



**GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI**




## **Violazioni di dati personali (Data Breach)**

### **Violazioni di dati personali (data breach), in base alle previsioni del Regolamento (UE) 2016/679**

La pagina contiene link alla normativa e a documenti interpretativi, schede informative e pagine tematiche,  
ed è in continuo aggiornamento.

**[IL SERVIZIO TELEMATICO DEDICATO AL DATABRECH](#)**

**Notifica di una violazione dei dati personali (data breach)**  
 art. 33 del Regolamento (UE) 2016/679 - art. 26 del D.Lgs. 51/2018

<p>PAGINA INFORMATIVA - VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)</p> 	<p>AUTO VALUTAZIONE (SELF ASSESSMENT) PER LA NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)</p> 	<p>VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) - MODELLO DI NOTIFICA AL GARANTE</p> 
---	--	---

**GDPDP** | GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## COSA È UNA VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)?\*

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:

- 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.

## COSA FARE IN CASO DI VIOLAZIONE DEI DATI PERSONALI?

Il titolare del trattamento (soggetto pubblico, impresa, associazione, partito, professionista, ecc.) **senza ingiustificato ritardo** e, ove possibile, **entro 72 ore dal momento in cui ne è venuto a conoscenza**, deve notificare la violazione al Garante per la protezione dei dati personali a meno che sia **improbabile** che la violazione dei dati personali comporti un **rischio** per i diritti e le libertà delle persone fisiche.

Il responsabile del trattamento che viene a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il titolare in modo che possa attivarsi.

**Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.**

Inoltre, se la violazione comporta un rischio elevato per i diritti delle persone, il titolare deve comunicarla a tutti gli interessati, utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurre l'impatto.

Il titolare del trattamento, a prescindere dalla notifica al Garante, **documenta** tutte le violazioni dei dati personali,

ad esempio predisponendo un apposito registro. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.

## CHE TIPO DI VIOLAZIONI DI DATI PERSONALI VANNO NOTIFICATE?

Vanno notificate unicamente le violazioni di dati personali che possono avere **effetti avversi significativi** sugli individui, causando danni fisici, materiali o immateriali.

Ciò può includere, ad esempio, la perdita del controllo sui propri dati personali, la limitazione di alcuni diritti, la discriminazione, il furto d'identità o il rischio di frode, la perdita di riservatezza dei dati personali protetti dal segreto professionale, una perdita finanziaria, un danno alla reputazione e qualsiasi altro significativo svantaggio economico o sociale.

## CHE INFORMAZIONI DEVE CONTENERE LA NOTIFICA AL GARANTE? <sup>\*\*</sup>

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 \(doc. web n. 9126951\)](#).

Qualora si utilizzi per la notifica il [modello allegato al provvedimento](#), è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione.

## COME INVIARE LA NOTIFICA AL GARANTE?

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo [protocollo@pec.gpdp.it](mailto:protocollo@pec.gpdp.it) <sup>\*\*\*</sup> oppure tramite posta elettronica ordinaria all'indirizzo [protocollo@gpdp.it](mailto:protocollo@gpdp.it) e deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale) ovvero con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.

L'oggetto del messaggio deve contenere obbligatoriamente la dicitura **"NOTIFICA VIOLAZIONE DATI PERSONALI"** e opzionalmente la denominazione del titolare del trattamento.

Per semplificare gli adempimenti previsti per i titolari del trattamento, il Garante ha ideato e messo disposizione un apposito [strumento di autovalutazione \(self assessment\)](#) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

## LE AZIONI DEL GARANTE

Il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

*\* La scheda ha mero valore divulgativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento (UE) 2016/679.*

*\*\* Il Garante renderà prossimamente disponibile una procedura online.*

*\*\*\* Questo indirizzo è configurato per ricevere SOLO comunicazioni provenienti da posta elettronica certificata*

## **LINEE GUIDA**

### **Linee guida in materia di notifica delle violazioni di dati personali (data breach notification) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679**

Adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017  
Versione emendata e adottata il 6 febbraio 2018

### **Linee guida 01/2021 sugli esempi riguardanti la notifica di violazione dei dati**

Adottate da EDPB il 14 gennaio 2021  
In consultazione pubblica

## **APPROFONDIMENTI**

- [Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali - Approccio basato sul rischio del trattamento e misure di accountability di titolari e responsabili](#)

- VIDEO - [Sicurezza, minimizzazione dei rischi e data breach](#) - Intervento tenuto nel corso dell'[incontro "Regolamento UE. Il Garante per la protezione dei dati personali incontra la PA"](#) (tappa di Bari, 15 gennaio 2018)