Naturallevia di Turrini Silvia, Via Ranuncoli, 7 - 74122 Taranto
(TA) P.IVA IT03109770739

PROCEDURA DA ADOTTARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI: DATA BREACH

Art. 4, 33, 34 del Regolamento UE 679/2016

Premessa

Il Regolamento Generale sulla Protezione dei Dati (Reg. UE 679/2016) introduce **l'obbligo di notificare una violazione dei dati personali** ("violazione o data breach") all'autorità di controllo nazionale competente e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.
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 dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, 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.
Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali 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 il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. **Oltre il termine di 72 ore**, tale notifica dovrebbe essere corredata delle **ragioni del ritardo** e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
Al fine di identificare e, se necessario, notificare correttamente un *data breach* all'autorità garante competente e/o agli interessati, **il Titolare intende definire, con la presente, le procedure da seguire qualora avvenga un presunto data breach all'interno dell'amministrazione**. Si ricorda che la mancata notifica, qualora sia essa necessaria, può comportare una sanzione amministrativa fino ad un importo di 10 milioni di euro oppure il 2% del fatturato dell'intera società.
La presente procedura è stata redatta sulla base delle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679, redatto dal gruppo di lavoro articolo 29 per la protezione dei dati, adottate il 3 ottobre 2017 e nella versione emendata e adottata in data 6 febbraio 2018.
Tali linee guida sono reperibili sul sito del garante per la protezione dei dati personali al link https://www.garanteprivacy.it/regolamentoue/databreach.

1 - Scopo e ambito di applicazione

Questa procedura è redatta al fine di tutelare le persone, i dati e le informazioni e documentare i flussi per la gestione delle violazioni dei dati personali trattati da Naturallevia di Turrini Silvia in qualità di Titolare del trattamento. La procedura definisce le modalità e le responsabilità per:

- Identificare la violazione
- Analizzare le cause della violazione
- Definire le misure da adottare per rimediare alla violazione dei dati personali e attenuarne i possibili effetti negativi
- Registrare le informazioni relative alla violazione, le misure identificate e l'efficacia delle stesse
- Notificare una violazione di dati personali al Garante, nel caso in cui la violazione comporti un rischio per i diritti e la libertà delle persone fisiche
- Comunicare una violazione dei dati personali all'interessato nel caso in cui il rischio fosse elevato.

Questa procedura si applica a qualunque attività svolta dal Titolare del trattamento con particolare riferimento a tutti gli archivi e/o documenti cartacei e a tutti i sistemi informativi attraverso cui sono trattati dati personali, anche con il supporto di fornitori esterni.

2 - A chi si rivolge questa procedura?

Questa procedura è rivolta a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza del Titolare del trattamento, in qualsiasi formato e con qualsiasi mezzo, quali:

- **i soggetti autorizzati**, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal tipo di rapporto intercorrente - abbiano accesso ai dati personali trattati nel corso del proprio impiego per conto del Titolare del trattamento;
- **qualsiasi soggetto** (persona fisica o persona giuridica) che, in ragione del rapporto contrattuale in essere con il Titolare del trattamento abbia accesso ai suddetti dati e agisca in qualità di Responsabile del trattamento ex art. 28 GDPR o di autonomo Titolare.

Il rispetto della presente procedura è obbligatorio per tutti i soggetti coinvolti e la mancata conformità alle regole di comportamento previste dalla stessa potrà comportare provvedimenti disciplinari a carico degli autorizzati inadempienti ovvero la risoluzione dei contratti in essere con terze parti inadempienti, secondo le normative vigenti in materia.

3 - Perché definire una procedura di gestione delle violazioni di dati personali (Data Breach)

Naturallevia di Turrini Silvia, ad integrazione delle procedure già adottate in materia di protezione dei dati personali ai sensi della legislazione vigente, ha predisposto azioni da attuare nell'eventualità in cui si presentino violazioni concrete, potenziali o sospette di dati personali trattati dallo stesso in qualità di Titolare, al fine di:

- evitare rischi per i diritti e le libertà degli interessati;
- evitare danni economici
- notificare la violazione (data breach) al Garante e/o agli interessati, nei tempi e nei modi previsti dalla normativa europea
- non incorrere nelle sanzioni previste dal GDPR per omessa notifica
- minimizzare l'impatto della violazione e prevenire che si ripeta.

4 - Definizione di violazione

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. All'articolo 4, punto 12, il regolamento definisce la "violazione dei dati personali" come segue:
"la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".
Di seguito una descrizione della terminologia, come descritto dal Garante per la Protezione dei Dati personali:
Distruzione: il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro; si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento.
Perdita: Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.
Divulgazione o accesso: un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.
Modifica: si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi.

5 - Procedura di gestione della violazione dei dati personali

Nel caso in cui uno dei soggetti di cui al punto 2 del presente documento venga a conoscenza di una concreta, potenziale o sospetta violazione di dati personali, dovrà essere attivato il flusso di adempimenti di seguito descritti e schematizzati. E' necessario subito informare il Titolare del trattamento, indicando i propri dati di contatto.
A questo punto il Titolare, in concerto con l'amministratore di sistema informatico (qualora si tratti di una violazione informatica), provvederà ad effettuare una prima indagine interna e a definire la gravità dell'eventuale violazione. In particolare, si dovrà procedere a identificare i possibili rischi da essa derivanti e a definire le ulteriori azioni da intraprendere.
La gestione della violazione concreta, potenziale o sospetta prevede l'attuazione delle seguenti attività:

1. Rilevazione e segnalazione della violazione dei dati personali
2. Raccolta delle informazioni sulla violazione e comunicazione della violazione
3. Valutazione del rischio
4. Individuazione delle azioni correttive
5. Comunicazione delle valutazioni effettuate e delle azioni da intraprendere
6. Notifica della violazione (se necessario)
7. Comunicazione agli interessati
8. Documentazione delle violazioni (Registro dei data breach)

Attività	Chi	A chi	Quando	Come
1) Rilevazione e segnalazione eventuale data breach	- tutto il personale - collaboratori - fornitori -responsabili	- al Responsabile della struttura di appartenenza - al Responsabile per la Sicurezza informatica e la Transizione al digitale (in caso di dati archiviati in formato digitale)	Appena se ne viene a conoscenza	Utilizzando le vie più brevi (telefono, e-mail etc.)
2) Raccolta delle informazioni sulla violazione e comunicazione del data breach	Il soggetto che ha rilevato la violazione dei dati	- al Responsabile della Struttura di appartenenza - al Responsabile per la Sicurezza informatica e la Transizione al digitale (in caso di dati archiviati in formato digitale)	Entro 24 0re	Modulo per raccolta delle informazioni sulla violazione
3) Valutazione del rischio	Responsabile digitale nel caso di dati contenuti in sistemi informatici		Appena ricevuta la comunicazione	Metodologia di valutazione del rischio connesso alla violazione

4) Individuazione delle azioni correttive	- Responsabile digitale nel caso di dati contenuti in sistemi informatici - Referenti di struttura per la sicurezza (se presenti)		Appena terminata la valutazione di impatto	Analizzando i risultati della valutazione del rischio
5) Comunicazione delle valutazioni effettuate e delle azioni da intraprendere	- Responsabile digitale nel caso di dati contenuti in sistemi informatici - Responsabili di struttura o loro Referenti	Al Titolare		
6) Notifica della violazione (se necessario)	Al Titolare	Al Garante	Entro 72 ore dalla rilevazione	Modulistica predisposta dal Garante
7) Comunicazione agli interessati (se necessario)	Titolare nella persona del Responsabile di struttura o suo Referente	Alle persone fisiche coinvolte	Nei termini indicati nella valutazione del rischio	Verbalmente o via e-mail *Nel caso in cui la segnalazione diretta richieda uno sforzo ritenuto sproporzionato, allora si potrà utilizzare una comunicazione pubblica, (in via esemplificativa tramite il sito web) che dovrà essere efficace al pari del contatto diretto con l'interessato.*
8) Documentazione delle violazioni	- Responsabile digitale o suo referente qualora la violazione riguardi dati contenuti in sistemi informatici - Referenti di struttura per la sicurezza (se presenti) - Responsabile di struttura o suo Referente		Appena concluse le fasi precedenti	Inserimento dati nel Registro delle violazioni attraverso apposita procedura informatica

6 – Modalità di notifica al Garante e agli interessati

Quando il titolare del trattamento notifica una violazione all'autorità di controllo, l'articolo 33, paragrafo 3 stabilisce che 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;
b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) 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.

A tal fine, l'autorità Garante per la Protezione dei Dati Personali ha messo a disposizione un modello di segnalazione dei data breach, disponibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9128501.
Il regolamento non definisce le categorie di interessati né le registrazioni di dati personali. Tuttavia, il Gruppo di lavoro suggerisce che le categorie di interessati si riferiscono ai vari tipi di persone fisiche i cui dati personali sono stati oggetto di violazione: a seconda dei descrittori utilizzati, ciò potrebbe includere, tra gli altri, minori e altri gruppi vulnerabili, persone con disabilità, dipendenti o clienti.

Il considerando 85 chiarisce che uno degli scopi della notifica consiste nel limitare i danni alle persone fisiche. Di conseguenza, se i tipi di interessati o di dati personali rivelano un rischio di danno particolare a seguito di una violazione è importante che la notifica indichi tali categorie. In questo modo, l'obbligo di descrivere le categorie si collega all'obbligo di descriverne le probabili conseguenze della violazione.

Il fatto che non siano disponibili informazioni precise (ad esempio il numero esatto di interessati coinvolti) non dovrebbe costituire un ostacolo alla notifica tempestiva delle violazioni. Il regolamento consente di effettuare approssimazioni sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte. Ci si dovrebbe preoccupare di far fronte agli effetti negativi della violazione piuttosto che di fornire cifre esatte. Di conseguenza, quando è evidente che c'è stata una violazione ma non se ne conosce ancora la portata, un modo sicuro per soddisfare gli obblighi di notifica è procedere a una notifica per fasi.

L'articolo 33, paragrafo 3, stabilisce che nella notifica il titolare del trattamento "deve almeno" fornire le informazioni previste; di conseguenza il titolare del trattamento può, se necessario, fornire ulteriori informazioni. I diversi tipi di violazioni (riservatezza, integrità o disponibilità)

possono richiedere la fornitura di ulteriori informazioni per spiegare in maniera esaustiva le circostanze di ciascun caso. In ogni caso, l'autorità di controllo può richiedere ulteriori dettagli nel contesto dell'indagine su una violazione.

Circostanze nelle quali non è richiesta la comunicazione agli interessati

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

1) il titolare del trattamento ha applicato misure tecniche e organizzative adeguate a proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe prevedere ad esempio la protezione dei dati personali con cifratura allo stato dell'arte oppure mediante tokenizzazione;

2) immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, a seconda delle circostanze del caso, il titolare del trattamento può aver immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo. È necessario altresì tenere in debito conto delle possibili conseguenze di qualsiasi violazione della riservatezza, anche in questo caso, a seconda della natura dei dati in questione;

3) contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. Si pensi, ad esempio, al magazzino di un ufficio statistico che si è allagato e i documenti contenenti dati personali erano conservati soltanto in formato cartaceo. In tale circostanza il titolare del trattamento deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace. In caso di sforzo sproporzionato, si potrebbe altresì prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, soluzione questa che potrebbe rivelarsi utile per le persone fisiche che potrebbero essere interessate da una violazione ma che il titolare del trattamento non può altrimenti contattare.

Conformemente al **principio di responsabilizzazione**, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.