14. DATA BREACH

14.1. PREMESSA

L'art. 4, comma 12, Reg. UE generale sul trattamento dei dati personali 2016/679 (il "GDPR") definisce la **violazione dei dati personali** (o *data breach*) come "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".
Si deve in primo luogo evidenziare come un *data breach* sia un tipo di **incidente di sicurezza** avente ad oggetto dati personali, la cui immediata conseguenza consiste nel fatto che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento, come stabiliti dall'art. 5 GDPR Come evidenziato dal Gruppo di lavoro ex art. 29 nelle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Reg. UE 2016/679 - nella versione emendata ed adottata in data 06/02/2018 - "mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali".
Quando si verifica un *data breach*, i dati personali, protetti o riservati, vengono dunque consultati o copiati o trasmessi o rubati o comunque utilizzati da uno o più soggetti non autorizzati.
In particolare, come specificato dal Gruppo di lavoro *ex* art. 29, un *data breach* può essere classificato sulla base dei seguenti **principi sulla sicurezza** delle informazioni, potendo consistere in una:
- "**violazione della riservatezza**", qualora i dati personali vengano divulgati o siano oggetto di accessi non autorizzati o accidentali;
- "**violazione della disponibilità**", in caso di perdita, distruzione o accesso accidentali o abusivi ai dati personali;
- "**violazione dell'integrità**", laddove i dati personali siano oggetto di modifiche non autorizzate o accidentali.

Va altresì osservato che, a seconda dei casi, **una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali**, nonché qualsiasi combinazione delle stesse.

Una delle componenti fondamentali della "disponibilità" è l'accesso. In tal senso, si veda il documento NIST SP800-53rev4, che definisce la disponibilità come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", nonché la norma ISO/IEC 27000:2016, che definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato".

Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è relativamente evidente, può essere meno ovvio determinare se vi è stata una violazione della disponibilità.

Esempi
Esempi di perdita di disponibilità possono aversi quando i dati vengono cancellati accidentalmente o da una persona non autorizzata, oppure, in caso di dati crittografati in maniera sicura, quando la chiave di decifratura viene persa. Se il titolare del trattamento non è in grado di ripristinare l'accesso ai dati, ad esempio ricorrendo a un backup, la perdita di disponibilità sarà considerata perma-

nente. Allo stesso modo, può verificarsi una perdita di disponibilità anche in caso di interruzione di corrente o attacco da blocco di servizio (denial of service) che rende i dati personali indisponibili.

Sebbene una perdita di disponibilità dei sistemi del titolare del trattamento possa essere solo temporanea e non avere un impatto sulle persone fisiche, è importante che il titolare del trattamento consideri tutte le **possibili conseguenze della violazione**, poiché quest'ultima potrebbe comunque dover essere segnalata per i motivi che saranno analizzati nel proseguio.

Esempi

Elenco di **esempi di *data breach* maggiormente ricorrenti**:

- la perdita o furto di documenti contenenti dati personali o di dispositivi (es. dispositivi mobili, computer, tablet, ecc.) della società o personali contenenti dati personali;
- accesso non autorizzato dall'interno o dall'esterno della rete della società (es. hacking) od ogni altra violazione dei sistemi IT che potrebbe determinare la perdita, la compromissione, l'accesso o la divulgazione delle informazioni della società;
- installazione di software malevolo o virus scaricato sui dispositivi forniti dalla società;
- informazioni cartacee o elettroniche della società inviate al di fuori dell'azienda che non giungano al destinatario voluto o che siano recapitate a un destinatario non voluto;
- violazione dei controlli obbligatori di sicurezza delle informazioni che potrebbe comportare la perdita o la compromissione delle informazioni della società;
- diffusione non sicura delle informazioni della Società che sono state classificate come interne, confidenziali o segrete.

GLI ELEMENTI DELLA VIOLAZIONE E CRITERI PER DETERMINARE L'EFFETTIVA CONOSCENZA 14.2.

Il GDPR impone al titolare del trattamento di **notificare una violazione senza ingiustificato ritardo** e, ove possibile, **entro 72 ore** dal momento in cui ne è venuto a conoscenza.

Momento della conoscenza 14.2.1.

Questo solleva la questione relativa al momento in cui il titolare del trattamento può considerarsi "a conoscenza" di una violazione. Il Gruppo di lavoro ritiene che ciò avvenga nel momento in cui "è **ragionevolmente certo** che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali" (Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, del Gruppo di lavoro *ex* art. 29, p. 4 ss.).

Il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione **dipenderà dalle circostanze della violazione**. In alcuni casi, sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi.

Un esempio di evidente conoscenza si verifica quando un terzo soggetto informa il titolare del trattamento di aver ricevuto accidentalmente i dati personali di uno dei suoi clienti e fornisce la prova della divulgazione non autorizzata. Dato che al titolare del trattamento è stata presentata una prova evidente di una violazione della riservatezza, non vi è dubbio che ne sia venuto "a conoscenza".

Al contrario, in caso di smarrimento temporaneo di un hard disk contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati.

Periodo di indagine 14.2.2.

Durante il periodo di indagine **il titolare del trattamento non può essere considerato "a conoscenza"**. Tuttavia, si prevede che l'indagine inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione. Ciò implica che se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, l'evento andrà notificato, qualora sussista una ragionevole certezza del fatto che si è verificata una violazione della disponibilità.

OBBLIGHI DI NOTIFICA 14.3.

Le norme in tema di *data breach* mirano a realizzare gli obiettivi di tutela rispetto agli interessati mediante un intervento che si articola in una triplice direzione:

- da un lato, la previsione a carico dei titolari di specifici **obblighi di comunicazione**;
- dall'altro, l'**obbligo di conservare un inventario delle violazioni** di dati personali;
- da un altro ancora, l'attribuzione al Garante Privacy di congrui **poteri di vigilanza e sanzionatori**.

14.3.1. Comunicazione

Con riguardo alle misure *ex post* da porre in essere in seguito alla violazione di dati personali, ruolo centrale è attribuito alla comunicazione **al Garante Privacy** e, ove prevista, **agli interessati** dell'avvenuta violazione. La comunicazione al Garante Privacy è finalizzata ad agevolare le funzioni di monitoraggio e controllo, avendo a disposizione dati il più possibile completi circa gli incidenti di sicurezza.

Inoltre, ai sensi del Considerando 85 del GDPR, viene chiarito dalle Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Reg. UE 2016/679 come uno degli obiettivi fondamentali della notifica sia quello di limitare i danni che il *data breach* può causare agli individui: "se i tipi di interessati o di dati personali rivelano un rischio di danno particolare a seguito di una violazione (ad esempio usurpazione d'identità, frode, perdite finanziarie, minaccia al segreto professionale) è importante che la notifica indichi tali categorie".

Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Durante questo periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto il requisito per la notifica e quali siano le azioni necessarie per far fronte alla violazione.

14.3.2. Valutazione dei rischi

Il titolare deve agire in modo da **arginare gli effetti del *data breach***, valutando in primo luogo i rischi probabili per gli interessati e le misure opportune per eliminare o, quantomeno, limitare tali rischi.

> Il titolare potrebbe già disporre di una **valutazione del rischio potenziale**, ad esempio perché ha eseguito una valutazione d'impatto, a norma dell'art. 35 GDPR. A tal fine, dovranno essere prese in considerazione tutte le circostanze del caso concreto.

In particolare, sussistono dei rischi quando il *data breach* occorso può causare un danno fisico, materiale o immateriale, per gli interessati quali, ad esempio, il furto o l'usurpazione d'identità, la discriminazione, il pregiudizio alla reputazione o il verificarsi di perdite patrimoniali. Un'adeguata valutazione del rischio - che deve in ogni caso essere condotta in maniera oggettiva - impone di tenere in considerazione tanto la probabilità quanto la gravità delle probabili conseguenze della violazione.

Nelle sue *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679,* il Gruppo di lavoro *ex* art. 29 non ha mancato di precisare quali fattori debbono essere considerati nella valutazione dei rischi connessi al verificarsi di un *data breach.* (Cfr. *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679,* p. 25 ss.).

14.3.3. Valutazione della gravità di un data breach

L'Agenzia dell'Unione Europea per la sicurezza delle reti e dell'informazione (ENISA) ha redatto delle raccomandazioni circa la metodologia di valutazione della gravità di un data breach. Cfr. *Recommendations for a methodology of the assessment of the severity of personal data breaches*, https://www.enisa.europa.eu/publications/dbn-severity.

Tali **fattori** vengono dunque riportati di seguito:

- il tipo di violazione occorsa, vale a dire se sia stata compromessa l'integrità e/o la disponibilità e/o la confidenzialità dei dati personali;
- la natura, il carattere sensibile ed il volume dei dati personali;
- la facilità di identificazione degli interessati;
- la gravità delle conseguenze per le persone fisiche;
- le caratteristiche particolari dell'interessato;
- il numero di persone fisiche interessate;
- le caratteristiche particolari del titolare del trattamento, in particolare il suo ruolo e le attività dallo stesso svolte;
- gli ulteriori elementi che caratterizzano il caso concreto, non dovendosi tralasciare nessuna delle circostanze che potrebbero incidere sugli interessati.

Focus sui fattori di rischio	
Tipologia di dati	Più i dati sono sensibili e maggiore è il rischio che gli interessati patiscano un danno. Inoltre, va tenuto presente come di norma una combinazione di dati abbia un carattere più sensibile rispetto ad un singolo dato personale.

Focus sui fattori di rischio	
Caratteristiche dell'interessato	Si pensi all'accesso non autorizzato ad un database contenente dati personali di minori o alla perdita di disponibilità dei dati relativi allo stato di salute dei pazienti di un ospedale.
Numerosità degli interessati	Più elevato è il numero di interessati coinvolti dalla violazione e maggiore sarà l'impatto del *data breach*.

Caratteristiche e contenuto della notifica 14.3.1.

La notifica deve contenere le informazioni previste all'art. 33, par. 3, Reg. UE 2016/679.

art. 33, comma 3, GDPR	La notifica […] deve almeno : a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

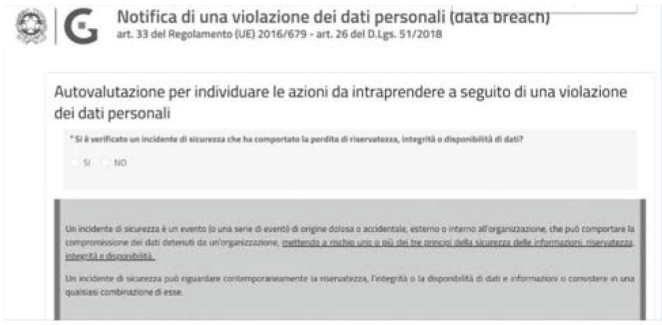
Sotto il profilo nazionale, invece, con il provvedimento n. 157 del 30/07/2019 il **Garante Privacy ha introdotto un modello ufficiale** contenente le informazioni minime necessarie per effettuare una notifica di violazione dei dati personali ai sensi dell'art. 33 GDPR (doc. web n. 9126951). In precedenza, il Garante Privacy aveva già introdotto modalità e requisiti specifici di notifica dei *data breach* in diversi settori e con il provvedimento in questione il Garante Privacy ha provveduto a razionalizzare ed uniformare i termini, i contenuti e le modalità della notifica.
Qualora si utilizzi per la notifica il modello allegato al provvedimento, è necessario scaricarlo sul proprio dispositivo e successivamente procedere alla sua compilazione delle seguenti sezioni:

Dati del soggetto che effettua la notifica	Inserendo i dati anagrafici e di contatto del soggetto che materialmente effettua la notifica (ove nominato, si tratta del DPO del titolare);
Dati relativi al titolare del trattamento	in cui andranno inseriti i dati identificativi del titolare (denominazione, C.F./P.IVA, indirizzo ecc.), i dati di contatto del soggetto da contattare per informazioni (ove nominato il DPO andrà indicato il relativo numero di protocollo assegnato dal Garante Privacy alla comunicazione dei dati di contatto tramite la procedura online disponibile sul sito) e i riferimenti di ulteriori soggetti coinvolti con indicazione del ruolo svolto;
Informazioni di sintesi sulla violazione	informazioni di dettaglio relative alla violazione, ivi incluse: la data esatta in cui si è verificata, il momento e le modalità in cui il titolare ne è venuto a conoscenza, i motivi del ritardo in caso di notifica oltre le 72 ore, la natura e la causa del *data breach* e le categorie di dati personali e soggetti interessati coinvolti, con indicazione dei relativi volumi;
Informazioni di dettaglio sulla violazione	a completamento della sezione precedente, in questa andranno indicati i dettagli relativi alla violazione descrivendo nello specifico l'incidente alla base del *breach*, le categorie di dati violate, i sistemi e le infrastrutture informatiche coinvolte nell'incidente, con indicazione della loro ubicazione e le misure di sicurezza tecniche e organizzative adottate;

Possibili conseguenze e gravità della violazione	si tratta di una sezione che richiede uno sforzo prognostico da parte del titolare il quale sarà tenuto a identificare i possibili impatti della violazione in base alla sua natura ed i potenziali effetti negativi per gli interessati; occorrerà inoltre effettuare una stima motivata della probabile gravità del *data breach*;
Misure adottate a seguito della violazione	in cui andranno segnalate tutte le contromisure sia tecniche che organizzative adottate per limitare gli impatti del *breach* e di futura attuazione onde prevenire incidenti futuri;
Comunicazione agli interessati	in questa sezione occorrerà specificare se la violazione è stata comunicata o meno agli interessati ai sensi dell'art. 34 GDPR, ed in caso di mancata comunicazione sarà necessario motivare la ragione che ha spinto il titolare prendere una tale decisione;
Altre informazioni	si tratta di una sezione di chiusura in cui inserire i dettagli circa l'impatto transfrontaliero del *data breach* e le eventuali segnalazioni già effettuate ad altre autorità.

Per essere in grado di effettuare la notifica il titolare dovrà pertanto assicurarsi di aver implementato le adeguate procedure organizzative - sia interne che esterne nei confronti dei responsabili - che gli consentano di ottenere in maniere tempestiva tutte le notizie necessarie per compilare ed effettuare la notifica.
La notifica deve essere **inviata al Garante Privacy 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.
Il Garante Privacy ha, inoltre, introdotto un nuovo servizio online per semplificare gli adempimenti e per supportare i titolari del trattamento negli adempimenti previsti in caso di *data breach* (violazioni dei dati personali). Sarà infatti possibile accedere al **modello di notifica al Garante Privacy** e alla **procedura di auto-valutazione (*self assessment*)** che aiuta il titolare nell'assolvimento degli obblighi in materia di Notifica di una violazione dei dati personali all'autorità di controllo e di Comunicazione di una violazione dei dati personali all'interessato.

Schermata del sito del Garante Privacy per la procedura di auto valutazione



14.3.2. Notifica per fasi

Ai sensi dell'art. 33, comma 4, GDPR ed a seconda della natura della violazione, il titolare può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. Ne deriva che il GDPR consente una notifica per fasi della violazione, **nel caso in cui il titolare non disponga di dettagli completi ed esaustivi** circa la violazione entro 72 ore dal momento in cui ne è venuto a conoscenza ed a condizione che il titolare del trattamento indichi i motivi del ritardo. Si pensi agli incidenti di sicurezza informatica nel contesto dei quali può essere necessaria un'indagine fo-

rense approfondita per stabilire appieno la natura della violazione e la portata della compromissione dei dati personali.

A tal proposito, il Gruppo di Lavoro, nelle sopra citate Linee Guida, raccomanda che, "all'atto della prima notifica all'autorità di controllo, il titolare del trattamento informi quest'ultima del fatto che non dispone ancora di tutte le informazioni richieste e che fornirà ulteriori dettagli in un momento successivo. L'autorità di controllo dovrebbe concordare le modalità e le tempistiche per la fornitura delle informazioni supplementari. Questo non impedisce al titolare del trattamento di trasmettere ulteriori informazioni in qualsiasi altro momento, qualora venga a conoscenza di ulteriori dettagli rilevanti sulla violazione che devono essere forniti all'autorità di controllo.".

A rigore di termini, **ogni singola violazione costituisce un incidente segnalabile**. Tuttavia, per evitare che il processo diventi eccessivamente oneroso, il titolare del trattamento può presentare una **notifica "cumulativa"** che rappresenta tutte le violazioni in questione, a condizione che riguardino il medesimo tipo di dati personali e che questi siano stati violati nel medesimo modo in un lasso di tempo relativamente breve. Se si verificano diverse violazioni riguardanti tipi diversi di dati personali, violati in maniere diverse, la notifica deve procedere secondo l'iter normale, segnalando ogni violazione conformemente all'art. 33.

CASO 1 - Invio di dati a un destinatario errato

Un dipendente di una società invia per errore un'e-mail, nel cui testo erano riportati dati personali di un intermediario, a un destinatario errato. Nello specifico, l'e-mail inoltrata per errore conteneva i seguenti dati personali: nome, cognome, telefono, fax e e-mail, oltre all'indirizzo email.

A seguito del riconoscimento dell'errore, il dipendente - dopo essersi confrontato con il responsabile competente all'interno della società - si è immediatamente attivato nel contattare il destinatario per richiedere la cancellazione immediata della e-mail richiedendo inoltre conferma che non fossero state effettuate copie o inoltro a soggetti terzi.

Alla luce delle informazioni raccolte dalla società è risultato che:

- i dati oggetto di violazione sono limitati ai dati di contatto di lavoro (e non personali) di un solo soggetto terzo, cosicché il volume dei dati oggetto di violazione è particolarmente ridotto così come anche il numero dei soggetti coinvolti (un solo intermediario);
- i dati oggetto di violazione non includono categorie particolari di dati ma solo i dati di contatto del terzo intermediario, cosicché dagli stessi non può derivare un rischio a carico dell'individuo a cui si riferiscono (al contrario è possibile che tali dati siano facilmente reperibili in pubblici registri considerazione dell'attività lavorativa dell'interessato);
- copia della email è tuttora in possesso della società che non ha pertanto perso la disponibilità delle informazioni ivi contenute.

Inoltre i dati di contatto del soggetto terzo sono stati condivisi con un unico soggetto il quale, a poche ore di distanza dal verificarsi del *data breach*, ed a seguito delle azioni intraprese dalla società, ha inviato un'apposita comunicazione contenente una conferma scritta della cancellazione dell'e-mail riportante il seguente testo: "In riferimento alla comunicazione riportata in seguito, preso atto che il sottoscritto non risulti in alcun modo destinatario della missiva, comunico di procedere con l'eliminazione definitiva della presente e-mail e di quella originaria. Distinti saluti.".

In presenza delle circostanze sopra indicate, né la notifica al Garante Privacy né la comunicazione agli interessati è necessaria.

CASO 2 - Invio di dati relativi ai clienti

Un dipendente di una società invia per errore ai propri 20 fornitori una email contenente quale allegato un file excel riportante i dati di contatto di 2.000 clienti della società. Tale documento excel contiene diverse categorie di dati personali, nello specifico, nome e cognome dei clienti, indirizzo email, numero di telefono cellulare, nazionalità, livello di fedeltà del cliente, frequenza di acquisto.

A seguito del riconoscimento dell'errore, è emerso che:

- i dati oggetto di violazione sono relativi ad un ampio numero di interessati;
- le categorie di dati comunicati includono i dati identificativi e di contatto dei clienti coinvolti nella violazione nonché le loro abitudini di spesa;
- le informazioni sono state condivise con un ampio numero di soggetti terzi, i quali potrebbero far uso o semplicemente visionare i dati contenuti nel file erroneamente condiviso per finalità non ben identificate;
- le informazioni erano visibili ai destinatari che hanno ricevuto la email;
- la email con cui è stato erroneamente condiviso il file non può essere richiamata né cancellata da remoto.

La società ha tuttavia rilevato come, alla luce del posizionamento del proprio brand e del costo dei suoi prodotti, le informazioni sulle abitudini di spesa non sono comunque in grado di fornire dettagli sulla personalità dell'individuo. Inoltre, la società ha provveduto ad inviare ai suddetti fornitori una comunicazione in cui richiede di procedere all'immediata cancellazione dell'email e informa che qualsiasi utilizzo dei dati allegata all'email non è autorizzato ed è in violazione della normativa sul trattamento dei dati personali. Per di più è emerso come i destinatari della comunicazione fossero tutti fornitori professionali (quali a titolo meramente esemplificativo, consulenti contabili, legali, partner commerciali) ed è stato valutato come "improbabile" il rischio che facciano un utilizzo non autorizzato dei dati ricevuti.
In presenza delle circostanze sopra indicate, è raccomandabile procedere alla notifica al Garante Privacy della violazione dei dati personali in quanto detta violazione potrebbe presentare un rischio per i diritti e le libertà delle persone fisiche per la quantità di informazioni fornite. Tuttavia, non si ritiene necessario procedere alla comunicazione agli interessati poiché, alla luce della natura dei dati oggetto della violazione, della tipologia di destinatari e delle misure adottate successivamente alla violazione, non si ritiene che sussista un rischio elevato per gli stessi.

14.4. LA COMUNICAZIONE AGLI INTERESSATI

Con riguardo invece alla comunicazione rivolta agli interessati, essa si rende necessaria ogni qualvolta la violazione possa arrecare loro pregiudizio sia rispetto alla tutela dei dati personali che della riservatezza, posto che in tali casi le conseguenze negative possono essere molteplici e significative sia sul piano economico che reputazionale, identitario e morale. Ai sensi dell'art. 34 GDPR, quando la violazione dei dati personali è suscettibile di presentare un **rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
Ne consegue che, rispetto ai soggetti interessati, non sarà sufficiente la semplice comunicazione dell'avvenuta violazione della sicurezza, bensì occorrerà anche rendere edotti quest'ultimi circa le **misure opportune onde limitare gli eventuali effetti pregiudizievoli** e le **modalità con cui ottenere maggiori informazioni** sull'accaduto. Il tema è trattato nel Considerando 86 del GDPR che evidenzia come "la comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o altra autorità competente".

Lo **scopo della comunicazione** è quello di fornire le informazioni che consentano loro di compiere le azioni necessarie per proteggersi dalla violazione. In tale circostanza, la comunicazione potrebbe contenere anche dei consigli pratici per mitigare le conseguenze della violazione, quali a titolo esemplificativo la modifica delle credenziali di accesso ad una determinata piattaforma.

La comunicazione agli interessati dovrà avvenire **mediante un linguaggio semplice e attraverso informazioni trasparenti** che non possano essere travisate dagli stessi. Esempi di modalità di comunicazione trasparenti possono considerarsi le e-mail inviate all'indirizzo personale, gli SMS o, altrimenti, i banner ben visibili all'interno dei siti web della società che ha subito la violazione. A seconda della gravità delle violazioni e dei rischi sottesi alla violazione, il titolare potrebbe anche utilizzare diverse modalità di comunicazione.

Come evidenziato dal Garante Privacy, nel Provvedimento in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali (c.d. *data breach*) – 04/04/2013 [2388260]: "Si ritiene, cioè, che in alcuni casi siano più utili forme di comunicazione di carattere pubblico, quali la diffusione di avvisi su quotidiani, anche on line, oppure per mezzo di emittenti radiofoniche, anche locali. Tali forme alternative di comunicazione ai contraenti o alle altre persone coinvolte dalla violazione vanno ovviamente realizzate anch'esse entro il più breve lasso di tempo e, comunque, entro il termine di 3 giorni […]".

Per quanto riguarda il **contenuto della comunicazione**, il GDPR rimanda al contenuto della notifica da effettuare all'Autorità di controllo in caso di *data breach*.
Stante il presupposto della natura potenzialmente pregiudizievole della violazione, **la comunicazione agli interessati non sarà dovuta** allorquando detto **pregiudizio non possa verificarsi**, perché:
– il titolare del trattamento abbia messo in atto le misure tecniche e organizzative adeguate di protezione dei dati personali e tali misure siano state applicate ai dati oggetto della violazione (e.g. cifratura);

- il titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione agli interessati richieda sforzi sproporzionati (in tal caso il titolare del trattamento procederà ad una comunicazione pubblica o misura similare con analoga efficacia).

Nel parere n. 03/2014 sulla notifica delle violazioni, il Gruppo di Lavoro ha spiegato che una violazione della riservatezza di dati personali crittografati con un algoritmo all'avanguardia costituisce in ogni caso una violazione dei dati personali e deve essere notificata. Se però la riservatezza della chiave rimane intatta (ossia se la chiave non è stata compromessa nell'ambito di una violazione della sicurezza), i dati risultano incomprensibili. Di conseguenza è improbabile che la violazione possa influire negativamente sulle persone fisiche e quindi non dovrebbe essere loro comunicata. A tal proposito, è stato tuttavia anche evidenziato che "se i dati sono crittografati, una perdita o alterazione può avere effetti negativi per gli interessati ove il responsabile del trattamento non disponga delle necessarie copie di riserva. In tal caso, la notifica agli interessati dovrebbe essere necessaria anche se sono state adottate misure di protezione mediante crittografia.".

Al riguardo, il Gruppo di Lavoro nelle sopra citate linee guida ha sottolineato che i titolari dovrebbero essere in grado di dimostrare all'autorità di controllo di soddisfare una o più delle predette condizioni.

CASO 3 - Divulgazione di dati di un ospedale
Un ospedale subisce una violazione che si traduce in una divulgazione accidentale delle cartelle cliniche dei pazienti. È probabile che vi sia un impatto significativo sugli interessati a causa della sensibilità dei dati e dei loro dettagli medici riservati che vengono resi noti a terzi. In virtù dell'alto rischio per i loro diritti e le loro libertà, l'ospedale sarà tenuto ad informare prontamente gli interessati dell'accaduto e delle conseguenze che possono derivare dalla violazione.

CASO 4 - Attacco *ransomware*
Una società subisce un attacco *ransomware* che causa la crittografia dei dati dei propri clienti online registrati sul sito della società: nome, indirizzo email, password, indirizzo di residenza, numero di telefono. Al momento dell'indagine, risulta evidente come l'attacco informatico sia risultato in una copia non autorizzata delle credenziali di accesso di tutti i clienti della società.
A seguito della notifica della violazione all'Autorità di controllo, il titolare del trattamento dovrebbe intervenire, ad esempio obbligando i titolari degli account interessati al reset delle password, nonché ad adottare ulteriori misure di sicurezza informatica per attenuare il rischio di ulteriori infrazioni.

Nel caso in cui, a seguito della notifica del *data breach*, sia rilevata una violazione delle disposizioni del GDPR, l'autorità di controllo può prescrivere al titolare del trattamento l'adozione di **misure correttive** - a norma dell'art. 58, comma 2, GDPR. Inoltre, sono previste **sanzioni amministrative pecuniarie** che possono giungere fino a 10 milioni di euro o, nel caso di imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

LE PROCEDURE INTERNE PER LA GESTIONE DEI *DATA BREACH* 14.5.

Per agevolare il rispetto degli artt. 33 e 34, il titolare del trattamento è tenuto a disporre di una **procedura di notifica documentata**, che stabilisca la procedura da seguire una volta individuata una violazione, ivi compreso come contenere, gestire e porre rimedio all'incidente, valutare il rischio e notificare la violazione. A questo proposito, per adempiere a quanto richiesto dal GDPR potrebbe anche essere utile dimostrare che i dipendenti sono stati informati dell'esistenza di tali procedure e meccanismi e che sanno come reagire alle violazioni. Si noti che la mancata corretta documentazione di una violazione può comportare l'esercizio da parte dell'autorità di controllo dei suoi poteri ai sensi dell'art. 58 e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83.

Linee guida per le società in caso di data breach 14.5.1.

Le procedure in materia di *data breach* contengono le linee guida per definire quale azione deve essere intrapresa dalle società in presenza di violazione dei principi sopra descritti. Nel presente documento trovano descrizione anche le circostanze, in presenza delle quali, viene ravvisato il bisogno di notificare e/o comunicare la violazione dei dati personali al Garante Privacy per la protezione dei dati personali e/o all'interessato.
I principali obiettivi e benefici, che una tale procedura può raggiungere, sono i seguenti:

- adeguato e tempestivo coinvolgimento delle funzioni aziendali apicali delle società con riferimento agli eventi critici in materia di violazione dei dati personali al fine di garantire un'azione immediata in conformità con la normativa applicabile;

- tempestiva adozione della soluzione da attuare al fine di limitare o mitigare l'impatto della violazione dei dati personali sulle attività di business;
- migliorare i propri strumenti di supervisione per evitare che situazioni analoghe si ripetano in futuro;
- usare i dati di "*Risk events*" in modo da migliorare l'identificazione e la valutazione del rischio;
- adempiere agli obblighi imposti dalla legge applicabile, dimostrando altresì al Garante Privacy per la protezione dei dati personali l'impegno delle Società nell'adozione di pratiche di gestione del rischio adeguate ai trattamenti effettuati.

Un primo aspetto da tenere in considerazione attiene alla **gestione dei flussi di comunicazione all'interno della società**; è infatti essenziale che tali flussi vengano delineati in maniera chiara, così da garantire che tutte le funzioni interessate dal *data breach* - o il cui intervento sia necessario al fine di una sua corretta gestione - siano tempestivamente informate dell'incidente di sicurezza occorso.

> L'importanza di tale aspetto è opportunamente evidenziata dal Gruppo di lavoro *ex* art. 29 nelle linee guida, ove si legge che "le informazioni relative a tutti gli eventi concernenti la sicurezza dovrebbero essere indirizzate a una persona responsabile o alle persone incaricate di gestire gli incidenti, stabilire l'esistenza di una violazione e valutare il rischio.". Cfr. *Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679*, p. 13.

La **creazione di un indirizzo e-mail dedicato** alla comunicazione di potenziali *data breach*, ad esempio, potrebbe rappresentare un'utile misura nell'ottica agevolare un efficiente flusso informativo. Tale indirizzo e-mail dovrebbe inoltre essere inserito all'interno degli accordi sottoscritti, a norma dell'art. 28, comma 3, GDPR, con i responsabili del trattamento, in modo che anche tali soggetti siano tenuti ad inviare le comunicazioni riguardanti possibili violazioni di dati personali utilizzando il canale dedicato, istituito dall'azienda.

Un ulteriore aspetto rilevante concerne la **corretta allocazione delle responsabilità**. Da un lato, la nomina di uno o più soggetti responsabili rappresenta una misura essenziale nell'ottica di garantire un'efficace prevenzione di possibili incidenti di sicurezza. D'altra parte, è altrettanto importante che tutti coloro che svolgono la propria attività all'interno dell'organizzazione aziendale siano sensibilizzati in modo adeguato della necessità di informare immediatamente le funzioni deputate - in primo luogo il DPO, se nominato - qualora rilevino o sospettino che si sia verificata una violazione dei dati personali.

Infine, le procedure sulla gestione dei *data breach* dovrebbero contenere **prescrizioni chiare ed indicazioni operative** sulle azioni da intraprendere al fine di compiere un *assessment* tempestivo circa i provvedimenti da prendere, a tutela degli interessati e dell'azienda e circa gli incidenti di sicurezza che compromettono dati personali, indipendentemente dal fatto che il titolare del trattamento abbia ritenuto necessario procedere alla notifica all'autorità di controllo.

14.5.2. L'individuazione della violazione

Ove **chiunque** delle Società rilevi o sospetti una violazione dei dati personali relativi ad altri dipendenti, ai soci, ai fornitori o a terze parti in contatto con le società, tale dipendente, non appena **individuata la violazione**, dovrebbe prontamente **inoltrare all'indirizzo e-mail dedicato una comunicazione** contenente le seguenti informazioni:

- la natura della violazione dei dati personali compresi e, ove possibile, le categorie e il numero approssimativo di individui che hanno subito la violazione dei dati personali;
- il progetto/servizi di terze parti per conto dei quali le società hanno trattato i dati (se disponibili);
- ogni terza parte coinvolta nella violazione che assume un ruolo attivo o passive (subcontraenti, ecc.);
- le categorie e il numero approssimativo di registrazione dei dati personali in questione, e
- ogni altra informazione volta ad individuare i dati oggetto di *data breach* e mitigarne le conseguenze negative.

14.5.3. I soggetti competenti a prendere decisioni a seguito di un *data breach*

In un'ottica di accountability**, il DPO** (o eventualmente la figura privacy preposta all'interno della società) **deve dare priorità alla comunicazione interna della violazione** dei dati. A tal fine, e dopo aver valutato le informazioni e concluso che sussiste un rischio effettivo di una imminente violazione dei dati personali in corso la procedura interna dovrebbe prevedere l'organizzazione di una **riunione** da tenersi il prima possibile, in cui devono partecipare i rappresentanti designati dei dipartimenti operazionali al fine di raccogliere ulteriori informazioni rispetto la violazione.

L'obiettivo di un tale incontro è quello di:
- definire l'analisi delle cause principali, natura e scopo della violazione, la quantità, tipologie e numero di dati collegati agli interessati e soggetti alla violazione tramite la raccolta delle informazioni per la notifica al Garante Privacy ai sensi dell'art. 33 con il supporto del dipartimento IT;
- analizzare le azioni già poste in essere e definire le azioni da intraprendere al fine di rimediare alla violazione e di mitigare ogni effetto negativo;
- valutare ove la notifica al Garante Privacy ai sensi dell'art. 33 GDPR e la comunicazione all'interessato ai sensi dell'art. 34 GDPR siano necessarie;
- decidere come, ove necessario o appropriato, informare le altre terze parti che possono essere state coinvolte nella violazione; e
- determinare quali misure devono essere implementate o che si vuole implementare (incluse le tempistiche per tale implementazione) per rimediare alla violazione o mitigarne gli effetti negativi;
- definire qualsiasi ulteriore azione urgente e se consiglieri esterni o altri specialisti nell'assistenza devono essere convocati;
- informare immediatamente il CEO e/o il Consiglio di Amministrazione rispetto quanto statuito durante la riunione.

Registro dei *data breach* 14.5.4.

Indipendentemente dal fatto che una violazione debba o meno essere notificata all'autorità di controllo, il titolare del trattamento deve **conservare la documentazione di tutte le violazioni**, come spiegato all'art. 33, par. 5, GDPR.
Il registro dei *data breach* è un documento che ha la duplice funzione di consentire, al titolare, un agevole **monitoraggio e controllo** di tutte le violazioni di dati personali avvenute nel corso delle proprie attività di trattamento e, al Garante Privacy di **verificare il rispetto dell'obbligo di notifica** tempestiva. Tale registro dovrà indicare i:
- *data breach* subiti in ordine di tempo con indicazione di chi ha effettuata la segnalazione,
- una breve descrizione del *data breach*,
- la tipologia di dati coinvolti ed il volume dei dati impattati,
- le misure adottate per rimediare al *data breach*,
- l'indicazione del fatto che sia stata fatta o meno una notifica al Garante Privacy, rinviando poi ai rilevanti report che giustifichino le scelte effettuate,
- specifiche sulla notifica ove questa sia stata effettuata,
- l'indicazione del fatto che sia stata fatta o meno una comunicazione agli interessati, rinviando poi al report che giustifichi le rilevanti scelte effettuate.

Oltre a queste informazioni, il Gruppo di lavoro raccomanda al titolare del trattamento di **documentare anche il ragionamento alla base delle decisioni** prese in risposta a una violazione. Lo scopo della tenuta di registri delle violazioni non notificabili, oltre a quelle notificabili, è collegato anche agli obblighi del titolare del trattamento ai sensi dell'art. 24 GDPR rubricato come "Responsabilità del titolare del trattamento", e l'autorità di controllo può richiedere di consultare tali registri. Di conseguenza il titolare del trattamento è incoraggiato a creare un registro interno delle violazioni, indipendentemente dal fatto che sia tenuto a effettuare la notifica o meno.
Tale ragionamento potrà essere descritto all'interno di un report che include le seguenti informazioni:
- il nome degli interessati (clienti, dipendenti, fornitori) colpiti dalla violazione;
- le conseguenze della violazione e qualsiasi ammontare del risarcimento danni da corrispondere agli interessati (inclusi I clienti, se presenti) ove conosciuto;
- perimetro delle aree operative colpite dall'evento;
- circostanze della violazione;
- i provvedimenti adottati per porre rimedio alla violazione o per attenuarne gli effetti negativi.

Il report della violazione non è un documento che viene indirizzato dal DPO alla società, ma un documento redatto dalla società stessa con la quale quest'ultima attesta di aver effettuato i controlli e le verifiche necessarie con riferimento alle decisioni assunte in materia di violazione dei dati.

In particolare, se una violazione non viene notificata, è opportuno documentare una giustificazione di tale decisione. La giustificazione dovrebbe includere i motivi per cui il titolare del trattamento ritiene improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. In alternativa, se ritiene che una delle condizioni di cui all'art. 34, par. 3, sia soddisfatta, il titolare del trattamento dovrebbe essere in grado di fornire prove adeguate della circostanza che ricorre nel caso di specie.