
 Via Petrarca nr,6 Nereto (TE) Reg.EU 2016/679	Procedura sulle violazioni e sulle segnalazioni all'Autorità garante	P03
		Ed 0 Rev 1 del 13.09.2018
		0005 - Pagina 1 di 4

Quando il Titolare del Trattamento si trova di fronte a una violazione dei dati personali, occorre affrontare l'evento mediante alcune aree principali di intervento:

Avviare senza indebito ritardo un piano di contenimento del danno e ripristino dell'efficacia delle misure	Coinvolgimento immediato delle figure in grado di fornire supporto informatico, legale, ecc.. Il Titolare deve incaricare una figura che conduca le indagini sulla violazione. Il Titolare, assieme al Responsabile incaricato, deve stabilire quali sono i soggetti ai quali la violazione deve essere comunicata. Occorre attivare tempestivamente procedure di business continuity, ad esempio recuperando i dati di back up, e opportune misure di blocco
Effettuare una valutazione del rischio connesso alla violazione	Non tutte le violazioni o perdite conducono agli stessi rischi per la società, per tale motivo è bene considerare i seguenti elementi: <ul style="list-style-type: none"> - Le eventuali conseguenze negative su individui - La gravità di queste conseguenze - La probabilità che esse si verifichino
Notificare, entro massimo 72 ore, al Garante della privacy. Se non è possibile effettuare la notifica entro le 72 ore, questa deve essere corredata dei motivi del ritardo	Ove si renda necessaria la comunicazione anche agli interessati coinvolti, il titolare deve provvedere entro un limite di tempo che il Regolamento definisce "senza ingiustificato ritardo"
Mettere in atto un piano di valutazione delle misure di reazione	Una volta investigato le cause della violazione, occorre valutare le modalità con cui l'azienda ha risposto all'evento e, quindi, tenere costantemente aggiornato la procedura di reazione alla violazione e la sensibilizzazione delle persone coinvolte. Per valutare la qualità delle misure di reazione, si raccomanda di svolgere le seguenti riflessioni: <ul style="list-style-type: none"> - Luoghi e i supporti su cui si trovano i dati personali sono tenuti sotto controllo - Avete individuato l'area di maggior rischio (esempio, i dati sensibili conservati in un unico archivio, privo di copie di back up, o esistono più copie, custodite in modo inappropriato) - Considerare di frequente le modalità di trasferimento dei dati a soggetti terzi (procedure di trasferimento con i relativi livelli di sicurezza definiti e con l'utilizzo di dati trasferiti che siano solo quelli indispensabili per la finalità. - Identificazione dei punti deboli nell'architettura delle misure di sicurezza - Svolgimento di periodici incontri di formazione agli addetti al trattamento - Individuazione di un gruppo di lavoro che si occupi di gestire le violazioni
Assumere decisioni in merito alla necessità di informare gli interessati cui i dati sono stati coinvolti nella violazione	Art. 34 Il regolamento prevede che si informino gli interessati qualora ci si trovi di fronte a un rischio elevato per i diritti e le libertà delle persone fisiche. Il Titolare deve in ogni caso valutare la situazione e lasciare traccia scritta delle ragioni che l'hanno portato a una specifica decisione

 Via Petrarca nr,6 Nereto (TE) Reg.EU 2016/679	Procedura sulle violazioni e sulle segnalazioni all'Autorità garante	P03
		Ed 0 Rev 1 del 13.09.2018
		0005 - Pagina 2 di 4

ALL'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Notifica di violazione dei dati personali (data breach) ai sensi dell'art. 33 del regolamento generale sulla protezione dei dati

Il sottoscritto responsabile del trattamento _____, a nome e per conto della azienda (dare le coordinate – ragione sociale, indirizzo)

Notifica di seguito la avvenuta violazione di dati personali, i cui tempi e modalità sono di seguito descritti in dettaglio

Art. 33 - comma 1

data ed ora della presente notifica _____

data ed ora in cui il responsabile del trattamento è venuto a conoscenza della violazione _____

data ed ora in cui al violazione si è verificata (se diversa dalla data precedente e se i dati sono disponibili) _____

NB- ove la notifica non sia stata effettuata entro 72 ore, compilare il campo sottostante

Si precisa che la notifica non è stata effettuata entro le 72 ore da quando il responsabile ne è venuto a conoscenza per i seguenti giustificati motivi

1

Art 33 – comma 2

Si precisa che l'incaricato del trattamento _____ ha allertato e informato il responsabile del trattamento immediatamente dopo aver accertato la violazione, in data _____ alle ore _____, con comunicazione

verbale,

scritta (dare estremi identificativi della comunicazione, se disponibili)

Art 33 – comma 3 , lettera a)


a.1 Descrizione della natura della violazione dei dati personali ²

² Per meglio consentire all'autorità Garante di comprendere la modalità di violazione, è bene premettere una sintetica illustrazione della architettura del sistema di trattamento informatico o manuale, che è stato oggetto di violazione.

D esempio, il titolare del trattamento potrà illustrare il luogo in cui si è verificata la violazione dei dati, se la violazione ai dati è avvenuta a seguito di smarrimento di dispositivi portatili di supporto, oppure di violazione deliberata da parte di soggetti criminali terzi, quale specifico tipo di violazione si sia verificata, ad esempio una lettura dei dati non autorizzata, che fa presumere che i dati non siano stati copiati, oppure una copia abusiva dei dati, che sono ancora presenti sul sistema di trattamento, oppure una asportazione dei dati, di cui non esiste più copia, oppure una alterazione, che fa sì che i dati siano presenti nel sistema di trattamento ma non siano affidabili, oppure una cancellazione di dati, che possono o meno essere ripristinabili, in funzione della disponibilità di copie di backup. Se possibile, dovranno essere indicati anche che i nomi dei soggetti che si ritiene possano essere stati coinvolti nella violazione, almeno in via ipotetica.

A completamento di questa illustrazione, sarà bene descrivere in dettaglio i supporti sui quali si trovavano i dati oggetto della violazione; tali supporti possono essere di tipo informatico fisso, di tipo informatico mobile, di tipo cartaceo od altro.

Segnalare anche il fatto che la violazione potrebbe coinvolgere anche interessati di altri paesi europei, per allertare le appropriate autorità nazionali

 Via Petrarca nr,6 Nereto (TE) Reg.EU 2016/679	Procedura sulle violazioni e sulle segnalazioni all'Autorità garante	P03
		Ed 0 Rev 1 del 13.09.2018
		0005 - Pagina 3 di 4

a.2 Descrizione delle categorie e il numero di interessati in questione e le categorie e il numero di registrazioni dei dati in questione

a.3 Descrizione delle categorie di dati personali ³

a.4 Numero di interessati in questione ⁴

a.5 Descrizione delle categorie e il numero di registrazioni dei dati in questione

Art 33 – comma 3, lettera b)


b.1 Identità e le coordinate di contatto del responsabile della protezione dei dati, o di altro punto di contatto presso cui ottenere più informazioni (dare anche n. di cellulare ed ogni altra indicazione utile per un immediato contatto da parte della autorità Garante, ad esempio dare contatti afferenti all'incaricato ed al responsabile della protezione dei dati personali)

Art 33 – comma 3, lettera c)

c.1 Descrizione delle conseguenze della violazione dei dati personali (indicare le conseguenze effettive ed anche quelle ragionevolmente prevedibili)

³ Dare una illustrazione articolata della natura dei dati violati, per permettere l'autorità Garante di effettuare una rapida valutazione della gravità della situazione. Una violazione di dati afferenti alla salute è potenzialmente più grave di una violazione afferente a dati anagrafici. Mettere in evidenza se questi dati possono o meno essere utilizzati per furti di identità. Si dovrà anche mettere in evidenza, nel descrivere la natura dei dati, se l'eventuale furto di identità può avere anche gravi e dirette ripercussioni economiche, come ad esempio avviene quando è stato sottratto un PIN e i dati di una tessera bancomat.

⁴ In molti casi non è possibile individuare con esattezza il numero degli interessati, i cui dati sono stati violati. Laddove possibile, indicare il numero approssimato, se è possibile fare queste ipotesi, oppure articolare in modo quanto più dettagliato possibile la categoria degli interessati coinvolti.

 Via Petrarca nr,6 Nereto (TE) Reg.EU 2016/679	Procedura sulle violazioni e sulle segnalazioni all'Autorità garante	P03
		Ed 0 Rev 1 del 13.09.2018
		0005 - Pagina 4 di 4

Art 33 – comma 3, lettera d)

d.1 Descrizione delle misure proposte e già adottate dal responsabile del trattamento per porre rimedio alla violazione dei dati personali ⁵

Art. 33 – comma 4

Specificare se saranno date informazioni in fase successive alla presente notifica e le motivazioni.

Art 33 – comma 5

Il titolare del trattamento dichiara che presso di lui è disponibile tutta la documentazione afferente alla violazione dei dati personali, incluse le circostanze in cui si è verificata, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Il titolare del trattamento dichiara altresì che la documentazione è tale da consentire all'autorità di controllo di verificare il rispetto del disposto dell'articolo 33. Ovviamente, si resta a disposizione per fornire ulteriori informazioni, atte a soddisfare i criteri e i requisiti concernenti l'accertamento della violazione di dati personali di cui ai commi 1 e 2 e le circostanze particolari in cui il responsabile del trattamento e l'incaricato del trattamento sono tenuti a notificare la violazione.

⁵ Rispetto a una descrizione delle misure che si intendono adottare occorre indicare un tempo limite entro il quale le misure in questione saranno adottate. Considerando eventuali problemi di natura economica, a finanziamento delle iniziative proposte.