VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

Art. 4, n. 12, Regolamento (UE) 2016/679

E' la 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.

AZIONI DA INTRAPRENDERE

1) **Notifica** della violazione all'autorità di controllo al più tardi entro 72 ore dalla conoscenza della violazione. L'eventuale ritardo deve essere motivato.

Eccezione alla notifica: **è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche** (ad esempio, perché sono state previamente attuate misure quali la criptazione o la pseudonimizzazione dei dati).

CONTENUTI DELLA NOTIFICA

- la natura della violazione dei dati personali (anche le categorie ed il numero approssimativo di interessati nonché le categorie ed il numero approssimativo di registrazioni di dati personali);

- i riferimenti del DPO o di altro referente dal quale avere informazioni;

- le probabili conseguenze della violazione;

- le misure adottate o proposte per rimediare alla violazione ed attenuarne gli effetti.

E’ necessario documentare e tenere traccia di tutte le violazioni di dati, anche al fine di consentire la verifica, in sede di eventuale ispezione, in merito alle procedure adottate dall’azienda.

Ad esempio, nel Registro per le attività di trattamento

AZIONI DA INTRAPRENDERE

2) **Comunicazione** della violazione all'interessato, qualora la violazione medesima sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

LINEE GUIDA 3 OTTOBRE 2017 SULLA VIOLAZIONE DEI DATI PERSONALI (WORKING PARTY 29)

- Danno la definizione di violazione dei dati personali;

- forniscono esempi di violazioni di dati;

- specificano i contenuti delle notifiche e delle comunicazioni da effettuare in caso di violazione dei dati;

- identificano fattori per facilitare l'individuazione del tipo di violazione e del livello di rischio che ne è scaturito.

ALCUNI CASI DI VIOLAZIONE DI DATI ESAMINATI DAL GARANTE

DOSSIER SANITARIO ELETTRONICO

Provvedimento n. 331/2015

Entro **48 ore** dalla conoscenza del fatto, le strutture sanitarie pubbliche e private sono tenute a comunicare al Garante – tramite l'apposito modello allegato al provvedimento – tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

BIOMETRIA

Provvedimento n. 513/2014

Entro **24 ore** dalla conoscenza del fatto, i titolari del trattamento (aziende, amministrazioni pubbliche, ecc.) sono tenuti a comunicare al Garante – tramite l'apposito modello allegato al provvedimento – tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui sistemi biometrici installati o sui dati personali custoditi.

SOCIETA' TELEFONICHE E INTERNET PROVIDER

Provvedimento n. 161/2013

- Entro **24 ore** dalla scoperta dell'evento, devono fornire al Garante le informazioni necessarie a consentire una prima valutazione dell'entità della violazione;

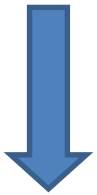
- entro **3 giorni** dalla scoperta, devono informare anche ciascun utente coinvolto;

- devono tenere un inventario costantemente aggiornato delle violazioni subìte.

LE SANZIONI ED IL RISARCIMENTO DEL DANNO

Le sanzioni devono essere **effettive, proporzionate e dissuasive.**

Le autorità di controllo possono infliggere sanzioni amministrative, svolgere attività ispettiva, indicare condizioni alle quali i titolari devono attenersi nel trattamento dei dati o persino vietarlo.



Misure di cui all'art. 58 Regolamento contestuali o alternative alle sanzioni amministrative (Ad esempio, rivolgere avvertimenti e ammonimenti, ingiungere di conformare i trattamenti alle disposizioni regolamentari, ingiungere di comunicare all'interessato una violazione di dati, imporre una limitazione provvisoria o definitiva del trattamento, ecc.).

LINEE GUIDA 3 OTTOBRE 2017 RIGUARDANTI L'APPLICAZIONE E LA PREVISIONE DELLE SANZIONI AMMINISTRATIVE PECUNIARIE (WORKING PARTY 29)

- Si tratta di un documento destinato soprattutto alle autorità di controllo nazionali per garantire una migliore applicazione e attuazione del regolamento;

- forniscono l'interpretazione delle disposizioni regolamentari in materia di sanzioni;

- identificano e precisano il contenuto dei criteri che la autorità di controllo devono utilizzare per valutare l'opportunità di una sanzione amministrativa e la sua misura.

Elementi di cui l'Autorità di controllo tiene conto al momento di decidere se infliggere una sanzione amministrativa

- la natura, la gravità e la durata della violazione;

- il carattere doloso o colposo della violazione;

- le misure adottate dal titolare o dal responsabile del trattamento per attenuare il danno per gli interessati ed il loro grado di responsabilità, tenuto conto delle misure organizzative messe in atto;

- eventuali precedenti violazioni;

- il grado di cooperazione con l'autorità di controllo

Elementi di cui l'Autorità di controllo tiene conto al momento di decidere se infliggere una sanzione amministrativa

- le categorie di dati personali;

- il modo in cui l'Autorità ha appreso della violazione;

- il rispetto di eventuali precedenti provvedimenti emanati ai sensi dell'art. 58 Regolamento;

- l'adesione a codici di condotta o a meccanismi di certificazione;

- eventuali altri fattori aggravanti o attenuanti.

L'entità delle sanzioni amministrative

Al momento sono previsti solo gli importi nel massimo.

Ad esempio, per la mancata notifica di una violazione di dati o l'omessa adozione del Registro per le attività di trattamento: sino a 10 milioni di euro o al 2% del fatturato mondiale di gruppo.

Per la violazione delle condizioni relative al consenso o dei diritti degli interessati: sino a 20 milioni di euro o al 4% del fatturato mondiale di gruppo.

E' comunque sempre salva la facoltà di agire giudizialmente in via ordinaria o d'urgenza da parte di chi subisca un danno provocato da una violazione del Regolamento.

Ed i provvedimenti sanzionatori di natura penale?

Gli Stati membri hanno facoltà di introdurre altre sanzioni.

Legge Delega 21 novembre 2017 – principi e criteri direttivi specifici:

"adeguare, nell'ambito delle modifiche al codice di cui al decreto legislativo 30 giugno 2003, n. 196, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del regolamento (UE) 2016/679 con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse".