

Un caso di *Data Breach*:

- la responsabilità in materia di trattamento dei dati personali e il risarcimento del danno;
- il nuovo regime sanzionatorio;
- accorgimenti operativi.

Avv. Paola Pucci Partner - DPO

spp@toffolettodeluca.it

»» 14 novembre 2017 - Confindustria Bergamo

IL DATA BREACH/LA VIOLAZIONE DEI DATI

Per “**violazione dei dati**” o “***data breach***” si intende qualsiasi 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.

- **per distruzione si intende che i dati non esistono più:** ad es. sono conservati soltanto in cartaceo e i relativi documenti sono bruciati;
- **per perdita si intende che il titolare dei dati non ha più accesso, anche temporaneamente, ai dati:** ad es. i dati sono soltanto su supporti informatici e i relativi server non sono accessibili per problemi tecnici;
- **per modifica, divulgazione o accesso non autorizzati si intendono operazione di alterazione dei dati o semplice consultazione degli stessi o, ancora, comunicazione a terzi da parte di soggetti non autorizzati.** È il classico caso dell'hacker che penetra in un sistema e modifica i dati o li rende noti al pubblico.

IL NUOVO REGOLAMENTO

La nuova procedura prevista, con efficacia dal 25 maggio 2018, in caso di violazione di dati personali (***Data Breach***) dal Regolamento è destinata a rappresentare una **sfida** per tutte le aziende: per adempiere correttamente alle nuove obbligazioni sarà necessario aver posto in essere **tutte le misure richieste dalla norma** in termini di **prevenzione, preparazione, struttura e gestione**.

LE LINEE GUIDA

Il tema è ritenuto centrale anche dagli stessi organi dell'Unione: il 3 ottobre 2017 il *Working Party 29* ha emanato delle **linee guida sul data breach**. Le linee guida sono fondamentali per una corretta comprensione degli adempimenti da porre in essere.

Nello specifico le linee guida sul data breach si occupano, tra l'altro, di:

- ▶ spiegare, anche attraverso esemplificazioni, concetti alla base della norma come il *data breach* e la conoscenza dello stesso;
- ▶ meglio identificare i contenuti delle comunicazioni previste dalla norma e i soggetti a cui la stessa, a seconda dei casi, vada inviata;
- ▶ individuare dei fattori specifici attraverso i quali è possibile identificare il tipo ed il livello di rischio generati dal *breach*.

IL CASO

IL CASO

Un *data breach* può nascere da qualsiasi avvenimento e colpire qualsiasi azienda: non è necessario essere vittime di un *hacker* perché la procedura debba essere attivata.

Il Direttore finanziario di una società ha lasciato il personal computer nell'auto parcheggiata al supermercato. L'auto viene rubata insieme al suo contenuto.

All'interno del pc sono presenti le seguenti informazioni:

- ▶ elenco dipendenti con relativa anagrafica, dati retributivi, fiscali e bancari nonché eventuali disabilità;
- ▶ elenco clienti con tutte le necessarie informazioni, anche relative alla loro solvibilità.

CHE FARE?

IL CASO

N.B. Dal momento della conoscenza del *breach*, comunque realizzata, scattano le 72 ore per le comunicazioni. Dovranno essere svolte, con la massima celerità, le seguenti azioni:

PRIMO PASSO

- Stabilite **le cause e la portata della violazione**. Le domande da porsi in tale fase includono: che **tipo di dati** sono coinvolti? Sono dati sensibili e quanto? Vi erano delle misure di protezione? **Cosa è accaduto ai dati**? Che cosa potrebbero **rivelare i dati ai terzi** circa i soggetti cui gli stessi ineriscono? Che danno potrebbero ricevere?
- Attivate il vostro **team aziendale** e **mettete in atto la vostra policy per le violazioni privacy**.

IL CASO

La comunicazione richiesta dalla norma presuppone l'invio di **informazioni chiare e complete**. Nessuna di tali informazioni può essere fornita se il titolare non ha organizzato la sua struttura in modo da conoscere i trattamenti effettuati. Ad esempio:

- **il tipo di dati coinvolti:** è necessario aver previamente identificato e separato tutti i trattamenti;
- **la natura della violazione:** è necessario aver previamente implementato un sistema di sicurezza in grado di riconoscere e delimitare tempestivamente l'incidente.

Per essere sicuri di adempiere agli obblighi previsti dalla norma in caso di *data breach*, dunque, è necessario ripensare e ridefinire tutti i processi aziendali coinvolti.

IL CASO - CONOSCERE I DATI

Solo se avrete svolto un audit sui dati potrete sapere quali dati sono stati violati. Solo se avete un team dedicato e una policy potrete reagire tempestivamente.

- È difficile sapere che dati avete perso se, come prima cosa, non sapete che dati trattate. Compilate un **inventario** dei dati trattati e tenetelo aggiornato;
- Una volta che conoscete i dati trattati, identificate le **finalità** del trattamento e l'origine dei dati. Siete titolari o responsabili?
- Identificate dove e come **conservate** i dati. La vostra resistenza alle violazioni coincide con quella dell'anello più debole, pertanto non dimenticate di revisionare gli accordi con i fornitori esterni;
- Se non avete già uno, create e implementate una **policy** per la conservazione dei dati per essere sicuri che conserviate solo ciò che è necessario;
- Considerate di svolgere un **audit** sul trattamento dei dati e sulla sicurezza informatica per identificare potenziali problemi e risolverli prima che vi sia una violazione.

IL CASO - IL *TEAM* DEDICATO

È necessaria la creazione di un apposito *team* per la gestione dei *breach*. Il *team* dovrà avere un responsabile che implementerà il progetto. Il responsabile formerà il *team* includendo:

- membri interni che rivestono ruoli di vertice dell'azienda. Dovrebbero essere anche identificati dei sostituti per ciascun ruolo (per il caso di assenza);
- fornitori esterni: investigatori forensi, esperti di pubbliche relazioni, assicuratori, avvocati, fornitori di servizi di ripristino e di emergenza.

IL CASO - LA POLICY

La *policy*, in genere, dovrà riportare:

- il nome del Responsabile;
- l'indicazione dei membri sia interni che esterni del *team* e i rispettivi ruoli;
- i contatti (con reperibilità possibilmente anche al di fuori dell'orario di lavoro);
- le procedure da seguire nel caso di scoperta di una violazione o di sospetto;
- le azioni fondamentali da intraprendere durante e dopo la violazione;
- le tempistiche per completare le azioni;
- i *template* per attività di relazione e riporto, incluse possibili comunicazioni interne ed esterne.

IL CASO

SECONDO PASSO

Completato il primo passo, dovrete avere tutte le informazioni rilevanti ed essere pronti per **compilare ed inviare le comunicazioni**.

Non tutti i dati raccolti grazie all'attivazione del *team* dedicato e alle investigazioni svolte devono necessariamente essere comunicati.

È necessario anche decidere cosa comunicare e come.

La creazione di template di comunicazione potrebbe aiutare.

Le comunicazioni vanno inviate:

- all'autorità di controllo;
- ai soggetti interessati, laddove una violazione dei dati personali potrebbe probabilmente determinare un elevato rischio per i diritti e le libertà della persona;
- alle forze dell'ordine qualora integri reato;
- a eventuali soggetti terzi, in virtù di accordi contrattuali che lo prevedano.

IL CASO

Una volta comunicata, **la violazione è di pubblico dominio**: a seconda della sua rilevanza potrebbe arrivare sui **social**, sui **forum** o addirittura sui **giornali**.

In questo caso è fondamentale attivare i propri **esperti di comunicazione** per mitigare i rischi in termini di **reputazione** e pubblicità negativa.

Inoltre, potrebbe essere necessario attivare i **legali dell'azienda** per capire come **difendersi da eventuali richieste di risarcimento del danno**.

IL CASO

Una volta individuate le cause del *breach*, è possibile porvi rimedio.

MA LE AZIONI DA COMPIERE NON SONO FINITE.

Sarà infatti necessario porre in essere azioni per **evitare il ripetersi dell'evento**. Nel nostro esempio, la **criptazione dei dati a monte** avrebbe certamente evitato il *breach*.

Ancora, è possibile introdurre la **pseudonimizzazione dei dati** o **bloccare le porte in uscita** dei computer aziendali.

IL CASO

Infine: di tutte le violazioni dei dati sarà necessario tenere traccia, anche al fine di permettere la verifica da parte degli ispettori sulle procedure adottate dall'azienda.

A tal fine è possibile utilizzare un registro specifico ma, vista anche la raccomandazione del Garante italiano a tutte le aziende di utilizzare il **Registro per le attività di trattamento** indipendentemente dal personale impiegato, si potrà registrare tutto in apposita sezione di questo Registro.

LE SANZIONI E IL RISARCIMENTO DEL DANNO

LE SANZIONI

Nessuno può permettersi di perdere questa sfida

Non solo le **sanzioni** amministrative per la violazione possono arrivare a **20 MLN di Euro** (o al 4% del fatturato mondiale di Gruppo) ma la violazione dei dati è suscettibile di determinare **ulteriori danni**:

- possibili **risarcimenti per gli individui coinvolti** (tanto maggiori quanto saranno numerosi i dati violati e i soggetti interessati);
- danni alla reputazione dei titolari ed alla pubblicità negativa, con **probabile perdita di clientela** o comunque di affidabilità.

LE SANZIONI

L'autorità di controllo gode di **rilevantissimi poteri in merito ai trattamenti non conformi alle disposizioni del GDPR**: può svolgere **ispezioni, indicare condizioni** alle quali i titolari devono attenersi per proseguire il trattamento o, addirittura, **vietarlo**.

Al momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso si tiene conto di alcuni elementi, tra i quali:

- la natura, la gravità e la durata della violazione;
- il carattere doloso o colposo della stessa;
- le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
- eventuali precedenti violazioni e il grado di collaborazione con l'autorità di controllo;
- eventuali ulteriori fattori aggravanti o attenuanti applicabili.

LE SANZIONI

Per le **violazioni più lievi** (ad es. la mancata adozione del Registro per le attività di trattamento) sono previste sanzioni nel massimo pari alla cifra più alta **tra 10 milioni di Euro e il 2% del fatturato mondiale di gruppo**. Per le **violazioni più gravi** (ad es. la mancanza di informativa sul trattamento) sono previste sanzioni nel massimo pari alla cifra più alta **tra 20 milioni di Euro e il 4% del fatturato mondiale di gruppo**.

Al momento **non vi sono indicazioni** sull'entità delle singole sanzioni che verranno applicate a ciascuna violazione: **le attuali sanzioni possono comunque rappresentare una valida indicazione**.

IL RISARCIMENTO DEL DANNO

Chiunque subisca un danno materiale o immateriale causato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.

L'onere di dimostrare che il danno non è in alcun modo imputabile al titolare o al responsabile è in capo agli stessi.

LE SANZIONI

...E le sanzioni penali?

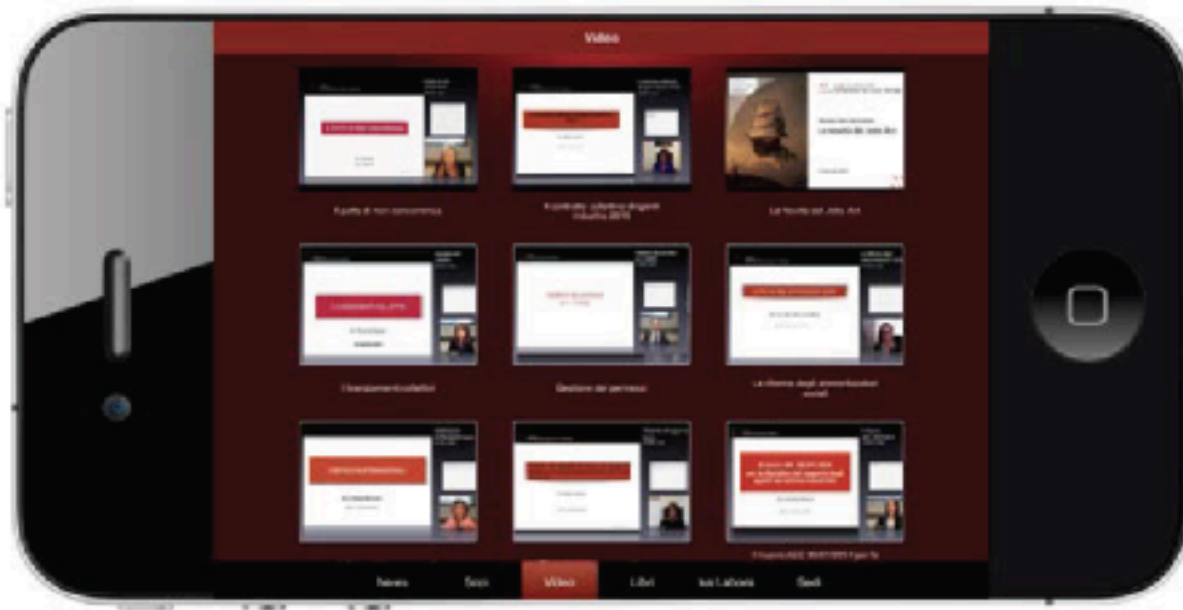
Per i singoli Stati membri resta comunque la possibilità di introdurre **ulteriori sanzioni**: al momento il Legislatore italiano non ha dato indicazioni e anche la sopravvivenza delle **sanzioni penali** previste dall'attuale Codice privacy è **dubbia, ma non è esclusa**.

Altrettanto dubbia è l'applicabilità delle sanzioni penali previste per le violazioni degli artt. 4 e 8 dello Statuto dei Lavoratori, poiché la previsione è contenuta nel Codice della Privacy, che sarà abrogato.

SERVIZI DIGITALI PER I NOSTRI CLIENTI

La nostra App

Attraverso l'APP scaricabile dall'App Store di Apple è possibile essere **costantemente aggiornati** sui temi di diritto del lavoro e sulle iniziative dello Studio. La APP offre informazioni in tempo reale sotto forma di news, tutti i video dei web seminar e tutte le nostre pubblicazioni.



GRAZIE

Milano

Via Rovello, 12
Milano - 20121
Tel. (+39) 02 721441
Fax (+39) 02 72144500

Napoli

Viale Antonio Gramsci, 14
Napoli - 80122
Tel. (+39) 081 684771
Fax (+39) 081 7614453

Roma

Piazza Cavour, 19
Roma - 00193
Tel (+39) 06 95550765
Fax(+39) 06 95550766

Bergamo

Via XX Settembre, 18/b
Bergamo - 24122
Tel. (+39) 02 721441
Fax (+39) 02 72144500

*La presentazione ha solo uno scopo formativo e didattico e non rappresenta un parere legale.
Lo studio nega ogni responsabilità per l'uso che dovesse esserne fatto senza coinvolgimento dei propri soci.*

North America: Canada - Mexico - United States

Central & South America: Argentina - Brazil - Chile - Colombia - Panama - Peru

Western Europe: Austria - Belgium - Cyprus - Denmark - Finland - France - Germany - Greece - Ireland - Italy
Luxembourg - Netherlands - Norway - Portugal - Spain - Sweden - Switzerland - United Kingdom

Eastern Europe: Belarus - Czech Republic - Estonia - Hungary - Latvia - Lithuania - Poland - Romania - Russia - Slovakia - Turkey - Ukraine

Middle East & Asia Pacific: China - India - Israel - Japan - Kazakhstan - Korea, Republic of - New Zealand - Singapore - United Arab Emirates