

**Beschluss
der Landesregierung****Deliberazione
della Giunta Provinciale**

Nr. 383
Sitzung vom 24/04/2018
Seduta del

ANWESEND SIND

Landeshauptmann
Landeshauptmannstellvertr.
Landeshauptmannstellvertr.
Landesräte

Generalsekretär

Arno Kompatscher
Christian Tommasini
Richard Theiner
Philipp Achammer
Waltraud Deeg
Florian Mussner
Arnold Schuler
Martha Stocker

Eros Magnago

SONO PRESENTI

Presidente
Vicepresidente
Vicepresidente
Assessori

Segretario Generale

Betreff:

Planung der IT Sicherheitsmaßnahmen
ausgerichtet an die Grundverordnung zum
Datenschutz der EU Nr. 2016/679 für die
Jahre 2018-2020.

Oggetto:

Pianificazione delle attività di sicurezza IT
orientate al Regolamento europeo sulla
protezione dei dati n. 2016/679 relativa agli
anni 2018-2020.

Vorschlag vorbereitet von
Abteilung / Amt Nr.

GD.2

Proposta elaborata dalla
Ripartizione / Ufficio n.

Am 6. April 2016 einigte sich die EU auf eine umfassende Reform ihres Datenschutz-Rechtsrahmens und verabschiedete das Datenschutz-Reformpaket. Das Paket umfasst die Datenschutz-Grundverordnung 2016/679 (im Folgenden als Grundverordnung bezeichnet), die die zwanzig Jahre alte Datenschutzrichtlinie 95/46/EG ersetzt, sowie die Richtlinie 2016/680 über die Datenübertragungen zu polizeilichen und gerichtlichen Zwecken. Die Grundverordnung wird als neues EU-weites Datenschutzinstrument am 25. Mai 2018, also zwei Jahre nach seiner Verabschiedung und seinem Inkrafttreten, anwendbar.

Die Grundverordnung gilt unmittelbar in allen EU-Mitgliedstaaten, das heißt, dass sie unabhängig von den nationalen Rechtsvorschriften verbindlich ist. Dennoch müssen auf nationaler Ebene die erforderlichen Schritte unternommen werden, um die jeweilige Gesetzgebung durch Aufhebung und Änderung bestehender Rechtsvorschriften der Grundverordnung anzupassen. In Italien wurde der Datenschutzkodex, der mit gesetzesvertretendem Dekret vom 30. Juni 2003, Nr. 196 erlassen wurde, jedoch noch nicht den neuen EU-Vorschriften angepasst.

Obwohl der neue Datenschutzrahmen auf den bisher geltenden Rechtsvorschriften aufbaut, wird er weitreichende Auswirkungen haben und in mancher Hinsicht erhebliche Anpassungen und ein strategisches Umdenken bei der Organisation erfordern.

Durch die Grundverordnung wurden bestehende Datenschutzvorschriften präzisiert und aktualisiert und eine Reihe neuer Elemente zur Stärkung des Schutzes der Rechte betroffener Personen hinzugefügt. Zentrale Punkte sind

- ein harmonisierter Rechtsrahmen, der zu einer einheitlichen Anwendung der Vorschriften in allen EU-Mitgliedstaaten führt, was sich positiv auf den europäischen digitalen Binnenmarkt auswirkt; die Grundverordnung schafft nämlich

Il 6 aprile 2016 l'Unione europea ha modificato radicalmente il quadro giuridico relativo alla protezione dei dati adottando il pacchetto di riforma in materia. Il pacchetto comprende il regolamento generale sulla protezione dei dati personali 2016/679 (di seguito definito Regolamento), che sostituisce la ventennale direttiva 95/46/CE ("regolamento generale sulla protezione dei dati") e la direttiva sulla protezione dei dati nell'ambito della cooperazione giudiziaria e di polizia. Il 25 maggio 2018, due anni dopo la sua adozione ed entrata in vigore, il regolamento diventerà direttamente applicabile quale nuovo strumento di protezione dei dati personali a livello dell'Unione.

Il regolamento è direttamente applicabile in tutti gli Stati membri UE. Ciò significa che entra in vigore e si applica senza necessità di alcun atto legislativo nazionale. Ciononostante, conformemente al regolamento, a livello nazionale devono essere adottate le misure necessarie per adattare la rispettiva legislazione, abrogando e modificando le leggi esistenti. Infatti, il Codice in materia di protezione dei dati personali, approvato con decreto legislativo 30 giugno 2003, n. 196, non è stato ancora adeguato alla nuova normativa UE.

Pur basandosi sulla normativa vigente, il nuovo quadro giuridico avrà effetti di ampia portata e, per certi aspetti, richiede notevoli adeguamenti e un ripensamento strategico degli assetti organizzativi.

Il regolamento chiarisce e modernizza le attuali norme in materia di protezione dei dati e introduce alcuni elementi innovativi che rafforzano la tutela dei diritti delle persone, in particolare:

- un quadro giuridico armonizzato che porta a un'applicazione uniforme delle norme in tutti gli Stati membri UE, a tutto vantaggio del mercato unico digitale dell'Unione; il regolamento stabilisce infatti un unico insieme di norme per i singoli

ein einheitliches Regelwerk für Einzelpersonen und Unternehmen und bewirkt damit eine wesentliche Verbesserung der bisherigen Situation, da die einzelnen Mitgliedstaaten die Vorschriften der früheren Datenschutzrichtlinie unterschiedlich umgesetzt hatten;

cittadini e le imprese, che rimedierà alla situazione attuale in cui gli Stati membri dell'Unione stanno applicando in modi diversi le precedenti norme in materia;

- die Hervorhebung der Grundsätze des Datenschutzes durch Technik (*data protection by design*) und durch datenschutzfreundliche Voreinstellungen (*data protection by default*), mit denen innovative Lösungen gefördert werden sollen, damit von Anfang an die Datenschutzinteressen berücksichtigt werden und die Erhebung der personenbezogenen Daten innerhalb der Verwaltung sich auf ein Minimum beschränkt;
- die Stärkung der Rechte natürlicher Personen, indem neue Transparenzanforderungen eingeführt, das Recht auf Information, auf Datenzugang und auf Datenlöschung („Recht auf Vergessenwerden“) gestärkt sowie neue Informationspflichten auferlegt werden, durch welche Einzelpersonen mehr Kontrolle über die sie betreffenden Daten erhalten;
- ein besserer Schutz gegen Datenmissbrauch (*data breach*): Mit der Grundverordnung wird die „Verletzung des Schutzes personenbezogener Daten“ genau definiert und es werden umfassende Vorschriften dazu erlassen; unter anderem besteht die Pflicht, der Aufsichtsbehörde – in Italien ist dies die Datenschutzbehörde – jede solche Verletzung binnen höchstens 72 Stunden zu melden, wenn sie zu einem Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person führt; in einigen Fällen muss auch die betroffene Person unverzüglich von der Verletzung des Schutzes der sie betreffenden Daten benachrichtigt werden;
- adozione dei principi di protezione dei dati fin dalla progettazione (*data protection by design*) e di protezione per impostazione predefinita (*data protection by default*) per promuovere soluzioni innovative atte a garantire sin dall'inizio risposte adeguate alla protezione dei dati e ridurre al minimo la raccolta dei dati personali all'interno dell'Amministrazione;
- diritti delle persone fisiche rafforzati. Il regolamento introduce nuovi requisiti in materia di trasparenza e diritti rafforzati in materia di informazione, accesso ai dati e cancellazione (“diritto all'oblio”), così come nuovi obblighi informativi, attraverso i quali le singole persone possono esercitare maggiore controllo sui dati che le riguardano;
- maggiore protezione contro la violazione dei dati (*data breach*). Il regolamento fornisce una chiara definizione di “violazione dei dati personali” e stabilisce un insieme completo di norme in materia; esso introduce inoltre l'obbligo di notifica entro 72 ore all'autorità di controllo (Garante per la protezione dei dati personali) quando la violazione dei dati potrebbe comportare un rischio per i diritti e le libertà delle persone fisiche; in alcune circostanze, impone l'obbligo di informare la persona interessata della violazione dei dati che la riguardano;

- die Befugnis der Aufsichtsbehörde, Geldbußen bis zu 20 Millionen Euro gegen Rechtsinhaber der Verarbeitung und Auftragsverarbeiter zu verhängen;
- eindeutige Vorschriften zu Verantwortung und Haftung (mit Rechenschaftspflicht) des Rechtsinhabers der Datenverarbeitung – in diesem Fall ist dies die Landesverwaltung – und der Auftragsverarbeiter, was einerseits mehr Flexibilität bringt, andererseits aber auch zur Festlegung geeigneter Maßnahmen und Vorgehensweisen und zur Aufbewahrung der entsprechenden Nachweise verpflichtet;
- der Grundsatz der Rechenschaftspflicht, der mit abgestuften Verpflichtungen je nach Risiko verbunden ist (z. B. Benennung eines/einer *Datenschutzbeauftragten* und *Verpflichtung zur Datenschutz-Folgenabschätzung*);
- die Datenschutz-Folgenabschätzung, die vor Beginn der Datenverarbeitung durchzuführen ist, wenn die Verarbeitung zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen kann. Drei Fälle sind ausdrücklich angeführt:
 - 1) die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die auf automatisierter Verarbeitung, einschließlich Profiling, gründet,
 - 2) die umfangreiche Verarbeitung von sensiblen oder Gerichtsdaten,
 - 3) die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;
 diese Liste kann von der nationalen Aufsichtsbehörde durch weitere Fälle ergänzt werden;
- mehr Klarheit über die Verantwortung und Haftung des Rechtsinhabers der Verarbeitung hinsichtlich der Auswahl externer
- il regolamento conferisce all'Autorità garante per la protezione dei dati il potere di infliggere sanzioni pecuniarie, fino a 20 milioni di euro, ai titolari del trattamento e ai responsabili del trattamento.
- maggiore flessibilità per il titolare del trattamento – in questo caso l'Amministrazione provinciale - e i responsabili del trattamento che trattano dati personali, grazie a disposizioni univoche in materia di responsabilità (*principio di responsabilizzazione*). Ciò comporta anche l'obbligo di adottare adeguate misure e procedure e di conservare le relative prove;
- il principio di responsabilizzazione attuato tramite obblighi modulabili in funzione del rischio (per esempio l'obbligo di designare un/una *responsabile della protezione dei dati* e l'obbligo di svolgere una *valutazione d'impatto sulla protezione dei dati*);
- la valutazione d'impatto sulla protezione dei dati, da effettuare prima di iniziare il trattamento, e ogniqualvolta quest'ultimo possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Tale valutazione è espressamente richiesta in caso di:
 - 1) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione,
 - 2) trattamento, su larga scala, di dati sensibili e giudiziari,
 - 3) sorveglianza sistematica su larga scala di una zona accessibile al pubblico;
 tale elenco potrà essere modificato e integrato da parte dell'Autorità garante nazionale;
- maggiore chiarezza riguardo alla responsabilità del titolare del trattamento a fronte della scelta di un responsabile esterno del

Auftragsverarbeiter sowie über die Pflichten dieser Auftragsverarbeiter.

trattamento e riguardo agli obblighi in capo a quest'ultimo.

Dies vorausgeschickt, ist es angesichts des näher rückenden Anwendungstermins (25. Mai) erforderlich und angebracht, alle Verwaltungsvorgänge einer Bestandsaufnahme zu unterziehen und auszuloten, welche weiteren Schritte geeignet wären, um sicherzustellen, dass alle Voraussetzungen für eine erfolgreiche Anwendung des neuen Rechtsrahmens gegeben sind.

Ciò premesso, con l'avvicinarsi della data di applicazione del regolamento (25 maggio), si ritiene necessario e opportuno fare il punto sullo stato di fatto delle procedure amministrative e valutare eventuali altri provvedimenti che potrebbero essere utili per garantire che tutto sia pronto per la riuscita applicazione del nuovo quadro giuridico.

Zu diesem Zweck sind folgende Verfahrensschritte geplant:

A tale scopo si procederà come segue:

1. Das Organisationsamt der Landesverwaltung aktualisiert die Vordrucke (die Mitteilungen an die betroffenen Personen zur Information laut Art. 13 und 14 sowie die Formulare, mit denen Bürgerinnen und Bürger gemäß Art. 15 ff. der Grundverordnung von ihren Rechten Gebrauch machen können) und bereitet die Entwürfe für die Verträge bzw. die Standardvertragsklauseln vor, mit denen die Beziehungen zwischen der Autonomen Provinz Bozen als Rechtsinhaber der Datenverarbeitung und anderen juristischen Personen als externe Auftragsverarbeiter gemäß Art. 28 der Grundverordnung geregelt werden.

1. L'ufficio provinciale Organizzazione sta aggiornando la modulistica (informative agli interessati ai sensi degli artt. 13 e 14, e moduli per l'esercizio dei diritti da parte dei cittadini ai sensi degli artt. 15 e segg. del Regolamento) e sta predisponendo i modelli di contratto e le clausole contrattuali tipo che dovranno essere utilizzati per disciplinare i rapporti tra la Provincia autonoma di Bolzano, in qualità di titolare del trattamento dei dati e altre persone giuridiche, in qualità di responsabili esterni, ai sensi dell'art. 28 del Regolamento.

Parallel dazu überarbeitet das Organisationsamt das Dekret des Landeshauptmanns Nr. 21/1994, um innerhalb der Landesverwaltung den einzelnen Akteuren die Pflichten und Verantwortungen zuzuteilen, die sie zur Umsetzung des neuen europäischen Rechtsrahmens übernehmen müssen.

In parallelo, l'ufficio Organizzazione sta procedendo alla riscrittura del decreto del Presidente della Giunta provinciale 21/1994, per ripartire, all'interno dell'Amministrazione provinciale, gli obblighi e le responsabilità fra i singoli attori chiamati ad attuare il nuovo quadro giuridico europeo.

2. In seiner Eigenschaft als Rechtsinhaber der Datenverarbeitung muss das Land die eigene Datenschutzpolitik überprüfen, um zu klären, welche Daten aufbewahrt werden und zu welchem Zweck und aufgrund welcher normativen Grundlage.

2. In qualità di titolare del trattamento dei dati, la Provincia deve riconsiderare la propria politica in materia di protezione dei dati per individuare chiaramente quali dati conservare, per quali finalità e su quale base giuridica.

In diesem Zusammenhang sieht Art. 30 der Grundverordnung vor, dass jeder Rechtsinhaber ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen muss.

A questo riguardo l'art. 30 del regolamento europeo prevede l'obbligo per ciascun titolare del trattamento di tenere un registro delle attività di trattamento svolte sotto la propria responsabilità.

Zu diesem Zweck wurde zwischen dem

A tal fine è stato concordato, tra il Direttore

Generaldirektor und dem Direktor der Abteilung Informationstechnik vereinbart, die derzeit vom Land für die Erstellung des Sicherheitsplans benutzte IT-Anwendung zur Verwaltung der Verarbeitungen – sie trägt die Bezeichnung „AXAM“ – den neuen Bestimmungen anzupassen, was sowohl formale als auch substanzielle Änderungen des Programms mit sich bringt. Durch die formalen Änderungen werden einige Felder umbenannt und weitere Informationen hinzugefügt, die bisher nicht erforderlich waren. Durch die substanziellen Änderungen werden etwaige neue Informationen zu den Verarbeitungen mit einer neuen Methodik der Risikoanalyse verknüpft. Diese beschränkt sich nicht ausschließlich auf das informationstechnische Risiko, dem die Daten ausgesetzt sind, sondern berücksichtigt auch die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen (Verarbeitungsrisiko). Zu einem späteren Zeitpunkt wird es möglich sein, alle Daten, die in AXAM gespeichert sind, auf eine neue Plattform zu übertragen, mit der die Verwaltung und die Steuerung der Datenverarbeitungsvorgänge vereinfacht und es dem Land ermöglicht wird, bei Kontrollen der Datenschutzbehörde die Erfüllung der von der Verordnung auferlegten Pflichten nachzuweisen.

3. Die Abteilung Informationstechnik legt mit Hilfe der In-House-Gesellschaft Südtiroler Informatik AG die geeigneten technischen und organisatorischen Sicherheitsmaßnahmen fest, die gemäß Art. 32 der Grundverordnung zu ergreifen sind; diese umfassen die Pseudonymisierung und Verschlüsselung der Daten, die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (zum Beispiel mit einem Disaster Recovery Plan), die Fähigkeit, die Verfügbarkeit der Daten und den Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (z. B. mittels *Back Up*), sowie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der

generale e il direttore della Ripartizione Informatica, l'adattamento - secondo la nuova normativa - dell'applicativo di gestione dei trattamenti, denominato "AXAM", attualmente in uso presso la Provincia (ex Documento Programmatico di Sicurezza -DPS); ciò comporterà modifiche al programma, sia di tipo formale che sostanziale. Le modifiche di tipo formale comporteranno la modifica delle denominazioni di alcuni campi e l'integrazione di ulteriori informazioni, finora non richieste. Le modifiche di tipo sostanziale, invece, andranno ad associare le eventuali nuove informazioni sui trattamenti a una nuova metodologia di analisi di rischio che non tiene esclusivamente conto del rischio di natura informatica sui dati, ma considera anche il rischio di varia gravità e probabilità per i diritti e le libertà delle persone fisiche (rischio connesso al trattamento).

In una successiva fase sarà possibile migrare tutti i dati presenti nell'applicativo AXAM su una nuova piattaforma tecnologica che, facilitando la gestione e la governance dei processi relativi al trattamento dei dati, agevolerà la Provincia nel dimostrare, in caso di controllo da parte dell'Autorità garante per la protezione dei dati, il rispetto degli obblighi sanciti nel Regolamento.

3. La Ripartizione Informatica, con l'ausilio della società *in house* Alto Adige Informatica Spa, sta definendo adeguate misure tecniche e organizzative di sicurezza da adottare ai sensi dell'art. 32 del Regolamento; esse comprendono la pseudonimizzazione e la cifratura dei dati, la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (ad. esempio mediante un piano di Disaster Recovery), la capacità di ripristinare tempestivamente la disponibilità dei dati e l'accesso agli stessi in caso di incidente fisico o tecnico (ad esempio mediante *back up*), nonché una procedura per testare l'efficacia delle misure adottate (*audit*).

getroffenen Maßnahmen (*Audit*).

4. Die Abteilung Informationstechnik legt mit Hilfe der In-House-Gesellschaft Südtiroler Informatik AG auch die Mindestmaßnahmen sowie weitere angemessene Maßnahmen zum Schutz der informationstechnischen Systeme des Landes fest (Siehe Rundschreiben der „Agenzia per l'Italia digitale“ vom 18. April 2017, Nr. 2 „Misure minime di sicurezza a contrasto della cybersecurity“); mit diesen Maßnahmen soll ein Sicherheitsniveau gewährleistet werden, das geeignet ist, etwaige Sicherheitszwischenfälle, die zu Verletzungen des Schutzes personenbezogener Daten führen können, zu vermeiden und zu verringern, oder, sollten sie sich trotzdem ereignen, in den gesetzlich vorgesehenen Fällen der Datenschutzbehörde zu melden und die betroffenen Personen zu benachrichtigen.

5. Bis 24. Mai 2018 muss die Autonome Provinz Bozen einen Datenschutzbeauftragten/eine Datenschutzbeauftragte laut Art. 37 ff. der Grundverordnung ernennen und dessen/deren Namen der Datenschutzbehörde melden.

6. Ein wesentlicher Teil des Anpassungsprozesses besteht darin sicherzustellen, dass sich die Führungskräfte und deren Mitarbeiterinnen und Mitarbeiter an den einzelnen Verfahrensschritten beteiligen und ihren Beitrag dazu leisten und dass sie regelmäßig über den Stand der Dinge informiert und im Hinblick auf Änderungen in der Datenschutzpolitik des Landes zu Rate gezogen werden. Zu diesem Zweck sind im Laufe der nächsten zwei Jahre Schulungen geplant, durch die das Bewusstsein für die neuen EU-Vorschriften geschärft und Aufklärungsarbeit geleistet werden soll.

All dies vorausgeschickt,

b e s c h l i e ß t

die Landesregierung einstimmig in gesetzmäßiger Weise,

4. La Ripartizione Informatica, con l'ausilio della società *in house* Alto Adige Informatica Spa, sta altresì individuando le misure minime e altre misure adeguate per la sicurezza dei sistemi informatici provinciali (vedasi circolare dell'Agenzia per l'Italia digitale del 18 aprile 2017, n. 2 “Misure minime di sicurezza a contrasto della cybersecurity”); dette misure devono garantire un livello di protezione adeguato in grado di prevenire e ridurre eventuali incidenti di sicurezza che potrebbero comportare la violazione dei dati; consentendo così, nei casi previsti dalla normativa, la notificazione all'Autorità garante, e se dovuta, agli interessati.

5. Entro il 24 maggio 2018 è obbligatoria la nomina di un/una responsabile della protezione dei dati (RPD) da parte della Provincia autonoma di Bolzano ai sensi degli artt. 37 e segg. del Regolamento; il suo nominativo deve essere altresì comunicato all'Autorità garante per la protezione dei dati nazionale.

6. Un elemento essenziale del processo di adeguamento di cui sopra è garantire il personale dirigente e i relativi collaboratori partecipino a tali attività, forniscano il loro contributo e siano periodicamente aggiornati e consultati in merito alle modifiche della politica provinciale in materia di protezione dei dati. A tale fine saranno programmate nell'arco dei prossimi due anni giornate di formazione allo scopo di sensibilizzare e istruire in merito ai nuovi obblighi prescritti dalla nuova normativa UE.

Tutto ciò premesso, la Giunta provinciale, a voti unanimi legalmente espressi,

d e l i b e r a

die beiliegende Planung der IT-Sicherheitsmaßnahmen ausgerichtet an die EU-Datenschutzgrundverordnung Nr. 2016/679 für die Jahre 2018-2020, welche integrierender Bestandteil dieses Beschlusses ist, zu genehmigen.

di approvare l'allegata Pianificazione delle attività di sicurezza IT orientate al Regolamento europeo sulla protezione dei dati n. 2016/679 relativa agli anni 2018-2020, costituente parte integrante della presente deliberazione.



Planung Maßnahmen IT Sicherheit, ausgerichtet am DSGVO

1)

Verzeichnis der Verarbeitung von Daten, einschließlich der Erhebung der Verarbeitungen, der Erhebung der IT-Infrastrukturen und der anzuwendenden Sicherheitsmaßnahmen.

Folgende Maßnahmen sind für die Erreichung des Zieles notwendig:

a) Tool für das Verzeichnis der Verarbeitungen

Zur Verfügungstellung auf einer IT-Plattform der Werkzeuge zur Unterstützung der Erstellung des Verzeichnisses der Verarbeitungen und der Beurteilung der Folgen auf den Schutz der Daten.

Die derzeit verwendete Plattform AXAM wird angepasst, um die Korrektur und Vervollständigung der Informationen durch die Organisationseinheiten der Landesverwaltung zu erlauben.

In Folge wird eine neue IT Plattform zur Verfügung gestellt, auf die derzeit in AXAM erfassten Daten migriert werden und mit der eine einfachere und vollständigere Beurteilung der Auswirkungen und Risikoanalyse möglich ist.

Beteiligte: Lieferanten, Abteilung Informationstechnik, Organisationsamt, SIAG

Beginn: 01.05.2018

Ende: 31.12.2018

b) Mapping zwischen Verarbeitungen und Anwendungen

Jede Verarbeitung, die mittels IT-Instrumenten erfolgt, muss mit den spezifischen IT-Systemen, wie spezielle Anwendungen oder Datenträger, in Zusammenhang gestellt werden.

Pianificazione Attività IT orientati al RGPD

1)

Registro delle attività di trattamento che comprende il censimento dei trattamenti, il censimento delle infrastrutture informatiche e le misure di sicurezza da adottare.

Per raggiungere l'obiettivo sono necessarie le seguenti attività:

a) Tool per registro dei trattamenti

Predisposizione su piattaforma informatica degli strumenti a supporto della redazione del registro delle attività di trattamento e delle valutazioni di impatto sulla protezione dei dati.

Verrà adeguata la piattaforma ad oggi in uso AXAM, per consentire la correzione e l'integrazione di informazioni da parte delle unità organizzative provinciali.

Successivamente sarà messa a disposizione una nuova piattaforma informatica verso la quale saranno migrati i dati presenti in AXAM e che permetterà una più agevole e completa valutazione di impatto e analisi di rischio.

Coinvolti: Fornitori, Ripartizione Informatica, ufficio Organizzazione, SIAG

Inizio: 01/05/2018

Fine: 31/12/2018

b) Mapping tra Trattamenti e Applicativi

Ogni trattamento svolto in modo informatizzato deve essere correlato con i sistemi informatici specifici a supporto, come software dedicati o supporti di memoria.



Beteiligte: Demand Manager Abteilung Informationstechnik, Organisationseinheiten der Landesverwaltung, Service Area Manager SIAG
 Beginn: 01.05.2018
 Ende: 31.12.2018

Coinvolti: Demand manager Ripartizione Informatica, U.O. della Provincia, Service Area Manager SIAG

Inizio: 01/05/2018
 Fine: 31/12/2018

c) Mapping zwischen Anwendungen, IT-Systemen und Sicherheitsmaßnahmen

Nach Erhebung der Zusammenhänge zwischen den Verarbeitungen und IT-Systemen, müssen die angemessenen Sicherheitsmaßnahmen für jede einzelne Verarbeitung herausgearbeitet werden.

Beteiligte: SIAG
 Beginn: 01.05.2018
 Ende: 31.12.2018

c) Mapping tra Applicativi, Sistemi informatici e Misure di sicurezza

A seguito della correlazione tra trattamenti e sistemi informatici occorre individuare le misure di sicurezza adeguate per ogni singolo trattamento.

Coinvolti: SIAG
 Inizio: 01/05/2018
 Fine: 31/12/2018

d) Data Protection Impact Analysis (DPIA)

Überwachung und zentrale Koordinierung für die Beurteilung der Auswirkungen auf den Datenschutz und der damit verbundenen Risikoanalyse. Die Maßnahme ist für die bereits aktiven Verarbeitungen notwendig; in Folge muss sie vor Aktivierung einer neuen Verarbeitung erfolgen.

Beteiligte: Verantwortlicher für den Datenschutz, Abteilung Informationstechnik, Abteilungen/OE der Landesverwaltung
 Beginn: 01.06.2018
 Ende: 31.12.2018

d) Data Protection Impact Analysis (DPIA)

Supervisione e coordinamento centrale per la valutazione di impatto sulla protezione dei dati e analisi di rischio correlato. L'attività è necessaria per i trattamenti già in essere; successivamente dovrà essere svolta prima di iniziare un nuovo trattamento.

Coinvolti: Responsabile per la protezione dei dati, Ripartizione Informatica, Ripartizioni/U.O. della Provincia

Inizio: 01/06/2018
 Fine: 31/12/2018

e) Data retention

i) Vorgaben des Inhabers – Festlegung der Aufbewahrungsfristen der personenbezogenen Daten seitens des Dateninhabers

Beteiligte: Organisationseinheiten der Landesverwaltung mit Unterstützung eines Beraters
 Beginn: 01.09.2018
 Ende: 30.06.2019

ii) Verwaltung – Vorbereitung der organisatorischen Abläufe und Technologien für eine entsprechende Verwaltung der Daten

Beteiligte: SIAG
 Beginn: 01.09.2018
 Ende: 30.06.2019

e) Data retention

i) Requisiti del titolare - Individuazione dei tempi di conservazione dei dati personali da parte del titolare dei dati

Coinvolti: unità organizzative della Provincia con supporto consulente

Inizio: 01/09/2018
 Fine: 30/06/2019

ii) Gestione data retention - predisposizione delle procedure organizzative e tecnologiche per una conseguente gestione dei dati

Coinvolti: SIAG
 Inizio: 01/09/2018
 Fine: 30/06/2019



2) Infrastrukturelle und technologische Anpassung zur Anhebung des Sicherheitsniveaus in Entsprechung der Datenschutzvorgaben

Folgende Maßnahmen sind für die Erreichung des Zieles notwendig:

a) GAP-analysis

Bewertung der Angemessenheit der Infrastruktur und der Technologie in Bezug auf die Vorgaben, die sich aus der Beurteilung des Datenschutzrisikos der sogenannten Gap Analysis ergeben. In Folge werden die Prioritäten der Anpassungsmaßnahmen an die neuen Vorgaben definiert. Diese Tätigkeit erfolgt periodisch, um eventuelle neue Schwachstellen der Systeme zu analysieren.

Beteiligte: SIAG

Beginn: 01.06.2018

Ende: 31.09.2018

b) SIEM (Security Information and Event Management)

Aktivierung eines Monitorings zur Überwachung aller Ereignisse, die Auswirkung auf die IT-Sicherheit haben; dies erlaubt die zeitgerechte Handhabung eventueller Sicherheitsunfälle zur Erkennung und Notifizierung von Data Breach.

Beteiligte: SIAG

Beginn: 01.06.2018

Ende: -

c) ICT Risk Assessment

Aktivierung des Prozesses ICT Risk Assessment zur Beurteilung der IT Risiken und zur Ausfindigmachung von Gegenmaßnahmen zur Reduzierung des Risikos und zur Gewährleistung der Kontinuität des Geschäftsbetriebs.

Beteiligte: SIAG

Beginn: 01.06.2018

Ende: -

d) Schulung Privacy

Weiterbildung aller Mitarbeiter der Landesverwaltung in Bezug auf die neue europäische Verordnung DSGVO und der IT-Sicherheit.

Beteiligte: Amt für Personalentwicklung

Beginn: 01.11.2018

2) Adeguamento infrastrutturale e tecnologico per innalzamento del livello di sicurezza, che sia adeguato a requisiti privacy

Per raggiungere l'obiettivo sono necessarie le seguenti attività:

a) GAP-analysis

Valutazione di adeguatezza infrastrutturale e tecnologica rispetto ai requisiti risultanti dalla valutazione del rischio privacy, cosiddetta Gap Analysis per definire le priorità di intervento per l'adeguamento ai nuovi requisiti. Questa attività viene ripetuta periodicamente per analizzare eventuali nuove vulnerabilità dei sistemi.

Coinvolti: SIAG

Inizio: 01/06/2018

Fine: 31/09/2018

b) SIEM (Security Information and Event Management)

Introduzione di un servizio per il monitoraggio di tutti gli eventi che hanno impatto sulla sicurezza informatica; permette di gestire tempestivamente eventuali incidenti di sicurezza per l'individuazione e la notifica di Data Breach.

Coinvolti: SIAG

Inizio: 01/06/2018

Fine: -

c) ICT Risk Assessment

Attivazione del processo di ICT Risk Assessment per la valutazione dei rischi informatici e l'individuazione delle contromisure informatiche da adottare per ridurre il rischio e garantire la continuità operativa informatica.

Coinvolti: SIAG

Inizio: 01/06/2018

Fine: -

d) Formazione privacy

Formazione continua verso tutti i collaboratori della Provincia sul nuovo Regolamento europeo per la protezione dei dati (RGPD) e sulla sicurezza informatica.

Coinvolti: Ufficio Sviluppo personale

Inizio: 01/11/2018



Ende: -

e) Anpassung IT Systeme

Technologische Anpassung und Weiterentwicklung der IT Infrastruktur (z.B.: Betriebssysteme von Clients und Servern, Antivirus und Antispam neuer Generation, Plattformen für ICT-Netzwerksicherheit)

Beteiligte: SIAG

Beginn: 01.01.2019

Ende: 31.12.2020

f) Disaster Recovery

Das europäische Projekt FESR2186-P sieht den Ausbau des Datacenters der Landesverwaltung in den von der Sanitätseinheit zur Verfügung gestellten Räumen im Krankenhaus Bruneck vor. Dieses Data Center wird von allen öffentlichen Verwaltungen in Südtirol als Business Continuity und Disaster Recovery Data Center genutzt werden, mit dem Ziel die Qualität und Zuverlässigkeit der an Körperschaften ausgeschütteten Dienste zu erhöhen.

Beteiligte: Südtiroler Sanitätsbetrieb, SIAG

Beginn: 01.07.2017

Ende: 30.06.2019

Bozen, 17. April 2018

Fine: -

e) Adeguamento sistemi informatici

Adeguamento tecnologico ed evoluzione dell'infrastruttura informatica (ad es.: sistemi operativi Client e Server, antivirus e antispam di nuova generazione, piattaforme di sicurezza di rete ICT).

Coinvolti: SIAG

Inizio: 01/01/2019

Fine: 31/12/2020

f) Disaster Recovery

Il progetto europeo FESR2186-P prevede l'estensione del Data Center Provinciale presso i locali messi a disposizione da Azienda Sanitaria nell'ospedale di Brunico. Tale Data Center sarà utilizzato da tutti gli enti pubblici sul territorio provinciale quale Data Center di Business Continuity e Disaster Recovery, con l'obiettivo di aumentare la qualità e affidabilità dei servizi erogati agli enti.

Coinvolti: Azienda sanitaria, SIAG

Inizio: 01/07/2017

Fine: 30/06/2019

Bolzano, 17 aprile 2018

Sichtvermerke i. S. d. Art. 13 L.G. 17/93
über die fachliche, verwaltungsgemäße
und buchhalterische Verantwortung

Visti ai sensi dell'art. 13 L.P. 17/93
sulla responsabilità tecnica,
amministrativa e contabile

Der Amtsdirektor 19/04/2018 10:45:48 Il Direttore d'ufficio
NOGLER PATRIZIA

Der Generaldirektor 19/04/2018 11:45:15 Il Direttore generale
STAFFLER HANSPETER

Laufendes Haushaltsjahr

Esercizio corrente

La presente delibera non dà luogo a
impegno di spesa.
Dieser Beschluss beinhaltet keine
Zweckbindung

zweckgebunden

impegnato

als Einnahmen
ermittelt

accertato
in entrata

auf Kapitel

sul capitolo

Vorgang

operazione

Der Direktor des Amtes für Ausgaben 19/04/2018 15:58:56 Il direttore dell'Ufficio spese
CELI DANIELE

Der Direktor des Amtes für Einnahmen Il direttore dell'Ufficio entrate

Diese Abschrift
entspricht dem Original

Per copia
conforme all'originale

Datum / Unterschrift

data / firma

Abschrift ausgestellt für

Copia rilasciata a



Der Landeshauptmann
Il Presidente

KOMPATSCHER ARNO

24/04/2018

Der Generalsekretär
Il Segretario Generale

MAGNAGO EROS

24/04/2018

Es wird bestätigt, dass diese analoge Ausfertigung, bestehend - ohne diese Seite - aus 16 Seiten, mit dem digitalen Original identisch ist, das die Landesverwaltung nach den geltenden Bestimmungen erstellt, aufbewahrt, und mit digitalen Unterschriften versehen hat, deren Zertifikate auf folgende Personen lauten:

nome e cognome: Arno Kompatscher

Si attesta che la presente copia analogica è conforme in tutte le sue parti al documento informatico originale da cui è tratta, costituito da 16 pagine, esclusa la presente. Il documento originale, predisposto e conservato a norma di legge presso l'Amministrazione provinciale, è stato sottoscritto con firme digitali, i cui certificati sono intestati a:

nome e cognome: Eros Magnago

Die Landesverwaltung hat bei der Entgegennahme des digitalen Dokuments die Gültigkeit der Zertifikate überprüft und sie im Sinne der geltenden Bestimmungen aufbewahrt.

Ausstellungsdatum

24/04/2018

Diese Ausfertigung entspricht dem Original

L'Amministrazione provinciale ha verificato in sede di acquisizione del documento digitale la validità dei certificati qualificati di sottoscrizione e li ha conservati a norma di legge.

Data di emanazione

Per copia conforme all'originale

Datum/Unterschrift

Data/firma