

*Comune di Azzate*  
*Provincia di Varese*

**Modello organizzativo  
per affrontare l'eventualità  
di violazione di dati personali (data breach)**

## 1. La definizione di “data breach”

Il “data breach” è una 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.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

Alcuni possibili esempi di tale perdita di sicurezza in materia di dati personali sono i seguenti:

- l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati;
- il furto o la perdita di dispositivi informatici contenenti dati personali;
- la deliberata alterazione di dati personali;
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc.;
- la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità;
- la divulgazione non autorizzata dei dati personali.

L'Ente, in accordo con il Responsabile della Protezione dei Dati personali, “Grafiche E. Gaspari s.r.l.”, assume il presente modello organizzativo come documento di prevenzione e misura di sicurezza e risposta alle possibili perdite di sicurezza.

Il presente documento costituisce pertanto elemento avanzato di *compliance* al principio di responsabilizzazione del Titolare previsto dal Regolamento UE n. 679/2016, aggiuntivo ed eventuale rispetto alle misure di sicurezza cui il titolare è tenuto nello svolgimento dei propri trattamenti di dati personali.

## 2. Workflow autovalutativo del data breach

In tutti i casi in cui si sospetti una perdita di sicurezza che possa coinvolgere dati personali, oltre ad attivare tutte le altre forme di tutela previste dall'ordinamento occorre – per quanto concerne l'ambito esclusivo della privacy - porsi una serie di domande, che conducono a specifici comportamenti conformi ai principi del Regolamento UE n. 679/2016.

### **PRIMA DOMANDA**

**Si è verificato un incidente di sicurezza che ha comportato la perdita di riservatezza, integrità o disponibilità di dati?**

*Un incidente di sicurezza è un evento (o una serie di eventi) di origine dolosa o accidentale, esterno o interno all'organizzazione, che può comportare la compromissione dei dati detenuti da un'organizzazione, mettendo a rischio uno o più dei tre principi della sicurezza delle informazioni: riservatezza, integrità e disponibilità.*

*Un incidente di sicurezza può riguardare contemporaneamente la riservatezza, l'integrità o la disponibilità di dati e informazioni o consistere in una qualsiasi combinazione di esse.*

### **ESEMPI**

Un incidente di sicurezza può verificarsi, ad esempio, in seguito ad un attacco informatico, ad un comportamento umano illecito o accidentale, ad una catastrofe naturale, a un malfunzionamento hardware o software.

Si verifica:

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

**Se la risposta è "NO"** → non si è verificato un incidente di sicurezza - che ha comportato la perdita di riservatezza, integrità o disponibilità di dati - di conseguenza **non c'è stata una violazione dei dati personali**.

**Se la risposta è "Sì"** → occorre porsi la

## **SECONDA DOMANDA:**

### **L'incidente di sicurezza ha coinvolto dati personali?**

*Un **dato personale** è «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 online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale, o sociale» (cfr. art. 4, punto 1), del Regolamento (UE) 2016/679 e art. 2, comma 1, lett. a), del D.Lgs 51/2018).*

### **ESEMPI**

Sono dati personali tutte quelle informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc..

L'identificazione richiede elementi che permettono di distinguere una persona dalle altre. Il nome e il cognome, ad esempio, permettono di identificare una persona direttamente, mentre dati personali come il numero di telefono, il codice fiscale, l'indirizzo IP, la targa di un veicolo permettono di identificare una persona indirettamente.

Sono dati personali, ad esempio, i dati anagrafici (nome, cognome, data di nascita, luogo di nascita), i dati di contatto (indirizzo postale, indirizzo di posta elettronica, numero di telefono fisso o mobile), dati di accesso e di identificazione (username, password), dati di geolocalizzazione, dati di pagamento.

Specialmente delicati sono **dati appartenenti a categorie particolari** (cfr. art. 9 del Regolamento), e cioè dati personali idonei a rivelare 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 e i **dati personali relativi a condanne penali e reati** (cfr. art. 10 del Regolamento).

**Se la risposta è "NO"** → l'incidente di sicurezza non ha coinvolto dati personali pertanto **non c'è stata una violazione dei dati personali**

**Se la risposta è "Sì"** → **L'incidente di sicurezza occorso costituisce una violazione dei dati personali.**

Una **violazione dei dati personali** è una «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» (cfr. art. 4, punto 12), del Regolamento (UE) 2016/679 e art. 2, comma 1, lett. m), del D.Lgs 51/2018).

Una violazione dei dati personali (personal data breach o, più comunemente, data breach) è, infatti, un particolare tipo di incidente di sicurezza che, causando perdita di riservatezza, integrità o disponibilità dei **dati personali**, fa sì che il titolare del trattamento non sia più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali (cfr. art. 5 del Regolamento (UE) 2016/679 e art. 3 del D.Lgs 51/2018).

#### ESEMPI

Una violazione dei dati personali può consistere, ad esempio:

- nell'accesso ai dati personali da parte di terzi non autorizzati;
- nella perdita di riservatezza a seguito dell'invio di una mail contenente dati personali a un destinatario errato;
- nella perdita o furto di un dispositivo o di un supporto di memorizzazione contenente dati personali;
- nella perdita di disponibilità di dati personali archiviati in un database, ad esempio attraverso un ransomware;
- nella perdita di disponibilità dei dati personali se, ad esempio, tali dati sono stati accidentalmente cancellati in maniera definitiva o resi temporaneamente indisponibili a causa dell'interruzione di un servizio.

#### **CONTATTARE IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI**

A quel punto, in qualità di titolare del trattamento, occorrerà porsi insieme al RPD

#### TERZA DOMANDA:

**È probabile che la violazione presenti un rischio per i diritti e le libertà degli interessati?**

*Il rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale, per le persone fisiche i cui dati sono stati violati.*

*Il considerando 85 del Regolamento elenca alcuni danni che possono derivare da una violazione dei dati personali, quali ad esempio: la discriminazione, il furto o l'usurpazione di identità, perdite finanziarie, il pregiudizio alla reputazione, la perdita di riservatezza dei dati personali protetti da segreto professionale, la decifratura non autorizzata della pseudonimizzazione o qualsiasi altro danno economico o sociale significativo.*

*In caso di violazione dei dati personali « il titolare del trattamento notifica la violazione all'autorità di controllo [...] a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche » (cfr. art. 33, par. 1, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018).*

*La norma chiarisce che se è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche – cioè, è improbabile che dalla violazione possa derivare un impatto negativo per le persone fisiche e il titolare sia in grado di dimostrarlo - la violazione occorsa non è soggetta all'obbligo di notifica all'Autorità di controllo.*

**La valutazione del rischio derivante da una violazione dei dati personali, che deve tener conto della probabilità e della gravità del suo impatto sulle persone fisiche i cui dati sono stati coinvolti (cfr. considerando 75 e 76 del Regolamento), è un importante adempimento che, conformemente al principio di responsabilizzazione, spetta unicamente al titolare del trattamento e dalla quale deriva il corretto adempimento dell'obbligo di notifica della violazione all'autorità di controllo e dell'eventuale comunicazione della violazione agli interessati.**

Al fine di valutare il potenziale rischio per le persone fisiche, le “Linee guida” suggeriscono di considerare diversi fattori, tra cui:

- tipo di violazione;
- natura, carattere sensibile e volume dei dati personali;
- facilità di identificazione delle persone fisiche;
- gravità delle conseguenze per le persone fisiche;
- caratteristiche particolari dell'interessato;
- caratteristiche particolari del titolare del trattamento;
- numero di persone fisiche interessate.

#### ESEMPI

Violazioni (cfr. Linee guida, par. II, lett. D) che potrebbero non presentare rischi per gli interessati, e quindi non essere soggette all'obbligo di notifica all'Autorità di controllo, sono:

- la violazione di dati personali già disponibili pubblicamente, in quanto potrebbe risultare improbabile il verificarsi di un danno fisico per gli interessati conseguente alla divulgazione di dati personali già pubblici;
- la perdita o il furto di una chiavetta USB contenente dati personali crittografati (con algoritmo di crittografia all'avanguardia e chiave di decifrazione non sia compromessa), di cui è disponibile un backup che consente un integrale e tempestivo ripristino dei dati.

Infine, l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato «Raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione dei dati personali», che possono essere utili ai fini della valutazione del rischio.

**Se la risposta è “NO” → Non è necessario effettuare la notifica al Garante e la comunicazione agli interessati.**

**Tuttavia occorre DOCUMENTARE LA VIOLAZIONE.**

**Il titolare del trattamento deve documentare tutte le violazioni dei dati personali che si verificano**, indipendentemente dal fatto che una violazione debba o meno essere notificata al Garante.

«Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di verificare il rispetto del presente articolo» (cfr. art. 33, par. 5, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018).

L'obbligo del titolare di documentare tutte le violazioni è collegato al principio di responsabilizzazione (cfr. art. 5, par. 2, del Regolamento (UE) 2016/679 e art. 3, comma 4, del D.Lgs 51/2018) e agli obblighi del titolare del trattamento responsabilizzazione (cfr. art. 24 del Regolamento (UE) 2016/679 e art. 15 del D.Lgs 51/2018).

Il titolare del trattamento è incoraggiato a creare un registro interno delle violazioni occorse – notificate o meno – e il Garante può chiedere di consultare tale registro.

Oltre ad informazioni quali cause, fatti, dati personali, effetti e conseguenze della violazione, le Linee guida raccomandano di documentare anche il ragionamento alla base delle decisioni prese in risposta a una violazione, come, ad esempio, il perché una determinata violazione non è stata notificata al Garante.

**Se la risposta è SÌ → «Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la**

**violazione all'interessato senza ingiustificato ritardo»** (cfr. art. 34, par. 1, del Regolamento (UE) 2016/679 e art. 27 del D.Lgs 51/2018).

Le Linee guida (cfr. All. B) forniscono un elenco non esaustivo di tipi di violazioni che comportano un rischio elevato per le persone fisiche e, di conseguenza, in cui il titolare del trattamento deve comunicarla agli interessati.

Inoltre, nell'individuazione delle violazioni che possono presentare un rischio elevato per i diritti e le libertà della persone fisiche, è opportuno considerare anche le tipologie di trattamenti indicati nelle «Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679», adottate dal Gruppo di lavoro articolo 29 per la protezione dei dati il 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

In questo caso occorre porsi la

#### **QUARTA DOMANDA:**

**La violazione comporta un rischio elevato per gli interessati?**

**Se la risposta è "NO"** → Se ritieni che la violazione occorsa **non comporti un rischio elevato per gli interessati**, non è obbligatorio effettuare la comunicazione agli interessati.

«Nel caso in cui il 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 paragrafo 3 è soddisfatta» (cfr. art. 34, par. 4, del Regolamento (UE) 2016/679 e art. 27 del D.Lgs 51/2018).

#### **DEVI NOTIFICARE LA VIOLAZIONE AL GARANTE**

«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» (cfr. art. 33, par. 1, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018).

Le Linee guida chiariscono che il titolare del trattamento può considerarsi «a conoscenza della violazione» nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha comportato la compromissione di dati personali.

Inoltre, il titolare dovrebbe predisporre «misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato» (cfr. considerando 87 del Regolamento).

#### **CONTENUTO DELLA NOTIFICA**

La notifica deve contenere le informazioni previste all'art. 33, par. 3, del Regolamento (UE) 2016/679 e indicate nell'allegato al provvedimento del Garante del 30 luglio 2019 sulla notifica delle violazioni dei dati personali (doc. web n. 9126951).

In particolare, la notifica deve almeno:

- descrivere **la natura della violazione** occorsa compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali;

- comunicare il **nome** e **dati di contatto** del RPD o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le **probabili conseguenze della violazione dei dati personali**;
- descrivere le **misure adottate** o di cui si propone l'adozione **per porre rimedio alla violazione** e anche, se del caso, **per attenuare i possibili effetti negativi per gli interessati**

## NOTIFICA PER FASI

«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» (cfr. art. 33, par. 4, del Regolamento (UE) 2016/679).

In tal caso il titolare, al momento della notifica, deve indicare che si tratta di una notifica preliminare, impegnandosi a comunicare tutte le informazioni e i dettagli circa la violazione occorsa non appena disponibili e senza ingiustificato ritardo, attraverso una notifica integrativa.

**A partire dal 1° luglio 2021**, la notifica di una violazione di dati personali deve essere inviata al Garante tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo <https://servizi.gpdp.it/databreach/s/> (VEDI: [Provvedimento del 27 maggio 2021](#)).

Nella stessa pagina è disponibile un modello facsimile, da NON utilizzare per la notifica al Garante ma utile per vedere in anteprima i contenuti che andranno comunicati al Garante.

Prima di procedere attuare la presente valutazione e contattare in ogni caso il Responsabile della Protezione dei Dati personali.

## DEVI DOCUMENTARE LA VIOLAZIONE (vedi sopra)

**Se la risposta è "Sì" → DEVI NOTIFICARE LA VIOLAZIONE AL GARANTE (vedi sopra)**

Inoltre, il titolare del trattamento dovrebbe anche fornire **consulenza specifica** alle persone fisiche **sul modo in cui proteggersi** dalle possibili conseguenze negative della violazione. Ad esempio:

- in caso di compromissione delle credenziali di accesso, il titolare dovrebbe fornire anche la raccomandazione di non utilizzare più la password compromessa né una simile nonché di modificare la password utilizzata per l'accesso a qualsiasi altro servizio online qualora coincidente o simile a quella oggetto di violazione;
- in caso di compromissione di dati relativi a conti correnti bancari o strumenti di pagamento (quali carte di credito o debito), il titolare dovrebbe fornire la raccomandazione di monitorare le movimentazioni economiche e/o richiedere supporto al proprio istituto bancario/finanziario.

## COME CONTATTARE L'INTERESSATO

La violazione dovrebbe essere comunicata direttamente agli interessati coinvolti (ad esempio mediante messaggi di posta elettronica, SMS, comunicazione postale), a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile (ad esempio banner o notifiche su siti web di primo piano, pubblicità di rilievo sulla stampa) che permetta di informare gli interessati con analoga efficacia (cfr. art. 34, par. 3, lett. c), del Regolamento (UE) 2016/679).

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che **non devono essere inviati insieme ad altre informazioni**, quali newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

## DEVI DOCUMENTARE LA VIOLAZIONE

**Il titolare del trattamento deve documentare tutte le violazioni dei dati personali che si verificano**, indipendentemente dal fatto che una violazione debba o meno essere notificata al Garante.

«Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di verificare il rispetto del presente articolo» (cfr. art. 33, par. 5, del Regolamento (UE) 2016/679 e art. 26 del D.Lgs 51/2018).

L'obbligo del titolare di documentare tutte le violazioni è collegato al principio di responsabilizzazione (cfr. art. 5, par. 2, del Regolamento (UE) 2016/679 e art. 3, comma 4, del D.Lgs 51/2018) e agli obblighi del titolare del trattamento responsabilizzazione (cfr. art. 24 del Regolamento (UE) 2016/679 e art. 15 del D.Lgs 51/2018).

Il presente Ente poredisporrà all'evenienza un registro interno delle violazioni occorse – notificate o meno – nel caso in cui il Garante richieda di consultare tale registro.