Deliberazione della Giunta Regionale 28 settembre 2018, n. 1-7574
Adempimenti in attuazione al Regolamento UE 2016/679. Designazione degli incaricati e istruzioni opertive. Disposizioni procedurali in materia di incidenti di sicurezza e di violazione di dati personali (Data Breach), adozione del relativo registro e modello di informativa.

A relazione del Presidente Chiamparino:

Premesso che:

- il 18 maggio 2018 è stata approvata la DGR n. 1-6847 avente ad oggetto "Adempimenti in attuazione del Regolamento (UE) 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). Revoca DGR n. 1-11491 del 3.06.2009";
- per adempiere al Regolamento UE sono necessari provvedimenti specifici richiamati solo in via essenziale nella DGR di cui sopra;
- il d.lgs. n.196/2003 capo IV, art. 2 quaterdecies, come modificato dal d.lgs. 101/2018 stabilisce che "il titolare del trattamento può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate che operano sotto la propria autorità e che il titolare del trattamento individua le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta";
- il Titolare, pertanto, ritiene di designare tutti i dipendenti della Regione Piemonte, nonché tutti i soggetti dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa, di cui all'art. 13 della l.r. n. 23/2008, come incaricati del trattamento dei dati personali effettuato nello svolgimento delle proprie funzioni in riferimento alla declaratoria delle competenze delle Strutture di appartenenza e nelle funzioni di supporto agli organi di direzione politico-amministrativa;
- il Titolare, valutata la rilevanza di quanto sopra espresso, ritiene opportuno predisporre istruzioni operative (Allegato 1) da diffondere a tutti i soggetti sopra richiamati.

Valutata, altresì, la necessità di dettare precise disposizioni procedurali (Allegato 2) in caso di incidenti di sicurezza e di violazioni di dati personali (Data Breach), in attuazione dell'art. 33 del Regolamento UE 2016/679, utilizzando il diagramma di flusso con i requisiti della notifica tratto dalle linee guida WP29 (Gruppo di lavoro istituito in virtù dell'art. n. 29 della Direttiva 95/45/CE) e di adottare il relativo registro delle violazioni al fine di consentire all'autorità di controllo di verificare il rispetto della norma, nonché di definire le responsabilità dei diversi soggetti coinvolti nel processo di Data Breach qualora la violazione impatti su risorse informatiche o analogiche oppure su entrambe attraverso la matrice RACI (Standard di matrice per l'individuazione di ruoli e responsabilità dei soggetti coinvolti).

Valutata la necessità di diffondere alle strutture regionali un modello di informativa da adottare nel caso di raccolta di dati personali dei soggetti interessati (Art. 13 Regolamento UE 2016/679) (Allegato 3).

Acquisito, altresì, il parere del responsabile della protezione dati (DPO);

visto il Regolamento generale sulla protezione dei dati 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;

visto il d.lgs. n. 196 del 30 giugno 2003 come modificato dal d.lgs. n. 101 del 10 agosto 2018;

vista la legge regionale n. 23 del 28 luglio 2008;

vista la d.g.r. n. 1- 6847 del 18.05.2018.

Dato atto che la presente deliberazione non comporta oneri a carico del bilancio regionale;

attestata la regolarità amministrativa del presente provvedimento ai sensi della dgr n. 1-4046 del 17.10.2016;

tutto quanto premesso e considerato, la Giunta regionale, a voti unanimi resi nelle forme di legge,

delibera

- di designare tutti i dipendenti della Regione Piemonte, nonché tutti i soggetti dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa, di cui all'art. 13 della l.r. n. 23/2008, come incaricati del trattamento dei dati personali effettuato nello svolgimento delle proprie funzioni in riferimento alla declaratoria delle competenze delle Strutture di appartenenza e nelle funzioni di supporto agli organi di direzione politico-amministrativa;

- di adottare dettagliate istruzioni operative, allegate alla presente deliberazione per farne parte integrante e sostanziale (Allegato 1), che verranno pubblicate sulla intranet aziendale e diffuse a tutti gli incaricati del trattamento mediante comunicazione personalizzata tramite il cedolino del primo mese utile attraverso l'apposita procedura telematica;

- di adottare le disposizioni procedurali, allegate alla presente deliberazione per farne parte integrante e sostanziale (Allegato 2), in caso di incidenti di sicurezza e di violazioni di dati personali (Data Breach), in attuazione dell'art.33 del Regolamento UE 2016/679, utilizzando il diagramma di flusso con i requisiti della notifica tratto dalle linee guida WP29 e di adottare il relativo registro delle violazioni al fine di consentire all'autorità di controllo di verificare il rispetto della norma, nonché di definire le responsabilità dei diversi soggetti coinvolti nel processo di Data Breach qualora la violazione impatti su risorse informatiche o analogiche oppure su entrambe attraverso la matrice RACI;

- di diffondere alle strutture regionali un modello di informativa da adottare nel caso di raccolta di dati personali dei soggetti interessati (Art. 13 Regolamento UE 2016/679) (Allegato 3);

- di dare atto che la presente deliberazione non comporta oneri a carico del bilancio regionale.

La presente deliberazione sarà pubblicata sul B.U. della Regione Piemonte ai sensi dell'art. 61 dello Statuto e dell'art. 5 della L.R. 22/2010 nonché nella Sezione Amministrazione Trasparente del Sito Internet dell'Ente ai sensi dell'articolo 18 del d.lgs. 33/2013.

(omissis)

Allegato

Allegato 1

ISTRUZIONI OPERATIVE PER L'ATTUAZIONE DEL REGOLAMENTO (UE) 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi della deliberazione della Giunta regionale n. 1-6847 del 18 maggio 2018 ha individuato tutti i dipendenti della Regione Piemonte, nonché tutti i soggetti dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa, come incaricati del trattamento dei dati effettuato nello svolgimento delle proprie funzioni.

Al fine di facilitare comportamenti corretti, è innanzitutto necessario condividere il significato di alcuni termini connessi al trattamento dei dati personali. Di seguito un breve glossario di quelli più utili:

trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

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

dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

Nell'ambito dell'attività lavorativa, il dipendente deve assicurarsi che i dati personali siano:

a) **trattati** in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) **raccolti** per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);
c) **adeguati, pertinenti e limitati** a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) **esatti** e, se necessario, **aggiornati**; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) **conservati** in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di

misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) **elaborati** in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (integrità e riservatezza).

Chiunque abbia accesso, nel ruolo di dipendente della Direzione/Settore/Struttura speciale/Struttura flessibile/ Ufficio di Comunicazione, a banche dati cartacee e informatiche gestite dalla Struttura di appartenenza, nell'ambito dello svolgimento delle proprie mansioni, deve eseguire tutte le operazioni di trattamento di dati personali**,** necessarie e opportune al corretto adempimento delle sue mansioni, nel rispetto del principio di liceità del trattamento.

Custodia degli strumenti di lavoro

Gli strumenti di lavoro messi a disposizione dalla Regione sono finalizzati all'uso professionale e destinati all'adempimento delle mansioni assegnate ed è responsabilità dei singoli assegnatari custodirli in modo appropriato e diligente al fine di evitare, per quanto possibile, il furto, l'appropriazione o anche solo l'utilizzo da parte di terzi non autorizzati. E' indispensabile segnalare prontamente alla struttura competente il danneggiamento, lo smarrimento o il furto di tali strumenti (si segnala la DGR 2-12269 del 5 ottobre 2009 "*Disciplinare per l'utilizzo di personal computer, dispositivi elettronici aziendali, posta elettronica e internet*").

E' altresì doveroso salvaguardare l'integrità e la sicurezza dei dati e dei documenti trattati o comunque accessibili attraverso gli strumenti di cui sopra, prestando la massima attenzione per le informazioni a carattere riservato e particolare.

In particolare è vietato memorizzare sui dischi interni delle postazioni di lavoro o dei dispositivi mobili documenti/report (nei vari formati es ODT, WORD, ODS, EXCEL, ODP, POWER-POINT, PDF, JPG etc) contenenti dati personali e/o particolari afferenti alle attività di trattamento svolte.

Dispositivi mobili

Particolare attenzione va posta verso i dispositivi mobili, per loro natura estremamente vulnerabili, che sono veri e propri punti di accesso al Sistema Informativo; è fondamentale proteggerne l'accesso mediante gli strumenti messi a disposizione dal loro sistema operativo, cambiando regolarmente i codici.

Memorizzazione dei dati

Gli incaricati del trattamento devono sempre utilizzare, per la memorizzazione, gli appositi share messi a disposizione da Regione (abilitati ai soli incaricati necessari) o i relativi database previsti dal progetto. In caso di necessità (anche solo temporanea) di mantenere per i fini di lavorazione una copia delle informazioni off-line (sul disco interno delle postazioni di lavoro), la copia locale deve essere cifrata (es. tramite funzioni di cifratura delle applicazioni) ed eliminata al termine della lavorazione.

E' buona regola la periodica pulizia degli spazi di memorizzazione delle unità di rete, dell'hard-disk della propria postazione di lavoro e della casella di posta, con cancellazione di file ed e-mail obsoleti e inutili contenenti dati personali, ed evitando la duplicazione dei dati memorizzati. La medesima attenzione dovrà essere riservata ai documenti cartacei contenenti dati personali che, per quanto possibile, non devono essere lasciati sulla scrivania, ma riposti, quando non utilizzati e comunque al termine dell'attività lavorativa, negli appositi archivi correnti come da misure di sicurezza.

Comportamento in caso di violazione della sicurezza

La “violazione” è definita all’art. 4 par. 12 GDPR come *“la violazione di sicurezza che comporta accidentalmente in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati”* (Data Breach).

Non appena viene a conoscenza di una violazione di dati personali, al momento del verificarsi del fatto o della sua scoperta, il dipendente deve attivare apposita procedura di segnalazione, che prevede l’immediata comunicazione scritta e inviata con posta elettronica:

- sia al delegato al trattamento dati (Direttore per i dipendenti in staff; Dirigente per i dipendenti nei Settori/Strutture temporanee o di progetto) o, in sua assenza, al Vicario quando individuato (indirizzando la segnalazione sia alla casella di posta elettronica personale del Direttore o Dirigente di riferimento sia a quella di Direzione/Settore/Struttura, se esistente);
- sia al referente privacy di Direzione.

Ai dipendenti delle strutture di supporto agli organi di direzione politico-amministrativa, di cui all’art. 13 della l.r. 23/2008, comportano i medesimi obblighi.

Esempi, a puro titolo esemplificativo, di eventi che possono comportare un *data breach*:

- pubblicazione dell’atto nella sua interezza senza omissione di dati personali/particolari;
- inoltro di messaggi contenenti dati personali/particolari a soggetti non interessati al trattamento;
- abbandono della postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, disattivare le procedure sulla risorsa informatica utilizzata, ecc..) e vi è evidenza che terzi abbiano avuto accesso alle informazion;
- perdita della chiave di decriptazione di dati crittografati in modo sicuro(*se l’unica copia a disposizione)* ;
- cancellazione dei dati in modo accidentale o da parte di soggetti non autorizzati (senza possibilità di recupero);
- *data exfiltration* (copia o trasferimento non autorizzati di dati);
- *ransomware/malware*;
- distruzione accidentale di uno spazio di memorizzazione;
- smarrimento, furto di PC o server;
- smarrimento, furto di dispositivo mobile (smartphone, USB KEY, CD/DVD HD, etc.);
- smarrimento, furto o distruzione accidentale di documenti o aggregazioni documentali negli archivi cartacei (correnti o di deposito).

Allegato 2

DISPOSIZIONI PROCEDURALI IN MATERIA DI INCIDENTI DI SICUREZZA E DI VIOLAZIONI DEI DATI PERSONALI ED ADOZIONE DEL RELATIVO REGISTRO (DATA BREACH ART. 33 REGOLAMENTO UE 2016/679 (GDPR) E MATRICE RACI.

GLOSSARIO

Ai fini del seguente provvedimento si intende per:

- **GDPR**- Regolamento Europeo in materia di protezione dei dati personali nonché della libera circolazione di tali dati che abroga la direttiva 95/46/CE sulla stessa materia. Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04/05/2016, entrato in vigore il 24/05/2016 e diventerà definitivamente applicabile in via diretta in tutti i paesi UE a partire dal 25/05/2018. L'acronimo GDPR si riferisce al termine anglosassone "*General Data Protection Regulation*" mentre l'acronimo RGPD si riferisce alla definizione nazionale "Regolamento Generale sulla Protezione dei Dati".
- **Codice** - D.Lgs 30 giugno 2003, n. 196.
- **Garante** : Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente, il GDPR identifica questa figura denominandola "Autorità di controllo" (vedasi art.li n. 51 e successivi del GDPR).
- **Titolare :**Titolare del trattamento - l'autorità (Giunta regionale) che singolarmente o insieme ad altri determina finalità e mezzi del trattamento di dati personali.
- **Responsabile protezione dati (DPO);**
- **Delegato al trattamento:** Direttore o Dirigente delegato nell'ambito delle attività di loro competenza;
- **Responsabile esterno:** Responsabile del trattamento - soggetto pubblico o privato che tratta dati personali per conto del Titolare del trattamento.
- **Data Breach:** evento in conseguenza del quale si verifica una "**violazione dei dati personali**". Con il termine "data breach" si intende un incidente di sicurezza in cui i dati: personali, sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato. La casistica è molto estesa, un "data breach" si può anche verificare a seguito di un problema hardware o software o con una divulgazione di dati riservati o confidenziali all'interno di un ambiente privo di misure di sicurezze (da esempio, su web) in maniera involontaria o volontaria, con il furto di dati, ecc..
- **Accountability:** principio per cui il titolare deve dimostrare l'adozione di politiche in materia di privacy e di misure adeguate in conformità al GDPR.
- **Privacy by design:** principio dal quale discende l'attuazione di adeguate misure tecniche e organizzative sia all'atto della progettazione che dell'esecuzione del trattamento di dati personali.
- **Privacy by default:** principio dal quale discende l'attuazione di adeguate misure tecniche e organizzative volte a tutelare la vita privata per "impostazione predefinita" solo per i dati personali necessari per ogni specifica finalità del trattamento.

- **RACI:** standard di matrice per l'individuazione di ruoli e responsabilità dei soggetti coinvolti (RPD, Titolare/Delegato al trattamento, referente privacy,…) ai fini dell'esecuzione del processo di data breach impattante su risorse analogiche o informatiche o di entrambe.
- **WP29:** gruppo di lavoro istituito in virtù dell'art. n. 29 della direttiva 95/45/CE (gruppo di lavoro indipendente con funzioni consultive dell'UE nell'ambito dalla protezione dei dati personali e della vita privata).

FASI DEL PROCESSO DI "*DATA BREACH*"

Il Titolare/Delegato del trattamento (Direttori/Dirigenti), venuto a conoscenza dell'incidente, deve identificare e verificare se riguarda dati personali/particolari, se l'incidente ha coinvolto archivi o strutture digitali o analogiche e provvedere alle eventuali comunicazioni. In questa fase il Titolare/Delegato del trattamento avvisa tempestivamente il Responsabile della Protezione dati (DPO) che lo supporta nell'attuazione delle fasi del processo.

Per la gestione del processo di "*data breach*" il Titolare/Delegato al trattamento si avvale dei responsabili esterni, qualora coinvolti per le rispettive competenze, per le fasi di seguito indicate:

- **acquisizione** (rilevazione, comunicazione dell'evento al Titolare/Delegato al trattamento);
- **gestione tecnica** (analisi; raccolta informazioni; definizione dei soggetti coinvolti; accertamento dell'effettiva sussistenza del "*data breach*");
- **valutazione** (occorre valutare se l'incidente riguarda o meno un evento che non presenti rischi per i diritti delle persone fisiche se deve essere notificato al Garante, comunicato agli interessati a CERT-PA e/o alle forze dell'ordine);
- **notifica al Garante**;
- **segnalazioni** agli organi di Polizia e, nel caso di incidente informatico, a CERT-PA;
- **comunicazione agli interessati** e raccolta riscontri dell'avvenuta comunicazione;
- **registrazione della violazione** oppure degli eventi che non necessitano di notifica.

ACQUISIZIONE DELLA SEGNALAZIONE

La prima fase nella gestione del "*data breach*" è quella della rilevazione, comunicazione dell'evento al Titolare/Delegato al trattamento (Direttore/Dirigente).

Il "*data breach*" può essere segnalato:

- dagli addetti all'amministrazione dei sistemi informativi;
- da personale interno all'ente;
- da parte di organi pubblici (altri enti, Polizia, Carabinieri, Magistratura ecc.);
- da parte dei responsabili esterni che agiscono per conto della Giunta regionale;
- da parte di cittadini o, comunque, di soggetti privati esterni all'ente.

È importante che la raccolta delle segnalazioni da parte degli uffici avvenga indicando più informazioni possibili (identificazione dei segnalatori, data ed ora in cui la segnalazione è avvenuta, dati descrittivi sulla violazione segnalata ecc.).

E' opportuno che chi riceve la segnalazione provveda anche a raccogliere informazioni di contatto sui segnalatori (indirizzo di reperibilità, numeri telefonici, indirizzo di posta elettronica).

Anche le segnalazioni anonime e/o verbali devono essere raccolte ed inviate al Titolare/Delegato del trattamento per consentire a quest'ultimo di accertare la reale sussistenza della violazione e disporre l'eventuale notifica o le comunicazioni al fine di assumere i provvedimenti atti ad evitare l'aggravamento della situazione.

Se la segnalazione proviene da un responsabile esterno incaricato di eseguire un trattamento o parte di esso per conto dell'ente (obbligato in tal senso da quanto disposto dall'art. 33, paragrafo n. 2, del GDPR), da un altro organismo pubblico o da un servizio interno, occorre darne immediata comunicazione al Titolare/Delegato al trattamento.

1. Modello di informativa da rendere al segnalatore

Chi raccoglie la segnalazione dovrà inoltre fornire al segnalante un'informativa scritta circa le modalità e finalità con cui i dati conferiti saranno trattati (come da modello allegato).

2. Comunicazione al Titolare /Delegato al trattamento

Immediatamente dopo aver raccolto la segnalazione, è necessario inoltrarla al Titolare/Delegato al trattamento. La segnalazione deve essere eseguita in forma scritta, anche utilizzando mezzi elettronici, deve contenere i riferimenti temporali in cui viene raccolta, acquisita ed inoltrata e deve essere completa e dettagliata (ivi comprese le modalità in cui si è venuti a conoscenza della presunta violazione).

Qualora la violazione si verifichi presso responsabili esterni il GDPR, all'art. 33 paragrafo n. 2, prevede espressamente che il responsabile esterno debba informare, senza ingiustificato ritardo, il Titolare.

GESTIONE TECNICA

La gestione tecnica riguarda l'esecuzione di tutte quelle operazioni, accertamenti e verifiche tese a supportare la fase di valutazione.

La responsabilità del processo di valutazione e notifica all'interessato è in capo al Titolare/Delegato al trattamento che deve essere supportato dai referenti privacy delle Direzioni, dal Responsabile dei Sistemi informativi, dal Responsabile A.O.O. ed, eventualmente, dai responsabili esterni esecutori di trattamenti per conto della Giunta regionale.

In particolare nel caso di violazioni di natura informatica è fondamentale, ai fini dell'istruttoria, il coinvolgimento del Responsabile dei Sistemi informativi.

Nel caso di violazioni di natura analogica è fondamentale, ai fini dell'istruttoria, il coinvolgimento dei Delegati al trattamento e, nei casi applicabili, del Responsabile dell'archivio di deposito.

A questa fase partecipano tutti i Delegati del Titolare interessati alla violazione del trattamento di dati coinvolti.

Nella successiva fase di valutazione, il Titolare/Delegato al trattamento deve stabilire quali azioni intraprendere (semplice registrazione, notifica al garante, comunicazione agli interessati, segnalazione agli organi di polizia ed altre azioni mirate al contenimento della violazione).

Il Titolare/Delegato al trattamento deve essere in grado di valutare l'impatto rispetto ai dati personali, ai diritti ed alla libertà degli interessati; pertanto, le attività svolte in questa fase devono essere documentate (cioè devono essere riportate le violazioni, le circostanze, le conseguenze, i rimedi, ed eventualmente quanto posto preventivamente in essere per evitare il verificarsi della violazione), ferma restando la facoltà in capo al Garante ed allo stesso Titolare/Delegato al trattamento di richiedere approfondimenti.

1. Analisi approfondita rispetto alla identificazione della violazione ed alla individuazione della categoria di appartenenza fra quelle identificate dal WP29

- di riservatezza, quando si verifica una divulgazione o un accesso ai dati non autorizzato o accidentale;
- di integrità, quando si verifica un'alterazione di dati personali non autorizzata o accidentale;
- di disponibilità, ovvero quando si verifica la perdita, l'inaccessibilità o la distruzione accidentale o non autorizzata.

Nel modello di segnalazione reso disponibile sul sito dell'Autorità Garante, in allegato al provvedimento del 22 luglio 2015, sono richieste le seguenti informazioni da fornire:

- denominazione della/e banca/banche dati oggetto di Data Breach e breve descrizione della violazione dei dati personali ivi trattati;
- indicazioni temporali sulla violazione (quando si è verificata);
- indicazioni sul luogo della violazione;
- tipo di violazione, dispositivo oggetto della violazione;
- descrizione sintetica dei sistemi di elaborazione/memorizzazione coinvolti e loro ubicazione;
- numero degli interessati coinvolti, anche indicativo;
- tipologia dei dati oggetto di violazione;
- livello di gravità attribuito alla violazione;
- misure tecniche e organizzative applicate ai dati oggetto di violazione;
- se gli interessati hanno ricevuto comunicazione della violazione ed il contenuto della comunicazione resa;
- indicazioni sulle misure tecnologiche e organizzative che sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future.

È, altresì, opportuno che dalla valutazione emerga se sono coinvolte categorie di dati particolari.

Qualora il numero degli interessati o potenziali interessati dalla violazione sia ridotto e questi siano identificabili, è opportuno stilare degli elenchi da utilizzare nel caso in cui il Titolare/Delegato al trattamento ritenga necessario inviare loro delle comunicazioni personalizzate.

Si dovranno, altresì, identificare eventuali carenze dei sistemi di sicurezza, raccogliere tutti gli elementi necessari per la valutazione ed i dati indispensabili da inserire nella notifica al Garante e nel registro degli incidenti ed, eventualmente, da citare nella comunicazione agli interessati e/o alle forze dell'ordine.

2. Analisi supplementare

L'analisi supplementare viene attivata se sono necessarie informazioni aggiuntive ad un'analisi già eseguita, qualora:

- il Titolare/Delegato al trattamento ritenga necessario un approfondimento finalizzato, ad es. all'integrazione di una notifica al Garante;
- l'Autorità Garante, gli organi di polizia o la magistratura ritengano necessarie informazioni aggiuntive o approfondimenti di informazioni fornite;
- non sia stato possibile, durante una delle fasi del processo di gestione del "*data breach*", coinvolgere pienamente i responsabili esterni o le comunicazioni non siano pervenute in tempo utile.

L'analisi supplementare può essere attivata più volte per la stessa violazione.

VALUTAZIONE

La responsabilità di questa fase è in capo al Titolare/Delegato al trattamento che può avvalersi dei referenti privacy delle Direzioni, del Responsabile dei Sistemi informativi, del Responsabile A.O.O., del Responsabile dell'archivio di deposito ed, eventualmente, dei responsabili esterni esecutori di trattamenti per conto della Giunta regionale.

Al termine della fase di "gestione tecnica" sopra descritta, il Titolare/Delegato al trattamento deve avere tutti gli elementi per poter identificare l'incidente di sicurezza e comprendere in che modo l'incidente ha impatto sui dati, se tra le informazioni coinvolte vi sono semplici dati personali o se sono coinvolte anche categorie particolari di dati, quante persone possono essere coinvolte, se fra queste vi sono soggetti appartenenti a particolati categorie (es. minori) e quali rischi o danni per le libertà ed i diritti delle persone ha causato o potrebbe causare la violazione.

Il Titolare/Delegato al trattamento può, quindi, stabilire se è necessario od opportuno:

- notificare la violazione al Garante, in che modo eseguire la notifica (ad es. in più fasi); in particolare dovrà essere stabilito (motivandolo) se si ritiene probabile o improbabile che la violazione comporti rischi per i diritti e le libertà delle persone;
- comunicare la violazione agli interessati ed in che modo è possibile eseguire la comunicazione (art. 34 GDPR);
- comunicare la violazione agli organi di polizia;
- richiedere ulteriori verifiche tecniche necessarie per un'ulteriore comunicazione.

In ogni caso occorre registrare sul registro delle violazioni l'evento documentando la violazione dei dati personali, le circostanze ad essa relative, le sue conseguenze e le valutazioni eseguite: questo per consentire al Garante di verificare il rispetto della normativa (art. 33 del GDPR).

Per la valutazione occorre tenere presente che:

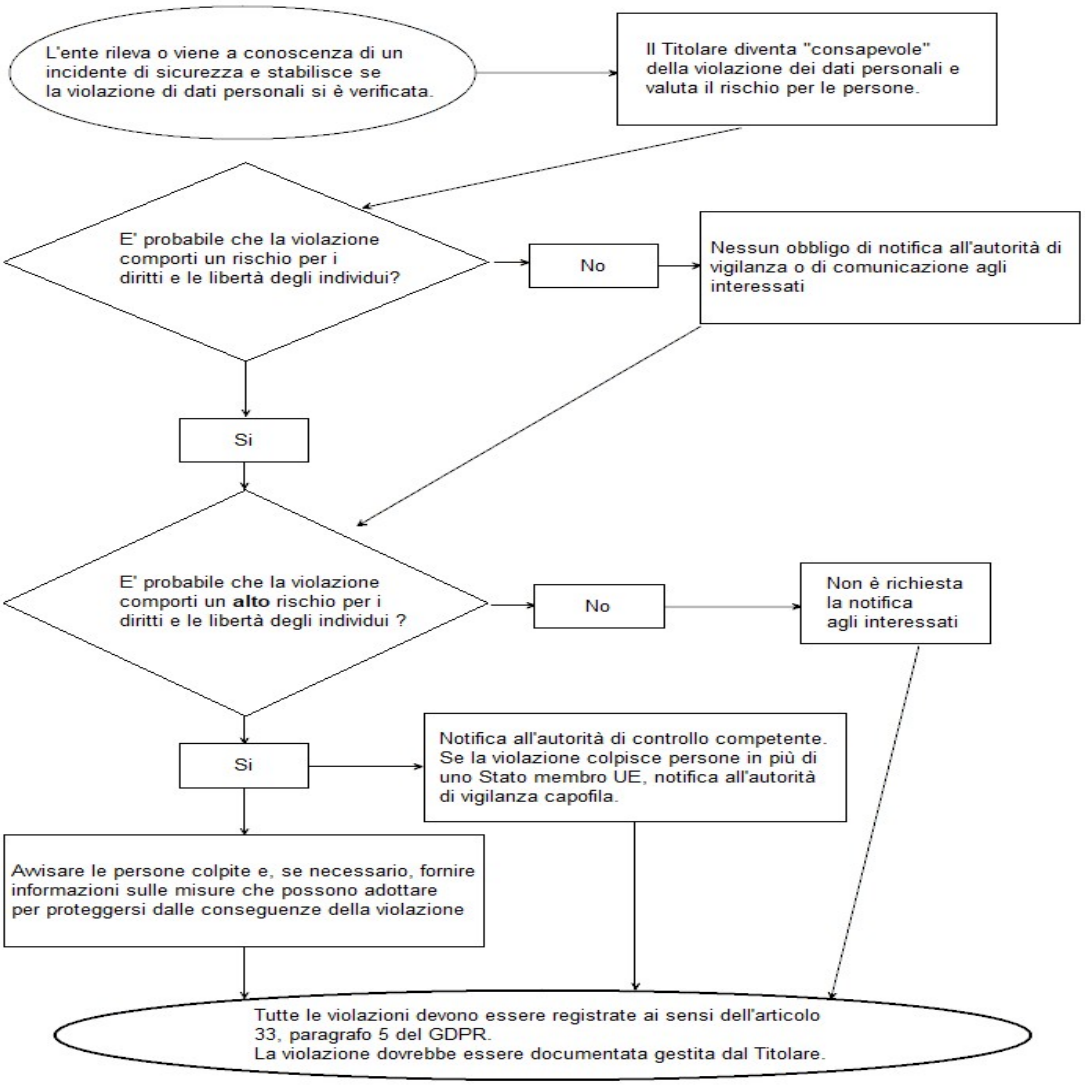
- vi è obbligo di notifica al Garante quando la violazione, così come definita all'art. 4 punto 12) del GDPR comporta un rischio, anche presunto, per i diritti e le libertà delle persone fisiche, cioè, quando si è verificata una violazione di sicurezza che abbia comportato, accidentalmente o in modo illecito, la distruzione, perdita, modifica, divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati sia che questi dati siano trattati all'interno che all'esterno dell'ente;
- la notifica deve essere eseguita entro il termine di 72 ore dal momento in cui il Titolare è venuto a conoscenza della violazione. Se non si osserva tale termine il Titolare/Delegato al trattamento deve corredare la comunicazione con la giustificazione del ritardo (par. 1 Art. 33 GDPR). Il ritardo nella comunicazione potrebbe causare ulteriori controlli da parte del Garante con le conseguenti possibili sanzioni;
- il WP29 nelle sue linee guida precisa che la mancata comunicazione può essere sanzionata, ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria;
- il WP29 raccomanda che il Titolare/Delegato al trattamento informi, comunque, l'autorità di vigilanza (notifica al Garante) anche se non ha tutte le informazioni richieste e provvedere successivamente all'integrazione della notifica. Questa può essere necessaria quando è stata accertata una violazione ma non è ancora nota la sua portata. Al riguardo il GDPR all'art. 33, paragrafo n. 4, riporta: "Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo";
- l'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che comporti un rischio per i diritti e le libertà delle persone fisiche; ovviamente il giudizio che determina l'improbabilità del rischio deve essere riportato nel registro delle violazioni;
- Il WP29 chiarisce che l'obiettivo dell'obbligo di notifica è di incoraggiare i Titolari/Delegati al trattamento ad agire prontamente in caso di violazione, contenendo i possibili danni, recuperare, se possibile, i dati personali compromessi e chiedere il parere all'autorità di controllo.
- l'art. 34 del GDPR stabilisce, inoltre, che la comunicazione agli interessati deve essere eseguita "senza ingiustificato ritardo", ne consegue che tale comunicazione può essere eseguita anche prima o contestualmente alla notifica al Garante;
- il considerato n. 88 del GDPR, inoltre, puntualizza che: "Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.
- la comunicazione agli organi di polizia è necessaria quando è accertato che la violazione sia da attribuirsi ad un comportamento illecito o fraudolento, per danno ricevuto o tutela dell'ente.

- la comunicazione è effettuata a CERT PA, come da matrice RACI, nel caso di incidente informatico.

NOTIFICA AL GARANTE

La notifica di una violazione al Garante è prevista all'art. 33 del GDPR.

Diagramma di flusso che mostra i requisiti di notifica
tratto dalle linee guida WP29



La notifica deve, almeno, contenere:

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

b) la comunicazione del nome ed i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;

c) la descrizione delle probabili conseguenze della violazione dei dati personali;

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

COMUNICAZIONE AGLI INTERESSATI

L'obbligo di dare comunicazione, senza ingiustificato ritardo, agli interessati di una violazione dei dati personali che li riguardano è previsto all'art.34 del GDPR quando la violazione è suscettibile di prestare rischio elevato per i diritti e le libertà delle persone fisiche.

La comunicazione agli interessati non è richiesta quando (art.34 paragrafo 3):

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione già applicate ai dati personali oggetto della violazione quali, ad esempio, la cifratura;

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;

c) la comunicazione richiederebbe sforzi sproporzionati. In tal caso la procedura prevede una comunicazione pubblica o analoga misura.

Al paragrafo n. 2 del citato art. 34, viene precisato che la comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e deve contenere almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d) del GDPR. Deve cioè contenere le seguenti informazioni:

a) il nome e i dati di contatto del responsabile della protezione dei dati;

b) descrivere le probabili conseguenze della violazione dei dati personali;

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

Spetta dunque al Titolare/Delegato al trattamento stabilire, in fase di valutazione, se la comunicazione agli interessati debba essere effettuata.

REGISTRAZIONE DELLA VIOLAZIONE

L'art. 33, paragrafo 5 del GDPR, prescrive al Titolare/Delegato al trattamento di registrare qualsiasi violazione dei dati personali, per consentire all'autorità di controllo di verificare il rispetto della norma.

A tal fine, viene istituito un Registro delle violazioni presso il Titolare .

Per supportare le fasi di verifica tecnica e di valutazione, a puro titolo esemplificativo, si riportano alcuni eventi che possono comportare un *data breach* nel caso in cui siano coinvolti dati personali:

- pubblicazione dell'atto nella sua interezza senza omissione di dati personali/particolari;
- inoltro di messaggi contenenti dati personali/particolari a soggetti non interessati al trattamento;

- perdita della chiave di decriptazione;
- cancellazione dei dati in modo accidentale o da parte di soggetti non autorizzati;
- *data exfiltration* (copia o trasferimento non autorizzati di dati);
- *ransomware/malware*;
- distruzione accidentale di uno spazio di memorizzazione;
- smarrimento, furto di PC o server;
- smarrimento, furto di dispositivo mobile (smartphone, USB KEY, CD/DVD HD, etc.);
- smarrimento, furto o distruzione accidentale di documenti o aggregazioni documentali negli archivi cartacei (correnti o di deposito).

MATRICE DI ASSEGNAZIONE DELLE RESPONSABILITÀ

In questa sezione del documento, sotto forma di matrice "RACI", sono individuate le risorse analogiche ed informatiche in relazione alle responsabilità delle figure coinvolte per l'attuazione delle varie fasi del processo di "*data breach*".

Di seguito sono fornite due diverse matrici: la prima contempla le attività da eseguire in caso di "*data breach*" impattante su risorse informatiche, mentre la seconda contempla le attività relative ad incidente su risorse analogiche.

Nel caso di "*data breach*" che impatti sia su risorse informatiche che analogiche si dovranno seguire entrambe le matrici per la parte di riferimento.

Ruoli chiave

La matrice prende la propria denominazione dalle iniziali dei ruoli previsti (in lingua inglese) per l'esecuzione delle attività dei processi aziendali. I ruoli previsti dalla matrice sono:

- **A - (Accountable)** è il responsabile dell'attività e/o colui che la approva (ci può essere una sola A per ogni attività);
- **R - (Responsible)** è il responsabile dell'esecuzione dell'attività, la dirige o per conto del quale l'attività è eseguita (possono esserci più R per ogni attività);
- **C - (Consulted)** rappresenta i soggetti che i responsabili (A ed R) avranno bisogno di consultare;
- **I – (Informed)** sono i soggetti (fisici o giuridici, interni od esterni) che non hanno bisogno di essere coinvolti attivamente nella parte del progetto in capo all'ente ma che devono essere informati relativamente a come progredisce o ai quali è necessario rivolgersi per le parti non di competenza del comune.

Definizione delle figure coinvolte

Figura	Descrizione della figura
Titolare	Giunta Regionale
RPD	Responsabile della protezione dei dati (art. 37 GDPR)
Delegato al trattamento	Soggetto delegato dal Titolare per sovrintendere alle operazioni di trattamento (Direttore/Dirigente)
Referenti Privacy delle Direzioni Regionali	Supportano il Delegato del trattamento
Resp. Trattamento Esterno	Soggetto esterno nominato "Responsabile" dal Titolare (art. 28 GDPR)
Resp. Sistemi informativi	Soggetto delegato dal Titolare per sovrintendere alle operazioni di trattamento eseguite con strumenti informatici. La figura coincide con quella di responsabile per la transazione al digitale (art. 17 CAD)
Responsabili Aree Organizzative Omogenee (A.O.O.)	Soggetto nominato Responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi (art. 3 DPCM 3/12/2013 e art. 61 D.P.R. 445/2000)
Garante Privacy	Autorità nazionale a tutela dei diritti derivanti dalle norme sulla protezione dei dati personali
Responsabile archivio di deposito	Dirigente responsabile pro tempore della struttura regionale cui è assegnata la competenza sulla conservazione e custodia della documentazione versata in archivio di deposito (artt. 7 e 32 DGR n. 2-8065 del 28/01/2008)
Forze dell'ordine	Organo di polizia o Magistratura a cui viene denunciata la violazione di sicurezza se ne ricorrono gli estremi
CERT-PA	Struttura che opera all'interno di AGID e ha il compito di supportare le amministrazioni nella prevenzione e nella risposta agli incidenti di sicurezza informatica
Interessati/Dipendenti	Persone fisiche i cui dati sono stati coinvolti nell'incidente

Matrice RACI per "data breach" impattante su risorse informatiche

FASI	1	2	3	4	5	6	7
Figure coinvolte	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine)	Segnalazioni (CERT-PA)	Comunicazioni interessati e riscontri	Registrazione della violazione
RDP	C	C	C	C		C	C
Titolare/Delegato/i al trattamento (Direttori/Dirigenti)	A/R	A/R	A/R	A/R		A/R	A/R
Referenti privacy	C	C	I	I		I	R
Resp. Trattamento Esterno (se coinvolto)	R/C	R	I	I		I	
Resp. Sistemi Informativi	R	C	I	C	A/R	I	I
Resp. A.O.O.	R	C	I	C		I	I
Garante Privacy			I			I	
Forze dell'ordine				I			
CERT-PA					I		
Interessato/Dipendente (colui che ha subito la violazione)						I	

Matrice RACI per "data breach" impattante su risorse analogiche

FASI	1	2	3	4	5	6
Figure coinvolte	Gestione Tecnica e Analisi	Valutazione	Notifica al Garante	Segnalazioni (Forze dell'ordine)	Comunicazioni interessati e riscontri	Registrazione della violazione
RDP	C	C	C	C	C	C
Titolare/Delegato/i al trattamento (Direttori/Dirigenti)	A/R	A/R	A/R	A/R	A/R	A/R
Referenti privacy	C	C	I	I	I	R
Resp. Trattamento Esterno (se coinvolto)	R/C	R	I	I	I	
Resp. archivio di deposito	R	C	I	C	I	I
Garante Privacy			I		I	
Forze dell'ordine				I		
Interessati/Dipendenti (colui che ha subito la violazione)					I	

Allegato 3

Informativa sul trattamento dei dati personali

ai sensi dell'art. 13 GDPR 2016/679

Gentile Utente,

La informiamo che i dati personali da Lei forniti a **……** saranno trattati secondo quanto previsto dal "Regolamento UE 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, di seguito GDPR)".

- i dati personali a Lei riferiti verranno raccolti e trattati nel rispetto dei principi di correttezza, liceità e tutela della riservatezza, con modalità informatiche ed esclusivamente per finalità di trattamento dei dati personali dichiarati nella domanda e comunicati a **……**.(Direzione o Settore). Il trattamento è finalizzato all'espletamento delle funzioni istituzionali definite……...(normativa/regolamento). I dati acquisiti a seguito della presente informativa……(attività es. bando, contributo, richiesta) saranno utilizzati esclusivamente per le finalità relative al/i procedimento/i amministrativo/i per il/i quale/i vengono comunicati;
- l'acquisizione dei Suoi dati ed il relativo trattamento sono obbligatori in relazione alle finalità sopradescritte; ne consegue che l'eventuale rifiuto a fornirli potrà determinare l'impossibilità del Titolare del trattamento ad erogare il servizio richiesto;
- I dati di contatto del Responsabile della protezione dati (DPO) sono dpo@regione.piemonte.it;
- Il Titolare del trattamento dei dati personali è la Giunta regionale, il Delegato al trattamento dei dati è …….. (Direzione/Settore);
- Il Responsabile (esterno) del trattamento è……;
- i Suoi dati saranno trattati esclusivamente da soggetti incaricati e Responsabili (esterni) individuati dal Titolare o da soggetti incaricati individuati dal Responsabile (esterno), autorizzati ed istruiti in tal senso, adottando tutte quelle misure tecniche ed organizzative adeguate per tutelare i diritti, le libertà e i legittimi interessi che Le sono riconosciuti per legge in qualità di Interessato;
- i Suoi dati, resi anonimi, potranno essere utilizzati anche per finalità statistiche (d.lgs. 281/1999 e s.m.i.);
- i Suoi dati personali sono conservati, per il periodo……...(vedi piano di fascicolazione e conservazione dell'Ente)
- i Suoi dati personali non saranno in alcun modo oggetto di trasferimento in un Paese terzo extraeuropeo, né di comunicazione a terzi fuori dai casi previsti dalla normativa in vigore[1], né di processi decisionali automatizzati compresa la

[1] **indicare se i dati vengono comunicati ad altri soggetti**

profilazione.

Potrà esercitare i diritti previsti dagli artt. da 15 a 22 del regolamento UE 679/2016, quali: la conferma dell'esistenza o meno dei suoi dati personali e la loro messa a disposizione in forma intellegibile; avere la conoscenza delle finalità su cui si basa il trattamento; ottenere la cancellazione, la trasformazione in forma anonima, la limitazione o il blocco dei dati trattati in violazione di legge, nonché l'aggiornamento, la rettifica o, se vi è interesse, l'integrazione dei dati; opporsi, per motivi legittimi, al trattamento stesso, rivolgendosi al Titolare, al Responsabile della protezione dati (DPO) o al Responsabile del trattamento, tramite i contatti di cui sopra o il diritto di proporre reclamo all'Autorità di controllo competente.

Firma per presa visione.