trasferimento di dati in Paesi extra UE sono necessarie particolari garanzie a tutela dei dati personali, soprattutto a seguito della sentenza della Corte di giustizia UE del 16 luglio 2020, Data Protection Commissioner /Facebook Ireland Limited e Maximilian Schrems, C-311/18 (sentenza Schrems 2). Tale sentenza ha invalidato il Privacy Shield, ovvero la previgente decisione di adeguatezza a favore degli USA, mettendo di fatto in discussione le basi giuridiche e la liceità dei trasferimenti di dati personali dagli Stati europei agli USA, in quanto la legislazione statunitense non è in grado di garantire un livello di protezione sostanzialmente equivalente a quello assicurato dallo Spazio Economico Europeo poiché “*renderebbe possibile, a causa del primato ivi riconosciuto alla sicurezza nazionale, ingerenze nei diritti fondamentali delle persone i cui dati sono trasferiti verso tale Paese terzo”*.
Queste particolari garanzie consistono in:

- una decisione di adeguatezza della Commissione europea;
- garanzie contrattuali di cui all’art. 46 del Regolamento: (per esempio clausole contrattuali tipo adottate dalla Commissione attraverso la decisione 2021/914/UE del 4 giugno 2021 o da un’autorità garante per la protezione dei dati personali nazionale, fermo restando l’introduzione di misure di sicurezza organizzative e tecniche aggiuntive ad opera dei titolari e dei loro responsabili del trattamento.

Diese Garantien kommen besonders dann zum Tragen, wenn die Organisationseinheiten des Landes beabsichtigen, eigenständig IT-Instrumente (z. B. Apps, Software, Cloud-Computing-Dienste) zu beschaffen, die alternativ und zusätzlich zu den von der Verwaltung angebotenen oder zur Verfügung gestellten Tools sind.

1.2 Maßnahmen

In Übereinstimmung mit dem Grundsatz der Rechenschaftspflicht und der Risikominimierung nehmen die einzelnen Organisationseinheiten als Sicherheitsanforderungen auch im Hinblick auf Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (*privacy by design and by default*) folgende Bedingungen in ihre Dokumente zur Lieferantenauswahl und -suche auf, die der Lieferant erfüllen muss:

a) **keine** personenbezogenen Daten außerhalb des Europäischen Wirtschaftsraums (EWR) zu übermitteln, es sei denn, der Staat, der die Daten empfängt, ist Gegenstand eines Angemessenheitsbeschlusses der Europäischen Kommission gemäß Artikel 45 der DSGVO,

b) auch **nicht** auf Unterlieferanten zurückgreifen, die ihrerseits die personenbezogenen Daten, die Gegenstand der Lieferung sind, außerhalb des EWR übermitteln können, unbeschadet der Bestimmungen unter a), wie z.B. Lieferanten von Supportleistungen für den Hauptlieferanten (z. B. Wartungsarbeiten). Im letzterem Fall würde nämlich ein Zugriff von Drittländern außerhalb des EWR erfolgen, was einer Übermittlung von Daten in Länder außerhalb des EWR gleichkommt, die vermieden werden muss, indem im Auftrag die Klausel aufgenommen wird, dass diese Bestimmung Vorrang vor allen anderen, möglicherweise widersprechenden Vertragsbestimmungen wie eine Standardbeschreibung der IT-Dienstleistungen hat.

Um eine einheitliche Datenschutzstrategie in der Landesverwaltung zu gewährleisten, beziehen die Organisationseinheiten die Abteilung Informationstechnik über die Demand Manager in den Einkauf von IT-Instrumente mit ein, da diese über den in der Abteilung eingerichteten Sicherheitsdienst für die Bewertung der technischen Konformität der angeforderten IT-Tools und die Erteilung der in der geltenden Regelung zur Nutzung der IT-Dienste vorgesehenen Genehmigung zuständig ist.

Der Antrag an SIAG muss seitens der Abteilung Informationstechnik unter Beifügung ihrer Stellungnahme auf Konformität eingereicht werden.

Queste garanzie possono venire in rilievo soprattutto nel caso in cui le strutture organizzative provinciali, intendano acquisire in autonomia strumenti informatici (quali app, programmi, software, servizi di cloud computing) alternativi ed aggiuntivi rispetto a quelli offerti o messi a disposizione dall'Amministrazione.

1.2 Cosa fare

Nel rispetto del principio di responsabilizzazione e di minimizzazione del rischio le singole strutture sono tenute ad inserire nei propri documenti di selezione e ricerca dei fornitori di prodotti e servizi IT, quali requisiti di sicurezza, anche in ottica di protezione dei dati fin dalla progettazione e protezione per impostazione predefinita **(***privacy by design and by default),* le seguenti condizioni a carico del fornitore ovvero di:

a) **non** trasferire dati personali al di fuori dello Spazio Economico Europeo (SEE), a meno che lo Stato destinatario dei dati non sia oggetto di una decisione di adeguatezza della Commissione europea ai sensi dell'articolo 45 del Regolamento;

b) **non** avvalersi di altri subfornitori che a loro volta possano trasferire i dati personali oggetto della fornitura al di fuori dello spazio SEE, fermo restando quanto previsto sub a), quali fornitori di un servizio di supporto al fornitore primario (per esempio attività di manutenzione o di assistenza tecnica). In questo caso ultimo caso si concretizzerebbe un accesso da remoto (da Paesi terzi extra-SEE) che risulta equivalente ad un trasferimento di dati in Paesi extra SEE, che deve essere scongiurato inserendo nell'incarico che, tale previsione prevale su qualsiasi altra disposizione potenzialmente contrastante del contratto, come una descrizione standard del prodotto o del servizio IT.

Al fine di garantire una strategia uniforme di protezione dei dati nell'Amministrazione provinciale, le strutture organizzative coinvolgono preventivamente la Ripartizione Informatica attraverso i Demand Manager di ogni Ripartizione nell'acquisto di strumenti informatici IT, in quanto quest'ultima tramite il Servizio di sicurezza, spetta la valutazione delle condizioni di conformità tecnica degli strumenti informatici richiesti ed il rilascio dell'autorizzazione di cui al vigente Disciplinare organizzativo sull'utilizzo dei servizi informatici.

La richiesta nei confronti di IAA deve pervenire dalla Ripartizione Informatica corredata di parere di conformità di quest'ultima. In caso di non conformità della soluzione richiesta, questa non sarà proseguita.

Entspricht die beantragte Lösung nicht den Anforderungen, wird sie nicht an SIAG weitergeleitet.

Diese Vorgehensweise ist auf der Grundlage der von der Landesregierung mit Beschluss Nr. 519/2022 genehmigten Rahmenvereinbarung 2022 und dem dazugehörigen, von der APB mit der SIAG unterzeichneten Addendum, das Bestandteil der Vereinbarung ist, erforderlich.

Wir möchten in diesem Zusammenhang darauf hinweisen, dass der Vertragsentwurf und die Vertragsklausel für die Ernennung des Auftragsverarbeiters gemäß Artikel 28 der DSGVO aktualisiert wurden und auf der Intranetseite http://homepage.prov.bz/intranet/ unter "Allgemeine Informationen / Datenschutz-GDPR / Inhaltsverzeichnis / Formulare und Texte" und zukünftig auf der MyNet-Seite bezüglich „Datenschutz“ (Dokumente) abgerufen werden können.

1.3 Ein praktisches Beispiel für eine mögliche Datenübermittlung in die USA: DeepL

Es wurde festgestellt, dass dieses automatische Textübersetzungsprogramm, das in der Landesverwaltung weit verbreitet ist, bei der PDF-Umwandlung auf die Infrastruktur von Adobe, einem Unternehmen mit Sitz in den Vereinigten Staaten, zurückgreift. Daher werden die Mitarbeiter und die Mitarbeiterinnen der einzelnen Organisationseinheiten, die diesen Dienst nutzen, im Einklang mit den Ausführungen in Punkt 1.1 aufgefordert:

a) den Text aus der PDF-Datei zu extrapolieren (Kopieren und Einfügen), um eine Konvertierung der PDF-Datei zu vermeiden,

b) zu vermeiden, dass Teile mit personenbezogenen Daten in den zu übersetzenden Text eingefügt werden.

2. Wahrnehmung der Rechte

2.1 Maßnahmen

In Ergänzung zum Punkt 4 des Rundschreibens Nr. 4/2018 des Generaldirektors werden die vertraglich vereinbarten Schritte und Kommunikationsmöglichkeiten zwischen Südtiroler Informatik AG (SIAG) und APB in Bezug auf die Behandlung von Anfragen zur Ausübung der Datenschutzrechte der betroffenen Person, für welche die APB als Verantwortlicher gilt, falls sie die Anfrage nicht selbstständig bearbeiten kann.

Tale procedura si rende necessaria sulla base dell’Accordo quadro 2022 approvato dalla Giunta provinciale con deliberazione n. 519/2022 e del relativo addendum sottoscritto da PAB con IAA, che ne costituisce parte integrante.

Si segnala che a questo proposito sono state aggiornate le bozze di contratto e di clausola contrattuale per le nomine dei responsabili del trattamento ex art 28 del GDPR accessibili alla pagina Intranet http://homepage.prov.bz/intranet/ seguendo il seguente percorso “Informazioni generali / Privacy GDPR / Indice dei contenuti / Modulistica e testi” e prossimamente alla pagina relativa alla “Protezione dei dati” in MyNet (documenti).

1.3 Un esempio pratico di possibile trasferimento di dati negli USA: DeepL

È stato accertato che questo strumento di traduzione automatica di testi, largamente utilizzato nell’Amministrazione provinciale, si avvale dell’infrastruttura di Adobe, società con sede negli Stati Uniti, nelle attività di conversione in formato PDF. Pertanto, in coerenza con quanto sopra indicato al punto 1.1 , si richiede ai collaboratori e alle collaboratrici di ogni struttura organizzativa fruitrice del servizio di:

a) estrapolare il testo dal pdf (copiare e incollare) così da evitare la conversione del pdf,

b) evitare di introdurre nel testo da tradurre le parti contenenti dati personali.

2. Esercizio dei diritti

2.1 Cosa fare

Ad integrazione del punto 4 della circolare del Direttore generale n. 4/2018 si descrivono le fasi e le modalità di comunicazione concordate a livello contrattuale tra Informatica Alto Adige SpA (IAA) e PAB per quanto riguarda la gestione delle richieste inerenti all’esercizio dei diritti dell’interessato in materia di protezione dei dati di cui PAB sia titolare qualora quest’ultima non possa provvedere autonomamente.

a) Wenn sie nicht in der Lage sind, Anträge auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung oder Widerspruch selbständig zu bearbeiten, leiten die Abteilungsdirektoren und Abteilungsdirektorinnen die Anträge an SIAG privacy@siag.it und, zur Kenntnis, an organisation@provinz.bz.it (Organisationsamt) weiter.

b) Die unter Buchstabe a) genannte E-Mail-Mitteilung muss als Anlage sowohl den Antrag der betroffenen Person als auch das unter Buchstabe c) genannte Formular enthalten.

c) Alle Anträge, die sich auf die von SIAG verwalteten Daten beziehen, müssen durch das Ausfüllen des Formulars in Anhang C1 gestellt werden, das auf der Intranetseite http://homepage.prov.bz/intranet/ unter "Allgemeine Informationen / GDPR-Datenschutz / Inhaltsverzeichnis / Formulare und Texte" und zukünftig auf der MyNet-Seite bezüglich „Datenschutz“ (Dokumente) abrufbar ist.

d) SIAG bestätigt den Eingang des Antrags per E-Mail innerhalb der folgenden drei Arbeitstage.

e) SIAG bearbeitet den Antrag und antwortet der APB (Direktor und Direktorin der zuständigen Abteilung und, zur Kenntnis, dem Organisationsamt) innerhalb der nächsten zwanzig Arbeitstage.

f) Alle Anfragen, die von den Betroffenen direkt an SIAG gerichtet werden und Daten betreffen, für welche APB der für die Datenverarbeitung Verantwortliche ist, werden an das Organisationsamt weitergeleitet, damit das festgelegte Verfahren eingehalten wird.

3. Verzeichnis von Verarbeitungstätigkeiten

3.1 Erklärungen

Artikel 30, Absatz 1 der DSGVO legt fest, dass „*jeder für die Verarbeitung Verantwortlich und gegebenenfalls sein Vertreter ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen, führen.“ „Genanntes Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann“.*

Die Führung des Verzeichnisses ist für Verantwortliche und (externe) Auftragsverarbeiter auch die Gelegenheit dafür, eine Erhebung der Verarbeitungstätigkeiten personenbezogener Daten, die ihrer Zuständigkeit unterliegen, sowie der von den verschiedenen Organisationseinheiten des Landes genutzten IT-Instrumente (Informationssysteme, Anwendungen) vorzunehmen, um diese den

a) I direttori di Ripartizione, qualora non possano provvedere ad evadere le richieste di accesso, di rettifica, di cancellazione, di limitazione del trattamento, di opposizione in autonomia trasmettono le richieste a IAA privacy@siag.it e, per conoscenza, ad organizzazione@provincia.bz.it (Ufficio Organizzazione).

b) La comunicazione a mezzo di e-mail di cui al punto a) dovrà prevedere come allegati sia la richiesta dell’interessato, sia il modulo di cui al successivo punto c).

c) Tutte le richieste relative ai dati gestiti da SIAG dovranno essere formalizzate attraverso la compilazione del modulo Appendice C1 accessibile alla pagina Intranet http://homepage.prov.bz/intranet/ seguendo il seguente percorso “Informazioni generali / Privacy GDPR / Indice dei contenuti / Modulistica e testi” e prossimamente alla pagina dedicata alla “Protezione dei dati” in MyNet (documenti).

d) IAA riscontrerà la presa in carico della richiesta mediante e-mail di risposta entro i tre giorni lavorativi successivi.

e) IAA evaderà la richiesta e darà riscontro a PAB (direttore e direttrice della Ripartizione competente e, per conoscenza all’Ufficio Organizzazione) nell’arco dei successivi venti giorni lavorativi.

f) Tutte le richieste che dovessero essere rivolte a IAA direttamente dagli interessati relative a dati di cui PAB risulti titolare del trattamento, saranno inoltrate all’Ufficio Organizzazione per seguire l’iter previsto.

3. Registro delle attività di trattamento

3.1 Spiegazioni

L’articolo 30, paragrafo 1, del GDPR stabilisce che *“Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità”.*
“I registri sono tenuti in forma scritta, anche in formato elettronico”.

La tenuta del registro rappresenta tra l’altro, per titolari e responsabili (esterni) del trattamento, l’occasione per effettuare la ricognizione dei trattamenti di dati personali di loro competenza e degli strumenti informatici (sistemi informativi, applicativi) utilizzati dalle varie strutture organizzative provinciali, in modo tale da poterli associare ai trattamenti in relazione ai quali sono impiegati; tale operazione costituisce

verschiedenen Verarbeitungstätigkeiten, für die sie verwendet werden, zuzuordnen. Diese Tätigkeiten stellen außerdem ein unverzichtbares Instrument für die Datenschutz-Folgenabschätzung dar. Durch die Zuordnung von Mitarbeitern und Mitarbeiterinnen zu den Organisationseinheiten, die für die Verarbeitung, die Gegenstand des Datenblatts ist, die Verantwortung tragen, kann die Ermächtigung (ehemalige Namhaftmachung als Beauftragte/r) gemäß Artikel 29 und 32 der DSGVO in digitaler Form erteilt werden.

Dasselbe gilt für die Maßnahme mit der den Direktoren und Direktorinnen – laut Artikel 2-quaterdecies des Datenschutzkodex - mit der Verarbeitung personenbezogener Daten zusammenhängende Aufgaben und Befugnisse übertragen werden.

3.2 Maßnahmen

Die Direktoren und die Direktorinnen der Organisationseinheiten des Landes sind verpflichtet, soweit sie es noch nicht veranlasst haben, bis zu maximal **drei** Mitarbeiter und Mitarbeiterinnen für jede einzelne Abteilung (samt zusammengehörigen Ämtern) zu benennen, deren Aufgabe es ist, die Verarbeitungstätigkeitkarteien auf der derzeit genutzten Plattform „KRC“ **innerhalb 30. Juni 2023** auszufüllen, sie zu vervollständigen und/oder sie zu berichtigen, damit diese Informationen veröffentlicht werden können.
Die Anleitungen zur Erfüllung der Pflichten im Zusammenhang mit der Nutzung des Verzeichnisses der Verarbeitungstätigkeiten finden Sie auf der Plattform in Form von FAQ, die vom Organisationsamt und für den technischen Teil von der Abteilung Informationstechnik erstellt wurden.

4. Die Datenschutz-Folgenabschätzung

4.1 Erklärungen

Artikel 35 der DSGVO verpflichtet grundsätzlich zur Durchführung einer Datenschutz-Folgenabschätzung, wenn die Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, d.h. wenn:

(a) neue Technologien verwendet werden (neue Programme, neue Datenbanken, Apps usw.),

(b) personenbezogene Aspekte natürlicher Personen mittels automatisierter Verarbeitung, einschließlich Profiling, systematisch und umfassend ausgewertet werden und Entscheidungen getroffen werden, die

inoltre uno strumento indispensabile per poter effettuare la valutazione d’impatto dei trattamenti. Inoltre, attraverso l’assegnazione dei collaboratori e delle collaboratrici alle strutture organizzative responsabili del trattamento oggetto della scheda, è possibile predisporre, in formato digitale, l’atto di autorizzazione (ex nomina ad incaricata/o) ai sensi degli articoli 29 e 32 del GDPR.

Ciò vale anche per quanto riguarda l’atto di nomina a preposto e preposta dei direttori e delle direttrici ai sensi dell’articolo 2-quaterdecies del Codice privacy.

3.2 Cosa fare

I direttori e le direttrici delle strutture organizzative provinciali sono tenuti a individuare, laddove non vi abbiano già provveduto, fino ad un massimo di **tre** compilatori per Ripartizione ed uffici da questa dipendente, ed a vigilare sul completamento delle schede di trattamento presenti nella piattaforma “KRC” attualmente in uso, in modo che queste siano integrate con i dati mancanti **entro il 30 giugno 2023**, onde poter procedere alla loro pubblicazione.
Le istruzioni per gli adempimenti connessi all’uso del registro dei trattamenti sono rinvenibili all’interno della piattaforma sottoforma di FAQ predisposte dall’Ufficio Organizzazione e, per la parte tecnica, dalla Ripartizione Informatica.

4. La valutazione di impatto sulla protezione dei dati

4.1. Spiegazioni

Indicativamente vi è un obbligo generale imposto dall’articolo 35 del GDPR di condurre una valutazione di impatto sulla protezione dei dati quando il trattamento dei dati comporta un rischio elevato per i diritti e le libertà degli interessati ovvero quando:

(a) si usano nuove tecnologie (nuovi programmi, app, ecc. ecc.)

(b) si valutano sistematicamente e globalmente aspetti personali relative a persone fisiche attraverso un trattamento automatizzato, compresa la profilazione e si prendono decisioni che hanno effetti

rechtliche Auswirkungen haben oder sie in ähnlicher Weise erheblich beeinträchtigen,

(c) die Verarbeitung von sensiblen und gerichtlichen Daten in großem Umfang erfolgt,

(d) eine groß angelegt systematische Überwachung eines der Öffentlichkeit zugänglichen Bereichs stattfindet (z. B. Videoüberwachung).

4.2 Maßnahmen

Die Folgenabschätzung wird mit Hilfe der KRC-Plattform durchgeführt. Sobald das Risiko für die Betroffenen als hoch eingestuft wird, wird das Dokument zur digitalen Unterschrift des und des zuständigen Direktors und Direktorin vorgelegt und als Beweismittel in das System hochgeladen. Es wird auf die in Abschnitt 3.2 genannte Frist für die Durchführung der Datenschutz-Folgenabschätzung, falls erforderlich, hingewiesen.

5. Data Breach (Meldung der Verletzung des Schutzes personenbezogener Daten)

5.1 Erklärungen

Artikel 4, Punkt 12 der DSGVO bezeichnet die Verletzung personenbezogener Daten als „*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.“*

Bekanntlich muss der Verantwortliche für die Datenverarbeitung „*der Aufsichtsbehörde Verletzungen personenbezogener Daten von der er Kenntnis hat, innerhalb von 72 Stunden und auf jedem Fall ohne ungerechtfertigte Verspätung mitteilen*“, aber dies nur wenn er es für voraussichtlich hält, dass diese Verletzung zu Risiken für die Rechte und Freiheiten natürlicher Personen führt. Sollte das Risiko als erhöht bewertet werden, muss die Verletzung auch allen betroffenen Personen mitgeteilt werden (Art. 33 und 34 der DSGVO). Die Direktoren und Direktorinnen der Organisationseinheiten des Landes können sich bei der Einhaltung ihrer Pflichten, vom externen Auftragsverarbeiter (Südtiroler Informatik AG oder von einem anderen externen Auftragsverarbeiter, denen sie die Verarbeitung übertragen haben) unterstützen lassen (Art. 28, Absatz 3, Buchstabe f)) der DSGVO.

giuridici o incidono in modo analogo significativamente su dette persone;

(c) il trattamento di dati sensibili e giudiziari è su larga scala;

(d) vi è sorveglianza sistematica su larga scala di una zona accessibile al pubblico (es: videosorveglianza).

4.2 Cosa fare

La valutazione di impatto viene condotta con l’ausilio della piattaforma KRC. Una volta che il rischio per gli interessati sia ritenuto elevato, il documento viene sottoposto alla firma digitale del direttore e della direttrice competente e caricato nel sistema in modo da costituire evidenza documentale. Si rinvia al termine indicato al punto 3.2 per la conduzione della valutazione di impatto, qualora necessaria.

5. Data breach (Notificazione delle violazioni dei dati personali)

5.1 Spiegazioni

L’articolo 4, punto 12 del GDPR definisce violazione dei dati personali “*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati”*.

Notoriamente il titolare del trattamento deve “*notificare, all'autorità di controllo, le violazioni di dati personali di cui venga a conoscenza, entro 72 ore e comunque senza ingiustificato ritardo",* ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà delle persone fisiche. Qualora il rischio sia ritenuto elevato, è necessario comunicare la violazione avvenuta anche a tutti gli interessati (artt. 33 e 34 del GDPR). I direttori e le direttrici delle strutture provinciali, nell’adempimento dell’obbligo richiamato potranno farsi assistere, come previsto dall’articolo 28, paragrafo 3, lettera f), del GDPR, dal responsabile esterno del trattamento (Informatica Alto Adige Spa o, eventualmente, altro responsabile esterno al quale le strutture provinciali hanno affidato i loro trattamenti).

5.2 Maßnahmen

Aufgrund des erneuten Rahmenabkommens zwischen APB und SIAG, sollte die Südtiroler Informatik AG eine Verletzung von personenbezogenen Daten feststellen, ist sie verpflichtet, dies dem Datenschutzbeauftragten des Landes und dem Organisationsamt umgehend und in jedem Fall innerhalb von 24 Stunden ab Kenntnisnahme, mitzuteilen.

Sollte die Verletzung hingegen „interne“ Informationssysteme oder Anwendungen (die autonom von der Organisationseinheit des Landes verwaltet werden) oder die Struktur dieser Organisationseinheit betreffen (z.B. unbefugter Zugang zu Büroräumen oder Archiven, Überschwemmungen, Brände, Verletzung durch Fehlverhalten des Personals), obliegt es dem Direktor/der Direktorin der jeweiligen Organisations-einheit, welche auf die Unterstützung des Dienstleisters zurückgreifen kann, innerhalb von 24 Stunden nach Kenntnisnahme der Verletzung das entsprechende Formular (auf der Webseite http://homepage.prov.bz/intranet/ unter „Allgemeine Informationen“ – „Privacy“ – „Formulare und Texte“ und zukünftig auf der MyNet-Seite bezüglich „Datenschutz“ (Dokumente), zugänglich) auszufüllen. Das Formular ist an die Mailadresse rpd_dsb@pec.prov.bz.it, zu übermitteln. In beiden oben beschriebenen Fällen bewerten das Organisationsamt mit dem und der Datenschutz-beauftragte des Landes die Situation und, sofern es sich um eine mitteilungspflichtige Verletzung handelt, melden sie dies der Aufsichtsbehörde und, wenn nötig den betroffenen Personen.

6. Cookie Richtlinie

6.1 Erklärungen

Gemäß Artikel 122 des Datenschutzkodex ist es nicht möglich, Informationen, die als "Cookies" bezeichnet werden, im Endgerät der Nutzer ohne ihre **vorherige Einwilligung** zu speichern, nachdem sie mit vereinfachtem Verfahren informiert wurden, es sei denn, es handelt sich um so genannte "technische" Cookies, deren Speicherung ausschließlich für die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz bestimmt ist, oder wenn dies für den Anbieter eines Dienstes der Informationsgesellschaft, unbedingt erforderlich ist, damit er diesen Dienst, der vom Nutzer ausdrücklich aufgerufen wurde, zur Verfügung stellen kann.

Diese Vorschrift findet in der Datenschutz- und Cookie- Policy der Websites des Landes Anwendung,

5.2 Cosa fare

A seguito del rinnovato Accordo quadro tra PAB e IAA, nell’ipotesi in cui Informatica Alto Adige Spa accertasse una violazione di dati personali, è tenuta a comunicare l’evento al DPO di PAB e all’Ufficio Organizzazione immediatamente e comunque non oltre entro 24 ore dalla conoscenza.

Qualora, invece, la violazione di dati personali riguardasse sistemi informativi e/o applicativi “interni” (e cioè gestiti in autonomia dalla singola struttura provinciale), o fosse connessa all’organizzazione della medesima struttura (ad es. abusivo accesso agli uffici o agli archivi cartacei, allagamenti, incendi, violazioni di dati causati dal comportamento del personale ecc.), spetterà al direttore e alla direttrice della struttura provinciale, fermo restando l’assistenza del responsabile esterno, compilare, entro 24 ore dall’avvenuta conoscenza della violazione, il modello reperibile alla pagina Intranet: http://homepage.prov.bz/intranet/ seguendo il seguente percorso: Informazioni generali/Privacy GDPR/Indice dei contenuti/Modulistica e testi/, e prossimamente alla pagina relativa alla “Protezione dei dati” in MyNet (documenti), ed inoltrarlo al seguente indirizzo email: rpd_dsb@pec.prov.bz.it, In entrambi i casi sopra descritti, l’Ufficio Organizzazione ed il DPO di PAB procederanno alle valutazioni del caso, e, nel caso di violazione da notificare, provvederanno a trasmetterlo all’autorità di controllo ed eventualmente agli interessati, se dovuto.

6. Cookie policy

6.1 Spiegazioni

Ai sensi dell’articolo 122 del Codice privacy non è possibile installare nell’apparecchio terminale di utenti informazioni chiamate “cookie” senza il **consenso preventivo** dello stesso, a meno che non si tratti di cookie detti “tecnici” ossia la cui archiviazione sia finalizzata unicamente ad effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica, o nella misura strettamente necessaria al fornitore di un servizio della società dell’informazione esplicitamente richiesto dall’utente ad erogare tale servizio.

Tale disposizione trova applicazione nella *privacy e cookie policy* dei siti web provinciali, che è in fase di

die derzeit in allen Domains des Landes aktualisiert wird, und dies in Übereinstimmung mit den "*Leitlinien des Datenschutzbehörde zu Cookies und anderen Tracking-Tools"* vom 10. Juni 2021 - am 10. Januar 2022 in Kraft getreten.

Zur Erteilung der ausdrücklichen Einwilligung verwendet die Verwaltung entsprechende Konfigurationen von Informatikprogrammen oder von Geräten, die vom Nutzer einfach und klar anwendbar sind (siehe insbesondere die Datenschutz- und Cookie-Policy und das Zustimmungsbanner am Ende der Webseite).

6.2 Maßnahmen

Damit die SIAG als Verwalter der Website des Landes die Installierung von Cookie von Drittanbietern ausschließlich mit der Zustimmung des Nutzers und nicht zuvor, zulassen kann, ist es erforderlich, dass diejenigen, die als ***Web-Content-Manager*** für die einzelnen Organisationseinheiten tätig sind und in dieser Rolle Medieninhalte (YouTube) oder die wichtigsten Social-Networks (wie Facebook, Twitter, LinkedIn, Instagram usw.) auf den Webseiten des Landes veröffentlichen oder veröffentlicht haben, ein Ticket beim Call Center APB öffnen und über service.pab@provinz.bz.it das Vorhandensein dieser Inhalte mitteilen. Nur so kann das verwendete Tool diese kleinen Textdateien als Cookies von Drittanbietern klassifizieren und verwalten, wobei die **vorherige Zustimmung** des Nutzers erforderlich ist, und sie auch in der Informationsmitteilung für die Öffentlichkeit transparent machen. Andernfalls besteht die Gefahr, dass das besagte Cookie:

a) bei fehlender vorheriger Zustimmung installiert wird,

b) in der öffentlich zugänglichen Cookie-Policy nicht angegeben wird.

Beide Vorgehensweisen stellen Verstöße gegen die DSGVO dar.

7. Rechtliche Grundlage

7.1 Erklärungen

Wir weisen bei dieser Gelegenheit darauf hin, dass jede Datenverarbeitung durch Einrichtungen auf den in Artikel 6 der DSGVO vorgesehenen Rechtsgrundlagen beruhen muss, wie z. B. der Wahrnehmung einer Aufgabe im öffentlichen Interesse, einer rechtlichen Verpflichtung, der Erfüllung eines Vertrags oder vorvertraglicher Maßnahmen, an denen die betroffene Person beteiligt ist (Artikel 6 Absatz 1 Buchstaben e), c) und b) der

aggiornamento in tutti i domini provinciali nel rispetto di quanto fissato dalle "*Linee guida del Garante per la protezione dei dati sui cookie e altri strumenti di tracciamento*" del 10 giugno 2021, entrate in vigore il 10 gennaio 2022.

Ai fini dell'espressione del consenso l'Amministrazione utilizza specifiche configurazioni di programmi informatici o dispositivi che siano di facile e chiara utilizzabilità per l'utente (vedasi in particolare la privacy, la cookie policy ed il banner per il rilascio del consenso posto in calce alla pagina web).

6.2 Cosa fare

Per fare in modo che IAA, in qualità di gestore dei sito web della Provincia, sia in grado di consentire l'installazione dei cookie di terze parti, esclusivamente a fronte del consenso prestato dell'utente, e non prima, è necessario che coloro che operano in qualità di ***web content manager*** per ciascuna struttura, ed in questo ruolo pubblicano o hanno pubblicato sulle pagine web provinciali contenuti multimediali (YouTube) o dei principali social network (come Facebook, Twitter, LinkedIn, Instagram ecc..), aprano un ticket al Call Center di PAB, comunicando la presenza di questi contenuti all'indirizzo service.pab@provincia.bz.it. Solo allora lo strumento in uso sarà in grado di classificare e di gestire questi piccoli file di testo come cookie di terza parte soggetti al **consenso preventivo** dell'utente, e renderli trasparenti al pubblico anche nell'informativa. In caso contrario si rischia che il suddetto cookie:

a) sia installato in mancanza di consenso preventivo,

b) non sia censito nella cookie policy da rendere accessibile al pubblico.

Entrambe le condotte costituiscono violazioni del GDPR.

7. Base giuridica

7.1 Spiegazioni

Si coglie l'occasione per ricordare che ogni trattamento di dati attuato dalle strutture deve trovare il proprio fondamento nelle basi giuridiche previste dall'articolo 6 del GDPR, quali l'esecuzione di un compito di un compito di interesse pubblico, un obbligo di legge, l'esecuzione di un contratto o di misure precontrattuali di cui l'interessato è parte (rispettivamente art. 6, par. 1 lett. e), c), b) del GDPR). Il consenso ai sensi della lett. a) del e il legittimo

DSGVO). Die Einwilligung im Sinne von Buchstabe a) und das berechtigte Interesse des für die Verarbeitung Verantwortlichen im Sinne von Buchstaben f) des vorgenannten Artikels stellen keine Rechtsgrundlage für die Datenverarbeitung durch öffentliche Verwaltungen dar, es sei denn, dies ist gesetzlich vorgesehen.

interesse del titolare ai sensi della lett. f), del predetto articolo non costituiscono le basi giuridiche per i trattamenti di dati svolti da pubbliche amministrazioni, eccetto i casi in cui è la legge a prevederlo.

Die Aufgabe im öffentlichen Interesse und der Gegenstand der Verpflichtung müssen von einer Gesetzes- oder Verordnungsvorschrift oder in allgemeinen Verwaltungsakten vorgesehen werden, die
a) den Zweck der Verarbeitung,

b) die oben genannten rechtlichen Grundlagen,

c) die Art der verarbeiteten Daten,

d) die Kategorien der betroffenen Personen,

e) die Rechtsubjekte, deren die Daten mitgeteilt werden können und den Zweck der Mitteilung,

f) die Zweckbindung,

g) die Dauer der Aufbewahrung,

h) die Maßnahmen für eine rechtmäßige und korrekte Datenverarbeitung, enthalten.

Dies gilt auch für die Verbreitung (Veröffentlichung) personenbezogener Daten, die nur dann zulässig ist, wenn sie durch eine Rechtsvorschrift oder einen allgemeinen Verwaltungsakt unter Einhaltung der Grundsätze der Datenminimierung, der Zweckbindung und der Speicherung, der Richtigkeit und der Sicherheit vorgesehen ist. Die Verbreitung von Daten in Ermangelung einer Vorschrift kann von der Aufsichtsbehörde mit einem Bußgeld von bis zu 20 Mio. EUR geahndet werden und stellt eine Straftat dar.

Il compito di interesse pubblico e l'oggetto dell'obbligo, devono essere previsti o da un atto normativo, o regolamentare, o da atti amministrativi generali che contengano:

a) la finalità del trattamento

b) le basi giuridiche di cui sopra

c) i tipi di dati trattati

d) l'indicazione degli interessati

e) i soggetti i cui dati possono essere comunicati e le finalità della comunicazione

f) la limitazione della finalità

g) i periodi di conservazione

h) le misure atte a garantire un trattamento lecito e corretto.

Quanto detto sopra trova anche applicazione per quanto riguarda la diffusione (pubblicazione) di dati personali che é ammessa esclusivamente quando sia prevista da una norma di legge o di regolamento o da atti amministrativi generali nel rispetto dei principi di minimizzazione, limitazione della finalità e della conservazione, esattezza e sicurezza dei dati. La diffusione di dati in assenza di una norma può comportare la comminazione di sanzione amministrative pecuniarie fino a 20 milioni di euro da parte dell'Autorità Garante ed un illecito penale.

7.2 Maßnahmen

Vor Beginn der Verarbeitung identifiziert jede Organisationseinheit die Rechtsgrundlage, die die Verarbeitung rechtfertigt, und zwar unter den in Artikel 6 der DSGVO vorgesehenen Rechtsgrundlagen, und prüft anschließend, ob die Rechtsvorschriften, die die Gewährung einer finanziellen Unterstützung oder einer Dienstleistung festlegen und/oder regeln, die unter Punkt 7.1 genannten Elemente von a) bis h) enthalten.

Werden Rechtslücken festgestellt, muss jede Organisationseinheit Maßnahmen ergreifen, um diese zu füllen, auch durch Rückgriff auf allgemeinen

7.2. Cosa fare

Prima dell'avvio del trattamento ogni struttura procede a rinvenire la base giuridica che lo legittima tra quelle previste all'articolo 6 del GDPR, e successivamente, procede alla ricognizione delle proprie fonti normative, verificando, se le fonti che istituiscono e/o disciplinano l'erogazione di un contributo o di un servizio, contengano gli elementi da a) a h) di cui al punto 7.1.

Se vengono constatati vuoti o lacune normativi, ogni struttura provvede a colmarli, anche avvalendosi di atti amministrativi a contenuto generale (deliberazioni di

Verwaltungsakten (Beschlüsse der Landesregierung, Rundschreiben, usw.). Dies gilt sowohl für die bereits bestehenden als auch für die in Zukunft einzuführenden Leistungen.

Giunta provinciale, circolari ecc..). Quanto detto vale sia per le prestazioni in essere che per quella futura introduzione.

8. Datenschutzerklärungen

8. Informative privacy

8.1 Erklärungen

8.1 Spiegazioni

Auf der Intranetseite http://homepage.prov.bz/intranet/ unter Allgemeine Informationen/GDPR-Datenschutzerklärung/Inhaltsverzeichnis/Formulare und Texte/, und zukünftig auf der MyNet-Seite bezüglich „Datenschutz“ (Dokumente), sind sowohl die kurze als auch die ausführlichen Fassungen der Datenschutzerklärungen gemäß Artikel 13 und 14 der DSGVO verfügbar.
Wir möchten an dieser Stelle darauf hinweisen, dass, während die Einfügung der ausführlichen Datenschutzerklärung immer erforderlich ist - unabhängig davon, ob sie in das Papierformblatt aufgenommen wird oder über einen Link von einem Online-Formular in digitaler Form oder von einem editierbaren PDF-Format zugänglich ist, welcher jeweils auf die in CIVIS oder auf der institutionelle Web Seite des jeweiligen Dienst veröffentlichen Informationen verweist- die Einfügung der kurzen Datenschutzerklärung hingegen eine Möglichkeit darstellt.

Alla pagina Intranet http://homepage.prov.bz/intranet/ seguendo il percorso Informazioni generali/Privacy GDPR/Indice dei contenuti/Modulistica e testi/, e prossimamente alla pagina relativa alla “Protezione dei dati” in MyNet (documenti), sono disponibili sia le versioni brevi che quelle estese delle informative privacy ai sensi degli articoli 13 e 14 del GDPR.
Preme ricordare in questa sede, che, mentre l’inserimento dell’informativa estesa è sempre obbligatorio - sia questa collocata all’interno del modulo cartaceo o accessibile tramite un link da un modulo digitale online od in formato PDF editabile, che rinvia rispettivamente a quanto pubblicato in CIVIS o sulla pagina web del sito istituzionale dedicata al servizio specifico - l’inserimento dell’informativa breve è una facoltà.

8.2 Maßnahmen

8.2 Cosa fare

Die Direktoren und die Direktorinnen sorgen dafür, dass die vorgenannten Datenschutzerklärungen, wo auch immer sie zu finden sind, auf dem aktuellen Stand sind und die letzten Fassungen in die Formulare aufgenommen werden.
Wenn Sie dies noch nicht getan haben, werden Sie darum ersucht, die Versionen der abweichenden Datenschutzerklärungen zu entfernen, wo immer sie sich befinden, sowohl in Papier- als auch in digitaler Form - und sie durch die aktualisierten zu ersetzen.

I direttori e le direttrici vigilano sull’aggiornamento delle informative di cui sopra, ovunque esse siano collocate, avendo cura che nei moduli vengano inserite le versioni più recenti.

Qualora non si sia già provveduto, si invita pertanto, a rimuovere le versioni delle informative difformi ovunque presenti sia in forma cartacea che digitale, e a sostituirle con quelle aggiornate ed attuali.

Wenn Sie sich für die Einfügung der kurzen Datenschutzerklärung in die editierbaren PDF- und in die Online-Formulare entscheiden:

Nel caso si opti per l’inserimento dell’informativa breve nei moduli PDF editabili ed in quelli online:

(a) muss unter dem vorgeschriebenen Text ein obligatorisches Kästchen mit folgendem Wortlaut eingefügt werden:

(a) sotto al testo previsto va aggiunto una check box obbligatoria recante la dicitura:

"Ich erkläre, dass ich die vollständigen Datenschutzerklärung gemäß der Grundverordnung (EU) 2016/679 gelesen habe",

"*Dichiaro di aver preso visione dell'informativa completa per la protezione dei dati personali ai sensi del Regolamento UE 2016/679* ";

(b) es muss ein Link eingefügt werden, der die Einsichtnahme in die erweiterten Datenschutz-erklärung, wie unter Abschnitt 8.1 beschrieben, ermöglicht.

Zwecks Einfügung der kurzen Datenschutzerklärung in die Online-Verfahren (nach dem Login), öffnen die *Content Manager* ein Ticket beim Call Center APB service.pab@provinz.bz.it mit Angabe der Identifikationsnummer bzw. der URL des Online-Dienstes.

Für alle Vorgaben vorliegenden Rundschreibens wird auf das Rundschreiben des Generaldirektors Nr. 4/2018 verwiesen.

Mit freundlichen Grüßen

(b) va inserito il link che permette la lettura dell'informativa estesa come descritto al punto 8.1.

Per l'inserimento dell'informativa breve nei procedimenti online (dopo il Login) i *content manager* aprono un ticket presso il Call Center PAB service.pab@provinz.bz.it precisando nella richiesta il numero identificativo e/o l'indirizzo URL del servizio online.

Per tutto quanto non disposto dalla presente circolare si rinvia alla circolare del Direttore generale n. 4/2018.

Cordiali saluti

Der Generaldirektor / Il Direttore generale

Alexander Steiner
(mit digitaler Unterschrift unterzeichnet / sottoscritto con firma digitale)

Firmato digitalmente da:
Alexander Steiner
Data: 05/04/2023 17:30:40