COMUNE DI PUTIFIGARI
Provincia di Sassari

PROCEDURA PER LA GESTIONE DELLA VIOLAZIONE DEI DATI PERSONALI

"DATA BREACH"

Allegato alla Deliberazione della Giunta Comunale n. 66 del 27 novembre 2020

Indice generale

PREMESSA

L'articolo 4 del Regolamento UE 2016/679 (d'ora in poi GDPR) definisce "data breach" (o, nella traduzione italiana, *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[1] trasmessi, conservati o comunque trattati[2] presso una Azienda o una Pubblica Amministrazione.

Gli articoli 33 e 34 del GDPR si occupano rispettivamente di disciplinare la notifica di una violazione dei dati personali all'autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato.

Il presente documento espone la procedura per lo svolgimento delle principali attività rivolte all'attuazione delle disposizioni del GDPR in caso di episodi di data breach che riguardino l'Ente. Dettagli e riferimenti sono stati inseriti nelle note al fine di rendere scorrevole la lettura del testo principale. Dette note non sono secondarie e migliorano la comprensione degli argomenti trattati.

1. DEFINZIONE DATA BREACH

[1] L'articolo 4 del GDPR definisce "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, i dati relativi all'ubicazione, un identificativo online) o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Sono categorie particolari di dati personali quei dati che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici (dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione), i dati biometrici (i dati personali, ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici), i dati relativi alla salute (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), alla vita sessuale o all'orientamento sessuale della persona.

[2] Per "trattamento" si intende 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.

Per Data Breach si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, l'art. 4 punto 12 del Regolamento (UE) 2016/679 (di seguito definito GDPR) definisce la violazione dei dati personali come 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.

Le Linee guida in materia di notifica delle violazioni di dati personali (Data Breach notification) – WP250Rev.01, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse. Anche un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Mentre l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza".

In ogni caso, una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'art. 33, paragrafo 5 del GDPR. Ciò al fine di aiutare il titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni. A seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche.

Conformemente all'art. 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso. Sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le possibili conseguenze della violazione, poiché quest'ultima potrebbe comunque dover essere segnalata per altri motivi. La mancata notifica può comportare ulteriori accertamenti da parte del Garante poiché può rappresentare un indizio di carenze che, se accertate, possono dar luogo a sanzioni. Tutti gli eventi di Data Breach, compresi quelli per cui non sono necessarie le notifiche, devono essere documentati (art. 33 paragrafo 5 del GDPR) su un Registro delle Violazioni.

2 – TIPOLOGIE DI VIOLAZIONE DI DATI

Di seguito sono elencati possibili eventi che possono determinare violazioni di dati personali (in termini di confidenzialità, integrità, disponibilità).

L'elencazione non è esaustiva e il verificarsi di uno degli eventi descritti non costituisce condizione sufficiente per stabilire l'effettiva sussistenza di un data breach. Il verificarsi di un evento (anche non espressamente indicato nel presente documento) che prospetti il rischio di una violazione di dati personali

costituisce sempre un fattore di allerta che richiede sempre un'analisi -anche a diversi livelli- per stabilire

se si è verificato un data breach.

L'elenco è suddiviso in due parti: una riferita ai trattamenti informatici e una ai trattamenti cartacei.

2.1- Eventi relativi a trattamenti informatici:

2.1.1- Eventi relativi a trattamenti informatici dovuti da eventi accidentali: sono determinati da eventi anomali determinati da fatti fortuiti che causano la perdita delle caratteristiche di sicurezza dei dati personali (confidenzialità, integrità o disponibilità) in caso di trattamenti informatici.

Rientrano in tali casistiche eventi generati nella gestione dei sistemi ICT (gestiti internamente oppure in

outsourcing) quali:

- **Esecuzione erronea di comandi e/o procedure**, ad esempio: pubblicazione erronea delle informazioni personali (non di dominio pubblico) su siti web dell'Ente; erroneo invio di informazioni a enti/soggetti esterni all'Ente, formattazione di dispositivi di memorizzazione, errori nell'implementazione di una policy di controllo e verifica periodica delle abilitazioni degli accessi; divulgazione accidentale di credenziali di accesso a colleghi o personale non autorizzato, ecc.
- **Rottura di componenti hardware**, ad esempio distruzione dei supporti di memorizzazione a causa di sbalzi di temperatura e/o di elettricità, umidità; corto circuito; caduta accidentale; eventi catastrofici; incendi, ecc.
- **Malfunzionamento di software**, ad esempio: esecuzione di uno script automatico non autorizzato; errori di programmazione del software che causano output errati, ecc.
- **Visibilità errata di dati sui siti web dell'Ente**, ad esempio: visibilità da parte di utenti di dati di altri utenti anche per casi di omonimia, ecc.
- **Fornitura di dati a persona diversa dall'interessato**, ad esempio: comunicazioni di dati di interessati a destinatari errati; gestione di informazioni avanzate da persone diverse dal Titolare o suo delegato, ecc.
- **Guasti alla rete**, ad esempio: caduta delle comunicazioni durante il trasferimento di dati e perdita di dati durante la trasmissione, ecc.

2.1.2 – Eventi dovuti a trattamenti informatici dovuti ad eventi dolosi: possono essere causati da personale interno o soggetti esterni realizzati tramite:

- accesso non autorizzato ai dati con lo sfruttamento di vulnerabilità dei sistemi interni e delle reti di comunicazione.
- compromissione o rivelazione abusiva di credenziali di autenticazione;
- utilizzo di software malevolo
- altro: in tale casistica sono compresi incidenti di sicurezza ICT che comportano la violazione di dati personali:
  - **furto:** furto di supporti di memorizzazione e/o elaborazione contenenti dati personali (es: furto laptop, hard disk, chiavette USB, smartphone, tablet, ecc.).
  - **truffa informatica esterna:** tutti i casi di frodi realizzate da un soggetto esterno all'Ente rivolto a procurare a sé o ad altri un profitto o, comunque, un vantaggio in termini economici, pubblicitari, ideologici/politici, qualora tali frodi causino perdita delle caratteristiche di sicurezza dei dati personali dei soggetti interessati (confidenzialità, integrità o disponibilità) trattati dall'ente o da suoi fornitori, ad esempio: accesso non autorizzato ed illecito alle basi dati dei sistemi contenenti i dati dei soggetti interessati tramite sfruttamento di vulnerabilità dei sistemi; appropriazione di dati bancari; appropriazione (e diffusione) delle credenziali di autenticazione ai servizi degli utenti.
  - **truffa informatica interna:** tutti i casi di frodi realizzate da personale interno all'Ente che comportano la violazione dei dati personali. Tali eventi possono derivare dall'utilizzo illecito e/o illegittimo delle informazioni a cui un incaricato del trattamento accede anche se autorizzato.

2.2 – Eventi relativi a trattamenti cartacei:

2.2.1 – Eventi relativi a trattamenti cartacei dovuti ad eventi accidentali: sono Eventi anomali, determinati da calamità o da fatti fortuiti, nell'ambito dei trattamenti non automatizzati effettuati su archivi cartacei contenenti dati personali in possesso dell'Ente quali:

- **Distruzione accidentale di documenti**, ad esempio in caso di incendio/allagamento dei locali dove sono presenti gli archivi cartacei presso le sedi dell'Ente e/o Enti collegati o di propri fornitori; distruzione per errore di documenti originali, senza eventuale copia; ecc.
- **Smarrimento di documenti:** ad esempio perdita di documenti contenenti dati personali; ecc.
- **Fornitura involontaria di dati** a persona diversa dall'interessato o a persona non autorizzata al trattamento

2.2.2 – Eventi relativi a trattamenti cartacei dovuti ad eventi dolosi: trattati di comportamenti dolosi da parte di personale interno o soggetti esterni realizzati, attraverso accessi non autorizzati, nell'ambito di trattamenti effettuati su archivi cartacei di dati personali dell'Ente e/o Enti collegati quali:

- **Distruzione dei documenti:** ad esempio incendio doloso provocato da personale interno o soggetti esterni che rende indisponibile in modo definitivo i documenti contenenti dati personali;

accesso non autorizzato da parte di terzi ad archivi interni dell'Ente e distruzione volontaria di documenti contenenti dati personali.

- **Accesso non autorizzato:** ad esempio accesso non autorizzato da parte di personale interno o soggetti esterni, con lettura e/o copia dei documenti, ad archivi documentali presso le sedi dell'Ente e/o Enti o propri fornitori. Non si verifica violazione se si ha la ragionevole certezza che non vi è stata lettura o copia dei documenti contenenti dati degli interessati.
- **Furto:** sottrazione da parte di personale interno o soggetti esterni (o non identificati) di documenti cartacei contenenti dati personali.

3 – GLI ATTORI DEL DATA BREACH

2.1 Soggetti attivi

I soggetti attivi (o attori) sono tutti coloro che si occuperanno dell'episodio di Data Breach dalla fase di rilevazione dell'incidente alla fase di notifica di cui agli artt. 33 e 34 del GDPR, i ruoli coinvolti sono:

- **Titolare, nella persona del suo delegato**: è la persona, fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
  l'Ente ha disposto la delega di funzioni in capo ai responsabili di P.O. Il Titolare, pertanto, in caso di data breach, è il responsabile di P.O. della struttura in cui si è rilevata la violazione o un episodio che possa determinarla.
- **RPD**: Responsabile Protezione Dati o Data Protection Officer (DPO): il soggetto nominato dell'Ente con riferimento agli articoli 37, 38, 39 del GDPR.
- **Referente privacy:** è il soggetto che svolge funzioni di referente per il supporto procedurale per il Data Breach per il cui tramite il delegato del titolare trasmette le notifiche in esito alla procedura di Data Breach**.**
- **Amministratore di sistema**: è la figura preposta alla gestione e supervisione del processo di Security Incident Management in ambito informatico che controlla gli assetti generali di rete, i sistemi di base dell'Ente e gli accessi al dominio.
- **Referente interno**: è il dipendente/collaboratore che ha rilevato o a cui è stato segnalato un evento anomalo di potenziale violazione di dati personali ed è tenuto alla comunicazione dell'incidente, quale persona autorizzata al trattamento dei dati.

4 – PROCESSO DI GESTIONE DEL DATA BREACH

Qualsiasi dipendente o collaboratore dell'Ente, a prescindere dal ruolo rivestito, nel momento in cui è a conoscenza di un episodio di potenziale Data Breach deve dare immediata comunicazione dello stesso al Delegato del Titolare (responsabile di P.O) della struttura presso la quale presta servizio secondo la procedura definita al paragrafo successivo. Deve, inoltre, avvertire il Segretario.

Se dalla prima analisi da parte del Delegato del Titolare emergono elementi tali da escludere la possibile violazione dei dati personali, l'anomalia viene gestita all'interno della struttura interessata.

Se, invece, dalla prima analisi emergono gli estremi per una probabile violazione, si procede ai necessari approfondimenti.

La seconda parte del processo è, pertanto, soltanto eventuale e si verifica quando il Delegato del Titolare ravvisa un data breach o ritiene che un evento possa configurarsi come data breach: in questo caso procede senza indugio (entro 24 ore dalla conoscenza della violazione da parte del dipendente o collaboratore), a segnalare l'episodio ad un gruppo di intervento costituito dallo stesso e dai seguenti soggetti:

- il/i Responsabile/i IT,
- il RPD

al fine di compiere le azioni necessarie per ridurre i rischi e comunque procedere alla raccolta delle informazioni necessarie per coadiuvare il Delegato del Titolare nell'effettuare le valutazioni in ordine alla sussistenza, dimensione e impatto della violazione e supportare lo stesso nella redazione della notifica all'autorità di controllo (Garante per la protezione dei dati personali), se dovuta.

Il gruppo degli attori sopra indicati si riunisce in tempi brevissimi e coinvolge all'occorrenza altri soggetti (Referente privacy, fornitori esterni Titolari del trattamento) che possano dare un contributo alle azioni di cui sopra. In caso di constatazione di violazione dei dati personali, il Delegato del Titolare, per il tramite del Referente privacy, notifica, ai sensi dell'art. 33 c. 1 del GDPR, la violazione all'autorità di controllo competente senza ingiustificato

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

Il Delegato del Titolare, nel caso in cui ricorrano le condizioni previste dall'art. 34 del GDPR procede altresì alla comunicazione agli interessati valutando la modalità idonea a garantire le finalità della disposizione normativa.

Qualora l'episodio riveli una matrice criminale o dolosa il Delegato del Titolare procede al coinvolgimento dell'Autorità di Pubblica Sicurezza (con ogni probabilità la Polizia Postale) mettendola a conoscenza di tutti gli elementi in proprio possesso ed evidenziando l'obbligo di notifica entro 72 ore dalla conoscenza della violazione all'autorità Garante Nazionale e se sussistano i presupposti per la notifica anche agli interessati.

Le azioni poste in essere devono risultare da atti formali. Pertanto, anche se per velocizzare gli interventi ci si avvarrà delle modalità più immediate, si dovranno formalizzare i passaggi salienti anche con la redazione di verbali.

4.1 - Fasi del processo

In caso di accertamento di violazione, è necessario seguire le seguenti fasi:

1. Rilevazione dell'incidente e segnalazione
2. Raccolta di informazioni, analisi e valutazione dell'evento
3. Comunicazioni
4. Altre segnalazioni dovute
5. Inserimento dell'evento nel Registro delle Violazioni.

4.1.1 – Rilevazione dell'incidente e segnalazione

In questa fase si acquisisce la notizia di una possibile violazione di dati personali.

La segnalazione di un Data Breach può essere interna o esterna all'Ente:

a) INTERNAMENTE la segnalazione può avvenire da parte del RPD/DPO, da personale dipendente o da personale convenzionato/stagisti/tirocinanti.
b) ESTERNAMENTE può avvenire da parte di Organi Pubblici (Agid, Polizia, Forze dell'Ordine ....), da parte di Responsabili Esterni al Trattamento, da parte degli stessi Interessati o da parte di ulteriori soggetti (Cittadini, Fornitori, ecc..).

Il dipendente/collaboratore che riceve la segnalazione dall'esterno o che rileva dall'interno l'evento anomalo di potenziale violazione di dati personali deve segnalarlo immediatamente, anche per le vie brevi, al Delegato del Titolare e al Segretario della organizzativa presso la quale presta servizio che potranno avvalersi del supporto del Responsabile IT di dominio della stessa struttura organizzativa e/o di altri soggetti responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, al fine di effettuare insieme una prima valutazione (rapida e di massima) ed assicurarsi con certezza che l'evento segnalato non costituisca un data breach.

Il Referente Interno (che ha rilevato o a cui è stato segnalato dall'esterno un evento anomalo di potenziale violazione di dati personali) deve provvedere alla compilazione del Modello di Comunicazione Interna di cui all'Allegato A) e trasmetterlo al Delegato del Titolare (Responsabile di P.O.) del Settore ove si è verificata la potenziale violazione.

Qualora venga ravvisato un pericolo di violazione di dati personali (Data Breach) e , comunque, nei casi dubbi, al fine di porre in essere le eventuali successive azioni da attivare tempestivamente per mitigare o eliminare i rischi, il Delegato del Titolare dovrà avvisare gli altri soggetti attivi, ossia:

- Il Responsabile IT (Amministratore di Sistema),
- Il RPD/DPO.

La fase di rilevazione dell'incidente e segnalazione deve concludersi entro 24 ore dalla conoscenza della violazione da parte del dipendente o collaboratore.

4.1.2 Raccolta delle informazioni inerenti l'evento

Qualora sia stato ravvisato un potenziale data breach e il Delegato del Titolare abbia proceduto a coinvolgere gli altri soggetti attivi, dovranno essere acquisiti gli elementi necessari per condurre la fase successiva di ulteriore valutazione al fine di escludere o confermare la sussistenza del data breach.

A tal fine è attivata senza indugio da parte del Referente data breach la riunione con i restanti soggetti attivi (Delegato del Titolare, Responsabile/i IT, RPD e, se necessario, Referente interno). Gli stessi procedono alla raccolta delle informazioni necessarie per la successiva fase di valutazione e a una prima analisi di identificazione della tipologia di violazione.

Il Referente data breach, anche su richiesta degli altri soggetti attivi, al fine di integrare l'analisi, coinvolge altri soggetti responsabili di attività da cui possono derivare ulteriori elementi conoscitivi, i quali devono garantire tempestivamente il supporto richiesto.

Se dalla prima analisi del gruppo di intervento emergono elementi tali da escludere la possibile violazione dei dati personali, la gestione dell'anomalia viene rimandata all'interno della struttura interessata.

Se, invece, emergono gli estremi per una probabile violazione, si procede ai necessari approfondimenti.

Nella pratica, rilevazione e valutazione dell'evento sono spesso interconnesse e già nell'immediato può essere riscontrato un rischio ragionevole di violazione e, anche se non sono disponibili subito maggiori informazioni di dettaglio, si rende necessaria una preventiva comunicazione al Garante da parte del Delegato del Titolare, per il tramite del Referente privacy.

Vi sono casi in cui è possibile definire se l'evento costituisca una violazione ai sensi del GDPR solo al termine della fase di valutazione a cui partecipano tutti i soggetti attivi. In quest'ultimo caso la decorrenza delle tempistiche per la comunicazione al Garante (72 ore) è dal momento della constatazione[3]. La notifica deve essere redatta dal Delegato del Titolare ai sensi dell'art. 33 del GDPR e inviata all'Autorità di controllo a cura del Referente data breach.

Il WP29 ha chiarito che, nell'ipotesi in cui i titolari del trattamento (o loro delegati) non siano in possesso di tutte le informazioni relative alla violazione nelle 72 ore successive al suo verificarsi, con *Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP250, versione emendata e adottata il 6 febbraio 2018 (https://www.garanteprivacy.it/regolamentoue/databreach)*, essi hanno la possibilità di comunicare entro il termine di legge all'Autorità di controllo la sola violazione subita, per poi fornire in un successivo momento tutte le informazioni richieste dal suddetto art. 33, corredandole con i motivi del ritardo.

[3] *Le Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) – WP250, versione emendata e adottata il 6 febbraio 2018 (https://www.garanteprivacy.it/regolamentoue/databreach) chiariscono quando il titolare del trattamento può considerarsi "a conoscenza" di una violazione: ...il regolamento impone al titolare del trattamento di notificare una violazione senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza. Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione. Il Gruppo di lavoro ritiene che il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali. Tuttavia, come già osservato, il regolamento impone al titolare del trattamento di attuare tutte le misure tecniche e organizzative di protezione adeguate per stabilire immediatamente se si è verificata una violazione e informare tempestivamente l'autorità di controllo e gli interessati. Afferma altresì che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato21. Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate. Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione. In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.*

4.1.3 Valutazione dell'evento

Scopo di questa fase è quello di confermare o meno l'avvenuta violazione, di circostanziare in modo completo l'evento e fornire una valutazione del possibile pregiudizio per gli interessati.

I soggetti attivi effettuano un'analisi di dettaglio, esaminano le informazioni aggiuntive e valutano il livello di rischio dell'evento e il livello di pregiudizio per gli eventuali interessati impattati dalla violazione.

Nel caso in cui, dall'analisi, si constati che l'evento costituisce una violazione dei dati personali, da questo momento decorrono le tempistiche (dal momento della conoscenza 72 ore[4]) previste dalla normativa in tema di comunicazioni al Garante.

La notifica all'Autorità di controllo deve essere redatta dal Delegato del Titolare ai sensi dell'art. 33 del GDPR e trasmessa a cura del Referente data breach.

Il gruppo di intervento accerta anche se la violazione di dati comporti un elevato pregiudizio per i diritti e le libertà degli interessati (cittadini, dipendenti, soggetti terzi, ecc.) a fini della comunicazione agli stessi. Nel caso in cui ricorrano le condizioni previste dall'art. 34 del GDPR, il Delegato del Titolare procede alla comunicazione agli interessati valutando la modalità idonea a garantire le finalità della disposizione normativa.

Qualora l'episodio riveli una matrice criminale o dolosa il Delegato del Titolare procede al coinvolgimento dell'Autorità di Pubblica Sicurezza (con ogni probabilità la Polizia Postale) mettendola a conoscenza di tutti gli elementi in proprio possesso. Nella comunicazione dovranno essere evidenziati l'obbligo di notifica entro 72 ore dalla conoscenza della violazione all'autorità Garante Nazionale e l'eventuale sussistenza dei presupposti per la notifica anche agli interessati.

4.1.4 Comunicazione

La comunicazione al Garante della Privacy (di cui all'art. 33 del GDPR) dovrà essere effettuata attraverso la compilazione del Modello reso disponibile dal Garante della privacy (Allegato B) che contiene tra gli altri i seguenti elementi:

- La descrizione della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie ed il numero approssimativo di registrazioni dei dati personali in questione;
- L'indicazione del nome ed i relativi dati di contatto del RDP/DPO;
- La descrizione delle probabili conseguenze della violazione;
- L'indicazione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e, se del caso, per attenuare i possibili effetti negativi.

Nello specifico, la comunicazione al Garante sarà effettuata dal Delegato del Titolare tramite PEC agli indirizzi indicati sul sito del Garante, inviata per conoscenza al RDP/DPO e al Referente Privacy

In caso di violazione dei dati che comporti un elevato pregiudizio per i diritti e le libertà degli interessati (cittadini, dipendenti, soggetti terzi, ecc.), ai sensi dell'art. 34 del GDPR, il Delegato del Titolare comunica la violazione agli stessi senza ingiustificato ritardo.

Il gruppo di intervento supporta il Delegato del Titolare nel verificare che siano o meno soddisfatte le condizioni di cui al c. 3 dell'art. 34 del GDPR per le quali non è previsto l'obbligo di comunicazione agli interessati.

Qualora non ricorra nessuna tali condizioni, il gruppo di intervento supporta il Delegato del Titolare nella predisposizione del testo della comunicazione e nella individuazione della modalità di diffusione.

La comunicazione agli interessati dovrà descrivere con un linguaggio semplice e chiaro la natura della violazione e contenere almeno le informazioni e le misure di cui all'art. 33 par. 3, lett. b), c) e d) del GDPR[5]. Nel caso in cui l'Autorità di Pubblica Sicurezza, interessata all'evento data breach, dovesse richiedere di ritardare la comunicazione agli interessati per non pregiudicare lo svolgimento delle indagini, il Referente data breach - su disposizione della

---

[4] *Come specificato dall'art.33 c. 1 del GDPR, in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.*

[5] *Nel caso in cui il Delegato del Titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al c. 3 è soddisfatta (c. 4 art. 34 del GDPR).*

Autorità di P.S. - può chiedere al Garante l'autorizzazione a ritardare la citata comunicazione per il tempo necessario all'espletamento delle stesse.

5- ALTRE SEGNALAZIONI DOVUTE

Il Delegato del Titolare, con il supporto dei soggetti attivi interessati, dovrà verificare la necessità di informare altri organi quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche);
- Gestore di Identità Digitale e Agid nel caso in cui si individui un uso anomalo di un'identità SPID (SistemaPubblico di Identità Digitale).

6- PROCESSO DI GESTIONE DEL DATA BREACH IN CASO DI SEGNALAZIONE DA PARTE DI FORNITORI

Nel caso in cui un fornitore dell'Ente, in qualità di responsabile del trattamento, venga a conoscenza di una violazione (o presunta tale) di dati personali trattati nell'ambito dell'erogazione di un servizio, effettua una prima analisi dell'accaduto e, ove accerti che si tratti di un data breach, invia la segnalazione al Delegato del Titolare e Segretario, al RPD/DPO, al/ai Responsabile/i IT, al Referente data breach senza ingiustificato ritardo. La segnalazione deve contenere tutti gli elementi utili alla comprensione/identificazione dell'evento.

Il fornitore garantisce, inoltre, assistenza al Delegato del Titolare fornendo eventuali informazioni aggiuntive per la corretta valutazione e gestione dell'evento.

Il Delegato del Titolare che riceve la segnalazione procede secondo quanto previsto ai paragrafi 4.1.2, 4.1.3, 4.1.4.

7 - ASPETTI SANZIONATORI

Secondo quanto disposto dall'art. 83 c. 4 del GDPR, la violazione degli obblighi del titolare del trattamento e del responsabile del trattamento previsti dagli artt. 8, 11, da 25 a 39, 42 e 43 è soggetta a sanzioni amministrative pecuniarie fino a 10.000.000 euro; rientrano, pertanto, anche le violazioni alla procedura in materia di data breach, previste dagli artt. 33-34 del GDPR.

Inoltre, l'art. 82 prevede che chiunque subisca 5 un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal soggetto al quale l'obbligo (violato) era imposto (salvo che quest'ultimo dimostri che l'evento dannoso non gli è imputabile).

Lo stesso GDPR, all'art. 83 c. 2, indica dei fattori che possono mitigare o aggravare la violazione; un elemento che può sicuramente mitigare il livello sanzionatorio, a fronte di una violazione, è legato al comportamento del titolare che può dimostrare come, intervenendo con tempismo, abbia fatto il possibile per ridurre la gravità, la natura e la durata della violazione. L'atteggiamento reattivo e cooperativo comporta sicuramente un'attenuazione delle sanzioni applicabili[6].

[6] Articolo 83, comma 2: "Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene debito conto, infatti, dei seguenti elementi: la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi, dal danno e il livello del danno da essi subito; il carattere doloso o colposo della violazione; le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e
k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione".

Dalla lettura dei punti indicati in nota e, in particolare dei punti c, e, f, h, k, appare evidente come una corretta gestione della procedura sia importante per limitare, in caso di violazione di una disposizione, l'applicazione delle sanzioni connesse.

In tal senso, fermo restando la necessità di una continua formazione del personale, si raccomanda di scoraggiare atteggiamenti reticenti o non pienamente collaborativi in quanto la segnalazione del possibile data breach e un pronto intervento di gestione rappresentano sicuramente comportamenti valutabili in senso positivo secondo quanto detto sopra[7].

8 - REGISTRO VIOLAZIONI

L'art. 33 paragrafo 5 del GDPR, prescrive al Titolare del trattamento di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Il Gruppo di Lavoro Articolo 29, nel documento WP250rev.01, sottolinea che il titolare dovrà documentare tutte le violazioni che si siano verificate, indipendentemente dall'obbligo di notifica, registrando i dettagli relativi alla violazione, comprese le circostanze, le sue conseguenze e i provvedimenti adottati per porvi rimedio. A tal proposito si è predisposto un modello di registro di cui all'Allegato C, precisando che non viene indicato dal GDPR un periodo di conservazione per tale documento ma, se tale documentazione contiene dati personali, spetta al titolare del trattamento determinare il periodo appropriato di conservazione.

La documentazione dovrà essere conservata, in conformità all'art. 33, paragrafo 5 del GDPR, nella misura in cui tale documentazione consenta all'Autorità di controllo di verificare il rispetto di tale articolo o, più in generale, del principio di responsabilizzazione che codesto Ente stima in anni 10.

Il Registro delle Violazioni è conservato dal Titolare del Trattamento per il tramite del Referente Privacy.

In tale Registro il Referente Privacy, di concerto con il RDP/DPO, annota tutte le informazioni richieste dalla normativa vigente, quali, ad es.:

(a) le circostanze relative alla violazione;
(b) le conseguenze;
(c) i provvedimenti adottati per contrastarla e limitarne gli effetti;
(d) i dati personali coinvolti, ecc.

A tal fine al RDP/DPO è trasmessa, a cura del Referente Privacy, tutta la documentazione necessaria allo stesso per supportare l'Ente nelle registrazioni, compresi i verbali delle riunioni dei soggetti attivi.

Le comunicazioni inviate al CERT-PA ai sensi dell'art. 4 della Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia digitale devono essere altresì trasmesse al RDP/DPO anche ai fini delle eventuali segnalazioni nel registro.

I dati presenti nel Registro delle violazioni sono trattati nel rispetto del principio di minimizzazione e secondo le misure per mitigare i rischi di violazione dei dati personali

ALLEGATI:
Allegato A) Modello di Comunicazione Interna Data Breach
Allegato B) Modello di Notifica al Garante
Allegato C) Modello registro delle violazioni

[7] Si rammenta quanto disposto dal D. Lgs. 30/06/2003, n. 196 all'art. 168 (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante) in vigore dal 19 settembre 2018:
c. 1 Salvo che il fatto costituisca più grave reato, chiunque, in un procedimento o nel corso di accertamenti dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.
c 2. Fuori dei casi di cui al comma 1, è punito con la reclusione sino ad un anno chiunque intenzionalmente cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al Garante o degli accertamenti dallo stesso svolti