VIOLAZIONI DI DATI PERSONALI ("DATA BREACH")

Cosa fare in caso di Data Breach? Di seguito un Vademecum

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

Una violazione della 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 sono:

- 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 Designato/Autorizzato/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, 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 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)**, meglio spiegate in seguito.

COME INVIARE LA NOTIFICA AL GARANTE?

La notifica deve essere inviata al Garante tramite posta elettronica certificata all'indirizzo **protocollo@pec.gpdp.it** oppure tramite posta elettronica ordinaria all'indirizzo **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.

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**.

VADEMECUM

Vediamo "Step by Step" come bisogna comportarsi in caso di violazione:

Una volta accertata la violazione dei dati personali, il Titolare del trattamento (sia esso un soggetto pubblico, un'azienda, un'associazione, un professionista, un partito politico) è tenuto a notificare (***attraverso il modello allegato***)[1] velocemente l'accaduto al Garante, cioè entro 72 ore dal momento in cui ne è venuto a conoscenza. Quando a venire a conoscenza della violazione è un altro soggetto (Designato/Autorizzati/Responsabile), questi deve tempestivamente comunicarlo al Titolare, così che possa a sua volta segnalarlo al Garante. ****Questo attraverso il modello allegato[2], che deve essere pubblicato sulla sezione "Privacy" del sito e divulgato all'interno dell'Ente a tutto il personale dipendente.***

La segnalazione al Garante può essere tralasciata solo nel caso in cui sia improbabile che tale violazione comporti un rischio per i diritti e le libertà delle persone fisiche. In caso contrario, se cioè la violazione comporta un rischio elevato per i diritti degli interessati e non sono state già prese adeguate misure che ne riducano l'impatto, il Titolare deve comunicarla anche a loro (agli Interessati), utilizzando i canali più idonei (se il numero dei soggetti coinvolti non è elevato si utilizza il modello allegato)[3]. Nel caso il numero sia elevato, dovrà essere comunicata attraverso altri canali (pubblicazione riviste, quotidiani, sito web, ecc).

[1] Allegato 1_Modello segnalazione Data Breach al Garante;
[2] Allegato 2_Modello segnalazione interna Data Breach;
[3] Allegato 3_Modello segnalazione Data Breach agli interessati;

Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo. Non solo, il Titolare del trattamento deve documentare (attraverso il Registro Data Breach allegato)[4] tutte le violazioni dei dati personali di cui è a conoscenza, così che le Autorità, in caso di controlli, possano effettuare le verifiche necessarie sul rispetto della normativa.

Che elementi deve contenere la notifica al Garante

Attraverso un modello allegato, il Garante indica ed individua le informazioni da fornire nella notifica del Data Breach. L'obiettivo è quello di semplificare il lavoro del Titolare e favorire, da parte sua, il corretto adempimento degli obblighi in materia di trattamento dei dati personali.

Il documento di notifica deve essere il più possibile completo e le informazioni fornite devono essere riassunte per sezioni. Anche se il quadro informativo fosse incompleto, la notifica va comunque mandata, con riserva di inviare una seconda notifica ad integrazione della prima. Ecco, qui di seguito, come deve essere costruita la suddivisione in sezioni e cosa devono contenere:

Sez. A – la notifica

• tipologia della notifica

• dati del soggetto che effettua la notifica

Sez. B – il Titolare del trattamento

– dati del Titolare del trattamento

– dati di contatto per informazioni relative alla violazione

– dati di ulteriori soggetti coinvolti nel trattamento

Sez. C – informazioni di sintesi sulla violazione

- quando è avvenuta la violazione

– momento in cui il titolare del trattamento è venuto a conoscenza della violazione

• modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione

[4] Allegato 4_Registro Data Breach;

• in caso di notifica oltre le 72 ore, quali sono i motivi del ritardo

• breve descrizione della violazione

• natura della violazione

• causa della violazione

• categorie di dati personali oggetto di violazione

• volume (anche approssimativo) dei dati personali oggetto di violazione

• categorie di interessati coinvolti nella violazione

• numero (anche approssimativo) di interessati coinvolti nella violazione

Sez. D – informazioni di dettaglio sulla violazione

• descrizione dell'incidente di sicurezza alla base della violazione

• descrizione delle categorie di dati personali oggetto della violazione

• descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione

• misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti

Sez. E – possibili conseguenze e gravità della violazione

• possibili conseguenze della violazione sugli interessati, in caso di perdita di confidenzialità, in caso di perdita di integrità, in caso di perdita di disponibilità

• ulteriori considerazioni sulle possibili conseguenze

• potenziali effetti negativi per gli interessati

• stima della gravità della violazione indicandone le motivazioni

Sez. F – misure adottate a seguito della violazione

– misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati

– misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future

Sez. G – comunicazione agli interessati

• la violazione è stata comunicata agli interessati?

• numero di interessati a cui è stata comunicata la violazione

• contenuto della comunicazione agli interessati

• canale utilizzato per la comunicazione agli interessati

Sez. H: altre eventuali informazioni

• la violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo? Se sì indicare quali

• la violazione coinvolge interessati di Paesi non appartenenti allo Spazio

Economico Europeo? Se si indicare quali

• la violazione è stata notificata ad altre autorità di controllo? Se si indicare quali

• la violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative? Se sì indicare quali

• è stata effettuata una segnalazione all'autorità giudiziaria o di polizia?

Data Protection Officer
Dott. Pasquale Nicolazzo