DATA BREACH POLICY

Procedura da seguire in caso di violazione dei dati personali ai sensi degli articoli 33 e seguenti Regolamento UE 679/2016 (Regolamento Generale sulla Protezione dei Dati - GDPR)

SOMMARIO

Premessa

La sicurezza del trattamento dei dati (art. 32 e considerando 83 Regolamento UE 679/2016)

Il Regolamento UE 679/2016 ("Regolamento generale sulla protezione dei dati", di seguito "GDPR") stabilisce una serie di principi in materia di sicurezza del trattamento dei dati personali, imponendo al Titolare del trattamento ed al Responsabile del trattamento di adottare tutte le misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Per mantenere la sicurezza e prevenire trattamenti in violazione al GDPR, il Titolare dovrebbe valutare i rischi inerenti al trattamento ed adottare le misure per limitare tali rischi, quali la cifratura. Tali misure devono assicurare un adeguato livello di sicurezza, inclusa la riservatezza, tenuto conto dello stato dell'arte e dei costi di attuazione rispetto ai rischi che presentano i trattamenti e alla natura dei dati personali da proteggere.

Nella valutazione del rischio per la sicurezza dei dati è opportuno tenere in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare un danno fisico, materiale o immateriale.

L'elemento chiave di qualsiasi policy sulla sicurezza dei dati deve essere quindi quello di evitare la loro violazione, e, qualora questo dovesse accadere, di reagire in modo tempestivo.

Il presente documento si propone di fornire una serie di informazioni sul concetto di violazione dei dati personali nonché di individuare le procedure da seguire in caso di avvenuta violazione, nel rispetto di quanto disposto dal GDPR.

2. Definizioni generali

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

Titolare del trattamento: 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.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

3. Definizione di data breach

La violazione dei dati personali, o "data breach", è definita all'art. 4 del GDPR come la "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione ai loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudominizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata (vd. considerando 85 GDPR). 4

Le linee guida del WP29 ("Article 29 Data Protection Working Party") del 03.10.2017 "Guidelines on Personal data breach notification under Regulation 2016/679" specificano che le violazioni possono essere suddivise nelle seguenti categorie:

1) **violazioni di riservatezza**: nel caso in cui si verifichi una divulgazione o un accesso a dati personali non autorizzato od accidentale;

2) **violazioni di integrità**: nel caso in cui si verifichi una modifica dei dati non autorizzata od accidentale;

3) **violazioni di disponibilità**: nel caso in cui si verifichi una non autorizzata od accidentale perdita delle credenziali di accesso o una distruzione dei dati.

La violazione dei dati, a seconda delle circostanze, può rientrare in uno solo dei casi di cui sopra, o in tutti e tre. La violazione dei dati non deve essere celata, in quanto l'oscuramento della notizia, oltre a esporre il Titolare del trattamento a gravi sanzioni amministrative pecuniarie, amplifica in modo sensibile gli effetti negativi dell'evento e può ostacolare la tutela dell'interessato.

4. Adempimenti da svolgere in caso di data breach

Qualora si verifichi un evento che possa comportare la violazione di dati personali, è necessario contattare immediatamente i seguenti soggetti:

- Ordine dei Dottori Agronomi e dei Dottori Forestali della Provincia di Reggio Calabria: Via Del Torrione, 103 C - 89125 Reggio Calabria (RC) - Codice Fiscale: 80013750809 - Telefono/Fax: 0965.891622 - E-mail: ordagrfor.rc@tiscali.it - PEC: protocollo.odaf.reggiocalabria@conafpec.it;

- Responsabile della Protezione dei Dati/Data Protection Officer (RPD/DPO): E-mail: info@garanteprivacyitalia.it – PEC: dpo@pec.garanteprivacyitalia.it – Telefono: 0968.462702

L'obbligo di informazione grava anche sui responsabili del trattamento, i quali devono informare il Titolare del trattamento, senza ingiustificato ritardo, dopo essere venuti a conoscenza della violazione.

La comunicazione deve essere tempestiva, in modo da permettere al Titolare di rispettare i termini per gli adempimenti di cui all'art. 33 GDPR.

Il Responsabile deve comunicare al Titolare qualsiasi violazione dei dati personali, a prescindere dai possibili rischi derivanti dalla violazione.

Una volta ricevuta la notizia di un potenziale data breach, il Titolare, coadiuvato da esperti qualificati, dovrà procedere immediatamente con le indagini più opportune volte ad accertare se effettivamente si sia verificata una violazione, raccogliendo tutte le prove e indizi possibili. Nel contempo, a seconda del tipo di violazione, dovrà adottare tutte le misure per limitare la violazione e recuperare gli eventuali dati persi, implementare il livello di sicurezza dei dati, istruendo in modo adeguato tutti i dipendenti.

4.1 Notifica al Garante

In base all'art. 33 GDPR, il titolare del trattamento deve notificare al Garante la violazione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è venuto a conoscenza dell'evento, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche. Decorso il termine di 72 ore, la notifica della violazione deve essere corredata dalle ragioni del ritardo.

Il termine di 72 decorre dal momento in cui il titolare ha avuto conoscenza della violazione dei dati, ovvero quando il titolare ha avuto un ragionevole livello di certezza circa l'avvenimento di un incidente alla sicurezza che ha determinato la compromissione di dati personali.

La consapevolezza della violazione dei dati personali può dipendere molto dalle circostanze, perché alcune violazioni possono essere facilmente individuabili, altre invece possono richiedere un'indagine più approfondita. Durante le indagini, il titolare può essere considerato come privo di un grado di conoscenza tale da far scattare immediatamente l'obbligo di notifica.

Ciò precisato, il WP29 sottolinea che il diligente comportamento del titolare sarà in ogni caso valutato sulla base della sua tempestiva attivazione in caso venga informato di una possibile infrazione. La fase investigativa, quindi, non deve essere abusata per prorogare illegittimamente il termine di notifica.

Di seguito si riportano alcuni esempi chiarificatori elaborati dal WP29:

1. perdita di una chiavetta USB i cui dati non sono cifrati: benché non sia possibile avere la certezza se un soggetto non autorizzato acceda o meno ai dati, la perdita della chiavetta rientra senza dubbio nei casi di violazione alla disponibilità dei dati, e la consapevolezza della violazione si ha nel momento in cui il titolare scopre lo smarrimento della chiavetta.
2. un soggetto terzo comunica al titolare di aver accidentalmente ricevuto dati relativi ad un suo cliente, mostrandogli prove adeguate. Il titolare diventa consapevole della violazione nel momento in cui riceve prove della stessa.
3. Il titolare scopre che c'è stata una possibile intrusione nel suo sistema, e nell'eseguire i controlli necessari, scopre che i dati ivi contenuti siano stati compromessi, momento nel quale il titolare diventa consapevole della violazione.

La notifica deve almeno:

a) descrivere la 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.

In base a quanto precisato dal WP29, è opportuno distinguere in modo adeguato le categorie di interessati, ad esempio: dipendenti, clienti, persone con disabilità, minori e altre categorie vulnerabili, nonché i tipi di dati: dati relativi alla salute, informazioni sulla sicurezza sociale, informazioni finanziarie, coordinate bancarie, dettagli dei documenti di riconoscimento).

Qualora la violazione comporti dei seri rischi per l'interessato (es. furto di identità, perdite finanziarie), la notifica deve fare chiaro riferimento a queste categorie di dati.

Qualora non sia possibile avere informazioni precise sul numero di interessati e di dati oggetto di violazione, la notifica deve essere comunque fatta nei termini, indicando le predette informazioni in numero approssimativo, specificando in seguito il numero esatto.

a) comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati (ove presente) o di altro punto di contatto presso cui ottenere più informazioni;
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.

4.1.1 Notifica in fasi

L'art. 33, paragrafo 4, GDPR, prevede la possibilità di procedere alla "notifica in fasi", stabilendo che "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'ipotesi riguarda prevalentemente i casi di violazioni molto complesse, nelle quali è necessario svolgere indagini approfondite per comprendere la natura della violazione e la misura in cui la violazione ha coinvolto i dati.

Alla luce di questo, qualora per la complessità o estensione della violazione, il titolare non sia in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie, potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica di alert, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri. Al momento della notifica, il titolare deve comunicare al Garante che provvederà a trasmettere in un secondo momento tutti i dettagli relativi alla violazione.

Il WP29 ha precisato che non incorre in alcuna sanzione il titolare che, dopo la notifica iniziale, abbia scoperto che l'incidente alla sicurezza sia stato arginato e non vi sia stata un'effettiva violazione dei dati personali. In questi casi, il titolare potrà aggiornare il Garante in tal senso, comunicandogli che in realtà non vi è stata una violazione di dati.

4.1.2 Casi in cui non è obbligatoria la notifica al Garante.

L'art. 33, paragrafo 1, GDPR, precisa che la notifica non è necessaria se è improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche. Il WP29 ha precisato che tale ipotesi ricorre in caso di violazione di dati già disponibili al pubblico, o nel caso in cui i dati siano crittografati e la chiave di decifratura non sia stata compromessa. In quest'ultimo caso, qualora in seguito il titolare scopra che la chiave in realtà è stata violata, allora dovrà procedere obbligatoriamente alla notifica.

Il titolare, quindi, è tenuto a effettuare un'attenta analisi sugli effetti che la violazione può comportare sui diritti degli interessati, al fine di decidere se procedere o meno alla notifica al Garante.

4.1.3 Sanzioni in caso di omessa notifica

La violazione degli obblighi del titolare del trattamento o del responsabile del trattamento previsti dagli articoli 33 e 34 GDPR comporta sanzioni pecuniarie fino a 10.000.000,00 €, o per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

4.2 Comunicazione della violazione dei dati personali all'interessato (art. 34 GDPR)

In base all'art. 34 GDPR, il titolare del trattamento è tenuto a comunicare la violazione all'interessato, senza ingiustificato ritardo, nei casi in cui la violazione dei dati personali è probabile che presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

La comunicazione all'interessato di cui al paragrafo 1 dell'art. 34 GDPR deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contenere almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d), GDPR, ovvero:

- la descrizione della natura della violazione;
- il nome e i contatti del responsabile della protezione dei dati personali (ove esistente) o di altro punto di contatto;
- una descrizione delle possibili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati e anche, se del caso, per attenuarne i possibili effetti negativi. E' opportuno che il titolare suggerisca agli interessati i possibili accorgimenti per proteggersi dagli effetti della violazione, come modificare le password.

La comunicazione deve essere effettuata privilegiando modalità di comunicazione dirette con gli interessati, ad esempio e-mail, SMS, messaggi diretti. E' opportuno evitare di inviare la comunicazione nel contesto di newsletter o update generali, in quanto gli interessati potrebbero non cogliere l'importanza del messaggio e confonderla con le comunicazioni periodiche. E' necessario tenere in considerazione la nazionalità degli interessati, in modo da inviare la comunicazione nella loro lingua.

Il considerando 88 precisa altresì che nel definire le modalità e le procedure applicabili alla notifica delle violazioni di dati personali, sia opportuno tenere in considerazione anche i 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. Di conseguenza, se richiesto

dalle autorità investigative, la comunicazione agli interessati può essere rinviate per il tempo necessario per lo svolgimento delle opportune attività di indagine.

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 dell'art. 34 GDPR se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; 8
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, art. 34 GDPR. Es. qualora il titolare del trattamento abbia individuato immediatamente il responsabile della violazione ed impedito che lo stesso potesse compiere qualsiasi azione in relazione ai dati;
c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. Es. allagamento di un archivio di documenti pubblici, conservati in forma solo cartacea. In questo caso la comunicazione agli interessati può essere fatta mediante comunicazione pubblica.

Da ultimo, si ricorda che nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, il Garante 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 paragrafo 3, articolo 34 GDPR, sia soddisfatta.

5. Valutazione dei rischi

E' opportuno sottolineare la differenza dei presupposti che impongono la notifica della violazione al garante e la comunicazione agli interessati, in quanto:

- la notifica al Garante è obbligatoria a meno che sia improbabile che la violazione presenti rischi per i diritti e le libertà delle persone fisiche;
- la comunicazione della violazione agli interessati è obbligatoria quando è probabile che presenti un rischio elevato per i diritti e le libertà delle persone fisiche.

Per valutare i rischi connessi alla violazione, il titolare deve prendere in considerazione i seguenti aspetti:

- **il tipo di violazione**: il tipo di violazione può influire sul livello di rischi cagionati agli interessati. Es. la divulgazione di dati sanitari a soggetti non autorizzati può comportare effetti diversi rispetto alla distruzione del dato sanitario.
- **la natura del dato**: la violazione di dati particolari (sensibili) è più dannosa rispetto alla violazione di dati non particolari, così come la violazione di dati particolarmente delicati (es. dati relativi ai documenti di identità, dati finanziari, numeri di carta di credito)

- **grado di identificazione degli interessati**: un ulteriore aspetto da valutare è il livello di facilità con il quale è possibile a risalire alle generalità dei singoli interessati soggetti alla violazione. Es. il furto di dati identificativi o di dati facilmente individuabili presenta livelli di rischio più elevati di dati crittografati.
- **gravità delle conseguenze sugli interessati**: la gravità può dipendere non solo dal tipo di dato violato ma anche dalle intenzioni e dall'utilizzo che gli autori della violazione intendono fare.
- **caratteristiche degli interessati**: la violazione di dati relativi a minori o altre categorie delicate può presentare rischi più elevati.
- **tipo di attività svolta dal titolare**: il tipo di attività svolta dal titolare può influire sul livello di rischio per gli interessati (es. attività sanitaria).
- **numero di soggetti coinvolti**: in genere, la violazione di dati relativi a numeri elevati di individui comporta rischi più elevati.

6. Registro delle violazioni (art. 33, paragrafo 5, GDPR)

A prescindere dall'obbligo di notifica al Garante e di comunicazione agli interessati, il titolare deve tenere il registro delle violazioni nel quale documentare qualsiasi violazione. Il registro deve indicare:

- le circostanze relative alla violazione;
- le conseguenze;
- i provvedimenti adottati per porvi rimedio.

Nel registro devono essere annotate tutte le decisioni adottate dal titolare in occasione del data breach, quale ad esempio la decisione di non effettuare la notifica al Garante, o in caso di notifica tardiva, i motivi del ritardo.

Allegati

Allegato 8.1_Disposizioni operative di prevenzione del Data Breach

Allegato 8.2_Segnalazione Data Breach

Allegato 8.3_Modello comunicazione al Garante Data Breach

Allegato 8.4_Modello di comunicazione Data Breach all'interessato

Allegato 8.5_Registro Data Breach