VIOLAZIONI DI DATI PERSONALI (DATA BREACH), IN BASE ALLE PREVISIONI DEL REGOLAMENTO (UE) 2016/679

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 indebiti ritardi** e, ove possibile, **entro 72 ore dalla scoperta**, 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 ridurne 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?

La notifica deve contenere almeno le informazioni sinteticamente riportate in questa pagina (art. 33, par. 3 del Regolamento (UE) 2016/679):

- ✓ una descrizione della natura della violazione dei dati personali, che comprenda, se possibile:
  a) le categorie e il numero approssimativo di persone interessate;
  b) le categorie e il volume approssimativo di dati personali interessati;
- ✓ il nome e i riferimenti di contatto del responsabile della protezione dei dati (se designato dal titolare) o comunque di un referente competente a fornire informazioni;
- ✓ una descrizione delle possibili conseguenze della violazione dei dati personali;
- ✓ una descrizione delle misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi;
- ✓ **SOLO in caso di notifica effettuata oltre il termine prescritto di 72 ore**, una descrizione dei motivi del ritardo.

La notifica va trasmessa al Garante per la protezione dei dati personali, inviandola all'indirizzo: **protocollo@pec.gpdp.it**

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**.