ISTITUTO TECNICO STATALE
"MARCHI – FORTI"

Viale Guglielmo Marconi, 16 - 51017 PESCIA (PT) - Tel: 0572-451565 - Fax: 0572-444593
E-mail: pttd01000e@istruzione.it - Sito internet: www.itsmarchiforti.edu.it

Via Caduti di Nassiriya, 87 – 51015 MONSUMMANO TERME (PT) - Tel. e Fax: 0572-950747
E-mail: istituto.forti@itsmarchiforti.edu.it - Sito internet: www.itsmarchiforti.edu.it

COMUNICATO DELLA PRESIDENZA n. 02 M/F

- Pubblicato sul sito della scuola in data 1 settembre 2023

Alla cortese attenzione

- Del personale docente
- Del personale ATA
- Dei referenti per la sicurezza
- Dell'DPO, Ing. Stefano Rodà

e, pc

- Del Direttore SGA
- Dell'AT Michele Ricco

OGGETTO: Obblighi di notifica in caso di violazione dei dati personali (c.d. "data breach") - Novità introdotte dalla versione aggiornata delle Linee Guida n. 09/2022 del Comitato Europeo per la Protezione dei Dati - Nota di trasmissione

Con la presente si trasmette, unitamente agli allegati, la nota prot. AOODGPOC 1248/2023, che illustra e sintetizza i contenuti della versione aggiornata delle Linee Guida n. 09/2022 del Comitato Europeo per la Protezione dei Dati sulla gestione e la notifica delle violazioni di dati personali (c.d. "data breach") nell'ottica di garantire un'omogenea applicazione del Regolamento UE 2016/679 (GDPR). I documenti sono pubblicati sul sito della scuola nella sezione "Privacy" che si invita a consultare periodicamente.

Si ringrazia per la collaborazione.

Pescia, 1 settembre 2023

Il Dirigente Scolastico

Prof.ssa Anna Paola Migliorini

(Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3, comma 2 del D.Lgs. 39/1993)

/DDR

ALLEGATI:

- ✓ Nota MIM n. 1248 del 28/07/2023 e relativi allegati

m_pi.AOODGPOC.REGISTRO UFFICIALE.U.0001248.28-07-2023.h.11:57

m_pi.AOODRTO.REGISTRO UFFICIALE.E.0011377.28-07-2023.h.23:41

Ministero dell'Istruzione e del Merito

Dipartimento per le risorse umane, finanziarie e strumentali
Direzione Generale
per la progettazione organizzativa, l'innovazione dei processi amministrativi, la comunicazione e i contratti
Ufficio III – Protezione dei dati personali del Ministero

All'Ufficio di Gabinetto

SEDE

Al Dipartimento per le risorse umane,
finanziarie e strumentali
SEDE

Al Dipartimento per il sistema educativo
di istruzione e di formazione
SEDE

Ai Direttori Generali dell'Amministrazione centrale
LORO SEDI

Ai Direttori Generali e ai Dirigenti titolari
degli Uffici scolastici regionali
LORO SEDI

e, p.c., Al *Computer Security Incident Response Team* (CSIRT) del Ministero
SEDE

OGGETTO: Obblighi di notifica in caso di violazione dei dati personali (c.d. *"data breach"*) - Novità introdotte dalla versione aggiornata delle Linee Guida n. 09/2022 del Comitato Europeo per la Protezione dei Dati

Con la presente si informano gli Uffici in indirizzo del fatto che, nel primo semestre del 2023, il Comitato Europeo per la Protezione dei Dati, organismo indipendente dell'UE istituito per garantire un'applicazione coerente del Regolamento Generale sulla Protezione dei Dati, noto anche come EDPB (acronimo inglese di "*European Data Protection Board*"), dopo una fase di consultazione pubblica preventiva avviata ad ottobre 2022, ha pubblicato la versione aggiornata delle Linee Guida n. 09/2022 sulla gestione e la notifica delle violazioni di dati personali (c.d. *"data breach*").

La prima versione del documento in questione (all. n. 1) era stata approvata poco dopo l'entrata in vigore del Regolamento UE 2016/679 (di seguito, anche "Regolamento" o "GDPR") ma, con il tempo, si sono rese necessarie talune modifiche al fine di aggiornare, allo stato dell'arte della tecnologia, le indicazioni fornite in passato e di armonizzare la pubblicazione alla casistica sviluppatasi in vigenza del GDPR.

Attraverso tale intervento di aggiornamento, l'EDPB (di seguito, anche "Comitato" o "Board") ha inteso quindi proseguire il percorso iniziato subito dopo l'entrata in vigore del Regolamento, con l'obiettivo di fare chiarezza sugli obblighi di notifica che sussistono, rispetto alle Autorità Garanti e agli interessati, nel caso in cui si verifichi una violazione dei dati personali (di seguito, anche "*data breach*"), allo scopo di supportare i Titolari e Responsabili del trattamento nella gestione degli incidenti di sicurezza eventualmente occorsi all'interno delle proprie organizzazioni.

Nel trasmettere agli Uffici in indirizzo il documento in parola, allo stato disponibile unicamente nella versione in lingua inglese (all. n. 2), si reputa utile offrire di seguito una panoramica delle principali novità introdotte in materia, con un richiamo anche ai più significativi aspetti già affrontati in precedenza dal Comitato e ribaditi nella versione aggiornata della pubblicazione.

Premesse generali in tema di violazione dei dati personali

Analizzando i punti salienti della versione 2.0 delle Linee Guida, emerge innanzitutto la volontà del Board di chiarire alcuni aspetti legati ai principi statuiti dal Regolamento in tema di violazione dei dati personali.

Com'è noto, il GDPR fornisce una definizione precisa della nozione di "*violazione dei dati personali*".

Secondo l'art. 4, n. 12 del Regolamento costituisce violazione di dati personali ogni "*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*".

In sostanza, una violazione di dati personali o *data breach* costituisce un incidente di sicurezza che abbia coinvolto dati personali e dal quale possano derivare rischi per gli interessati.

Da tanto discende che, mentre ogni *data breach* rappresenta sempre la conseguenza più severa di un incidente di sicurezza (*security incident*), non ogni incidente di sicurezza è destinato a sfociare in un'effettiva violazione di dati e, quindi, a dare luogo a un *data breach*.

Ebbene, nel soffermarsi sul punto, il Comitato ha ritenuto utile ricordare come le violazioni di dati personali possano essere classificate in tre diverse tipologie connesse alla sicurezza delle informazioni (c.d. Triade R.I.D.):

- violazione della *riservatezza*, in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
- violazione dell'*integrità*, in caso di modifica non autorizzata o accidentale dei dati personali;
- violazione della *disponibilità*, in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Ribadendo quanto già osservato nelle precedenti edizioni delle Linee Guida, l'EDPB ha inoltre osservato che, a seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi loro combinazione.

Come rammentato dal Comitato, nel caso in cui si verifichi una violazione dei dati personali è necessario indagare tempestivamente su quanto accaduto, al fine di identificare le caratteristiche dell'evento negativo, per poterlo classificare e valutare.

La classificazione e la valutazione dell'incidente occorso costituiscono, infatti, un passaggio indispensabile per poter affrontare il *data breach* in modo adeguato e conforme alla normativa, perché è sulla base delle valutazioni effettuate dal Titolare che dovranno essere definiti gli *step* successivi da seguire.

Qualora, infatti, dalle verifiche effettuate emerga la sussistenza di un potenziale rischio per i diritti e le libertà delle persone fisiche, l'art. 33 del Regolamento richiede al Titolare del trattamento di notificare la violazione all'Autorità Garante competente senza ingiustificato ritardo e, ove possibile, non oltre le 72 ore dal momento in cui sia venuto a conoscenza della violazione dei dati personali.

Nel caso in cui, poi, la violazione dei dati personali sia suscettibile di presentare un rischio non soltanto probabile, ma elevato per i diritti e le libertà delle persone fisiche, all'onere di notifica all'Autorità di controllo si aggiunge per il Titolare, ai sensi dell'art. 34 del GDPR, anche quello di dare comunicazione della violazione agli interessati, senza ingiustificato ritardo.

L'evento identificato, analizzato ed eventualmente notificato e comunicato deve inoltre essere sempre riportato nel Registro delle violazioni (noto anche come "Registro degli incidenti di sicurezza" o "Registro dei *data breach")*, per poter tenere traccia delle violazioni subite, in un'ottica di responsabilizzazione della organizzazione (c.d. *accountability*).

Il corretto adempimento degli obblighi sopra descritti riveste fondamentale importanza ai fini della protezione dei diritti degli interessati e l'inosservanza delle disposizioni richiamate è sanzionata a norma dell'art. 83 GDPR.

Una violazione di dati personali può, del resto, se non affrontata in modo adeguato e tempestivo provocare agli interessati danni fisici, materiali e immateriali, come la limitazione dei diritti, la discriminazione, il furto o l'usurpazione di identità, un pregiudizio alla reputazione e/o altri nocumenti di natura tanto economica, quanto sociale.

Proprio per tale ragione, nella nuova versione delle Linee Guida, il Board ha ritenuto indispensabile fornire ulteriori chiarimenti e indicare nuovi esempi pratici che possano orientare al meglio i Titolari e i Responsabili del trattamento nella gestione di eventuali *data breach*.

Le principali novità introdotte

I tempi di notifica del *data breach* nelle nuove Linee Guida

Le nuove Linee Guida EDPB mettono innanzitutto alcuni punti fermi in merito ad una circostanza essenziale nello sviluppo diacronico delle procedure relative alla gestione delle violazioni dei dati, ovvero il momento dal quale decorrono i ristretti termini per la notifica all'Autorità Garante (entro 72 ore) e per la comunicazione agli interessati (da effettuarsi senza ingiustificato ritardo).

Come si è avuto modo di anticipare in precedenza, l'articolo 33 del GDPR specifica che "*in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza*".

La tempestività, infatti, come sopra accennato, assume rilievo fondamentale nelle procedure di notifica dei *data breach*.

In tale prospettiva, risulta decisivo individuare il momento dal quale decorrono le 72 ore per la notifica della violazione all'Autorità di controllo competente (in Italia, il Garante per la Protezione dei Dati Personali – di seguito, anche "Garante" o "GPDP").

Nell'intervenire sul punto l'EDPB si è preoccupato di sgomberare il campo da possibili usi distorti della normativa, ricordando che i principi generali del GDPR impongono ai Titolari l'adozione di misure tecnico-organizzative a protezione dei dati tali da consentire di venire a conoscenza delle violazioni in tempi rapidi.

In considerazione di ciò è quindi indispensabile scongiurare situazioni di tardiva rilevazione di eventuali violazioni di dati personali intervenute, in quanto le stesse sono considerate indice di scarsa o inadatta organizzazione dell'Ente in termini di conformità alla normativa vigente, nonché di implementazione di misure di sicurezza a tutela dei dati personali

degli interessati e, come tali, si rivelano potenzialmente idonee a costituire autonoma fonte di sanzione.

Tuttavia, resta fermo il principio per cui l'obbligo di notifica sorge in concreto nel momento in cui il Titolare diventi "consapevole" del *data breach*.

La precisa individuazione di questo momento varia da caso a caso, poiché dipende dalle circostanze specifiche della violazione, che possono richiedere ulteriori indagini, nonché notificazioni *follow up* all'Autorità Garante.

Ebbene, al fine di supportare i Titolari e i Responsabili del trattamento nella corretta individuazione di tale momento, il Board, nel puntualizzare che un Titolare o un Responsabile del trattamento può considerarsi "*a conoscenza*" della violazione quando abbia conseguito un "*ragionevole grado di certezza che la violazione si sia verificata*" e che abbia causato una compromissione di dati personali, ha ritenuto utile indicare, a titolo esemplificativo, una serie di "*situazioni-tipo*" reputate idonee a far cogliere con maggiore chiarezza i momenti di conoscenza di eventuali violazioni nella prassi.

Ad esempio, è stato evidenziato come il Titolare e/o il Responsabile del trattamento possa considerarsi "*a conoscenza*" della violazione nel caso in cui:

- abbia ricevuto una e-mail da un utente che lo abbia avvisato di essere stato contattato da un soggetto terzo che impersonava il Titolare e che possa verosimilmente aver avuto accesso ai dati dell'organizzazione del Titolare medesimo;
- sia stata condotta una rapida indagine in grado di suffragare la segnalazione dell'utente, attraverso l'acquisizione di prove puntuali di un'intromissione nel sistema.

Oppure, quando:

- un terzo lo informi di aver ricevuto da suoi dipendenti/operatori, per errore, una comunicazione contenente i dati personali di altri utenti e fornisca la prova dell'intervenuta divulgazione non autorizzata (in tal caso, dal momento che il Titolare del trattamento è stato reso edotto, anche attraverso il supporto di prove evidenti, di una violazione della riservatezza, non possono sussistere dubbi circa il fatto che la stessa si sia verificata e che il Titolare stesso ne sia venuto a conoscenza).

O, ancora:

- in caso di smarrimento di una chiavetta USB contenente dati personali non criptati gestiti dall'organizzazione del Titolare (in tale evenienza, infatti, non essendo effettivamente possibile constatare con assoluta certezza se persone non autorizzate abbiano avuto o meno accesso a tali dati, si deve presumere un accesso non autorizzato possa essersi determinato).

Da quanto illustrato, emerge, dunque, come il momento esatto "di presa coscienza" da parte del Titolare e/o del Responsabile possa variare in base alle circostanze.

La conoscenza dovrà considerarsi immediata in tutti quei casi in cui il Titolare del trattamento dati sia stato informato di una violazione, tramite segnalazione documentata di un terzo, ovvero abbia rilevato, direttamente e/o per il tramite del Responsabile del trattamento eventualmente designato, l'evento.

Diversamente, potrebbero ricorrere situazioni in cui la consapevolezza/conoscenza della violazione non possa dirsi immediata, rendendosi necessario l'espletamento di apposite indagini volte ad appurare se il *data breach* abbia effettivamente avuto luogo.

In tali evenienze, secondo quanto affermato dall'EDPB, il Titolare del trattamento non può considerarsi pienamente "consapevole" *ab origine*. È, tuttavia, necessario che, in siffatte ipotesi, le indagini iniziali vengano avviate dal Titolare il prima possibile e siano quanto più dettagliate possibile per permettere di stabilire rapidamente e con un ragionevole grado di certezza la sussistenza e la gravità della violazione.

Da ultimo, va rammentato come, per quanto il Titolare conservi una responsabilità generale in tema di protezione dei dati personali, un ruolo rilevante nel consentire a quest'ultimo di adempiere ai propri obblighi in materia di rilevazione, verifica e notifica dei *data breach*, sia riconosciuto anche al Responsabile del trattamento (es. fornitore esterno) eventualmente nominato.

L'art. 28, paragrafo 3, del GDPR, nello stabilire che il ruolo del Responsabile del trattamento debba essere disciplinato da un contratto o da un altro atto giuridico, precisa, alla lettera f), che detto contratto o altro atto giuridico deve prevedere che il Responsabile del trattamento "*assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento*".

L'articolo 33, paragrafo 2, del GDPR chiarisce inoltre che, se il Titolare ricorre a un Responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare, deve notificarla al Titolare "*senza ingiustificato ritardo*".

Va, inoltre, evidenziato che il Responsabile del trattamento non deve valutare la probabilità del rischio sui diritti e le libertà delle persone fisiche prima di notificare la violazione al Titolare. Spetta, infatti, a quest'ultimo effettuare tale valutazione nel momento in cui viene a conoscenza del *data breach*. Il Responsabile del trattamento è tenuto soltanto verificare se sia occorsa una violazione e notificarla al Titolare.

La valutazione del rischio a seguito di *data breach* nelle nuove Linee Guida

In linea con l'orientamento adottato nella versione 1.0 il Comitato, in occasione dell'aggiornamento delle Linee Guida, ha rimarcato anche che il Titolare, una volta che sia venuto a conoscenza di un *data breach*, è tenuto a valutare il rischio che tale violazione comporti per i diritti e le libertà delle persone fisiche coinvolte dal trattamento dei dati e a vagliare, caso per caso, la necessità o meno della notifica al Garante, nonché della comunicazione agli interessati.

Il Titolare è chiamato, dunque, a classificare la violazione, stabilendo se la stessa sia effettivamente suscettibile di comportare o meno un rischio per i diritti e le libertà degli interessati coinvolti e, nel primo caso, se si tratti o meno di un rischio elevato. Laddove, invece, risulti improbabile che la violazione dei dati personali possa generare rischi per i diritti e le libertà delle persone fisiche, il titolare può decidere di non inoltrare la notifica.

In caso di *data breach*, quindi, la misura del rischio va determinata in funzione dei seguenti due distinti elementi:

- **probabilità**: da intendersi come grado di effettiva possibilità che si verifichino uno o più eventi temuti (es. la perdita totale dei dati);
- **gravità**: da intendersi come rilevanza del rischio, in termini di effetti pregiudizievoli che lo stesso è in grado di produrre sui diritti e le libertà delle persone coinvolte (es. impedendo il controllo da parte dell'interessato sulla diffusione dei propri dati).

A seconda della probabilità e del grado del rischio rilevato, il Titolare dovrà quindi:

1. Notificare la violazione dei dati personali all'Autorità di controllo competente senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui sia venuto a conoscenza della stessa, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro le 72 ore, è necessario che la stessa sia corredata dei motivi del ritardo;
2. Comunicare all'interessato la violazione dei dati personali senza ingiustificato ritardo, nel caso in cui la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
3. Riportare l'evento nel Registro delle violazioni (tale ultima attività dovrà essere compiuta a prescindere, sia nel caso in cui il Titolare abbia provveduto alla notifica e/o alla comunicazione dell'incidente di sicurezza, sia quando la violazione subita non presenti alcun rischio per i diritti e le libertà dei soggetti coinvolti - es.: breve

interruzione della fornitura di energia elettrica o compromissione di dati già pubblicamente disponibili).

Al fine di vagliare la gravità del rischio, il Comitato suggerisce ai Titolari di tenere conto dei seguenti fattori:

a. il tipo di violazione occorsa;
b. la natura, la tipologia (es. dati comuni ovvero appartenenti a categorie particolari o relativi a condanne penali o reati) e il volume dei dati compromessi;
c. la facilità per soggetti terzi non autorizzati di identificare gli individui i cui dati sono stati compromessi;
d. le possibili conseguenze per gli individui;
e. le caratteristiche peculiari degli individui coinvolti (es. nel caso di minori o individui vulnerabili);
f. le caratteristiche peculiari del Titolare (es. se si tratta di una struttura sanitaria);
g. il numero di interessati coinvolti.

Ad ogni modo, secondo il Board, sussistono rischi per gli interessati quando il *data breach* possa causare agli stessi un danno fisico, materiale o immateriale. Nell'effettuare quest'analisi, è bene, quindi, che siano considerate e tenute presenti anche tutte le possibili conseguenze secondarie della violazione, che potrebbero produrre impatti significativi nella vita degli interessati.

Suggerimenti per la notifica all'Autorità di controllo

Come sottolineato dal Board nelle Linee Guida, scopo della notifica non è soltanto quello di ottenere indicazioni dall'Autorità Garante circa l'opportunità di comunicare o meno la violazione agli interessati.

In alcuni casi, del resto, può risultare immediatamente evidente, in considerazione della natura della violazione e della gravità del rischio, la necessità di effettuare tale comunicazione, senza indugio, in favore delle persone interessate.

Ad esempio, nel caso in cui sia rilevata una minaccia immediata di furto d'identità, oppure nell'eventualità in cui siano state divulgate *online* categorie particolari di dati personali, non possono sussistere dubbi sul fatto che il Titolare del trattamento debba agire senza ritardo per contenere la violazione e per informare prontamente dell'accaduto le persone coinvolte.

In circostanze eccezionali e di particolare gravità, inoltre, tale comunicazione potrebbe dover essere effettuata addirittura prima della notifica del *data breach* all'Autorità di controllo.

In ogni caso, va tenuto presente che la notifica al Garante non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato, laddove la comunicazione risulti con ogni evidenza necessaria.

Obiettivo precipuo dell'obbligo di notifica è, invero, quello di incoraggiare il Titolare del trattamento ad agire rapidamente in caso di *data breach*, al fine di contenerlo e, se possibile, di recuperare tempestivamente i dati personali compromessi.

Per tale ragione, l'art. 33 del GDPR, al paragrafo 1, richiede al Titolare di procedere alla notifica all'Autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, non oltre 72 ore dal momento in cui sia venuto a conoscenza della violazione.

L'anzidetta disposizione normativa, tuttavia, al successivo paragrafo 4, aggiunge altresì che: "*Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo*."

Il Regolamento, quindi, prende anche atto del fatto che non sempre sono acquisibili, nel ristretto termine indicato dalla norma, tutte le informazioni necessarie su un incidente di sicurezza.

In considerazione di ciò, il Board, nella nuova versione delle Linee Guida, ha riproposto una serie di indicazioni utili per l'eventualità in cui il Titolare non entri immediatamente in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva del *data breach* occorso, con un *focus* particolare sull'ipotesi in cui la notifica venga effettuata in ritardo.

L'EDPB ha ricordato, innanzitutto, come il Regolamento, nel prevedere che le informazioni possano essere fornite in fasi successive senza ulteriore ingiustificato ritardo, consenta al Titolare di procedere, laddove necessario, ad una notifica "per fasi", da attuarsi attraverso una prima e rapida notifica di *alert* (in occasione della quale il Titolare del trattamento deve comunque aver cura di informare l'Autorità del contenuto solo parziale della segnalazione), seguita dalla comunicazione di tutte le informazioni aggiuntive acquisite, attraverso l'invio di successive notifiche integrative.

Non va, inoltre, dimenticato che, anche dopo aver completato le attività di notifica, il Titolare ha comunque la facoltà di aggiornare l'Autorità di controllo, fornendo eventuali ulteriori dettagli di cui sia venuto a conoscenza nel tempo. Ciò a maggior ragione nel caso in cui, nel corso dell'indagine, venga appurato che l'incidente verificatosi sia stato contenuto e che non si sia effettivamente verificata alcuna violazione dei dati.

Queste informazioni, infatti, ben possono essere aggiunte a quelle già fornite all'Autorità di controllo, con conseguente registrazione dell'incidente come una non-violazione (o "falso positivo").

Non è prevista, del resto, come precisato dal Board, alcuna sanzione per il caso in cui venga effettuata una segnalazione di un incidente che successivamente, non avendo effettivamente dato luogo ad alcuna violazione, si riveli essere un falso positivo.

Passando poi alle notifiche effettuate in ritardo, il Comitato ha rimarcato come qualora la notifica all'Autorità di controllo non venga effettuata entro le 72 ore indicate dal GDPR, essa debba essere accompagnata dall'indicazione documentata dei motivi del ritardo.

Il Regolamento prevede, altresì, la possibilità di effettuare una "notifica differita" dopo le 72 ore previste dall'articolo 33 nel caso in cui, ad esempio, si subiscano violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al Titolare e l'invio dilazionato di un numero elevato di notificazioni tra loro identiche, il Titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

E' stato, inoltre, ribadito che, nel caso in cui il Titolare ometta di notificare una violazione dei dati all'Autorità di controllo o agli interessati, oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34 del Regolamento, l'Autorità Garante potrebbe venirsi a trovare nella condizione di dover prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'irrogazione di una sanzione amministrativa pecuniaria appropriata in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, del Regolamento, oppure come sanzione indipendente.

La comunicazione del Titolare agli interessati

Un altro degli aspetti chiave da considerare in caso di *data breach* è l'eventuale raggiungimento del livello di "allarme" più elevato, che ricorre nel caso in cui venga rilevato un rischio elevato per le libertà ed i diritti degli interessati e si debba quindi procedere alla comunicazione della violazione agli interessati coinvolti.

L'EDPB, nell'intervenire sul punto, ha fornito talune indicazioni rispetto alla comunicazione che il Titolare deve rivolgere agli interessati vittime di *data breach*.

In particolare, il Board ha precisato che:

- la comunicazione relativa ad un *data breach* deve essere data utilizzando un linguaggio semplice e chiaro, volto a specificare la natura della violazione, i dati di contatto del DPO o di altro punto di contatto da cui ottenere maggiori informazioni, le possibili conseguenze della violazione, le misure messe in atto dal Titolare per contenere danni e rischi (ivi inclusi consigli agli individui interessati per mitigare gli effetti della violazione, come ad esempio un repentino aggiornamento delle credenziali);

- la comunicazione in questione non deve essere confondibile con le comunicazioni "ordinarie" del Titolare. Ad esempio, non è lecito "nascondere" una comunicazione di *data breach* all'interno di una *newsletter* periodica;
- l'avviso deve essere fornito con il mezzo di comunicazione più efficace (a meno che tale soluzione non comporti uno sforzo sproporzionato in capo al Titolare);
- è preferibile utilizzare comunicazioni dirette rispetto a quelle indirette: una e-mail risulta avere maggiore efficacia rispetto ad un comunicato stampa, oltre ad essere uno strumento più idoneo a veicolare la comunicazione ad una pluralità di soggetti;
- in ogni caso, è fondamentale che il Titolare si adoperi per "moltiplicare" gli strumenti utilizzati per far circolare l'informazione, così da garantirne la massima diffusione (ad esempio fornendo la notizia su tutti i canali *social* dell'organizzazione, oltre che sul relativo sito istituzionale e a mezzo stampa).

Il meccanismo dello Sportello Unico (c.d. "*one-stop-shop*")

Le modifiche apportate in sede di aggiornamento del documento hanno interessato inoltre, in particolare, i paragrafi 70 e seguenti delle Linee Guida, che sono incentrati sul meccanismo dello Sportello Unico o del c.d. "*One Stop Shop*".

Con tale espressione si fa riferimento a una delle principali novità introdotte dal GDPR allo scopo di assicurare l'applicazione uniforme delle norme in materia di protezione dei dati personali nel territorio dell'Unione Europea.

Per i trattamenti di dati personali transfrontalieri – ovvero quei trattamenti realizzati da un Titolare che possieda sedi e stabilimenti situati in più Stati membri, ovvero che, pur avendo un'unica sede nel territorio UE, effettui trattamenti che incidono in modo sostanziale su interessati residenti in più di uno Stato membro –, il GDPR, allo scopo di evitare il moltiplicarsi di interventi e di pronunce potenzialmente confliggenti delle varie Autorità di controllo, ha optato per la soluzione dello Sportello Unico.

Per effetto del meccanismo del c.d. "*One Stop Shop*", i trattamenti sopra indicati ricadono, in linea di principio, nella competenza di un'unica Autorità di controllo, da individuarsi nell'Autorità Garante dello Stato membro in cui il Titolare del trattamento abbia stabilito la sua sede principale (amministrazione centrale o sede delle decisioni su finalità e mezzi del trattamento) ovvero la sede unica, che funge da Autorità 'capofila' (c.d."*leading authority*"). Questa Autorità è tenuta a coordinare, nel corso delle indagini, le autorità di controllo degli altri Stati membri interessate allo specifico caso e a coinvolgerle nel processo decisionale. L'obiettivo è giungere a una decisione condivisa, alla quale il destinatario (titolare) dovrà conformare le proprie attività di trattamento nell'Unione.

Ebbene, nella versione aggiornata delle Linee Guida, il Board ha precisato però che, nel caso in cui il Titolare del trattamento non abbia stabilito una propria sede all'interno dell'UE, ma disponga unicamente di un mero rappresentante in uno Stato Membro, il meccanismo dello Sportello Unico o "*One Stop Shop*" non può trovare applicazione. Di conseguenza, in siffatte ipotesi, al Titolare del trattamento si richiede, in caso di *data breach*, di notificare, entro il termine di 72 ore, la violazione della sicurezza dei dati occorsa ad "*ogni singola autorità per la quale gli interessati risiedono nel loro Stato membro*", ossia a tante autorità di protezione dei dati dei Paesi UE quante sono le nazionalità UE degli interessati coinvolti dall'incidente di sicurezza.

Esempi di *data breach*

Pregio della versione aggiornata delle Linee Guida è anche quello di indicare una nuova serie di esempi di *data breach,* utili ad orientare al meglio l'azione dei Titolari e dei Responsabili del trattamento nella classificazione e valutazione delle possibili casistiche di violazione e nella gestione dei processi decisionali conseguenti alla rilevazione di incidenti di sicurezza intervenuti nelle organizzazioni di appartenenza.

Detti esempi vanno, invero, ad ampliare il novero (non esaustivo) di possibili scenari di violazione già delineato in un ulteriore documento di indirizzo diramato in tempi più recenti dall'EDPB in materia di *data breach*.

Va ricordato infatti che, dopo l'emanazione delle già citate Linee Guida del 2017 - ora riproposte nella versione 2.0 -, il Comitato aveva pubblicato un ulteriore documento di indirizzo, ovverosia le Linee Guida 1/2021 su esempi riguardanti la notifica di una violazione dei dati personali (all. n. 3), con l'intento specifico di fornire una serie di indicazioni operative, accompagnate dall'esame di vari tipi di violazioni afferenti a più settori e a più scenari, che andassero a integrare, attraverso la disamina dettagliata di questioni pratiche, gli indirizzi già formulati in precedenza.

Con tale più recente pubblicazione, diffusa allo scopo di aiutare i titolari del trattamento a decidere come gestire le violazioni dei dati e quali fattori prendere in considerazione durante la valutazione del rischio, il Board ha fornito una guida pratica basata su casi concreti tratti dall'esperienza collettiva delle autorità di controllo, rispetto ai quali lo stesso gruppo di Garanti ha presentato delle proprie proposte di valutazione e di analisi delle singole fattispecie considerate, accompagnate da indicazioni specifiche sulle misure corrette da adottare.

Ebbene, nell'aggiornare le Linee Guida del 2017, il Comitato ha ritenuto di dover arricchire la casistica di *data breach* già inclusa nelle Linee Guida del 2021, indicando ulteriori possibili scenari di violazione.

Ad esempio, il Board ha incluso nel novero dei *data breach* anche l'ipotesi di una "*breve interruzione della fornitura di energia elettrica*" che per qualche minuto impedisca il

funzionamento di un call center che abbia, tra le sue funzioni, quella di agevolare il contatto tra clienti e titolare per l'esercizio dei relativi diritti.

Sebbene, come ricordato dallo stesso EDPB, qualsiasi modifica concreta delle circostanze di fatto riferite alle singole fattispecie descritte nel documento possa comportare livelli di rischio diversi o più significativi rispetto a quelli indicati e, quindi, rendere necessarie valutazioni e misure diverse o supplementari rispetto a quelle prospettate, le nuove Linee Guida non prescrivono per la tipologia di incidente sopra indicato, la notifica all'Autorità Garante e la comunicazione agli interessati i cui dati siano stati compromessi, evidenziando unicamente la necessità di aggiornare il Registro delle violazioni, con l'inserimento dell'evento e delle circostanze del caso.

Un altro esempio di *data breach* indicato nella versione aggiornata delle Linee Guida è quello della compromissione di dati già pubblicamente disponibili o, addirittura, di dati adeguatamente crittografati.

Anche in questo caso è stata segnalata unicamente la necessità di provvedere all'aggiornamento del Registro dei *data breach* (e non anche di procedere alla notifica e alla comunicazione).

Il Board, in ogni caso, nell'intervenire sul punto, ha precisato che solo una crittografia "sicura" consente di considerare i dati come non accessibili da terzi non autorizzati e questo richiede una conoscenza specifica in capo ai Titolari e ai Responsabili del trattamento circa i meccanismi di crittografia (es. complessità delle *password*, necessità di variare credenziali di *default*, crittografia durante lo *stand-by* del dispositivo, adeguamento tempo per tempo degli strumenti di crittografia ecc.).

Un dato che, ad ogni modo, è possibile trarre dalle novità introdotte è che il "*Registro dei data breach*" deve diventare un elenco molto dettagliato di ogni violazione dei dati personali eventualmente occorsa, indipendentemente dall'effettiva gravità della stessa e dai reali rischi ai quali abbia esposto gli interessati.

Misure pratiche e consigli tecnici

Nelle nuove Linee Guida viene, infine, riaffermato che è onere del Titolare e del Responsabile del trattamento implementare misure tecniche ed organizzative di protezione idonee ad assicurare la rilevazione tempestiva di eventuali violazioni, in modo tale da consentire all'organizzazione di poter reagire rapidamente e appropriatamente alle stesse.

L'art. 32 del GDPR, in merito alla "sicurezza del trattamento" specifica che nell'implementazione di misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio, occorre considerare, tra l'altro, "*la capacità di garantire la riservatezza,*

l'integrità, la disponibilità e la resilienza continue dei sistemi di trattamento e dei dati personali".

Nel pronunciarsi sul punto, l'EDPB ha ricordato innanzitutto che:

- le informazioni relative a tutti gli eventi legati alla sicurezza devono essere rese note dal Titolare ad una o più persone deputate, all'interno dell'organizzazione, ad affrontare gli incidenti di sicurezza, ad appurare l'esistenza di una violazione e a valutare il rischio;
- il rischio derivante dalla violazione – a carico degli interessati – deve essere valutato secondo i seguenti gradi: probabilità di rischio assente, rischio medio o rischio elevato, informando, di conseguenza, le sezioni pertinenti dell'organizzazione;
- se necessario, si deve procedere alla notifica all'Autorità di controllo e alla comunicazione della violazione alle persone interessate;
- allo stesso tempo, il Titolare del trattamento, con il supporto del Responsabile del trattamento ove nominato, deve agire per contenere i pericoli e i danni derivanti dalla violazione;
- è, inoltre, necessario documentare i singoli passaggi della violazione mediante la redazione di apposita documentazione (una relazione, ad esempio, mediante la quale dare atto delle misure correttive approntate - si legga il paragrafo 39 delle Linee Guida).

Nel documento vengono, inoltre, elencati ulteriori consigli tecnici per rilevare ed affrontare una violazione nel migliore dei modi.

In particolare, per individuare alcune irregolarità nel trattamento dei dati, viene suggerito ai Titolari del trattamento di avvalersi di strumenti specifici come analizzatori di flussi di dati e di *log*, grazie ai quali risulta più agevole riconoscere gli eventi e far scattare gli allarmi, puntualizzando come tali misure e meccanismi di rilevazione debbano essere quanto più dettagliati possibile al fine di consentire un maggiore controllo, nonché una migliore gestione nei piani di risposta agli incidenti e/o negli accordi di governance del titolare (paragrafo 37 delle Linee Guida).

Relativamente alle misure organizzative viene posto, poi, l'accento sul tema della "prevenzione", evidenziando come un adeguato livello di protezione dei dati non possa essere assicurato senza l'attuazione di appositi programmi di formazione e sensibilizzazione del personale sugli obblighi di *privacy* e sicurezza.

Oltre all'attivazione di specifici percorsi di formazione e consapevolezza in tema di protezione dei dati personali, le Linee Guida ricordano che può essere particolarmente utile, in tal senso, anche richiamare periodicamente l'attenzione dei dipendenti sui più comuni errori nel trattamento dati e sulle strategie per evitarli, magari trasmettendo l'importanza di una banale

politica di "*clean-desk*" per mantenere l'ordine nell'organizzazione di file e dei documenti o anche di un'attenta azione di riesame dei *file* prima dell'invio.

Passando dalle misure organizzative a quelle più tecniche, è stata evidenziata l'importanza dell'utilizzo di politiche di controllo degli accessi, che prevedano eventualmente misure di autenticazione più rigide per l'accesso a dati sensibili (ad esempio, registrandone tutti gli accessi, da consentire, a seconda dei casi, solo previa specifica motivazione).

Altre misure si focalizzano poi sulla prevenzione di possibili azioni malevole da parte dei dipendenti: la disabilitazione degli *account* istituzionali nel momento in cui un dipendente abbandona l'organizzazione dev'essere certamente tempestiva, ma è possibile anche monitorare (attraverso segnali di *alert*) insoliti flussi di dati tra *server* e postazioni di lavoro degli impiegati, allo scopo di gestire con immediatezza i casi di esfiltrazione.

Ulteriori suggerimenti riguardano, infine, la gestione delle interfacce *input/output* da BIOS (per bloccare o sbloccare l'uso di USB o altri supporti di memorizzazione) e la disabilitazione delle funzioni di stampa dello schermo nel sistema operativo.

In sostanza, viene ribadita la necessità per il Titolare di considerare tutte le possibili soluzioni per evitare o ridurre errori simili.

Il ruolo del Responsabile della Protezione dei Dati (RPD/DPO) nelle nuove Linee Guida

Le Linee Guida si soffermano, infine, sul ruolo del Responsabile della Protezione dei Dati o *Data Protection Officer* (RPD/DPO) che, nel caso di *data breach*, deve fornire assistenza e informazione al Titolare, monitorando il rispetto del GDPR e supportando l'organizzazione nella ricostruzione dell'incidente, per constatare se sia stato gestito in maniera efficiente ed efficace e per individuarne le eventuali cause.

Nella versione aggiornata del documento viene osservato inoltre come, sebbene tale compito non rientri tra quelli "ordinari" del DPO, il Titolare possa anche valutare l'opportunità di affidare al Responsabile della Protezione dei Dati l'incarico di tenere il Registro dei *data breach*, in cui documentare gli incidenti eventualmente occorsi e da esibire all'Autorità di controllo in caso di eventuali verifiche e ispezioni.

Il duplice ruolo del DPO, del resto, emerge con particolare chiarezza in questa delicata fase, in quanto il Titolare, nel notificare una violazione, deve indicare anche i dati e i recapiti del Responsabile per la Protezione dei Dati, cosicché quest'ultimo possa in seguito fungere da tramite fra l'Autorità Garante ed il Titolare.

Da ultimo, nel suggerire a codesti Spett.li Uffici di tenere conto, nell'espletamento dei relativi compiti, dei vari indirizzi dell'EDPB sopra richiamati, appare utile ricordare come

specifiche e dettagliate indicazioni sulle procedure da seguire in caso di eventuali violazioni di dati siano rinvenibili nelle "*Linee Guida per la gestione operativa dei data breach*" appositamente elaborate dal Ministero, che per ogni utilità, nelle more del relativo aggiornamento attualmente in corso, si trasmettono nuovamente (all. n. 4).

In considerazione della rilevanza della materia e della necessità di assicurare che tutto il personale dell'Amministrazione sia adeguatamente informato e istruito in merito agli obblighi da osservare e alle attività da porre in essere in caso di *data breach*, si chiede, infine, agli Spett.li Uffici in indirizzo di invitare, con le modalità ritenute più opportune, tutti i dipendenti in servizio nelle rispettive strutture a prendere visione della documentazione trasmessa, nonché a procedere alla periodica consultazione delle informazioni e dei documenti pubblicati nella sezione "Privacy", rinvenibile all'Area Riservata del sito del Ministero.

Si ringrazia per la consueta e fattiva collaborazione.

Il Responsabile della Protezione dei Dati
Alessia Auriemma

Firmato digitalmente da AURIEMMA ALESSIA
C=IT
O=MINISTERO DELL'ISTRUZIONE E DEL MERITO

Il Direttore Generale
Antonino Di Liberto

Firmato digitalmente da DI LIBERTO ANTONINO
C=IT
O=MINISTERO DELL'ISTRUZIONE

Allegati:

1. Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, adottate il 3 ottobre 2017 e poi emendate e pubblicate il 6 febbraio 2018, dal Gruppo di Lavoro Articolo 29 (Working Party 29 – WP29, poi divenuto EDPB);
2. Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679, Versione 2.0, adottate il 28 marzo 2023, dal Comitato Europeo per la Protezione dei Dati (EDPB) – versione in lingua inglese;
3. Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali, adottate il 14 dicembre 2021 dal Comitato Europeo per la Protezione dei Dati (EDPB);
4. Linee Guida per la gestione operativa dei *data breach* del Ministero – Versione Agosto 2021;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI

18/IT

WP250rev.01

Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679

adottate il 3 ottobre 2017

Versione emendata e adottata in data 6 febbraio 2018

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

istituito ai sensi della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995,

visti gli articoli 29 e 30 della stessa,

visto il suo regolamento interno,

HA ADOTTATO LE PRESENTI LINEE GUIDA:

INDICE

INTRODUZIONE

Il regolamento generale sulla protezione dei dati introduce l'obbligo di notificare una violazione dei dati personali (in appresso: "violazione") all'autorità di controllo[1] nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Attualmente l'obbligo di notifica delle violazioni esiste già per determinate organizzazioni, quali i fornitori di servizi di comunicazione elettronica accessibili al pubblico (come specificato nella direttiva 2009/136/CE e nel regolamento (UE) n. 611/2013)[2]. Inoltre, alcuni Stati membri dell'UE prevedono già un obbligo nazionale di notifica delle violazioni, che può consistere nell'obbligo di notificare violazioni che coinvolgono categorie di titolari del trattamento diversi dai fornitori di servizi di comunicazione elettronica accessibili al pubblico (ad esempio Germania e Italia) oppure nell'obbligo di segnalare tutte le violazioni riguardanti dati personali (ad esempio Paesi Bassi). Altri Stati membri dispongono di codici di buona pratica (ad esempio Irlanda[3]). Sebbene un certo numero di autorità di protezione dei dati dell'UE incoraggi già il titolare del trattamento a segnalare le violazioni, la direttiva 95/46/CE sulla protezione dei dati[4], che viene sostituita dal regolamento generale sulla protezione dei dati, non contiene uno obbligo specifico di notifica delle violazioni, pertanto tale obbligo sarà nuovo per numerose organizzazioni. Il regolamento generale sulla protezione dei dati rende ora la notifica obbligatoria per tutti i titolari del trattamento a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche[5]. Anche i responsabili del trattamento hanno un ruolo importante da svolgere e devono notificare qualsiasi violazione al proprio titolare del trattamento[6].

Il Gruppo di lavoro articolo 29 ("Gruppo di lavoro") ritiene che il nuovo obbligo di notifica presenti una serie di vantaggi. All'atto della notifica all'autorità di controllo, il titolare del trattamento può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. In effetti l'autorità di controllo può ordinare al titolare del trattamento di informare le persone fisiche interessate dalla violazione[7]. La comunicazione della violazione alle persone fisiche interessate consente al titolare del trattamento di fornire loro informazioni sui rischi derivanti dalla violazione e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione. Qualsiasi piano di risposta alle violazioni dovrebbe mirare a proteggere le persone fisiche e i loro dati personali. Di conseguenza, la notifica della violazione dovrebbe essere vista come uno

---

[1] Cfr. l'articolo 4, punto 21, del regolamento generale sulla protezione dei dati.

[2] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32009L0136 e http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32013R0611.

[3] Cfr. (in inglese) https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

[4] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:31995L0046.

[5] I diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea, disponibile all'indirizzo: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:12012P/TXT.

[6] Cfr. articolo 33, paragrafo 2. Questo concetto è analogo all'articolo 5 del regolamento (UE) n. 611/2013 nel quale si afferma che un fornitore incaricato di erogare una parte dei servizi di comunicazione elettronica (che non ha un legame contrattuale diretto con gli abbonati) è tenuto a notificare il fornitore che lo ha ingaggiato in caso di violazione di dati personali.

[7] Cfr. articolo 34, paragrafo 4 e articolo 58, paragrafo 2, lettera e).

strumento per migliorare la conformità in materia di protezione dei dati personali. Allo stesso tempo, va osservato che la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo può comportare l'imposizione di una sanzione al titolare del trattamento ai sensi dell'articolo 83.

I titolari e i responsabili del trattamento sono pertanto incoraggiati a pianificare anticipatamente e a mettere in atto processi per essere in grado di rilevare e limitare tempestivamente gli effetti di una violazione, valutare il rischio per le persone fisiche[8] e stabilire se sia necessario notificare la violazione all'autorità di controllo competente e comunicarla alle persone fisiche interessate, ove necessario. La notifica all'autorità di controllo dovrebbe costituire parte del piano di intervento in caso di incidente.

Il regolamento contiene disposizioni che specificano quando e a chi la violazione deve essere notificata e quali informazioni devono essere fornite nel contesto della notifica. Le informazioni richieste per la notifica possono essere fornite procedendo per fasi, tuttavia il titolare del trattamento deve agire sempre in maniera tempestiva in caso di violazione.

Nel parere 03/2014 sulla notifica delle violazioni dei dati personali[9], il Gruppo di lavoro ha fornito orientamenti ai titolari del trattamento per aiutarli a decidere se effettuare la notifica agli interessati in caso di violazione. Il parere ha preso in considerazione l'obbligo dei fornitori di comunicazioni elettroniche ai sensi della direttiva 2002/58/CE e ha fornito esempi afferenti a più settori, nel contesto dell'allora progetto di regolamento generale sulla protezione dei dati, e ha illustrato le buone prassi per tutti i titolari del trattamento.

Le presenti linee guida spiegano gli obblighi di notifica e di comunicazione delle violazioni sanciti dal regolamento, nonché alcune misure che i titolari e i responsabili del trattamento possono intraprendere per soddisfare questi nuovi obblighi. Forniscono inoltre esempi di vari tipi di violazioni e i soggetti ai quali esse devono essere notificate nei diversi scenari.

I. Notifica delle violazioni dei dati personali ai sensi del regolamento generale sulla protezione dei dati

A. Considerazioni di base in materia di sicurezza

Una delle prescrizioni del regolamento prevede che, mediante misure tecniche e organizzative adeguate, i dati personali siano trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali[10].

Di conseguenza, il regolamento impone tanto al titolare quanto al responsabile del trattamento di disporre di misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato al rischio cui sono esposti i dati personali trattati. Tali soggetti dovrebbero tenere conto: dello stato

[8] Ciò può essere garantito rispettando l'obbligo di monitoraggio e riesame previsto da una valutazione d'impatto sulla protezione dei dati, richiesta per i trattamenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche (articolo 35, paragrafi 1 e 11).

[9] Cfr. parere 03/2014 sulla notifica delle violazioni dei dati personali (in inglese) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[10] Cfr. articolo 5, paragrafo 1, lettera f) e articolo 32.

dell'arte e dei costi di attuazione; della natura, dell'oggetto, del contesto e delle finalità del trattamento; del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche[11]. Inoltre, il regolamento impone di mettere in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali, il che a sua volta consente di stabilire se scatta l'obbligo di notifica[12].

Di conseguenza, un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

B. Che cos'è una violazione dei dati personali?

1. Definizione

Per poter porre rimedio a una violazione occorre innanzitutto che il titolare del trattamento sia in grado di riconoscerla. All'articolo 4, punto 12, il regolamento definisce la "violazione dei dati personali" come segue:

> "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".

Il significato di "distruzione" dei dati personali dovrebbe essere abbastanza chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento. Anche il concetto di "danno" dovrebbe essere relativamente evidente: si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi. Con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso. Infine, un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a ricevere (o ad accedere a) i dati oppure qualsiasi altra forma di trattamento in violazione del regolamento.

Esempio

Un esempio di perdita di dati personali può essere la perdita o il furto di un dispositivo contenente una copia della banca dati dei clienti del titolare del trattamento. Un altro esempio può essere il caso in cui l'unica copia di un insieme di dati personali sia stata crittografata da un *ransomware* (*malware* del riscatto) oppure dal titolare del trattamento mediante una chiave non più in suo possesso.

Ciò che dovrebbe essere chiaro è che una violazione è un tipo di incidente di sicurezza. Tuttavia, come indicato all'articolo 4, punto 12, il regolamento si applica soltanto in caso di violazione di *dati personali*. La conseguenza di tale violazione è che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del regolamento. Questo punto mette in luce la differenza tra un incidente di sicurezza e una violazione

[11] Articolo 32; cfr. anche considerando 83.

[12] Cfr. considerando 87.

dei dati personali: mentre tutte le violazioni dei dati personali sono incidenti di sicurezza, non tutti gli incidenti di sicurezza sono necessariamente violazioni dei dati personali[13].

I potenziali effetti negativi di una violazione sulle persone fisiche sono esaminati in appresso.

2. Tipi di violazioni dei dati personali

Nel parere 03/2014 sulla notifica delle violazioni, il Gruppo di lavoro ha spiegato che le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni[14]:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso[15] o distruzione accidentali o non autorizzati di dati personali.

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.

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. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.

Esempio

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 permanente.

Può verificarsi perdita di disponibilità anche in caso di interruzione significativa del servizio abituale di un'organizzazione, ad esempio un'interruzione di corrente o attacco da "blocco di servizio" (*denial of service*) che rende i dati personali indisponibili.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del

[13] Va osservato che un incidente di sicurezza non si limita ai modelli di minacce nei quali un attacco viene effettuato ai danni di un'organizzazione dall'esterno della stessa, bensì include anche incidenti derivanti dal trattamento interno che violano i principi di sicurezza.

[14] Cfr. parere 03/2014.

[15] È un fatto assodato che "l'accesso" è una componente fondamentale della "disponibilità". Cfr. ad esempio il documento NIST SP800-53rev4, che definisce la "disponibilità" come la "garanzia di un accesso e un uso tempestivi e affidabili delle informazioni", disponibile (in inglese) all'indirizzo http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. Anche il documento CNSSI-4009 fa riferimento a un "accesso tempestivo e affidabile ai dati e ai servizi dell'informazione per gli utenti autorizzati." Cfr. https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. Anche la norma ISO/IEC 27000:2016 definisce la "disponibilità" come la "proprietà di essere accessibile e utilizzabile su richiesta da un soggetto autorizzato": (in inglese) https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en.

regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5. Ciò aiuta il titolare del trattamento a dimostrare l'assunzione di responsabilità all'autorità di controllo, che potrebbe chiedere di consultare tali registrazioni[16]. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il titolare del trattamento dovrà valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33, il titolare del trattamento dovrà effettuare la notifica a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Questo punto dovrà chiaramente essere valutato caso per caso.

Esempi

L'indisponibilità, anche solo temporanea, di dati medici critici di pazienti di un ospedale potrebbe presentare un rischio per i diritti e le libertà delle persone interessate, poiché, ad esempio, potrebbe comportare l'annullamento di operazioni e mettere a rischio le vite dei pazienti.

Viceversa, se i sistemi di una società di comunicazione non sono disponibili per diverse ore (ad esempio a causa di un'interruzione dell'alimentazione) e tale società non riesce a inviare newsletter ai propri abbonati è improbabile che ciò presenti un rischio per i diritti e le libertà delle persone fisiche.

Va notato che, 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 altri motivi.

Esempio

Un'infezione da *ransomware* (software dannoso che cifra i dati del titolare del trattamento finché non viene pagato un riscatto) potrebbe comportare una perdita temporanea di disponibilità se i dati possono essere ripristinati da un backup. Tuttavia, si è comunque verificata un'intrusione nella rete e potrebbe essere richiesta una notifica se l'incidente è qualificato come violazione della riservatezza (ad esempio se chi ha effettuato l'attacco ha avuto accesso a dati personali) e ciò presenta un rischio per i diritti e le libertà delle persone fisiche.

[16] Cfr. articolo 33, paragrafo 5.

3. Possibili conseguenze di una violazione dei dati personali

Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali, ad esempio la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo alle persone fisiche interessate[17].

Di conseguenza, il regolamento impone al titolare del trattamento di notificare le violazioni all'autorità di controllo competente, fatta salva l'improbabilità che la violazione presenti il rischio che si verifichino detti effetti negativi. Laddove sia altamente probabile che tali effetti negativi si verifichino, il regolamento impone al titolare del trattamento di comunicare la violazione alle persone fisiche interessate non appena ciò sia ragionevolmente fattibile[18].

L'importanza di essere in grado di identificare una violazione, di valutare il rischio per le persone fisiche e, di conseguenza, di effettuare la notifica se necessario, è sottolineata nel considerando 87 del regolamento:

> "È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

Ulteriori linee guida sulla valutazione del rischio di effetti negativi per le persone fisiche sono considerate nella sezione IV.

Se il titolare del trattamento omette di notificare una violazione dei dati all'autorità di controllo o agli interessati oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34, l'autorità di controllo dovrà effettuare una scelta e prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'imposizione di una sanzione amministrativa pecuniaria appropriata[19], in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, oppure come sanzione indipendente. Qualora l'autorità opti per una sanzione amministrativa pecuniaria il suo valore può ammontare fino a un massimo di 10 000 000 EUR o fino al 2% del fatturato totale annuo globale di un'impresa ai sensi dell'articolo 83, paragrafo 4, lettera a), del regolamento. È altresì importante ricordare che, in alcuni casi, la mancata notifica di una violazione potrebbe rivelare l'assenza di misure di sicurezza o la loro inadeguatezza. Gli orientamenti del Gruppo di lavoro in materia di sanzioni amministrative affermano che "qualora nell'ambito di un singolo caso siano state commesse congiuntamente più violazioni diverse, l'autorità di controllo può applicare le sanzioni amministrative pecuniarie a un livello che risulti effettivo, proporzionato e dissuasivo entro i limiti

[17] Cfr. anche considerando 85 e 75.

[18] Cfr. anche il considerando 86.

[19] Per ulteriori dettagli, consultare le linee guida del Gruppo di lavoro riguardanti l'applicazione e la previsione delle sanzioni amministrative pecuniarie disponibili qui: https://www.garanteprivacy.it/documents/10160/0/WP+253++Linee+guida+sanzioni+amministrative+pecuniarie+Reg+UE+2016+679.

della violazione più grave". In tal caso, l'autorità di controllo avrà altresì la possibilità di comminare sanzioni per la mancata notifica o comunicazione della violazione (articoli 33 e 34), da un lato, e l'assenza di misure di sicurezza (adeguate) (articolo 32), dall'altro, in quanto si tratta di due infrazioni separate.

II. Articolo 33 - Notifica all'autorità di controllo

A. Quando effettuare la notifica

1. Prescrizioni dell'articolo 33

L'articolo 33, paragrafo 1, stabilisce che:

> "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Il considerando 87[20] stabilisce che:

> "È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato. È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato. Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento".

2. Quando il titolare del trattamento viene "a conoscenza" di una violazione?

Come indicato in precedenza, il regolamento 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. 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 il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali.

Tuttavia, come già osservato, il regolamento impone al titolare del trattamento di attuare tutte le misure tecniche e organizzative di protezione adeguate per stabilire immediatamente se si è verificata una violazione e informare tempestivamente l'autorità di controllo e gli interessati. Afferma altresì che è opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione e delle sue conseguenze e dei suoi effetti negativi per l'interessato[21]. Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate.

[20] Anche il considerando 85 è importante in questo caso.

[21] Cfr. considerando 87.

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. Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario.

Esempi

1. In caso di perdita di una chiave USB contenente dati personali non crittografati spesso non è possibile accertare se persone non autorizzate abbiano avuto accesso ai dati. Tuttavia, anche se il titolare del trattamento non è in grado di stabilire se si è verificata una violazione della riservatezza, tale caso deve essere notificato, in quanto sussiste una ragionevole certezza del fatto che si è verificata una violazione della disponibilità; il titolare del trattamento si considera venuto "a conoscenza" della violazione nel momento in cui si è accorto di aver perso la chiave USB.

2. Un terzo 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".

3. Un titolare del trattamento rileva che c'è stata una possibile intrusione nella sua rete. Controlla quindi i propri sistemi per stabilire se i dati personali ivi presenti sono stati compromessi e ne ottiene conferma. Ancora una volta, dato che il titolare del trattamento ha una chiara prova di una violazione non può esserci dubbio che sia venuto "a conoscenza" della stessa.

4. Un criminale informatico viola il sistema del titolare del trattamento e lo contatta per chiedere un riscatto. In tal caso, dopo aver verificato il suo sistema per accertarsi dell'attacco, il titolare del trattamento dispone di prove evidenti che si è verificata una violazione e non vi è dubbio che ne sia venuto a conoscenza.

Se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza". Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata.

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. Tuttavia, il titolare del trattamento potrebbe già disporre di una valutazione iniziale del rischio potenziale che potrebbe derivare da una violazione come parte di una valutazione d'impatto sulla protezione dei dati[22] effettuata prima dello svolgimento del trattamento interessato. Tuttavia, tale valutazione può essere più generale rispetto alle circostanze specifiche di un'effettiva violazione e, pertanto, in ogni caso dovrà essere effettuata una valutazione aggiuntiva che tenga conto di tali circostanze. Per maggiori dettagli sulla valutazione del rischio, si rinvia alla sezione IV.

[22] Cfr. le linee guida del Gruppo di lavoro in materia di valutazioni d'impatto sulla protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

Nella maggior parte dei casi queste azioni preliminari dovrebbero essere completate subito dopo l'allerta iniziale (ossia quando il titolare o il responsabile del trattamento sospetta che si sia verificato un incidente di sicurezza che potrebbe interessare dati personali); dovrebbe richiedere più tempo soltanto in casi eccezionali.

Esempio

Una persona informa il titolare del trattamento di aver ricevuto un'e-mail da un soggetto che si fa passare per il titolare del trattamento, contenente dati personali relativi al suo (effettivo) utilizzo del servizio del titolare del trattamento, aspetto questo che suggerisce che la sicurezza del titolare del trattamento sia stata compromessa. Il titolare del trattamento conduce una breve indagine e individua un'intrusione nella propria rete e la prova di un accesso non autorizzato ai dati personali. Il titolare del trattamento si considera "a conoscenza" della violazione in questo momento e dovrà procedere alla notifica all'autorità di controllo a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il titolare del trattamento dovrà prendere le opportune misure correttive per far fronte alla violazione.

Di conseguenza, il titolare del trattamento dovrebbe disporre di procedure interne per poter rilevare una violazione e porvi rimedio. Ad esempio, per rilevare talune irregolarità nel trattamento dei dati, il titolare o il responsabile del trattamento può utilizzare alcune misure tecniche certe come il flusso di dati e gli analizzatori di registri, dai quali è possibile definire eventi e allerte correlando qualsiasi dato di registro[23]. È importante che quando viene rilevata una violazione, la stessa venga segnalata al livello superiore appropriato di gestione, in maniera da poter essere trattata e, se del caso, notificata in conformità all'articolo 33 e, se necessario, all'articolo 34. Tali misure e meccanismi di segnalazione potrebbero essere dettagliati nei piani di intervento in caso di incidente del titolare del trattamento e/o nei dispositivi di governo societario. Ciò consentirà al titolare del trattamento di pianificare in maniera efficace e di stabilire chi ha la responsabilità operativa all'interno dell'organizzazione per la gestione di una violazione, nonché le modalità o l'opportunità di segnalare un incidente al livello gerarchico superiore, se del caso.

Il titolare del trattamento dovrebbe inoltre disporre di accordi con i responsabili del trattamento ai quali fa ricorso, i quali hanno a loro volta l'obbligo di notificare al titolare del trattamento eventuali violazioni (cfr. in appresso).

Sebbene spetti al titolare e al responsabile del trattamento mettere in atto misure adeguate per essere in grado di prevenire, reagire e affrontare una violazione, alcune misure pratiche dovrebbero essere prese in ogni caso:

- 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;
- il rischio per le persone fisiche a seguito di una violazione dovrebbe quindi essere valutato (probabilità di nessun rischio, di rischio o di rischio elevato) e le sezioni pertinenti dell'organizzazione dovrebbero esserne informate;
- se necessario si dovrebbe procedere alla notifica all'autorità di controllo ed eventualmente alla comunicazione della violazione alle persone fisiche interessate;
- allo stesso tempo, il titolare del trattamento dovrebbe agire in maniera tale da arginare la violazione e risolverla;

[23] Va osservato che anche i dati di registro che facilitano la verificabilità, ad esempio, della memorizzazione, delle modifiche o della cancellazione dei dati possono essere considerati dati personali relativi alla persona che ha avviato il trattamento corrispondente.

- la violazione dovrebbe essere documentata durante tutta la sua evoluzione.

Di conseguenza, dovrebbe essere chiaro che il titolare del trattamento è tenuto ad agire in relazione a qualsiasi allerta e stabilire se effettivamente si sia verificata una violazione. Tale breve periodo consente lo svolgimento di alcune indagini e dà al titolare del trattamento la possibilità di raccogliere prove e altre informazioni pertinenti. Tuttavia, dopo che il titolare del trattamento ha stabilito con ragionevole certezza che si è verificata una violazione, qualora siano soddisfatte le condizioni di cui all'articolo 33, paragrafo 1, è quindi necessario informare l'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore[24]. Se il titolare del trattamento non agisce in maniera tempestiva e risulta evidente che si è verificata una violazione, la sua inazione potrebbe essere considerata una mancata notifica ai sensi dell'articolo 33.

L'articolo 32 chiarisce che il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello adeguato di sicurezza dei dati personali: la capacità di individuare, trattare e segnalare tempestivamente una violazione deve essere considerata un aspetto essenziale di queste misure.

3. Contitolari del trattamento

L'articolo 26 riguarda i contitolari del trattamento e specifica che essi devono determinare le rispettive responsabilità in merito all'osservanza del regolamento[25]. Ciò includerà la determinazione di chi sarà responsabile di adempiere agli obblighi di cui agli articoli 33 e 34. Il Gruppo di lavoro raccomanda che gli accordi contrattuali tra i contitolari del trattamento includano disposizioni che stabiliscano quale titolare del trattamento assumerà il comando o sarà responsabile del rispetto degli obblighi di notifica delle violazioni previsti dal regolamento.

4. Obblighi del responsabile del trattamento

Sebbene il titolare del trattamento conservi la responsabilità generale per la protezione dei dati personali, il responsabile del trattamento svolge un ruolo importante nel consentire al titolare del trattamento di adempiere ai propri obblighi, segnatamente in materia di notifica delle violazioni. L'articolo 28, paragrafo 3, dispone che il trattamento da parte di un responsabile del trattamento è disciplinato da un contratto o da un altro atto giuridico, e precisa, alla lettera f), che il contratto o altro atto giuridico deve prevedere che il responsabile del trattamento "assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

L'articolo 33, paragrafo 2, chiarisce che se il titolare del trattamento ricorre a un responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del titolare del trattamento, il responsabile del trattamento deve notificarla al titolare del trattamento "senza ingiustificato ritardo". Va notato che il responsabile del trattamento non deve valutare la probabilità di rischio derivante dalla violazione prima di notificarla al titolare del trattamento; spetta infatti a quest'ultimo effettuare la valutazione nel momento in cui viene a conoscenza della violazione. Il responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e quindi notificarla al titolare del trattamento. Poiché quest'ultimo si serve del responsabile del trattamento per conseguire le proprie finalità, in linea di principio dovrebbe considerarsi "a conoscenza" della violazione non appena il responsabile del trattamento gliela

[24] Cfr. il regolamento (CEE, Euratom) n. 1182/71 che stabilisce le norme applicabili ai periodi di tempo, alle date e ai termini, disponibile all'indirizzo: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:31971R1182&from=IT.

[25] Cfr. anche il considerando 79.

notifica. L'obbligo del responsabile del trattamento di effettuare la notifica al titolare del trattamento consente a quest'ultimo di far fronte alla violazione e di stabilire se deve notificarla all'autorità di controllo ai sensi dell'articolo 33, paragrafo 1, e alle persone fisiche interessate ai sensi dell'articolo 34, paragrafo 1. Il titolare del trattamento potrebbe anche indagare sulla violazione, in quanto il responsabile del trattamento potrebbe non conoscere tutti i fatti pertinenti connessi alla violazione, ad esempio potrebbe ignorare se il titolare del trattamento detiene comunque una copia o un backup dei dati personali distrutti o persi. Tale circostanza può influire sull'eventualità che il titolare del trattamento debba effettuare la notifica.

Il regolamento non fissa un termine esplicito entro il quale il responsabile del trattamento deve avvertire il titolare del trattamento, salvo specificare che deve farlo "senza ingiustificato ritardo". Di conseguenza, il Gruppo di lavoro raccomanda al responsabile del trattamento di effettuare la notifica al titolare del trattamento tempestivamente, fornendo successivamente le eventuali ulteriori informazioni sulla violazione di cui venga a conoscenza. Ciò è importante al fine di aiutare il titolare del trattamento a soddisfare l'obbligo di notifica all'autorità di controllo entro 72 ore.

Come precedentemente spiegato, il contratto tra il titolare del trattamento e il responsabile del trattamento dovrebbe specificare le modalità per il soddisfacimento delle prescrizioni di cui all'articolo 33, paragrafo 2, e delle altre disposizioni del regolamento, tra cui i requisiti per la notifica tempestiva da parte del responsabile del trattamento, che serve per aiutare il titolare del trattamento a rispettare l'obbligo di segnalare la violazione all'autorità di controllo entro 72 ore.

Qualora fornisca servizi a più titolari del trattamento tutti interessati dal medesimo incidente, il responsabile del trattamento dovrà segnalare i dettagli dell'incidente a ciascun titolare del trattamento.

Il responsabile del trattamento può effettuare la notifica per conto del titolare del trattamento qualora quest'ultimo gli abbia concesso l'opportuna autorizzazione e ciò faccia parte degli accordi contrattuali tra il titolare del trattamento e il responsabile del trattamento. La notifica deve essere effettuata conformemente agli articoli 33 e 34. Tuttavia, è importante osservare che la responsabilità legale della notifica rimane in capo al titolare del trattamento.

B. Fornire informazioni all'autorità di controllo

1. Informazioni da fornire

Quando il titolare del trattamento notifica una violazione all'autorità di controllo, l'articolo 33, paragrafo 3 stabilisce che 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".

Il regolamento non definisce le categorie di interessati né le registrazioni di dati personali. Tuttavia, il Gruppo di lavoro suggerisce che le categorie di interessati si riferiscono ai vari tipi di persone fisiche i cui dati personali sono stati oggetto di violazione: a seconda dei descrittori utilizzati, ciò potrebbe includere, tra gli altri, minori e altri gruppi vulnerabili, persone con disabilità, dipendenti o clienti.

Analogamente, le categorie di registrazioni dei dati personali fanno riferimento ai diversi tipi di registrazioni che il titolare del trattamento può trattare, quali dati sanitari, registri didattici, informazioni sull'assistenza sociale, dettagli finanziari, numeri di conti bancari, numeri di passaporto, ecc.

Il considerando 85 chiarisce che uno degli scopi della notifica consiste nel limitare i danni alle persone fisiche. Di conseguenza, 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. In questo modo, l'obbligo di descrivere le categorie si collega all'obbligo di descriverne le probabili conseguenze della violazione.

Il fatto che non siano disponibili informazioni precise (ad esempio il numero esatto di interessati coinvolti) non dovrebbe costituire un ostacolo alla notifica tempestiva delle violazioni. Il regolamento consente di effettuare approssimazioni sul numero di persone fisiche interessate e di registrazioni dei dati personali coinvolte. Ci si dovrebbe preoccupare di far fronte agli effetti negativi della violazione piuttosto che di fornire cifre esatte. Di conseguenza, quando è evidente che c'è stata una violazione ma non se ne conosce ancora la portata, un modo sicuro per soddisfare gli obblighi di notifica è procedere a una notifica per fasi (cfr. in appresso).

L'articolo 33, paragrafo 3, stabilisce che nella notifica il titolare del trattamento "deve almeno" fornire le informazioni previste; di conseguenza il titolare del trattamento può, se necessario, fornire ulteriori informazioni. I diversi tipi di violazioni (riservatezza, integrità o disponibilità) possono richiedere la fornitura di ulteriori informazioni per spiegare in maniera esaustiva le circostanze di ciascun caso.

Esempio

Nell'ambito della notifica all'autorità di controllo, il titolare del trattamento può ritenere utile indicare il nome del responsabile del trattamento, qualora quest'ultimo sia la causa di fondo della violazione, in particolare se quest'ultima ha provocato un incidente ai danni delle registrazioni dei dati personali di molti altri titolari del trattamento che fanno ricorso al medesimo responsabile del trattamento.

In ogni caso, l'autorità di controllo può richiedere ulteriori dettagli nel contesto dell'indagine su una violazione.

2. Notifica per fasi

A seconda della natura della violazione, il titolare del trattamento può avere la necessità di effettuare ulteriori accertamenti per stabilire tutti i fatti pertinenti relativi all'incidente. L'articolo 33, paragrafo 4, afferma pertanto:

"Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo".

Ciò significa che il regolamento prende atto del fatto che il titolare del trattamento non sempre dispone di tutte le informazioni necessarie su una violazione entro 72 ore dal momento in cui ne è venuto a conoscenza, dato che non sempre sono disponibili entro tale termine dettagli completi ed esaustivi su un incidente. Pertanto, il regolamento consente una notifica per fasi. È più probabile che ciò si verifichi in caso di violazioni più complesse, quali alcuni tipi di incidenti di sicurezza informatica nel contesto dei quali, ad esempio, può essere necessaria un'indagine forense approfondita per stabilire appieno la natura della violazione e la portata della compromissione dei dati personali. Di conseguenza, in molti casi il titolare del trattamento dovrà effettuare ulteriori indagini e dare seguito alla notifica fornendo informazioni supplementari in un secondo momento. Ciò è

consentito a condizione che il titolare del trattamento indichi i motivi del ritardo, in conformità all'articolo 33, paragrafo 1. Il Gruppo di lavoro 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.

L'obiettivo dell'obbligo di notifica consiste nell'incoraggiare il titolare del trattamento ad agire prontamente in caso di violazione, a contenerla e, se possibile, a recuperare i dati personali compromessi e a chiedere un parere pertinente all'autorità di controllo. La notifica all'autorità di controllo entro le prime 72 ore può consentire al titolare del trattamento di assicurarsi che le decisioni in merito alla notifica o alla mancata notifica alle persone fisiche siano corrette.

Tuttavia, lo scopo della notifica all'autorità di controllo non è solo di ottenere orientamenti sull'opportunità di effettuare o meno la notifica alle persone fisiche interessate. In certi casi sarà evidente che, a causa della natura della violazione e della gravità del rischio, il titolare del trattamento dovrà effettuare la notifica alle persone fisiche coinvolte senza indugio. Ad esempio, se esiste una minaccia immediata di usurpazione d'identità oppure se categorie particolari di dati personali[26] vengono divulgate online, il titolare del trattamento deve agire senza ingiustificato ritardo per contenere la violazione e comunicarla alle persone fisiche coinvolte (cfr. sezione III). In circostanze eccezionali, ciò potrebbe persino aver luogo prima della notifica all'autorità di controllo. Più in generale, la notifica all'autorità di controllo non può fungere da giustificazione per la mancata comunicazione della violazione all'interessato laddove la comunicazione sia richiesta.

È opportuno inoltre precisare che se, dopo la notifica iniziale, una successiva indagine dimostra che l'incidente di sicurezza è stato contenuto e che non si è verificata alcuna violazione il titolare del trattamento può informarne l'autorità di controllo. Tali informazioni possono quindi essere aggiunte alle informazioni già fornite all'autorità di controllo e l'incidente può essere quindi registrato come un evento che non costituisce una violazione. Non si incorre in alcuna sanzione se si segnala un incidente che alla fine si rivela non essere una violazione.

Esempio

Un titolare del trattamento notifica all'autorità di controllo entro 72 ore l'individuazione di una violazione derivante dalla perdita di una chiave USB contenente una copia dei dati personali di alcuni dei suoi clienti. In seguito scopre che la chiave USB non era stata messa al suo posto e la recupera. Il titolare del trattamento aggiorna l'autorità di controllo e chiede la modifica della notifica.

Va osservato che un approccio per fasi alla notifica esiste già in forza degli obblighi di cui alla direttiva 2002/58/CE, del regolamento 611/2013 e nel quadro di altri incidenti segnalati di propria iniziativa.

3. Notifiche effettuate in ritardo

L'articolo 33, paragrafo 1, chiarisce che, qualora non sia effettuata entro 72 ore, la notifica all'autorità di controllo deve essere corredata dei motivi del ritardo. Questa disposizione, unitamente al concetto di notifica in fasi, riconosce che il titolare del trattamento potrebbe non essere sempre in grado di notificare una violazione entro tale termine e che una notifica tardiva può essere consentita.

[26] Cfr. articolo 9.

Tale scenario potrebbe aver luogo, ad esempio, qualora il titolare del trattamento subisca in poco tempo violazioni della riservatezza multiple e simili che coinvolgono allo stesso modo un gran numero di interessati. Il titolare del trattamento potrebbe prendere atto di una violazione e, nel momento in cui inizia l'indagine e prima della notifica, rilevare ulteriori violazioni analoghe, che hanno cause differenti. A seconda delle circostanze, il titolare del trattamento può impiegare del tempo per stabilire l'entità delle violazioni e, anziché notificare ciascuna violazione separatamente, effettuare una notifica significativa che rappresenta diverse violazioni molto simili tra loro, con possibili cause diverse. La notifica all'autorità di controllo potrebbe quindi aver luogo in ritardo, oltre le 72 ore dopo che il titolare del trattamento è venuto a conoscenza di tali violazioni.

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'articolo 33.

Sebbene il regolamento consenta di effettuare la notifica in ritardo, questa non dovrebbe essere vista come la regola. È opportuno sottolineare che le notifiche cumulative possono essere effettuate anche per più violazioni analoghe segnalate entro 72 ore.

C. Violazioni transfrontaliere e violazioni presso stabilimenti non UE

1. Violazioni transfrontaliere

In caso di trattamento transfrontaliero[27] dei dati personali, una violazione può riguardare interessati in più Stati membri. L'articolo 33, paragrafo 1, chiarisce che quando si è verificata una violazione, il titolare del trattamento deve effettuare una notifica all'autorità di controllo competente ai sensi dell'articolo 55 del regolamento[28]. L'articolo 55, paragrafo 1, afferma che:

> "Ogni autorità di controllo è competente a eseguire i compiti assegnati e a esercitare i poteri a essa conferiti a norma del presente regolamento nel territorio del rispettivo Stato membro".

Tuttavia, l'articolo 56, paragrafo 1, stabilisce che:

> "Fatto salvo l'articolo 55, l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare del trattamento o responsabile del trattamento, secondo la procedura di cui all'articolo 60".

Inoltre, l'articolo 56, paragrafo 6, afferma che:

> "L'autorità di controllo capofila è l'unico interlocutore del titolare del trattamento o del responsabile del trattamento in merito al trattamento transfrontaliero effettuato da tale titolare del trattamento o responsabile del trattamento".

[27] Cfr. articolo 4, paragrafo 23.

[28] Cfr. anche il considerando 122.

Ciò significa che ogniqualvolta si verifichi una violazione nel contesto di un trattamento transfrontaliero e si renda necessaria la notifica, il titolare del trattamento dovrà effettuare la notifica all'autorità di controllo capofila[29]. Pertanto, nel redigere il proprio piano di risposta alle violazioni, il titolare del trattamento deve valutare quale autorità di controllo sia l'autorità capofila a cui indirizzare le notifiche[30]. Il titolare del trattamento sarà così in grado di rispondere tempestivamente alle violazioni e di adempiere i propri obblighi di cui all'articolo 33. Dovrebbe essere chiaro che, in caso di violazione che comporta un trattamento transfrontaliero, la notifica deve essere effettuata all'autorità di controllo capofila, che non si trova necessariamente nel luogo in cui si trovano gli interessati coinvolti o dove si è verificata la violazione. Al momento della notifica all'autorità capofila, il titolare del trattamento dovrebbe indicare, se del caso, se la violazione coinvolge stabilimenti situati in altri Stati membri e gli Stati membri in cu potrebbero esserci interessati colpiti dalla violazione. Se nutre dei dubbi sull'identità dell'autorità di controllo capofila, il titolare del trattamento deve come minimo effettuare la notifica all'autorità di controllo locale del luogo in cui si è verificata la violazione.

2. Violazioni presso stabilimenti non UE

L'articolo 3 definisce l'ambito di applicazione territoriale del regolamento, che si applica anche al trattamento di dati personali effettuato da un titolare del trattamento o un responsabile del trattamento che non è stabilito nell'UE. In particolare, l'articolo 3, paragrafo 2, afferma che[31]:

> "Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:
>
> a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
>
> b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione".

Anche l'articolo 3, paragrafo 3, è pertinente al riguardo e afferma che[32]:

> "Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico".

Se un titolare del trattamento non stabilito nell'UE è soggetto all'articolo 3, paragrafo 2, oppure all'articolo 3, paragrafo 3, e constata una violazione, è quindi comunque vincolato agli obblighi di notifica di cui agli articoli 33 e 34. L'articolo 27 impone al titolare del trattamento (e al responsabile del trattamento) di designare un rappresentante nell'Unione europea nel caso in cui si applichi l'articolo 3, paragrafo 2. In tali casi, il Gruppo di lavoro raccomanda di inviare la notifica all'autorità

---

[29] Cfr. linee guida del Gruppo di lavoro per l'individuazione dell'autorità di controllo capofila in relazione a uno specifico titolare del trattamento o responsabile del trattamento, disponibile (in inglese) all'indirizzo http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[30] Un elenco dei dati di contatto per tutte le autorità nazionali europee per la protezione dei dati è disponibile (in inglese) all'indirizzo: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

[31] Cfr. anche considerando 23 e 24.

[32] Cfr. anche il considerando 25.

di controllo dello Stato membro in cui è stabilito il rappresentante del titolare del trattamento nell'UE[33]. Analogamente, se un responsabile del trattamento è soggetto all'articolo 3, paragrafo 2, sarà tenuto a rispettare gli obblighi imposti ai responsabili del trattamento, in particolare l'obbligo di notificare una violazione al titolare del trattamento ai sensi dell'articolo 33, paragrafo 2.

D. Circostanze nelle quali non è richiesta la notifica

L'articolo 33, paragrafo 1, chiarisce che se è "improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche" tale violazione non è soggetta a notifica all'autorità di controllo. Un esempio potrebbe essere quello di dati personali già disponibili pubblicamente, la cui divulgazione non costituirebbe un rischio probabile per la persona fisica. Questa esenzione dalla notifica è in contrasto con gli attuali obblighi di notifica delle violazioni imposti ai fornitori di servizi di comunicazione elettronica accessibili al pubblico di cui alla direttiva 2009/136/CE, che stabilisce che tutte le violazioni rilevanti devono essere notificate all'autorità competente.

Nel parere 03/2014 sulla notifica delle violazioni[34], 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 ed è stata generata in maniera tale da non poter essere individuata con i mezzi tecnici disponibili da qualcuno che non è autorizzato ad accedervi), in linea di principio i dati risultano incomprensibili. Di conseguenza è improbabile che la violazione possa influire negativamente sulle persone fisiche e quindi non dovrebbe essere loro comunicata[35]. Tuttavia, anche 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.

Il Gruppo di lavoro ha altresì spiegato che lo stesso ragionamento si applica anche nel caso in cui dati personali, quali password, siano stati codificati in modo sicuro con un hash e un salt, il valore hash sia stato calcolato con una funzione di hash con chiave crittografica all'avanguardia, la chiave utilizzata per l'hashing dei dati non sia stata compromessa nell'ambito di una violazione della sicurezza e sia stata generata in maniera tale da non poter essere individuata con i mezzi tecnologici a disposizione di qualcuno che non è autorizzato ad accedervi.

Di conseguenza, se i dati personali sono stati resi sostanzialmente incomprensibili ai soggetti non autorizzati e se esiste una copia o un backup, una violazione della riservatezza che coinvolga dati personali correttamente crittografati potrebbe non dover essere notificata all'autorità di controllo, poiché è improbabile che tale violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche. Di conseguenza potrebbe non essere necessario nemmeno informare la persona interessata, dato che è improbabile che vi siano rischi elevati. Tuttavia, si dovrebbe tenere presente che, sebbene inizialmente la notifica possa non essere richiesta se non esiste un rischio probabile per i diritti e le libertà delle persone fisiche, la situazione può cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato. Ad esempio, se la chiave risulta successivamente essere stata compromessa o essere stata esposta a una vulnerabilità nel software di cifratura, è possibile che sia ancora necessario procedere alla notifica.

---

[33] Cfr. considerando 80 e articolo 27.

[34] Gruppo di lavoro, Parere 03/2014 sulla notifica delle violazioni, (in inglese): http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[35] Cfr. anche articolo 4, paragrafi 1 e 2, del regolamento 611/2013.

Inoltre, va osservato che se si verifica una violazione in assenza di backup dei dati personali crittografati si è in presenza di una violazione della disponibilità che potrebbe presentare rischi per le persone fisiche e pertanto potrebbe richiedere la notifica. Analogamente, laddove si verifichi una violazione che implichi la perdita di dati crittografati, anche se esiste una copia di backup dei dati personali si potrebbe comunque trattare di una violazione soggetta a segnalazione, a seconda del periodo di tempo necessario per ripristinare i dati dal backup e dell'effetto che la mancanza di disponibilità ha sulle persone fisiche. Come afferma l'articolo 32, paragrafo 1, lettera c), un importante fattore di sicurezza è "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Esempio

Una violazione che non richiederebbe la notifica all'autorità di controllo sarebbe la perdita di un dispositivo mobile crittografato in maniera sicura, utilizzato dal titolare del trattamento e dal suo personale. Se la chiave di cifratura rimane in possesso del titolare del trattamento e non si tratta dell'unica copia dei dati personali, questi ultimi sarebbero inaccessibili a qualsiasi pirata informatico. Ciò significa che è improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati in questione. Se in seguito diventa evidente che la chiave di cifratura è stata compromessa o che il software o l'algoritmo di cifratura è vulnerabile, il rischio per i diritti e le libertà delle persone fisiche cambia e potrebbe quindi essere necessaria la notifica.

Tuttavia, si avrà mancato rispetto dell'articolo 33 se il titolare del trattamento non effettua la notifica all'autorità di controllo nel caso in cui i dati non siano stati effettivamente crittografati in maniera sicura. Di conseguenza, nel selezionare il software di cifratura, il titolare del trattamento deve valutare attentamente la qualità e la corretta attuazione della cifratura offerta, capire il livello di protezione effettivamente offerto e se quest'ultimo è appropriato in ragione dei rischi presentati. Il titolare del trattamento dovrebbe altresì avere familiarità con le specifiche modalità di funzionamento del prodotto di cifratura. Ad esempio, un dispositivo può essere crittografato una volta spento, ma non mentre è in modalità stand-by. Alcuni prodotti che utilizzano la cifratura dispongono di "chiavi predefinite" che devono essere modificate da ciascun cliente per essere efficaci. La cifratura potrebbe essere considerata adeguata dagli esperti di sicurezza al momento della sua messa in atto, ma diventare obsoleta nel giro di pochi anni, il che significa che può essere messo in discussione il fatto che i dati siano sufficientemente crittografati dal prodotto in questione e che quest'ultimo fornisca un livello appropriato di protezione.

III. Articolo 34 – Comunicazione all'interessato

A. Informare l'interessato

In alcuni casi, oltre a effettuare la notifica all'autorità di controllo, il titolare del trattamento è tenuto a comunicare la violazione alle persone fisiche interessate.

L'articolo 34, paragrafo 1, afferma che:

"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".

Il titolare del trattamento dovrebbe tenere a mente che la notifica all'autorità di controllo è obbligatoria a meno che sia improbabile che dalla violazione possano derivare rischi per i diritti e le libertà delle persone fisiche. Inoltre, laddove la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche occorre informare anche queste ultime. La soglia per la comunicazione

delle violazioni alle persone fisiche è quindi più elevata rispetto a quella della notifica alle autorità di controllo, pertanto non tutte le violazioni dovranno essere comunicate agli interessati, il che li protegge da inutili disturbi arrecati dalla notifica.

Il regolamento afferma che la comunicazione di una violazione agli interessati dovrebbe avvenire "senza ingiustificato ritardo", il che significa il prima possibile. L'obiettivo principale della comunicazione agli interessati consiste nel fornire loro informazioni specifiche sulle misure che questi possono prendere per proteggersi[36]. Come osservato in precedenza, a seconda della natura della violazione e del rischio presentato, la comunicazione tempestiva aiuterà le persone a prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

L'allegato B delle presenti linee guida fornisce un elenco non esaustivo di esempi di casi in cui una violazione può presentare un rischio elevato per le persone fisiche e, di conseguenza, in cui il titolare del trattamento deve comunicarla agli interessati.

B. Informazioni da fornire

Ai fini della comunicazione alle persone fisiche, l'articolo 34, paragrafo 2, specifica che:

> "La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d)".

Secondo tale disposizione, il titolare del trattamento deve fornire almeno le seguenti informazioni:

- una descrizione della natura della violazione;
- il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto;
- una descrizione delle probabili conseguenze della violazione;
- una descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione e anche, se del caso, per attenuarne i possibili effetti negativi.

Come esempio di misure adottate per far fronte alla violazione e attenuarne i possibili effetti negativi, il titolare del trattamento può dichiarare che, dopo aver notificato la violazione all'autorità di controllo pertinente, ha ricevuto consigli sulla gestione della violazione e sull'attenuazione del suo impatto. Se del caso, il titolare del trattamento dovrebbe anche fornire consulenza specifica alle persone fisiche sul modo in cui proteggersi dalle possibili conseguenze negative della violazione, ad esempio reimpostando le password in caso di compromissione delle credenziali di accesso. Ancora una volta, il titolare del trattamento può scegliere di fornire informazioni supplementari rispetto a quanto richiesto qui.

C. Contattare l'interessato

In linea di principio, la violazione dovrebbe essere comunicata direttamente agli interessati coinvolti, a meno che ciò richieda uno sforzo sproporzionato. In tal caso, si procede a una comunicazione pubblica o a una misura simile che permetta di informare gli interessati con analoga efficacia (articolo 34, paragrafo 3, lettera c).

[36] Cfr. anche il considerando 86.

Nel comunicare una violazione agli interessati si devono utilizzare messaggi dedicati che non devono essere inviati insieme ad altre informazioni, quali aggiornamenti regolari, newsletter o messaggi standard. Ciò contribuisce a rendere la comunicazione della violazione chiara e trasparente.

Esempi di metodi trasparenti di comunicazione sono: la messaggistica diretta (ad esempio messaggi di posta elettronica, SMS, messaggio diretto), banner o notifiche su siti web di primo piano, comunicazioni postali e pubblicità di rilievo sulla stampa. Una semplice comunicazione all'interno di un comunicato stampa o di un blog aziendale non costituirebbe un mezzo efficace per comunicare una violazione all'interessato. Il Gruppo di lavoro raccomanda al titolare del trattamento di scegliere un mezzo che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate. A seconda delle circostanze, ciò potrebbe significare che il titolare del trattamento dovrebbe utilizzare diversi metodi di comunicazione, anziché un singolo canale di contatto.

Inoltre il titolare del trattamento potrebbe dover garantire che la comunicazione sia accessibile in formati alternativi appropriati e lingue pertinenti al fine di assicurarsi che le persone fisiche siano in grado di comprendere le informazioni fornite loro. Ad esempio, nel comunicare una violazione a una persona, sarà di norma appropriata la lingua utilizzata durante il precedente normale corso degli scambi commerciali con il destinatario. Tuttavia, se la violazione riguarda interessati con i quali il titolare del trattamento non ha precedentemente interagito o, in particolare, interessati che risiedono in un altro Stato membro o in un altro paese non UE diverso da quello nel quale è stabilito il titolare del trattamento, la comunicazione nella lingua nazionale locale potrebbe essere accettabile, tenendo conto della risorsa richiesta. L'obiettivo principale è aiutare gli interessati a comprendere la natura della violazione e le misure che possono adottare per proteggersi.

Il titolare del trattamento è nella posizione migliore per stabilire il canale di contatto più appropriato per comunicare una violazione agli interessati, soprattutto se interagisce frequentemente con i suoi clienti. Tuttavia, è chiaro che il titolare del trattamento dovrebbe essere cauto nell'usare un canale di contatto compromesso dalla violazione, in quanto tale canale potrebbe essere utilizzato anche da autori di attacchi che si fanno passare per il titolare del trattamento.

Il considerando 86 spiega che:

> "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 da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione".

Il titolare del trattamento potrebbe quindi contattare e consultare l'autorità di controllo non soltanto per chiedere consiglio sull'opportunità di informare gli interessati in merito a una violazione ai sensi dell'articolo 34, ma anche sui messaggi appropriati da inviare loro e sul modo più opportuno per contattarli.

Parallelamente, il considerando 88 indica che la notifica di una violazione dovrebbe tenere "conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali". Ciò può significare che in determinate circostanze, ove giustificato e su consiglio delle autorità incaricate dell'applicazione della legge, il titolare del trattamento può ritardare la comunicazione della violazione agli interessati fino a quando la comunicazione non pregiudica più tale indagine. Tuttavia, passato tale arco di tempo, gli interessati dovrebbero comunque essere tempestivamente informati.

Se non ha la possibilità di comunicare una violazione all'interessato perché non dispone di dati sufficienti per contattarlo, il titolare del trattamento dovrebbe informarlo non appena sia ragionevolmente possibile farlo (ad esempio quando l'interessato esercita il proprio diritto ai sensi dell'articolo 15 di accedere ai dati personali e fornisce al titolare del trattamento le informazioni supplementari necessarie per essere contattato).

D. Circostanze nelle quali non è richiesta la comunicazione

L'articolo 34, paragrafo 3, stabilisce tre condizioni che, se soddisfatte, non richiedono la comunicazione agli interessati in caso di violazione, ossia:

- il titolare del trattamento ha applicato misure tecniche e organizzative adeguate per proteggere i dati personali prima della violazione, in particolare misure atte a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi. Ciò potrebbe prevedere ad esempio la protezione dei dati personali con cifratura allo stato dell'arte oppure mediante tokenizzazione;
- immediatamente dopo una violazione, il titolare del trattamento ha adottato misure destinate a garantire che non sia più probabile che si concretizzi l'elevato rischio posto ai diritti e alle libertà delle persone fisiche. Ad esempio, a seconda delle circostanze del caso, il titolare del trattamento può aver immediatamente individuato e intrapreso un'azione contro il soggetto che ha avuto accesso ai dati personali prima che questi fosse in grado di utilizzarli in qualsiasi modo. È necessario altresì tenere in debito conto delle possibili conseguenze di qualsiasi violazione della riservatezza, anche in questo caso, a seconda della natura dei dati in questione;
- contattare gli interessati richiederebbe uno sforzo sproporzionato[37], ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. Si pensi, ad esempio, al magazzino di un ufficio statistico che si è allagato e i documenti contenenti dati personali erano conservati soltanto in formato cartaceo. In tale circostanza il titolare del trattamento deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace. In caso di sforzo sproporzionato, si potrebbe altresì prevedere l'adozione di disposizioni tecniche per rendere le informazioni sulla violazione disponibili su richiesta, soluzione questa che potrebbe rivelarsi utile per le persone fisiche che potrebbero essere interessate da una violazione ma che il titolare del trattamento non può altrimenti contattare.

Conformemente al principio di responsabilizzazione, il titolare del trattamento dovrebbe essere in grado di dimostrare all'autorità di controllo di soddisfare una o più di queste condizioni[38]. Va tenuto presente che, sebbene la comunicazione possa inizialmente non essere richiesta se non vi è alcun rischio per i diritti e le libertà delle persone fisiche, la situazione potrebbe cambiare nel corso del tempo e il rischio dovrebbe essere rivalutato.

Se il titolare del trattamento decide di non comunicare una violazione all'interessato, l'articolo 34, paragrafo 4, spiega che l'autorità di controllo può richiedere che lo faccia, qualora ritenga che la violazione possa presentare un rischio elevato per l'interessato. In alternativa, può ritenere che siano state soddisfatte le condizioni di cui all'articolo 34, paragrafo 3, nel qual caso la comunicazione all'interessato non è richiesta. Qualora stabilisca che la decisione di non effettuare la comunicazione

[37] Cfr. linee guida del Gruppo di lavoro sulla trasparenza, che prendono in considerazione la questione dello sforzo sproporzionato, disponibile (in inglese) all'indirizzo http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

[38] Cfr. articolo 5, paragrafo 2.

all'interessato non sia fondata, l'autorità di controllo può prendere in considerazione l'esercizio dei poteri e delle sanzioni a sua disposizione.

IV. Valutazione dell'esistenza di un rischio o di un rischio elevato

A. Rischio come fattore che fa scattare l'obbligo di notifica

Sebbene il regolamento introduca l'obbligo di notificare una violazione, non è obbligatorio farlo in tutte le circostanze:

- la notifica all'autorità di controllo competente è obbligatoria a meno che sia improbabile che la violazione possa presentare un rischio per i diritti e le libertà delle persone fisiche;
- la comunicazione di una violazione alle persone fisiche diventa necessaria soltanto laddove la violazione possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Ciò significa che non appena il titolare del trattamento viene a conoscenza di una violazione, è fondamentale che non si limiti a contenere l'incidente, ma valuti anche il rischio che potrebbe derivarne. Questo per due motivi: innanzitutto conoscere la probabilità e la potenziale gravità dell'impatto sulle persone fisiche aiuterà il titolare del trattamento ad adottare misure efficaci per contenere e risolvere la violazione; in secondo luogo, ciò lo aiuterà a stabilire se è necessaria la notifica all'autorità di controllo e, se necessario, alle persone fisiche interessate.

Come spiegato in precedenza, la notifica di una violazione è obbligatoria a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche, mentre la comunicazione di una violazione agli interessati deve essere effettuata se è probabile che la violazione presenti un rischio *elevato* per i diritti e le libertà delle persone fisiche. Tale rischio sussiste quando la violazione può comportare un danno fisico, materiale o immateriale per le persone fisiche i cui dati sono stati violati. Esempi di tali danni sono la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie e il pregiudizio alla reputazione. Il verificarsi di tale danno dovrebbe essere considerato probabile quando la violazione riguarda dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, oppure che includono dati genetici, dati relativi alla salute o dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza[39].

B. Fattori da considerare nella valutazione del rischio

I considerando 75 e 76 del regolamento suggeriscono che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità del rischio per i diritti e le libertà degli interessati. Inoltre il regolamento afferma che il rischio dovrebbe essere valutato in base a una valutazione oggettiva.

Va osservato che la valutazione del rischio per i diritti e le libertà delle persone fisiche a seguito di una violazione esamina il rischio in maniera diversa rispetto alla valutazione d'impatto sulla protezione dei dati[40]. Quest'ultima considera tanto i rischi del trattamento dei dati svolto come pianificato, quanto quelli in caso di violazione. Nel considerare una potenziale violazione, esamina in termini generali la probabilità che la stessa si verifichi e il danno all'interessato che potrebbe

[39] Cfr. considerando 75 e 85.

[40] Cfr. le linee guida del Gruppo di lavoro in materia di valutazioni d'impatto sulla protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati.

derivarne; in altre parole, si tratta di una valutazione di un evento ipotetico. Nel caso di una violazione effettiva, l'evento si è già verificato, quindi l'attenzione si concentra esclusivamente sul rischio risultante dell'impatto di tale violazione sulle persone fisiche.

Esempio

Una valutazione d'impatto sulla protezione dei dati suggerisce che l'uso proposto di un determinato software di sicurezza per proteggere i dati personali costituisce una misura adeguata per garantire un livello di sicurezza adeguato al rischio che il trattamento presenterebbe altrimenti per le persone fisiche. Tuttavia, laddove una vulnerabilità diventi nota successivamente, ciò modifica l'idoneità del software a contenere il rischio per i dati personali protetti e richiede quindi una rivalutazione nel contesto di una valutazione d'impatto sulla protezione dei dati in corso.

Una vulnerabilità nel prodotto viene sfruttata in un secondo momento e si verifica una violazione. Il titolare del trattamento dovrebbe valutare le circostanze specifiche della violazione, i dati interessati e il potenziale livello di impatto sulle persone fisiche, nonché la probabilità che tale rischio si concretizzi.

Di conseguenza, nel valutare il rischio per le persone fisiche derivante da una violazione, il titolare del trattamento dovrebbe considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi. Pertanto il Gruppo di lavoro raccomanda che la valutazione tenga conto dei seguenti criteri[41].

- Tipo di violazione

Il tipo di violazione verificatosi può influire sul livello di rischio presentato per le persone fisiche. Ad esempio, una violazione della riservatezza che ha portato alla divulgazione di informazioni mediche a soggetti non autorizzati può avere conseguenze diverse per una persona fisica rispetto a una violazione in cui i dettagli medici di una persona fisica sono stati persi e non sono più disponibili.

- Natura, carattere sensibile e volume dei dati personali

Ovviamente, un elemento fondamentale della valutazione del rischio sono il tipo e il carattere sensibile dei dati personali che sono stati compromessi dalla violazione. Solitamente più i dati sono sensibili, maggiore è il rischio di danni per le persone interessate; tuttavia si dovrebbero prendere in considerazione anche altri dati personali che potrebbero già essere disponibili sull'interessato. Ad esempio, è improbabile che la divulgazione del nome e dell'indirizzo di una persona fisica in circostanze ordinarie causi un danno sostanziale. Tuttavia, se il nome e l'indirizzo di un genitore adottivo sono divulgati a un genitore biologico, le conseguenze potrebbero essere molto gravi tanto per il genitore adottivo quanto per il bambino.

Violazioni relative a dati sulla salute, documenti di identità o dati finanziari come i dettagli di carte di credito, possono tutte causare danni di per sé, ma se tali dati fossero usati congiuntamente si potrebbe avere un'usurpazione d'identità. Di norma una combinazione di dati personali ha un carattere più sensibile rispetto a un singolo dato personale.

[41] L'articolo 3, paragrafo 2, del regolamento 611/2013 fornisce orientamenti sui fattori che dovrebbero essere presi in considerazione in relazione alla notifica di violazioni nel settore dei servizi di comunicazione elettronica che possono essere utili nel contesto della notifica ai sensi del regolamento generale sulla protezione dei dati. Cfr. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:it:PDF.

Alcuni tipi di dati personali possono sembrare relativamente innocui, tuttavia occorre valutare attentamente ciò che questi dati possono rivelare sull'interessato. Un elenco di clienti che accettano consegne regolari potrebbe non essere particolarmente sensibile, tuttavia gli stessi dati relativi a clienti che hanno richiesto l'interruzione delle loro consegne durante le vacanze potrebbero essere informazioni utili per dei criminali.

Analogamente, una piccola quantità di dati personali altamente sensibili può avere un impatto notevole su una persona fisica, mentre una vasta gamma di dettagli può rivelare molte più informazioni in merito alla stessa persona. Inoltre, una violazione che interessa grandi quantità di dati personali relative a molte persone può avere ripercussioni su un numero corrispondentemente elevato di persone.

- Facilità di identificazione delle persone fisiche

Un fattore importante da considerare è la facilità con cui un soggetto che può accedere a dati personali compromessi riesce a identificare persone specifiche o ad abbinare i dati con altre informazioni per identificare persone fisiche. A seconda delle circostanze, l'identificazione potrebbe essere possibile direttamente dai dati personali oggetto di violazione senza che sia necessaria alcuna ricerca speciale per scoprire l'identità dell'interessato, oppure potrebbe essere estremamente difficile abbinare i dati personali a una particolare persona fisica, ma sarebbe comunque possibile a determinate condizioni. L'identificazione può essere direttamente o indirettamente possibile a partire dai dati oggetto di violazione, tuttavia può dipendere anche dal contesto specifico della violazione e dalla disponibilità pubblica dei corrispondenti dettagli personali. Quest'ultima eventualità potrebbe essere più rilevante per le violazioni della riservatezza e della disponibilità.

Come indicato in precedenza, i dati personali protetti da un livello appropriato di cifratura saranno incomprensibili a persone non autorizzate che non dispongono della chiave di decifratura. Inoltre, anche una pseudonimizzazione opportunamente attuata (definita all'articolo 4, punto 5, come "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile") può ridurre la probabilità che le persone fisiche vengano identificate in caso di violazione. Tuttavia, le tecniche di pseudonimizzazione da sole non possono essere considerate sufficienti a rendere i dati incomprensibili.

- Gravità delle conseguenze per le persone fisiche

A seconda della natura dei dati personali coinvolti in una violazione, ad esempio categorie particolari di dati, il danno potenziale alle persone che potrebbe derivarne può essere particolarmente grave soprattutto se la violazione può comportare furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Se la violazione riguarda dati personali relativi a persone fisiche vulnerabili, queste ultime potrebbero essere esposte a un rischio maggiore di danni.

Il fatto che il titolare del trattamento sappia o meno che i dati personali sono nelle mani di persone le cui intenzioni sono sconosciute o potenzialmente dannose può incidere sul livello di rischio potenziale. Prendiamo una violazione della riservatezza nel cui ambito i dati personali vengono comunicati a un terzo di cui all'articolo 4, punto 10, o ad altri destinatari per errore. Una tale situazione può verificarsi, ad esempio, nel caso in cui i dati personali vengano inviati accidentalmente all'ufficio sbagliato di un'organizzazione o a un'organizzazione fornitrice utilizzata frequentemente. Il titolare del trattamento può chiedere al destinatario di restituire o distruggere in maniera sicura i dati ricevuti. In entrambi i casi, dato che il titolare del trattamento ha una relazione continuativa con tali soggetti e potrebbe essere a conoscenza delle loro procedure, della loro storia e di altri dettagli pertinenti, il destinatario può essere considerato "affidabile". In altre parole, il titolare del trattamento può ritenere che il destinatario goda di una certa affidabilità e può ragionevolmente aspettarsi che non

leggerà o accederà ai dati inviati per errore e che rispetterà le istruzioni di restituirli. Anche se i dati fossero stati consultati, il titolare del trattamento potrebbe comunque confidare nel fatto che il destinatario non intraprenderà ulteriori azioni in merito agli stessi e restituirà tempestivamente i dati al titolare del trattamento e coopererà per garantirne il recupero. In tali casi, questo aspetto può essere preso in considerazione nella valutazione del rischio effettuata dal titolare del trattamento in seguito alla violazione; il fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione, anche se questo non significa che non si sia verificata una violazione. La probabilità che detta violazione presenti un rischio per le persone fisiche verrebbe però meno, quindi non sarebbe più necessaria la notifica all'autorità di controllo o alle persone fisiche interessate. Ancora una volta, tutto dipenderà dalle circostanze del caso concreto. Ciò nonostante il titolare del trattamento deve comunque conservare informazioni relative alla violazione nel contesto del suo dovere generale di conservare registrazioni in merito alle violazioni (cfr. seguente sezione V).

Si dovrebbe altresì tener conto della permanenza delle conseguenze per le persone fisiche laddove l'impatto possa essere considerato maggiore qualora gli effetti siano a lungo termine.

- Caratteristiche particolari dell'interessato

Una violazione può riguardare dati personali relativi a minori o ad altre persone fisiche vulnerabili, che possono di conseguenza essere soggette a un rischio più elevato di danno. Altri fattori concernenti la persona fisica potrebbero influire sul livello di impatto della violazione sulla stessa.

- Caratteristiche particolari del titolare del trattamento di dati

La natura e il ruolo del titolare del trattamento e delle sue attività possono influire sul livello di rischio per le persone fisiche in seguito a una violazione. Ad esempio, un'organizzazione medica tratterà categorie particolari di dati personali, il che significa che vi è una minaccia maggiore per le persone fisiche nel caso in cui i loro dati personali vengano violati, rispetto a una mailing list di un quotidiano.

- Numero di persone fisiche interessate

Una violazione può riguardare solo una o poche persone fisiche oppure diverse migliaia di persone fisiche, se non molte di più. Di norma, maggiore è il numero di persone fisiche interessate, maggiore è l'impatto che una violazione può avere. Tuttavia, una violazione può avere ripercussioni gravi anche su una sola persona fisica, a seconda della natura dei dati personali e del contesto nel quale i dati sono stati compromessi. Ancora una volta, l'aspetto fondamentale consiste nel considerare la probabilità e la gravità dell'impatto sulle persone interessate.

- Aspetti generali

Pertanto, nel valutare il rischio che potrebbe derivare da una violazione, il titolare del trattamento dovrebbe considerare tanto la gravità dell'impatto potenziale sui diritti e sulle libertà delle persone fisiche e quanto la probabilità che tale impatto si verifichi. Chiaramente, se le conseguenze di una violazione sono più gravi, il rischio è più elevato; analogamente, se la probabilità che tali conseguenze si verifichino è maggiore, maggiore è anche il rischio. In caso di dubbio, il titolare del trattamento dovrebbe restare molto prudente ed effettuare la notifica. L'allegato B fornisce alcuni esempi utili di diversi tipi di violazioni che comportano rischi o rischi elevati per le persone fisiche.

L'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) ha elaborato raccomandazioni in merito a una metodologia di valutazione della gravità di una violazione, che

possono essere utili per i titolari del trattamento e i responsabili del trattamento nella progettazione del loro piano di risposta per la gestione delle violazioni[42].

V. Responsabilizzazione e tenuta di registri

A. Documentare le violazioni

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'articolo 33, paragrafo 5:

> "Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

Tale obbligo è collegato al principio di responsabilizzazione, di cui all'articolo 5, paragrafo 2. 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'articolo 24, 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[43].

Sebbene spetti al titolare del trattamento determinare quale metodo e struttura utilizzare per documentare una violazione, determinate informazioni chiave dovrebbero essere sempre incluse. Come richiesto dall'articolo 33, paragrafo 5, il titolare del trattamento è tenuto a registrare i dettagli relativi alla violazione, comprese le cause, i fatti e i dati personali interessati. Dovrebbe altresì indicare gli effetti e le conseguenze della violazione e i provvedimenti adottati per porvi rimedio.

Il regolamento non specifica un periodo di conservazione della documentazione. Nel caso in cui i registri contengano dati personali, spetterà al titolare del trattamento stabilire il periodo appropriato di conservazione in conformità ai principi connessi al trattamento dei dati personali[44] e soddisfare una base legittima per il trattamento[45]. Dovrà conservare la documentazione in conformità dell'articolo 33, paragrafo 5, nella misura in cui può essere chiamato a fornire prove all'autorità di controllo in merito al rispetto di tale articolo oppure, più in generale, del principio di responsabilizzazione. Ovviamente se i registri non contengono dati personali, il principio di limitazione della conservazione[46] previsto dal regolamento non si applica.

---

[42] ENISA, *Recommendations for a methodology of the assessment of severity of personal data breaches* [Raccomandazioni in merito a una metodologia di valutazione della gravità delle violazioni dei dati personali], (disponibile in inglese) https://www.enisa.europa.eu/publications/dbn-severity.

[43] Il titolare del trattamento può scegliere di documentare le violazioni nel contesto del suo registro delle attività di trattamento che è mantenuto ai sensi dell'articolo 30. Non è richiesto un registro separato, a condizione che le informazioni rilevanti per la violazione siano chiaramente identificabili come tali e possano essere estratte su richiesta.

[44] Cfr. articolo 5.

[45] Cfr. articolo 6 e anche articolo 9.

[46] Cfr. articolo 5, paragrafo 1, lettera e).

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. 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[47]. In alternativa, se ritiene che una delle condizioni di cui all'articolo 34, paragrafo 3, sia soddisfatta, il titolare del trattamento dovrebbe essere in grado di fornire prove adeguate della circostanza che ricorre nel caso di specie.

Se il titolare del trattamento notifica una violazione all'autorità di controllo, ma la notifica avviene in ritardo, il titolare del trattamento deve essere in grado di fornire i motivi del ritardo; la documentazione relativa a tale circostanza potrebbe contribuire a dimostrare che il ritardo nella segnalazione è giustificato e non eccessivo.

Laddove comunichi una violazione alle persone fisiche interessate, il titolare del trattamento dovrebbe essere trasparente in merito alla violazione e comunicare in maniera efficace e tempestiva. Di conseguenza, conservando le prove di tale comunicazione il titolare del trattamento faciliterebbe la dimostrazione della propria assunzione di responsabilità e del proprio rispetto delle norme.

Per agevolare il rispetto degli articoli 33 e 34, sarebbe vantaggioso tanto per il titolare del trattamento quanto per il responsabile del trattamento 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 dimostrare il rispetto del regolamento 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'articolo 58 e l'imposizione di una sanzione amministrativa pecuniaria ai sensi dell'articolo 83.

B. Ruolo del responsabile della protezione dei dati

Il titolare del trattamento o il responsabile del trattamento può avere un responsabile della protezione dei dati[48], come richiesto dall'articolo 37 oppure su decisione volontaria come buona prassi. L'articolo 39 del regolamento stabilisce una serie di compiti obbligatori per il responsabile della protezione dei dati, ma non impedisce l'assegnazione di ulteriori compiti da parte del titolare del trattamento, se del caso.

Tra i compiti obbligatori del responsabile della protezione dei dati di particolare rilevanza per la notifica delle violazioni figurano quelli di fornire consulenza e informazioni al titolare del trattamento o al responsabile del trattamento, sorvegliare l'osservanza del regolamento e fornire un parere in merito alle valutazioni d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve inoltre cooperare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo e per gli interessati. Va inoltre osservato che, ai fini della notifica della violazione all'autorità di controllo, l'articolo 33, paragrafo 3, lettera b), impone al titolare del trattamento di fornire il nome e i dati di contatto del responsabile della protezione dei dati o di un altro punto di contatto.

---

[47] Cfr. considerando 85.

[48] Cfr. le linee guida del Gruppo di lavoro sui responsabili della protezione dei dati qui: https://www.garanteprivacy.it/documents/10160/0/WP+243+-+Linee-guida+sui+responsabili+della+protezione+dei+dati+%28RPD%29.pdf.

Per quanto riguarda la documentazione delle violazioni, il titolare del trattamento o il responsabile del trattamento potrebbe chiedere il parere del proprio responsabile della protezione dei dati in merito alla struttura, all'impostazione e all'amministrazione della documentazione. Al responsabile della protezione dei dati potrebbe altresì essere affidato il compito di tenere i registri.

Questi compiti indicano che il responsabile della protezione dei dati dovrebbe svolgere un ruolo chiave nel fornire assistenza nella prevenzione delle violazioni o nella preparazione alle stesse, fornendo consulenza e monitorando il rispetto delle norme, nonché durante una violazione (ossia nel processo di notifica all'autorità di controllo) e durante qualsiasi successiva indagine da parte dell'autorità di controllo. In tale ottica, il Gruppo di lavoro raccomanda di informare tempestivamente il responsabile della protezione dei dati dell'esistenza di una violazione e di coinvolgerlo nella gestione delle violazioni e nel processo di notifica.

VI. Obblighi di notifica a norma di altri strumenti giuridici

Separatamente e in aggiunta alla notifica e alla comunicazione delle violazioni ai sensi del regolamento, il titolare del trattamento deve altresì essere a conoscenza di qualsiasi obbligo di notifica di incidenti di sicurezza previsto da altri atti legislativi associati cui potrebbe essere soggetto, e dell'eventuale obbligo parallelo di notificare all'autorità di controllo una violazione dei dati personali. Tali obblighi possono variare a seconda degli Stati membri. Esempi di obblighi di notifica sanciti in altri strumenti giuridici e di modalità con cui si correlano con il regolamento generale sulla protezione dei dati sono i seguenti:

- Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS)[49].

L'articolo 19, paragrafo 2, del regolamento eIDAS impone ai prestatori di servizi fiduciari di notificare all'organismo di vigilanza una violazione della sicurezza o la perdita di integrità che hanno un impatto significativo sul servizio fiduciario fornito o sui dati personali conservati in tale contesto. Ove applicabile, ossia quando tale violazione o perdita costituiscono altresì una violazione dei dati personali ai sensi del regolamento generale sulla protezione dei dati, il prestatore di servizi fiduciari deve effettuare la notifica anche all'autorità di controllo.

- Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS)[50].

Gli articoli 14 e 16 della direttiva NIS impongono agli operatori di servizi essenziali e ai fornitori di servizi digitali di notificare gli incidenti di sicurezza alle loro autorità competenti. Come riconosciuto dal considerando 63 della direttiva NIS[51], gli incidenti di sicurezza possono spesso comportare una compromissione di dati personali. Sebbene la direttiva NIS imponga alle autorità competenti e alle autorità di controllo di cooperare e scambiare informazioni in tale contesto, rimane comunque il fatto che qualora tali incidenti siano o diventino violazioni di dati personali ai sensi del regolamento generale sulla protezione dei dati, tali operatori e/o fornitori sono tenuti a effettuare la notifica

[49] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ITA.

[50] Cfr. http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ITA.

51 Considerando 63: *"In molti casi gli incidenti compromettono dati personali. Al riguardo è opportuno che le autorità competenti e le autorità responsabili della protezione dei dati collaborino e si scambino informazioni su tutti gli aspetti pertinenti per affrontare le violazioni ai dati personali determinate dagli incidenti".*

all'autorità di controllo in maniera distinta dagli obblighi di notifica degli incidenti a norma della direttiva NIS.

Esempio

Un fornitore di servizi cloud che notifica una violazione ai sensi della direttiva NIS può comunque essere tenuto a notificarla al titolare del trattamento se tale violazione include una violazione dei dati personali. Analogamente, un prestatore di servizi fiduciari che effettua una notifica a norma del regolamento eIDAS può anche essere tenuto a effettuare una notifica all'autorità competente per la protezione dei dati in caso di violazione.

- Direttiva 2009/136/CE (direttiva sui diritti dei cittadini) e regolamento (UE) n. 611/2013 (regolamento sulla notifica delle violazioni).

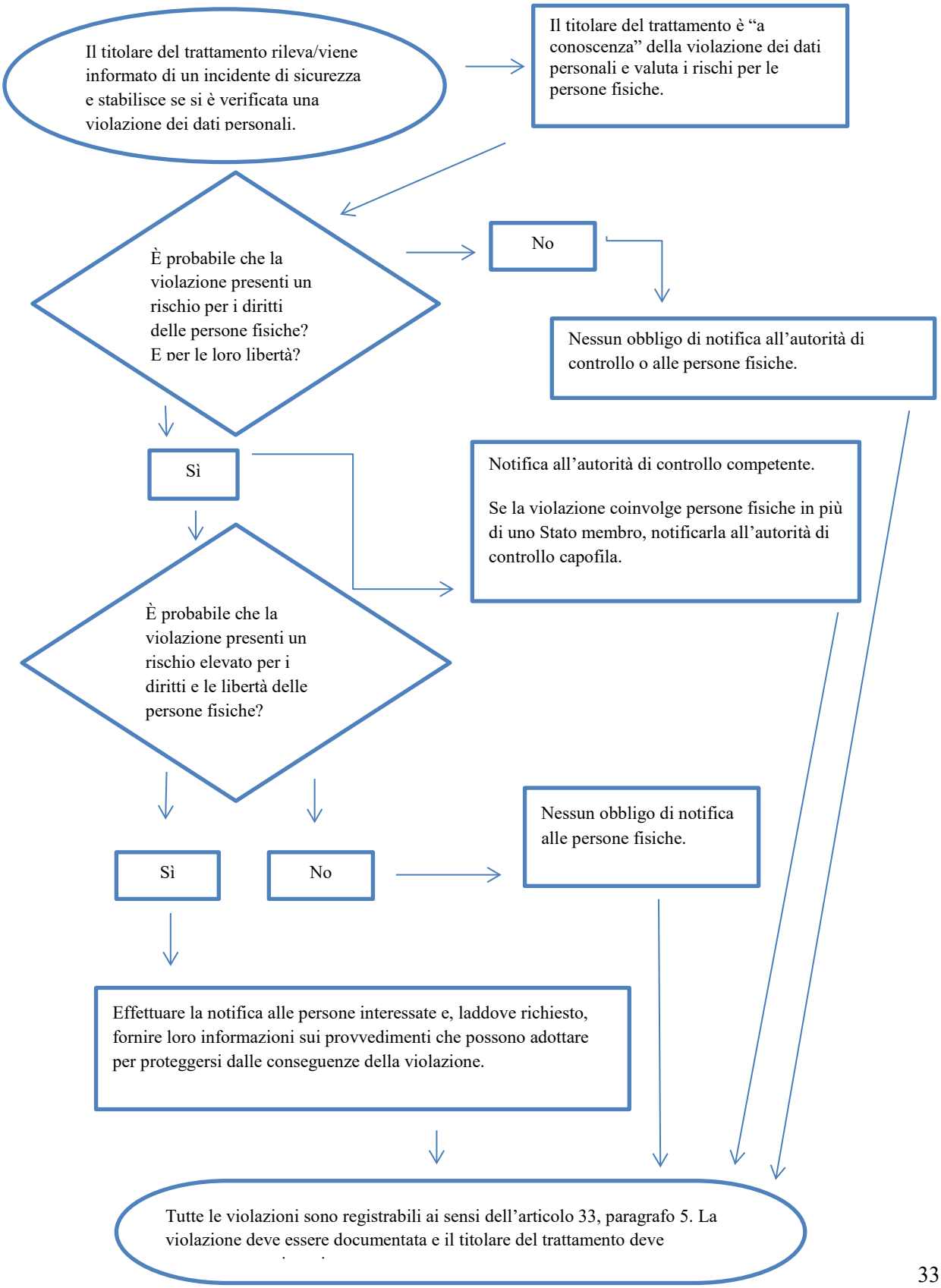
I fornitori di servizi di comunicazione elettronica accessibili al pubblico nel contesto della direttiva 2002/58/CE[52] devono notificare le violazioni alle autorità nazionali competenti.

Il titolare del trattamento dovrebbe altresì essere a conoscenza di eventuali ulteriori obblighi di notifica in ambito giuridico, medico o professionale previsti da altri regimi applicabili.

[52] Il 10 gennaio 2017, la Commissione europea ha proposto un direttiva relativa alla vita privata e alle comunicazioni elettroniche che sostituirà la direttiva 2009/136/CE e sopprimerà gli obblighi di notifica. Tuttavia, fino a quando tale proposta non sarà approvata dal Parlamento europeo, l'attuale obbligo di notifica rimane in vigore, cfr. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

VII. **Allegato**

A. Diagramma di flusso che illustra gli obblighi di notifica



B. Esempi di violazioni dei dati personali e dei soggetti a cui notificarle

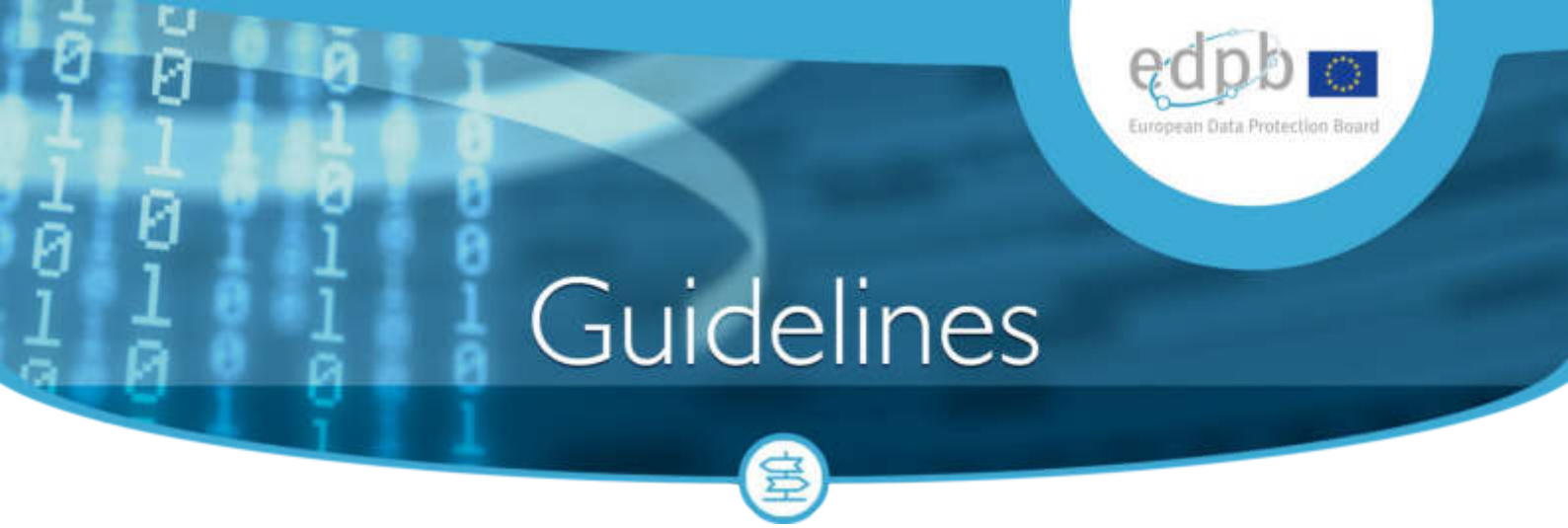
I seguenti esempi non esaustivi aiuteranno il titolare del trattamento a stabilire se deve effettuare la notifica in diversi scenari di violazione dei dati personali. Questi esempi possono altresì contribuire a distinguere tra rischio e rischio elevato per i diritti e le libertà delle persone fisiche.

Esempio	**Notifica all'autorità di controllo?**	**Comunicazione all'interessato?**	**Note/raccomandazioni**
Un titolare del trattamento ha effettuato un backup di un archivio di dati personali crittografati su una chiave USB. La chiave viene rubata durante un'effrazione.	No.	No.	Fintantoché i dati sono crittografati con un algoritmo all'avanguardia, esistono backup dei dati, la chiave univoca non viene compromessa e i dati possono essere ripristinati in tempo utile, potrebbe non trattarsi di una violazione da segnalare. Tuttavia, se la chiave viene successivamente compromessa, è necessaria la notifica.
ii. Un titolare del trattamento gestisce un servizio online. A seguito di un attacco informatico ai danni di tale servizio, i dati personali di persone fisiche vengono prelevati. Il titolare del trattamento ha clienti in un solo Stato membro.	Sì, segnalare l'evento all'autorità di controllo se vi sono probabili conseguenze per le persone fisiche.	Sì, segnalare l'evento alle persone fisiche a seconda della natura dei dati personali interessati e se la gravità delle probabili conseguenze per tali persone è elevata.	
iii. Una breve interruzione di corrente di alcuni minuti presso il call center di un titolare del trattamento impedisce ai clienti di chiamare il titolare del trattamento e accedere alle proprie registrazioni.	No.	No.	Questa non è una violazione soggetta a notifica, ma costituisce comunque un incidente registrabile ai sensi dell'articolo 33, paragrafo 5. Il titolare del trattamento deve conservare adeguate registrazioni in merito.
iv. Un titolare del trattamento subisce un	Sì, effettuare la segnalazione	Sì, effettuare la segnalazione alle	Se fosse stato disponibile un backup e i dati

attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono essere ripristinati. Durante le indagini, diventa evidente che l'unica funzionalità dal *ransomware* era la cifratura dei dati e che non vi erano altri *malware* presenti nel sistema.	all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di disponibilità.	persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di disponibilità dei dati, nonché di altre possibili conseguenze.	avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone fisiche, in quanto non si sarebbe verificata nessuna perdita permanente di disponibilità o di riservatezza. Tuttavia, qualora l'autorità di controllo fosse venuta a conoscenza dell'incidente con altri mezzi, avrebbe potuto prendere in considerazione lo svolgimento di un'indagine al fine di valutare il rispetto dei requisiti di sicurezza più ampi di cui all'articolo 32.
v. Una persona telefona al call center di una banca per segnalare una violazione dei dati. La persona ha ricevuto l'estratto conto mensile da un soggetto diverso. Il titolare del trattamento intraprende una breve indagine (ossia la conclude entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e che vi è una potenziale carenza sistemica che potrebbe comportare il coinvolgimento già occorso o potenziale di altre persone fisiche.	Sì.	La comunicazione va effettuata soltanto alle persone fisiche coinvolte in caso di rischio elevato e se è evidente che altre persone fisiche non sono state interessate dall'evento.	Se dopo ulteriori indagini si stabilisce che l'evento ha interessato un numero maggiore di persone fisiche è necessario comunicare questo sviluppo all'autorità di controllo, e il titolare del trattamento deve informarne le altre persone fisiche interessate se sussiste un rischio elevato per loro.

vi. Un titolare del trattamento gestisce un mercato online e ha clienti in più Stati membri. Tale mercato subisce un attacco informatico a seguito del quale i nomi utente, le password e la cronologia degli acquisti vengono pubblicati online dall'autore dell'attacco.	Sì, segnalare l'evento all'autorità di controllo capofila se la violazione riguarda un trattamento transfrontaliero.	Sì, dato che la violazione potrebbe comportare un rischio elevato.	Il titolare del trattamento dovrebbe prendere delle misure, ad esempio forzare il ripristino delle password degli account interessati, e altri provvedimenti per attenuare il rischio. Il titolare del trattamento dovrebbe altresì considerare qualsiasi altro obbligo di notifica, ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali.
vii. Una società di *hosting* di siti web che funge da responsabile del trattamento individua un errore nel codice che controlla l'autorizzazione dell'utente. A causa di tale vizio, qualsiasi utente può accedere ai dettagli dell'account di qualsiasi altro utente.	In veste di responsabile del trattamento, la società di *hosting* di siti web deve effettuare la notifica ai clienti interessati (i titolari del trattamento) senza ingiustificato ritardo. Supponendo che la società di *hosting* di siti web abbia condotto le proprie indagini, i titolari del trattamento interessati dovrebbero essere ragionevolmente certi di aver subito una violazione e pertanto è probabile che vengano considerati "a conoscenza" della violazione nel momento in cui hanno ricevuto la notifica da parte della società di *hosting* (il responsabile del trattamento). Il titolare del trattamento deve quindi effettuare la notifica all'autorità di controllo.	Qualora non vi siano probabili rischi elevati per le persone fisiche non è necessario effettuare una comunicazione a tali persone.	La società di *hosting* di siti web (responsabile del trattamento) deve prendere in considerazione qualsiasi altro obbligo di notifica (ad esempio ai sensi della direttiva NIS, trattandosi di un fornitore di servizi digitali). Qualora non vi sia alcuna prova che tale vulnerabilità sia sfruttata presso uno dei suoi titolari del trattamento, la violazione potrebbe non essere soggetta all'obbligo di notifica, tuttavia potrebbe essere una violazione da registrare o essere il segno di un mancato rispetto dell'articolo 32.

viii. Le cartelle cliniche di un ospedale sono indisponibili per un periodo di 30 ore a causa di un attacco informatico.	Sì, l'ospedale è tenuto a effettuare la notifica in quanto può verificarsi un rischio elevato per la salute e la tutela della vita privata dei pazienti.	Sì, informare le persone fisiche coinvolte.	
ix. I dati personali di un gran numero di studenti vengono inviati per errore a una mailing list sbagliata con più di 1 000 destinatari.	Sì, segnalare l'evento all'autorità di controllo.	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	
x. Una e-mail di marketing diretto viene inviata ai destinatari nei campi "a:" o "cc:", consentendo così a ciascun destinatario di vedere l'indirizzo e-mail di altri destinatari.	Sì, la notifica all'autorità di controllo può essere obbligatoria se è interessato un numero elevato di persone, se vengono rivelati dati sensibili (ad esempio una mailing list di uno psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, il messaggio di posta elettronica contiene le password iniziali).	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.



Guidelines 9/2022 on personal data breach notification under GDPR

Version 2.0

Adopted 28 March 2023

Version history

Version 1.0	10 October 2022	Adoption of the Guidelines (updated version of the previous guidelines WP250 (rev.01) adopted by the Working Party 29 and endorsed by the EDPB on 25 May 2018) for a targeted public consultation.
Version 2.0	28 March 2023	Adoption of the Guidelines following the targeted public consultation on the subject of data breach notification for controllers not established in the EEA.

TABLE OF CONTENTS

The European Data Protection Board

Having regard to Article 70(1)(e) and (l) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Having regard to the Article 29 Working Party Guidelines on Personal data breach notification under Regulation 2016/679, WP250 rev.01,

HAS ADOPTED THE FOLLOWING GUIDELINES

0 PREFACE

1. On 3 October 2017, the Working Party 29 (hereinafter "WP29") adopted its Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01)[2], which were endorsed by the European Data Protection Board (hereinafter "EDPB") at its first Plenary meeting[3]. This document is a slightly updated version of those guidelines. Any reference to the WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) should, from now on, be interpreted as a reference to these EDPB Guidelines 9/2022.

2. The EDPB noticed that there was a need to clarify the notification requirements concerning the personal data breaches at non-EU establishments. The paragraph concerning this matter has been revised and updated, while the rest of the document was left unchanged, except for editorial changes. The revision concerns, more specifically, paragraph 73 in Section II.C.2 of this document.

INTRODUCTION

3. The GDPR introduced the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[4] (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

4. Obligations to notify in cases of breaches existed for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)[5]. There were also some Member States that already had their own

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] WP29 Guidelines on Personal data breach notification under Regulation 2016/679 (WP250 rev.01) (last revised and updated on 6 February 2018), available at https://ec.europa.eu/newsroom/article29/items/612052.
[3] See https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] See Article 4(21) GDPR.
[5] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A32013R0611

national breach notification obligation. This might included the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States might had relevant Codes of Practice (for example, in Ireland[6]). Whilst a number of EU data protection authorities encouraged controllers to report breaches, the Data Protection Directive 95/46/EC[7], which the GDPR replaced, did not contain a specific breach notification obligation and therefore such a requirement was new for many organisations. The GDPR makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[8]. Processors also have an important role to play and they must notify any breach to their controller[9].

5. The EDPB considers that the notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach[10]. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 GDPR a possible sanction is applicable to the controller.

6. Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals[11], and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.

7. The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.

8. In its Opinion 03/2014 on personal data breach notification[12], WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.

9. The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these obligations. They

---

[6] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[8] The rights enshrined in the Charter of Fundamental Rights of the EU, available at http://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[9] See Article 33(2) GDPR. This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

[10] See Articles 34(4) and 58(2)(e) GDPR.

[11] This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11).

[12] See WP29 Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

also give examples of various types of breaches and who would need to be notified in different scenarios.

I. PERSONAL DATA BREACH NOTIFICATION UNDER THE GDPR

A. Basic security considerations

10. One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage[13].

11. Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons[14]. Also, the GDPR requires all appropriate technological protection an organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged [15].

12. Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

B. What is a personal data breach?

1. Definition

13. As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a "personal data breach" in Article 4(12) as:

> "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."

14. What is meant by "destruction" of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. "Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete. In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

> **Example**
>
> An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.

15. What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of personal data. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the

[13] See Articles 5(1)(f) and 32 GDPR.
[14] Article 32; see also Recital 83 GDPR.
[15] See Recital 87 GDPR.

processing of personal data as outlined in Article 5 GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches[16].

16. The potential adverse effects of a breach on individuals are considered below.

2. Types of personal data breaches

17. In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[17]:

- "**Confidentiality breach**" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "**Integrity breach**" - where there is an unauthorised or accidental alteration of personal data.
- "**Availability breach**" - where there is an accidental or unauthorised loss of access[18] to, or destruction of, personal data.

18. It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

19. Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

Example

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

20. The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 GDPR, "security of processing", explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to "*the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and*

[16] It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.

[17] See WP29 Opinion 03/2014.

[18] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP80053rev4, which defines "availability" as: "Ensuring timely and reliable access to and use of information," available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: "Timely, reliable access to data and information services for authorized users". See https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines "availability" as "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

services," and "*the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*".

21. Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12) GDPR.

22. As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5) GDPR. This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[19]. However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33 GDPR, the controller will need to notify unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

Example

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.

Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.

23. It should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.

Example

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

3. The possible consequences of a personal data breach

24. A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals[20].

25. Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a

[19] See Article 33(5) GDPR.
[20] See also Recitals 85 and 75 GDPR.

likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[21].

26. The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR:

> "*It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation*."

27. Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.

28. If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 GDPR are fulfilled, then the supervisory authority is presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine[22], either accompanying a corrective measure under Article 58(2) GDPR or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 Guidelines on administrative fines state: "*The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement*". In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34 GDPR) on the one hand, and absence of (adequate) security measures (Article 32 GDPR) on the other hand, as they are two separate infringements.

II. ARTICLE 33 - NOTIFICATION TO THE SUPERVISORY AUTHORITY

A. When to notify

1. Article 33 requirements

29. Article 33(1) GDPR provides that:

> "*In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*."

30. Recital 87 GDPR states[23]:

[21] See also Recital 86 GDPR.

[22] For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[23] Recital 85 GDPR is also important here.

"*It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation*."

2. When does a controller become "aware"?

31. As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. The EDPB considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

32. However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject[24]. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

33. When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".

[24] See Recital 87 GDPR.

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

34. After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

35. Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact assessment (DPIA)[25] made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.

36. In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

Example

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

37. The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data[26]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.

38. The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).

[25] See WP29 Guidelines WP248 on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[26] It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.

39. Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.

    - Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
    - Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
    - Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
    - At the same time, the controller should act to contain and recover the breach. Documentation of the breach should take place as it develops.

40. Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) GDPR have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[27]. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33 GDPR.

41. Article 32 GDPR makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

3. Joint controllers

42. Article 26 GDPR concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[28]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34 GDPR. The EDPB recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

4. Processor obligations

43. The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) GDPR specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

44. Article 33(2) GDPR makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether

---

[27] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[28] See also Recital 79 GDPR.

a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

45. The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, the EDPB recommends the processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

46. As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.

47. Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.

48. A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34 GDPR. However, it is important to note that the legal responsibility to notify remains with the controller.

B. Providing information to the supervisory authority

1. Information to be provided

49. When a controller notifies a breach to the supervisory authority, Article 33(3) GDPR states that, at the minimum, it should:

> *"(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;*
>
> (b) *communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;*
>
> (c) *describe the likely consequences of the personal data breach;*
>
> (d) *describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects*."

50. The GDPR does not define categories of data subjects or personal data records. However, the EDPB suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.

51. Recital 85 GDPR makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.

52. Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.

53. Thus, when it has become clear that here has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.

54. Article 33(3) GDPR states that the controller "shall at least" provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

Example

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

55. In any event, the supervisory authority may request further details as part of its investigation into a breach.

2. Notification in phases

56. Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) GDPR therefore states:

"*Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay*."

57. This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1) GDPR. The EDPB recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.

58. The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.

59. However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data[29] are disclosed online, the controller should act without undue delay to contain the breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to communicate the breach to the data subject where it is required.

60. It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

Example

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

61. It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.

3. Delayed notifications

62. Article 33(1) GDPR makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

63. Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

64. Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

[29] See Article 9 GDPR.

65. Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.

C. Cross-border breaches and breaches at non-EU establishments

1. Cross-border breaches

66. Where there is cross-border processing[30] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) GDPR makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR[31]. Article 55(1) GDPR says that:

> "*Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*."

67. However, Article 56(1) GDPR states:

> "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60*."

68. Furthermore, Article 56(6) GDPR states:

> "*The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor*."

69. This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[32]. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify[33]. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

2. Breaches at non-EU establishments

70. Article 3 GDPR concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) GDPR states[34]:

---

[30] See Article 4(23) GDPR.

[31] See also Recital 122 GDPR.

[32] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[33] A list of contact details for all European national data protection authorities can be found at: https://edpb.europa.eu/about-edpb/about-edpb/members_en

[34] See also Recitals 23 and 24 GDPR.

"*This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

(a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

(b) *the monitoring of their behaviour as far as their behaviour takes place within the Union*."

71. Article 3(3) GDPR is also relevant and states[35]:

"*This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law*."

72. Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) GDPR and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34 GDPR. Article 27 GDPR requires a controller (and a processor) to designate a representative in the EU where Article 3(2) GDPR applies.

73. However, the mere presence of a representative in a Member State does not trigger the one-stop-shop system.[36] For this reason the breach will need to be notified to every supervisory authority for which affected data subjects reside in their Member State. This (These) notification(s) shall be the responsibility of the controller.[37]

74. Similarly, where a processor is subject to Article 3(2) GDPR, it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2) GDPR.

D. Conditions where notification is not required

75. Article 33(1) GDPR makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.

76. In its Opinion 03/2014 on breach notification[38], WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not

[35] See also Recital 25 GDPR.

[36] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[37] In line with guidelines 3/2018 on the territorial scope of the GDPR (Article 3), available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, the EDPB considers the function of a representative in the Union as not compatible with the role of an external data protection officer ("DPO"), therefore the responsibility to notify the supervisory authority in case of a personal data breach remains that of the controller in line with Article 27(5) GDPR. A representative can however be involved in the notification process if this has been explicitly stipulated in the written mandate.

[38] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

require communication to those individuals[39]. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.

77. WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.

78. Consequently, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.

79. Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) GDPR states, an important factor of security is the "*the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*".

Example

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

80. However, a failure to comply with Article 33 GDPR will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have "default keys" that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years' time,

[39] See also Article 4(1) and (2) of Regulation 611/2013.

meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

III. ARTICLE 34 – COMMUNICATION TO THE DATA SUBJECT

A. Informing individuals

81. In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.

Article 34(1) GDPR states:

> "*When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay*."

82. Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.

83. The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves[40]. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

84. Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.

B. Information to be provided

85. When notifying individuals, Article 34(2) GDPR specifies that:

> "*The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3)*."

86. According to this provision, the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

87. As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from

[40] See also Recital 86 GDPR.

possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.

C. Contacting individuals

88. In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner (Article 34(3)(c) GDPR).

89. Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.

90. Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. The EDPB recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.

91. Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.

92. Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the breach as this channel could also be used by attackers impersonating the controller.

93. At the same time, Recital 86 GDPR explains that:

> "*Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication*."

94. Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

95. Linked to this is the advice given in Recital 88 GDPR that notification of a breach should "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it

would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

96. Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).

D. Conditions where communication is not required

97. Article 34(3) GDPR states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort[41] to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

98. In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions [42]. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

99. If a controller decides not to communicate a breach to the individual, Article 34(4) GDPR explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) GDPR have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

[41] See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] See Article 5(2) GDPR.

IV. ASSESSING RISK AND HIGH RISK

A. Risk as a trigger for notification

100. Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

101. This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

102. As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur[43].

B. Factors to consider when assessing risk

103. Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

104. It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)[44]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

Example

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA. A vulnerability in the product is later exploited and

[43] See Recital 75 and Recital 85 GDPR.

[44] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

105. Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. The EDPB therefore recommends the assessment should take into account the following criteria[45]:

- **The type of breach**

106. The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.

- **The nature, sensitivity, and volume of personal data**

107. Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.

108. Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

109. Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

110. Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

- **Ease of identification of individuals**

111. An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

[45] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

112. As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) GDPR as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

- **Severity of consequences for individuals**

113. Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

114. Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).

115. Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

- **Special characteristics of the individual**

116. A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

- **Special characteristics of the data controller**

117. The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

- **The number of affected individuals**

118. A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

- **General points**

119. Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.

120. The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan[46].

V. ACCOUNTABILITY AND RECORD KEEPING

A. Documenting breaches

121. Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) GDPR explains:

> "*The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article*."

122. This is linked to the accountability principle of the GDPR, contained in Article 5(2) GDPR. The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24 GDPR, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not[47].

123. Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5) GDPR, the controller needs to record details concerning the breach, which should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.

124. The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data[48] and to meet a lawful basis for processing[49]. It will need to retain documentation in accordance with Article 33(5)

---

[46] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[47] The controller may choose to document breaches as part of if its record of processing activities which is maintained pursuant to Article 30 GDPR. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.

[48] See Article 5 GDPR.

[49] See Article 6 and also Article 9 GDPR.

GDPR insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle[50] of the GDPR does not apply.

125. In addition to these details, the EDPB recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals[51]. Alternatively, if the controller considers that any of the conditions in Article 34(3) GDPR are met, then it should be able to provide appropriate evidence that this is the case.

126. Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.

127. Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

128. To aid compliance with Articles 33 and 34 GDPR, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.

129. It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 GDPR and, or imposing an administrative fine in accordance with Article 83 GDPR.

B. Role of the Data Protection Officer

130. A controller or processor may have a Data Protection Officer (DPO)[52], either as required by Article 37 GDPR, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.

131. Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) GDPR requires the controller to provide the name and contact details of its DPO, or other contact point.

132. In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.

133. These factors mean that the DPO should play an key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach

[50] See Article 5(1)(e) GDPR.

[51] See Recital 85 GDPR.

[52] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

(i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, the EDPB recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

VI. NOTIFICATION OBLIGATIONS UNDER OTHER LEGAL INSTRUMENTS

134. In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following:

- *Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)*[53].

135. Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

- *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)*[54].

136. Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS[55], security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

Example

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

- *Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).*

137. Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[56] must notify breaches to the competent national authorities.

---

[53] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[54] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[55] Recital 63: *"Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents."*

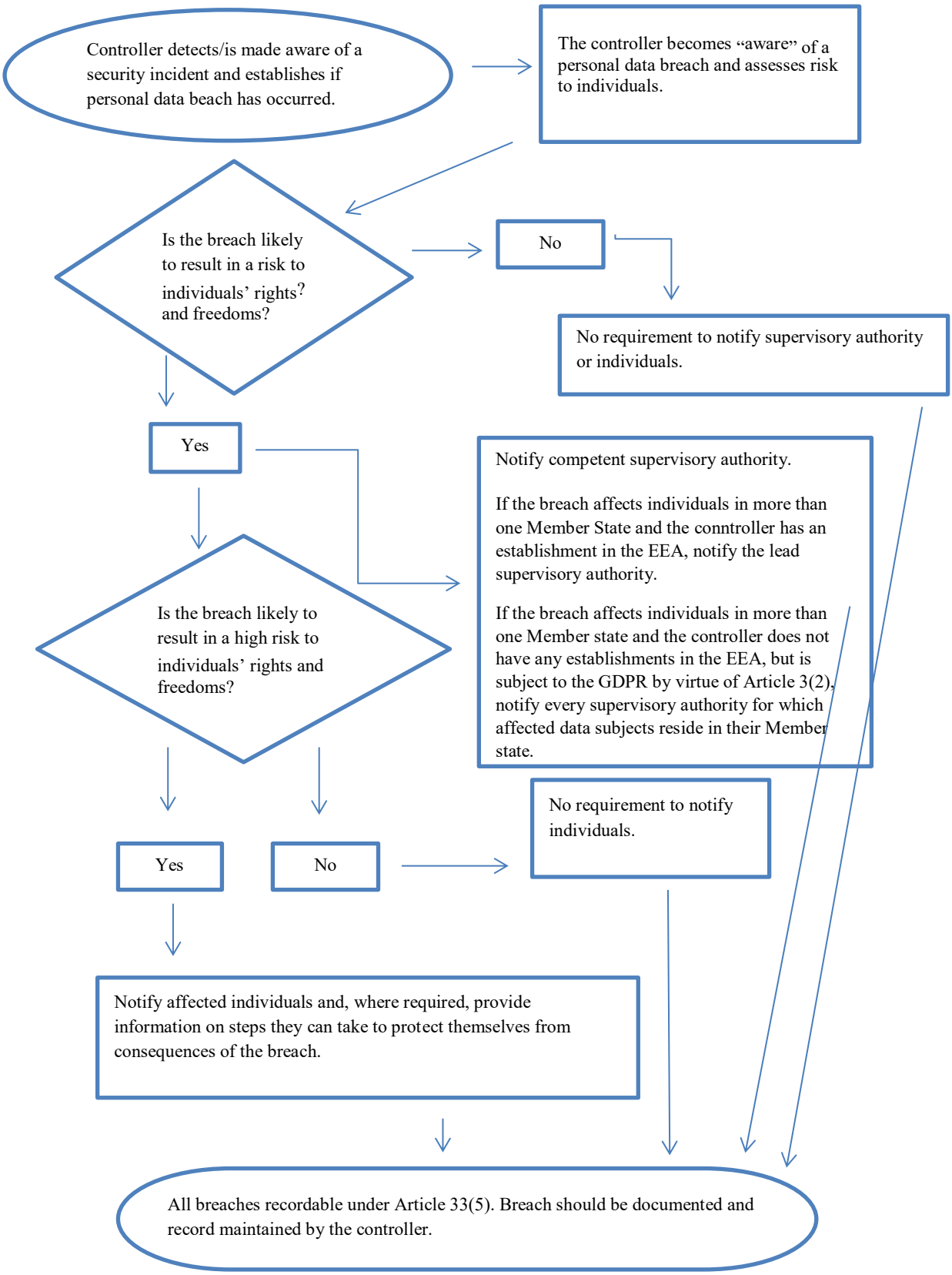
[56] On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in

138. Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.

force, see https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. ANNEX

A. Flowchart showing notification requirements



B. Examples of personal data breaches and who to notify

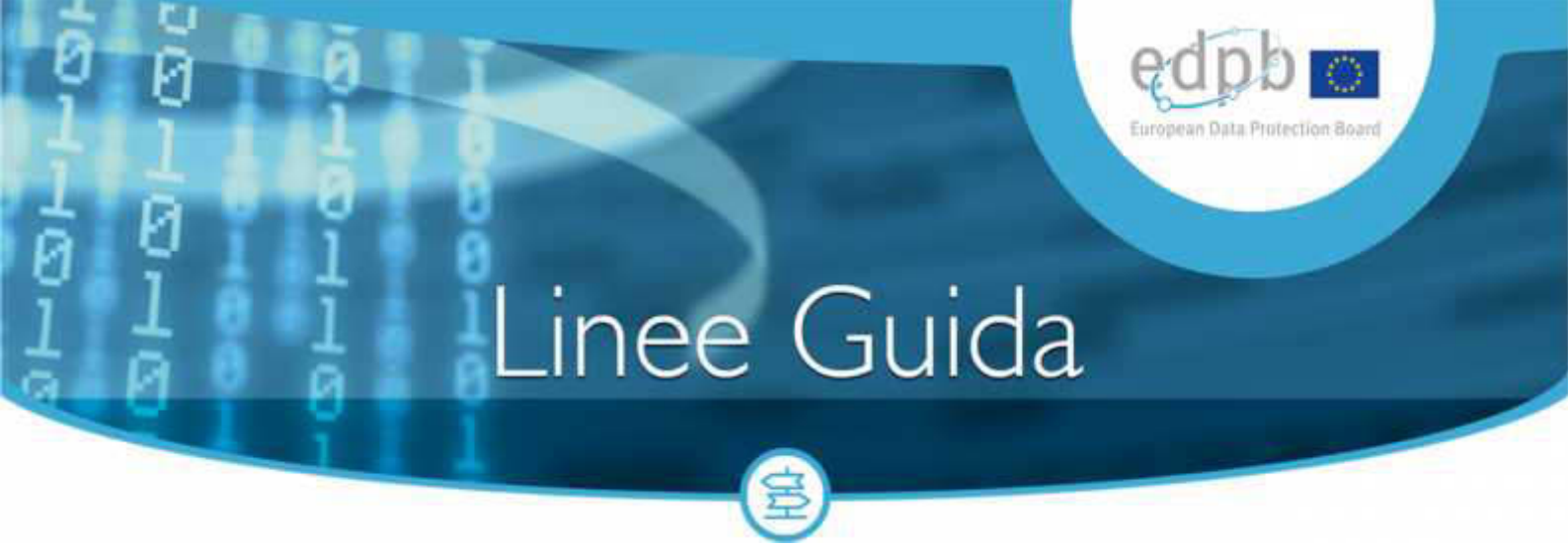
The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

	Example	Notify the supervisory authority	Notify the data subject	Notes/recommendations
i	A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii	A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii	A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv	A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, if the supervisory authority became aware of the

	was to encrypt the data, and that there was no other malware present in the system.			incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.

v	An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi	A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii	A website hosting company acting as a data processor identifies an error in the code which controls user authorisation. The effect of the flaw means that any user	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting	If there is likely no high risk to the individuals they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive as a digital service provider). If there is no evidence of this vulnerability being

	can access the account details of any other user	company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority		exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii	Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix	Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x	A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.



Linee-guida 01/2021 su esempi riguardanti la notifica di una violazione dei dati personali

Adottate il 14 dicembre 2021

Cronologia delle versioni

Versione 2.0	14 12 2021	Adozione delle linee guida dopo la consultazione pubblica
Versione 1.0	14 01 2021	Adozione delle linee guida per consultazione pubblica

Indice

IL COMITATO EUROPEO PER LA PROTEZIONE DEI DATI

Visto l'articolo 70, paragrafo 1, lettera e), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (in appresso "GDPR"),

Visto l'accordo SEE, in particolare l'allegato XI e il protocollo 37 dello stesso, modificati dalla Decisione del 6 luglio 20181,

Visti l'articolo 12 e l'articolo 22 del suo regolamento,

Vista la comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo "La protezione dei dati quale pilastro della responsabilizzazione dei cittadini e dell'approccio dell'UE alla transizione digitale — due anni di applicazione del regolamento generale sulla protezione dei dati"2,

HA ADOTTATO LE SEGUENTI LINEE-GUIDA

1 INTRODUZIONE

1. Il GDPR introduce, in alcuni casi, l'obbligo di notificare una violazione dei dati personali all'autorità nazionale di controllo competente e di comunicare la violazione alle persone i cui dati personali sono stati interessati dalla violazione (articoli 33 e 34).

2. Nell'ottobre 2017 il gruppo di lavoro "Articolo 29" ha già elaborato linee-guida generali sulla notifica delle violazioni dei dati, analizzando le sezioni pertinenti del regolamento generale sulla protezione dei dati (Linee-guida sulla notifica delle violazioni dei dati personali a norma del regolamento (UE) 2016/679, WP 250) (di seguito "Linee-guida WP250"3). Tuttavia, a causa della loro natura e della tempistica prevista, tali linee-guida non hanno affrontato tutte le questioni pratiche in modo sufficientemente dettagliato. Pertanto, è emersa la necessità di una guida pratica e basata su casi concreti, che utilizzi le esperienze acquisite dalle autorità di controllo da quando GDPR è divenuto pienamente applicabile.

3. Il presente documento è inteso a integrare gli orientamenti WP 250 e rispecchia le esperienze comuni delle autorità di controllo dello Spazio Economico Europeo (SEE) successivamente alla piena applicabilità del regolamento generale sulla protezione dei dati. Il suo obiettivo è aiutare i titolari del trattamento a decidere come gestire le violazioni dei dati e quali fattori prendere in considerazione durante la valutazione del rischio.

4. Qualsiasi tentativo di porre rimedio a una violazione presuppone che il titolare e il responsabile del trattamento siano in grado di riconoscerla. L'articolo 4, paragrafo 12, del regolamento generale sulla protezione dei dati definisce una "violazione dei dati personali" come "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 altrimenti trattati".

5. Nel suo parere 03/2014 sulla notifica delle violazioni4 e nelle Linee-guida WP 250, il WP29 ha spiegato che le

1 I riferimenti agli "Stati membri" nel presente documento sono da intendersi come riferimenti agli "Stati membri del SEE".
2 COM (2020) 264 final del 24 giugno 2020.
3 WP29 WP250 rev.1, 6 febbraio 2018, Linee guida sulla notifica delle violazioni dei dati personali a norma del regolamento 2016/679 — approvate dal comitato europeo per la protezione dei dati, https://ec.europa.eu/newsroom/article29/item-detail.cfm7item id = 612052.
4 WP29 WP213, 25 marzo 2014, Parere 03/2014 sulla notifica di una violazione dei dati personali, pag. 5,

violazioni possono essere classificate in base ai seguenti tre noti principi di sicurezza delle informazioni:

- "Violazione della riservatezza" — in caso di divulgazione non autorizzata o accidentale di dati personali o di accesso non autorizzato o accidentale agli stessi.
- "Violazione dell'integrità" — in caso di modifica non autorizzata o accidentale di dati personali.
- "Violazione della disponibilità" — in caso di perdita accidentale o non autorizzata dell'accesso ai dati personali o di loro distruzione accidentale o non autorizzata.5

6. Una violazione può avere potenzialmente numerosi effetti negativi significativi sulle persone fisiche, che possono causare danni fisici, materiali o immateriali. Il GDPR spiega che ciò può includere la perdita del controllo da parte degli interessati sui loro dati personali, la limitazione dei loro diritti, la discriminazione, il furto o l'usurpazione d'identità, perdite finanziarie, la decifratura non autorizzata della pseudonimizzazione, il pregiudizio alla reputazione e la perdita di riservatezza dei dati personali protetti da segreto professionale, nonché qualsiasi altro danno economico o sociale significativo per le persone fisiche interessate. Uno degli obblighi più importanti del titolare del trattamento è valutare tali rischi per i diritti e le libertà degli interessati e attuare misure tecniche e organizzative adeguate per affrontarli.

7. Di conseguenza, il GDPR impone al titolare del trattamento di:

- documentare le violazioni dei dati personali, comprese le circostanze della violazione dei dati personali, le sue conseguenze e le azioni correttive adottate6;
- notificare la violazione dei dati personali all'autorità di controllo, a meno che sia improbabile che la violazione dei dati presenti un rischio per i diritti e le libertà delle persone fisiche7;
- comunicare la violazione dei dati personali all'interessato quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche8.

8. Le violazioni dei dati sono di per sé problematiche, ma possono anche essere sintomi di un regime di sicurezza dei dati vulnerabile e forse obsoleto, oppure segnalare carenze del sistema da affrontare. In linea generale, è sempre meglio prevenire le violazioni dei dati preparandosi in anticipo, dal momento che diverse conseguenze sono per loro natura irreversibili. Prima che un titolare del trattamento possa valutare *appieno* il rischio derivante da una violazione causata da una qualche forma di attacco, occorre individuare la causa alla radice del problema, al fine di stabilire se le vulnerabilità che hanno determinato l'incidente siano ancora presenti e siano pertanto ancora sfruttabili. In molti casi il titolare del trattamento è in grado di individuare che l'incidente può comportare un rischio e deve pertanto essere notificato. In altri casi non si dovrà rinviare la notifica fino a quando il rischio e l'impatto della violazione non siano stati pienamente valutati, poiché la valutazione completa del rischio può avvenire parallelamente alla notifica e le informazioni così ottenute possono essere fornite all'autorità di controllo in fasi successive senza ulteriore e ingiustificato ritardo9.

9. La violazione dovrebbe essere notificata quando il titolare del trattamento ritiene che possa comportare un rischio per i diritti e le libertà dell'interessato. I titolari dovrebbero effettuare tale valutazione nel momento in cui vengono a conoscenza della violazione. Un titolare non dovrebbe attendere gli esiti di un'analisi forense dettagliata e l'applicazione di azioni di mitigazione del rischio (precoci) prima di valutare se la violazione dei dati possa comportare un rischio e debba pertanto essere notificata.

10. Se un titolare del trattamento valuta autonomamente che un rischio sia improbabile, ma tale rischio di fatto

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index en.htm # maincontentSec4.

5 Cfr. le Linee-guida WP 250, pag. 7. — Occorre tener conto del fatto che una violazione dei dati può riguardare una o più categorie simultaneamente.

6 Articolo 33, paragrafo 5, del GDPR.

7 Articolo 33, paragrafo 1, del GDPR.

8 Articolo 34, paragrafo 1, del GDPR.

9 Articolo 33, paragrafo 4, del GDPR.

si concretizza, l'autorità di controllo competente può avvalersi dei suoi poteri correttivi e può decidere di comminare sanzioni.

11. Ogni titolare e responsabile del trattamento dovrebbe disporre di piani e procedure per la gestione di eventuali violazioni dei dati. Si dovrebbero prevedere linee gerarchiche chiare e specifiche figure responsabili di determinati aspetti del processo di recupero.

12. Anche la formazione e la sensibilizzazione in materia di protezione dei dati per il personale del titolare e del responsabile del trattamento sono essenziali, concentrandosi sulla gestione delle violazioni dei dati personali (identificazione di un incidente di violazione dei dati personali e ulteriori azioni da intraprendere, ecc.). Tale formazione dovrebbe essere ripetuta periodicamente, a seconda del tipo di trattamento e delle dimensioni della struttura del titolare, esaminando le più recenti tendenze e segnalazioni derivanti da attacchi informatici o altri incidenti di sicurezza.

13. Il principio di responsabilizzazione e il concetto di protezione dei dati fin dalla progettazione potrebbero contemplare un'analisi intesa a confluire in una sorta di "Manuale per la gestione delle violazioni dei dati" messo a punto dal titolare e dal responsabile del trattamento, in cui definire gli elementi fattuali in rapporto a ogni sfaccettatura del trattamento in ciascuna delle fasi principali dell'operazione. Tale manuale, ove redatto preventivamente, fornirebbe una fonte di informazioni molto più rapida per consentire ai titolari e ai responsabili del trattamento di mitigare i rischi e di adempiere ai rispettivi obblighi senza indebito ritardo. Così facendo, in caso di violazione dei dati personali, il personale saprà cosa fare e l'incidente potrà essere gestito più rapidamente di quanto avverrebbe in assenza di misure di mitigazione o dei predetti piani.

14. Sebbene i casi presentati di seguito siano fittizi, essi si basano su casi tipici tratti dall'esperienza collettiva delle autorità di controllo in materia di notifiche di violazioni dei dati. Le analisi proposte si riferiscono esplicitamente ai casi in esame, ma con l'obiettivo di fornire assistenza ai titolari del trattamento per la valutazione delle violazioni dei dati che li riguardino. Qualsiasi modifica delle circostanze riferite alle fattispecie descritte di seguito può comportare livelli di rischio diversi o più significativi, e quindi rendere necessarie misure diverse o supplementari. In queste linee-guida, i casi sono presentati in base a determinate categorie di violazioni (ad esempio "attacchi ransomware"). Alcune misure di mitigazione sono necessarie in tutte le fattispecie appartenenti a una determinata categoria di violazioni. Tali misure non sono necessariamente ripetute in ciascuna analisi riferita a un caso appartenente alla stessa categoria di violazioni. Per i casi appartenenti alla stessa categoria sono indicate solo le differenze. Pertanto, il lettore dovrebbe tenere conto dell'intera casistica riferita alla pertinente categoria di violazione al fine di individuare e distinguere tutte le misure corrette da adottare.

15. La documentazione interna di una violazione è un obbligo indipendente dai rischi connessi alla violazione stessa e deve essere predisposta in ogni singolo caso. I casi presentati di seguito cercano di chiarire se notificare o meno la violazione all'autorità di controllo e comunicarla agli interessati coinvolti.

2 RANSOMWARE

16. Una causa frequente di notifica di violazione dei dati è un attacco ransomware subito dal titolare del trattamento. In questi casi un codice malevolo cifra i dati personali e successivamente l'autore dell'attacco chiede al titolare del trattamento un riscatto in cambio della chiave di decifratura. Questo tipo di attacco può di norma essere classificato come una violazione della disponibilità, ma spesso potrebbe comportare anche una violazione della riservatezza.

2.1 Caso n. 01: Ransomware in presenza di backup adeguato e senza esfiltrazione

I sistemi informatici di una piccola impresa manifatturiera sono stati esposti a un attacco ransomware e i dati memorizzati in tali sistemi sono stati cifrati. Il titolare ha utilizzato la cifratura dei dati memorizzati (at rest), per cui tutti i dati ai quali ha avuto accesso il ransomware erano conservati in forma cifrata utilizzando

un algoritmo di cifratura conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa nell'attacco, ossia l'autore dell'attacco non ha potuto accedervi né utilizzarla indirettamente. Di conseguenza, l'autore dell'attacco ha avuto accesso solo a dati personali cifrati. In particolare, né il sistema di posta elettronica della società né i sistemi clienti utilizzati per accedervi sarebbero stati interessati. L'impresa si avvale delle competenze di una società esterna di cybersecurity per indagare sull'incidente. Sono disponibili le registrazioni (log) di tutti i flussi dati in uscita dall'impresa (compresa la posta elettronica in uscita). Dopo aver analizzato i log e i dati raccolti dai sistemi di rilevazione utilizzati dall'impresa, un'indagine interna supportata dalla società esterna di cybersecurity ha stabilito *con certezza* che l'autore del reato si è limitato a cifrare i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i clienti e i dipendenti dell'impresa, per un totale di poche decine di persone. Un backup era prontamente disponibile e i dati sono stati ripristinati poche ore dopo l'attacco. La violazione non ha avuto alcuna conseguenza sull'operatività del titolare del trattamento. Non vi sono stati ritardi nei pagamenti dei dipendenti o nella gestione delle richieste dei clienti.

17. In questo caso, rispetto alla definizione di "violazione dei dati personali" si sono concretizzati i seguenti elementi: una violazione della sicurezza ha comportato una modifica illecita e l'accesso non autorizzato ai dati personali conservati.

2.1.1 Caso n. 01 — Misure in essere e valutazione del rischio

18. Come per tutti i rischi posti da attori esterni, la probabilità che un attacco ransomware abbia successo può essere drasticamente ridotta rafforzando la sicurezza dei dati mediante controllo del contesto. La maggior parte di queste violazioni può essere evitata garantendo l'adozione di adeguate misure di sicurezza organizzative, fisiche e tecnologiche. Esempi di tali misure sono la corretta gestione delle patch e l'uso di un adeguato sistema di rilevamento di malware. Disporre di un backup adeguato e separato contribuirà ad attenuare le conseguenze di un eventuale attacco riuscito. Inoltre, un programma di istruzione, formazione e sensibilizzazione dei dipendenti in materia di sicurezza (SETA) contribuirà a prevenire e riconoscere questo tipo di attacco. (Un elenco di misure consigliate è riportato nella sezione 2.5.) Tra tali misure, una delle più importanti è una corretta gestione delle patch che assicuri che i sistemi siano aggiornati e che tutte le vulnerabilità note dei sistemi installati siano state corrette poiché la maggior parte degli attacchi ransomware sfrutta proprio vulnerabilità ben note.

19. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sulla violazione e individuare il tipo di codice malevolo per comprendere le possibili conseguenze dell'attacco. Tra i rischi da considerare figura il rischio che i dati siano stati esfiltrati senza lasciare traccia nei log dei sistemi.

20. In questo esempio, l'attaccante ha avuto accesso ai dati personali ed è stata compromessa la riservatezza del testo cifrato contenente dati personali in forma cifrata. Tuttavia, i dati che potrebbero essere stati esfiltrati non possono essere letti o utilizzati dall'autore dell'attacco, almeno per il momento. La tecnica di cifratura utilizzata dal titolare è conforme allo stato dell'arte. La chiave di decifratura non è stata compromessa e presumibilmente non può essere determinata con altri mezzi. Di conseguenza, i rischi in termini di riservatezza per i diritti e le libertà delle persone fisiche sono ridotti al minimo, salvi i progressi delle tecniche crittografiche che in futuro potrebbero rendere i dati cifrati intelligibili.

21. Il titolare del trattamento dovrebbe considerare il rischio per le persone fisiche dovuto alla violazione10. In questo caso, sembra che i rischi per i diritti e le libertà degli interessati derivino dalla mancanza di disponibilità

10 Per orientamenti sui trattamenti *"che possono comportare un rischio elevato"*, si veda il gruppo di lavoro A29 "Guidelines on Data Protection Impact Assessment (DPIA) and determining if processing is likely to be a high risk" (Linee guida sulla valutazione d'impatto sulla protezione dei dati e sulla determinazione della probabilità che il trattamento possa comportare un rischio elevato) ai fini del regolamento 2016/679, WP248 rev. 01, approvato dall'EDPB, https://ec.europa.eu/newsroom/article29/items/611236, pag. 9.

dei dati personali e che la riservatezza dei dati personali non sia compromessa11. In questo esempio, gli effetti negativi della violazione sono stati attenuati in tempi contenuti dopo il verificarsi della violazione stessa. Disporre di un adeguato regime di backup12 riduce gli effetti negativi della violazione e in questo caso il titolare del trattamento è stato in grado di avvalersene in modo efficace.

22. Per quanto riguarda la gravità delle conseguenze per gli interessati, è stato possibile individuare solo conseguenze minori, poiché i dati sono stati ripristinati in poche ore e la violazione non ha avuto conseguenze sull'operatività del titolare del trattamento né effetti significativi sugli interessati (ad esempio pagamenti ai dipendenti o gestione delle richieste dei clienti).

2.1.2 Caso n. 01 — Misure di mitigazione e obblighi

23. In assenza di un backup, il titolare del trattamento può adottare poche misure per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti. In questo caso particolare, tuttavia, gli effetti dell'attacco potrebbero essere contenuti efficacemente "ripulendo" tutti i sistemi compromessi dal codice malevolo, correggendo le vulnerabilità e ripristinando i dati interessati entro breve tempo dall'attacco. In assenza di backup, i dati sarebbero andati persi e la gravità può aumentare di pari passo con i rischi o gli impatti per le persone.

24. La tempestività di un ripristino efficace dei dati utilizzando un backup prontamente disponibile è una variabile fondamentale nell'analisi della violazione. La definizione di una tempistica adeguata per il ripristino di dati compromessi dipende dalle circostanze specifiche della violazione. Il regolamento generale sulla protezione dei dati stabilisce che una violazione dei dati personali deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Si potrebbe pertanto stabilire che in nessun caso è consigliabile superare il termine di 72 ore, ma quando si tratta di casi caratterizzati da un rischio elevato, anche il rispetto di tale termine può risultare insoddisfacente.

25. In questo caso, grazie a procedure dettagliate per la valutazione d'impatto e la risposta agli incidenti, il titolare del trattamento ha stabilito che era improbabile che la violazione comportasse un rischio per i diritti e le libertà delle persone fisiche; pertanto non è necessaria alcuna comunicazione agli interessati, né la violazione richiede una notifica all'autorità di controllo. Tuttavia, come tutte le violazioni dei dati, è necessario conservarne la documentazione conformemente all'articolo 33, paragrafo 5. La struttura del titolare potrebbe anche necessitare di (o essere successivamente tenuta a effettuare, su disposizione dell'autorità di controllo) aggiornamenti e correzioni delle misure e procedure organizzative e tecniche messe in atto per la gestione della sicurezza dei dati personali e la mitigazione dei rischi. Nell'ambito di tale aggiornamento e revisione, si dovrebbe indagare approfonditamente sulla violazione individuandone le cause e definendo i metodi utilizzati dall'autore dell'attacco al fine di prevenire eventi analoghi in futuro.

Azioni necessarie in base ai rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati

11 Dal punto di vista tecnico, la cifratura dei dati comporta l' "accesso" ai dati originali e, nel caso di ransomware, la cancellazione dei dati originali — il codice ransomware deve accedere ai dati per cifrarli e rimuovere i dati originali. L'autore di un attacco può effettuare una copia dell'originale prima dell'eliminazione, ma i dati personali non verranno sempre estratti.. Con l'avanzare delle indagini svolte dal titolare, potrebbero emergere nuove informazioni tali da modificare la suddetta valutazione. L'accesso che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata dei dati personali o un rischio per la sicurezza dell'interessato, anche in assenza di interpretazione dei dati, può essere tanto grave quanto l'accesso seguito da interpretazione dei dati personali.

12 Le procedure di backup dovrebbero essere strutturate, coerenti e ripetibili. Esempi di procedure di backup sono il metodo 3-2-1 e il metodo grandfather-father-son. Qualsiasi metodo dovrebbe sempre essere testato per verificarne l'efficacia in termini di copertura nonché in sede di ripristino dei dati. I test dovrebbero inoltre essere ripetuti a intervalli regolari, in particolare quando intervengono cambiamenti nel trattamento o nelle sue circostanze, al fine di garantire l'integrità del sistema.

✓	X	X

2.2 Caso n. 02: Ransomware senza un adeguato backup

Uno dei computer utilizzati da un'azienda agricola è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'attaccante. L'impresa si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'impresa (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna condotta con l'ausilio dell'impresa di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati, senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i dipendenti e i clienti dell'impresa, per un totale di poche decine di persone. Non sono state interessate categorie particolari di dati. Non era disponibile alcun backup in formato elettronico. La maggior parte dei dati è stata ripristinata da backup cartacei. Il ripristino dei dati ha richiesto 5 giorni lavorativi e ha comportato lievi ritardi nella consegna degli ordini ai clienti.

2.2.1 Caso n. 02 — Misure in essere e valutazione del rischio

26. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.9. La principale differenza rispetto al caso precedente è la mancanza di un backup in formato elettronico e la mancanza di cifratura dei dati memorizzati (at rest). Ciò comporta differenze critiche nelle fasi successive.

27. Nel valutare i rischi, il titolare del trattamento dovrebbe indagare sul metodo di infiltrazione e individuare la tipologia di codice malevolo per comprendere le possibili conseguenze dell'attacco. In questo esempio il ransomware cifrava i dati personali senza esfiltrarli. Di conseguenza, i rischi per i diritti e le libertà degli interessati sembrano derivare dalla mancanza di disponibilità dei dati personali e la riservatezza dei dati personali non risulterebbe compromessa. Per determinare il rischio è essenziale un esame approfondito dei log dei firewall e delle relative implicazioni. Su richiesta, il titolare del trattamento dovrebbe presentare le risultanze documentate di tali indagini.

28. Il titolare del trattamento deve tenere presente che, se l'attacco è più sofisticato, il malware è in grado di modificare i file di log e rimuovere le tracce. Pertanto, poiché i log non sono trasmessi o replicati a un server centrale, anche dopo un'indagine approfondita che ha accertato che i dati personali non sono stati esfiltrati dall'attaccante, il titolare del trattamento non può affermare che l'assenza di log dimostri l'assenza di esfiltrazione; ne consegue l'impossibilità di escludere in via assoluta la probabilità di una violazione della riservatezza.

29. Il titolare del trattamento dovrebbe valutare i rischi di questa violazione13 se l'attaccante ha avuto accesso ai dati. Nel corso della valutazione del rischio, il titolare dovrebbe tenere conto anche della natura, della sensibilità, del volume e del contesto dei dati personali interessati dalla violazione. In questo caso non sono coinvolte categorie particolari di dati personali e la quantità di dati violati e il numero di interessati colpiti sono ridotti.

30. La raccolta di informazioni esatte sull'accesso non autorizzato è fondamentale per determinare il livello di rischio e prevenire un nuovo attacco o la prosecuzione di un attacco in corso. Se i dati fossero stati copiati dalla banca dati, ciò sarebbe stato ovviamente un fattore di incremento del rischio. In caso di incertezza circa le specificità dell'accesso illegittimo, si dovrebbe prendere in considerazione lo scenario peggiore e il rischio dovrebbe essere valutato in termini conseguenti.

31. L'assenza di un backup può essere considerata un fattore di incremento del rischio a seconda della gravità delle conseguenze derivanti per gli interessati dall'indisponibilità dei dati.

13 Per indicazioni sulle operazioni di trattamento "che possono comportare un rischio elevato ", cfr. la nota 10.

2.2.2 Caso n. 02 — Misure di mitigazione e obblighi

32. In assenza di un backup, sono poche le misure che il titolare del trattamento può adottare per porre rimedio alla perdita di dati personali e i dati devono essere nuovamente raccolti, a meno che sia disponibile un'altra fonte (ad esempio, e-mail di conferma degli ordini). Senza un backup, i dati possono andare persi e la gravità dipenderà dall'impatto per le persone.

33. Il ripristino dei dati non dovrebbe rivelarsi eccessivamente problematico14 se i dati sono ancora disponibili su supporto cartaceo; tuttavia, data la mancanza di un backup in formato elettronico , si ritiene necessaria una notifica all'autorità di controllo, in quanto il ripristino dei dati ha richiesto un certo tempo e potrebbe causare ritardi nella consegna degli ordini ai clienti mentre potrebbe risultare impossibile recuperare una notevole quantità di metadati (ad esempio log, marcatura temporale).

34. La comunicazione agli interessati in merito alla violazione può dipendere anche dal periodo di indisponibilità dei dati personali e dalle difficoltà che ne potrebbero derivare per l'operatività del titolare del trattamento (ad esempio ritardi nel trasferimento dei pagamenti ai dipendenti). Poiché tali ritardi nei pagamenti e nelle consegne possono comportare perdite finanziarie per le persone i cui dati sono stati compromessi, si potrebbe anche sostenere che la violazione comporti un rischio elevato. Inoltre, potrebbe risultare impossibile evitare di informare gli interessati se il loro contributo è necessario per ripristinare i dati cifrati.

35. Questo caso è un esempio di attacco ransomware con rischi per i diritti e le libertà degli interessati, senza che si raggiunga un rischio elevato. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, e notificata all'autorità di controllo a norma dell'articolo 33, paragrafo 1. La struttura del titolare può anche necessitare di (o ricevere disposizioni dall'autorità di controllo per) aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

2.3 Caso n. 03: Attacco ransomware nei confronti di un ospedale con backup e senza esfiltrazione

Il sistema informativo di un ospedale/centro sanitario è stato esposto a un attacco ransomware e una parte significativa dei dati è stata cifrata dall'attaccante. L'azienda sanitaria si avvale delle competenze di una società esterna di cybersecurity per monitorare la propria rete. Sono disponibili log che tracciano tutti i flussi di dati in uscita dall'azienda (comprese le e-mail in uscita). Dopo aver analizzato i log e i dati raccolti dagli altri sistemi di rilevamento, l'indagine interna svolta con l'ausilio della società di cybersecurity ha stabilito che l'autore dell'attacco ha soltanto cifrato i dati senza esfiltrarli. I log non mostrano alcun flusso di dati verso l'esterno nell'arco di tempo dell'attacco. I dati personali interessati dalla violazione riguardano i dipendenti e i pazienti, complessivamente varie migliaia di persone. I backup erano disponibili in formato elettronico. La maggior parte dei dati è stata ripristinata, ma questa operazione ha richiesto 2 giorni lavorativi, causando notevoli ritardi nelle cure rese ai pazienti con annullamento o rinvio di interventi chirurgici e un abbassamento del livello di servizio a causa dell'indisponibilità dei sistemi.

2.3.1 Caso n. 03 — Misure in essere e valutazione del rischio

36. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.5. La principale differenza rispetto al caso precedente è l'elevata gravità delle conseguenze per un numero

14 Ciò dipenderà dalla complessità e dalla struttura dei dati personali. Negli scenari più complessi, il ripristino dell'integrità dei dati, la coerenza con i metadati, la garanzia della correttezza delle relazioni all'interno delle strutture di dati e il controllo dell'accuratezza dei dati possono richiedere risorse e sforzi significativi.

sostanziale di interessati15.

37. La quantità di dati violati e il numero di interessati colpiti dalla violazione sono elevati, in quanto gli ospedali generalmente trattano grandi quantità di dati. L'indisponibilità dei dati ha un forte impatto su una parte sostanziale degli interessati. Esiste inoltre un rischio residuo di elevata gravità per la riservatezza dei dati dei pazienti.

38. La tipologia della violazione, la natura, la sensibilità e il volume dei dati personali interessati dalla violazione sono importanti. Sebbene esistesse un backup per i dati e questi abbiano potuto essere ripristinati in pochi giorni, sussiste un rischio elevato a causa della gravità delle conseguenze per gli interessati derivanti dall'indisponibilità dei dati al momento dell'attacco e nei giorni successivi.

2.3.2 Caso n. 03 — Misure di mitigazione e obblighi

39. Si ritiene necessaria una notifica all'autorità di controllo, in quanto si tratta di categorie particolari di dati personali e il ripristino dei dati potrebbe richiedere molto tempo, con notevoli ritardi nelle cure dei pazienti. Comunicare la violazione agli interessati è necessario a causa dell'impatto sui pazienti, anche dopo il ripristino dei dati cifrati. Anche se sono stati criptati dati relativi a tutti i pazienti trattati in ospedale negli ultimi anni, la violazione ha interessato soltanto i dati relativi ai pazienti che dovevano essere sottoposti a terapie in ospedale durante il periodo di indisponibilità del sistema informatico. Il titolare del trattamento dovrebbe comunicare la violazione dei dati direttamente a tali pazienti. L'eccezione di cui all'articolo 34, paragrafo 3, lettera c), può non rendere necessaria la comunicazione diretta agli altri pazienti, alcuni dei quali possono non essere stati ricoverati in ospedale da più di venti anni. In tal caso, si procede invece a una comunicazione pubblica16 o a una misura analoga, tramite la quale gli interessati sono informati con pari efficacia. In tal caso, l'ospedale dovrebbe rendere pubblico l'attacco ransomware e i suoi effetti.

40. Questo caso serve da esempio di un attacco ransomware con un rischio elevato per i diritti e le libertà degli interessati. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, notificata all'autorità di controllo in conformità dell'articolo 33, paragrafo 1, e comunicata agli interessati in conformità dell'articolo 34, paragrafo 1. L'azienda sanitaria deve inoltre aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all' autorità di controllo	Comunicazione agli interessati
✓	✓	✓

2.4 Caso n. 04: Attacco ransomware senza backup e con esfiltrazione

Il server di una società di trasporto pubblico è stato esposto a un attacco ransomware e i dati sono stati cifrati dall'autore dell'attacco. Secondo i risultati dell'indagine interna, l'autore dell'attacco non solo ha cifrato i dati, ma li ha anche esfiltrati. La tipologia dei dati violati consiste nei dati personali di clienti e dipendenti e delle diverse migliaia di persone che utilizzano i servizi della società (ad esempio, per l'acquisto di biglietti online). Oltre ai dati identificativi di base, sono coinvolti nella violazione i numeri dei documenti d'identità e dati finanziari come i dati della carta di credito. Era disponibile un backup, ma anch'esso è stato

15 Per indicazioni sulle operazioni di trattamento "che possono comportare un rischio elevato ", cfr. la nota 10.

16 Il considerando 86 del regolamento generale sulla protezione dei dati spiega che *"Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta cooperazione con l'autorità di controllo, nel rispetto degli orientamenti forniti da quest'ultima o da altre autorità competenti, quali le autorità di contrasto. Ad esempio, la necessità di attenuare un rischio immediato di danno richiederebbe che la comunicazione con gli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione".*

criptato dall'aggressore.

2.4.1 Caso n. 04 — Misure in essere e valutazione del rischio

41. Il titolare del trattamento avrebbe dovuto adottare le stesse misure di cui alla parte 2.1 e alla sezione 2.5. Sebbene disponibile, anche il backup è stato compromesso dall'attacco. Questa circostanza di per sé solleva interrogativi sulla qualità delle misure di sicurezza informatica in essere e dovrebbe essere oggetto di approfondimenti ulteriori durante l'indagine poiché, in un regime di backup ben progettato, devono essere conservati in modo sicuro più backup senza consentire l'accesso dal sistema principale, altrimenti potrebbero essere compromessi nello stesso attacco. Inoltre, gli attacchi ransomware possono rimanere occulti per giorni cifrando lentamente dati utilizzati di rado. Ciò può rendere inutile l'esecuzione di più backup, per cui dovrebbero essere eseguiti anche backup periodici e poi essere isolati. In tal modo si aumenterebbe la probabilità di recupero seppur con una perdita maggiore di dati.

42. La violazione riguarda non solo la disponibilità dei dati, ma anche la riservatezza, in quanto l'autore dell'attacco può aver modificato e/o copiato i dati dal server. Pertanto, il tipo di violazione comporta un rischio elevato17.

43. La natura, la sensibilità e il volume dei dati personali aumentano ulteriormente i rischi, poiché il numero di persone interessate è elevato, così come la quantità complessiva di dati personali compromessi. Al di là dei dati identificativi di base, sono coinvolti anche documenti di identità e dati finanziari come i dati della carta di credito. Una violazione dei dati relativa a queste categorie di informazioni presenta di per sé un rischio elevato e i dati oggetto di compromissione, se utilizzati congiuntamente, potrebbero servire, tra l'altro, a realizzare furti di identità o frodi.

44. A causa di errori dei controlli logici o organizzativi del server, i backup sono stati compromessi dal ransomware e ciò ha impedito il ripristino dei dati e aumentato il rischio.

45. Questa violazione dei dati presenta un rischio elevato per i diritti e le libertà delle persone, in quanto potrebbe comportare sia un danno materiale (ad esempio una perdita finanziaria dovuta alla compromissione dei dati della carta di credito) sia immateriale (ad esempio furto o usurpazione d'identità in quanto i dati della carta d'identità sono stati compromessi).

2.4.2 Caso n. 04 — Misure di mitigazione e obblighi

46. La comunicazione agli interessati è essenziale affinché possano adottare le misure necessarie per evitare danni materiali (ad esempio bloccare le loro carte di credito).

47. Oltre a documentare la violazione ai sensi dell'articolo 33, paragrafo 5, anche in questo caso la notifica all'autorità di controllo è obbligatoria (articolo 33, paragrafo 1) e il titolare del trattamento è altresì tenuto a comunicare la violazione agli interessati (articolo 34, paragrafo 1). Quest'ultima comunicazione potrebbe essere effettuata a ogni singolo interessato, ma per le persone in cui i dati di contatto non sono disponibili, il titolare del trattamento dovrebbe dare pubblica comunicazione purché ciò non sia suscettibile di determinare ulteriori conseguenze negative per gli interessati - ad esempio mediante una notifica sul suo sito web. In quest'ultimo caso è necessaria una comunicazione chiara e precisa, ben visibile sulla homepage del titolare del trattamento, con riferimenti esatti alle pertinenti disposizioni del GDPR. La società può inoltre dover aggiornare e correggere le misure e procedure organizzative e tecniche di gestione della sicurezza dei dati personali e di mitigazione dei rischi.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati

17 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

✓	✓	✓

2.5 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di ransomware

48. Il fatto che si sia verificato un attacco ransomware è solitamente la spia dell'esistenza di una o più vulnerabilità del sistema del titolare del trattamento. Ciò vale anche nei casi di attacchi ransomware con cifratura dei dati personali ma senza esfiltrazione. Indipendentemente dall'esito e dalle conseguenze dell'attacco, non si evidenzierà mai a sufficienza quanto sia cruciale una valutazione complessiva del sistema di sicurezza dei dati, con particolare riguardo alla sicurezza informatica. Le debolezze individuate e le lacune di sicurezza devono essere documentate e affrontate senza indugio.

49. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Mantenere aggiornato il firmware, il sistema operativo e il software applicativo sui server, sui client, sui componenti attivi di rete e su ogni altra macchina presente dulla stessa LAN (compresi i dispositivi Wi-Fi). Garantire l'esistenza di adeguate misure di sicurezza informatica, accertarne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Ciò comprende la conservazione di log dettagliati dei patch applicati e della rispettiva marcatura temporale.
- Progettazione e organizzazione di sistemi e infrastrutture di trattamento in modo da segmentare o isolare sistemi e reti di dati per evitare la propagazione di software malevolo all'interno dell'organizzazione e verso sistemi esterni.
- Esistenza di una procedura di backup aggiornata, sicura e testata. I mezzi di supporto per il back-up a medio e lungo termine dovrebbero essere tenuti separati dalla conservazione dei dati operativi e fuori dalla portata di soggetti terzi anche in caso di attacco riuscito (per esempio, un backup incrementale giornaliero e un backup settimanale completo).
- Disporre di/procurarsi un software antimalware adeguato, aggiornato, efficace e integrato.
- Disporre di un firewall e sistemi per il rilevamento e la prevenzione delle intrusioni adeguati, aggiornati, efficaci e integrati. Instradare il traffico di rete attraverso il firewall/il sistema rilevamento intrusioni, anche in caso di lavoro agile o in mobilità (ad esempio utilizzando connessioni VPN dotate di meccanismi organizzativi di sicurezza per l'accesso a Internet).
- Formazione dei dipendenti sui metodi di riconoscimento e prevenzione degli attacchi informatici. Il titolare del trattamento dovrebbe fornire gli strumenti per stabilire se le e-mail e i messaggi ottenuti con altri mezzi di comunicazione siano autentici e affidabili. I dipendenti dovrebbero essere formati per riconoscere quando si verifica un attacco del genere, sapere come rimuovere dalla rete l'endpoint ed essere tenuti a segnalarlo immediatamente al responsabile della sicurezza.
- Sottolineare la necessità di individuare il tipo di codice malevolo per comprendere le conseguenze dell'attacco ed essere in grado di individuare le misure giuste per attenuare il rischio. Nel caso in cui un attacco ransomware abbia avuto successo e non sia disponibile alcun back-up, per recuperare i dati possono essere utilizzati strumenti come quelli del progetto "no more ransom" (nomoreransom.org). Tuttavia, nel caso in cui sia disponibile un backup sicuro, è consigliabile ripristinare i dati attraverso il backup.
- Inoltrare o replicare tutti i log a un server centrale (compresa eventualmente la marcatura temporale crittografica o la firma delle registrazioni dei log).
- Cifratura robusta e autenticazione a più fattori, in particolare per l'accesso amministrativo ai sistemi informatici, adeguata gestione delle chiavi e delle password.

- Test di vulnerabilità e di penetrazione a cadenze regolari.
- Istituire un gruppo di risposta agli incidenti di sicurezza (CSIRT) o un gruppo di risposta alle emergenze informatiche (CERT) all'interno dell'organizzazione o aderire a un CSIRT/CERT collettivo. Creare un piano di risposta agli incidenti, un piano di *disaster recovery* (ripristino in caso di evento catastrofico) e un piano di continuità operativa e assicurarsi che tali piani siano testati in modo approfondito.
- Nel valutare le contromisure, si dovrebbe riesaminare, testare e aggiornare l'analisi dei rischi.

3 ATTACCHI DI ESFILTRAZIONE DEI DATI

50. Gli attacchi che sfruttano le vulnerabilità dei servizi offerti dal titolare del trattamento a terzi su Internet, ad esempio mediante attacchi di *injection* (es. attacchi SQL *injection*, *path traversal*), compromissione di siti web e simili, possono assomigliare ad attacchi ransomware in quanto il rischio deriva dall'azione di un terzo non autorizzato, ma mirano generalmente a copiare, esfiltrare e utilizzare dati personali per fini dolosi. Si tratta quindi principalmente di violazioni della riservatezza e, eventualmente, anche dell'integrità dei dati. Allo stesso tempo, se il titolare del trattamento è a conoscenza delle caratteristiche di questo tipo di violazioni, vi sono numerose misure che possono ridurre considerevolmente il rischio di un attacco efficace.

3.1 Caso n. 05: Esfiltrazione dei dati delle domande di impiego da un sito web

Un'agenzia per l'impiego è stata vittima di un attacco informatico, che ha inserito un codice malevolo sul suo sito web. Questo codice ha reso accessibili a soggetti non autorizzati le informazioni personali contenute nei moduli di richiesta di impiego conservati sul server web. 213 di tali moduli potrebbero essere interessati, e le analisi hanno accertato che nessuna categoria particolare di dati era oggetto della violazione. Il i malware installato aveva funzionalità che consentivano all'attaccante di rimuovere qualsiasi traccia di esfiltrazione e di monitorare il trattamento effettuato sul server e di carpire dati personali. Il malware è stato individuato solo un mese dopo la sua installazione.

3.1.1 Caso n. 05 — Misure in essere e valutazione del rischio

51. La sicurezza dell'ambiente del titolare del trattamento è estremamente importante, dal momento che la maggior parte di queste violazioni può essere evitata garantendo che tutti i sistemi siano costantemente aggiornati, che i dati sensibili siano cifrati e che le applicazioni siano sviluppate secondo elevati standard di sicurezza quali autenticazione forte, misure contro attacchi di forza bruta, "escape" (evasione) o "sanitizing" (sanificazione) "18 degli input degli utenti, ecc. . Anche gli audit periodici di sicurezza informatica, le valutazioni delle vulnerabilità e i test di penetrazione sono necessari per individuare e correggere tali tipi di vulnerabilità. Nel caso specifico, l'impiego di strumenti di monitoraggio dell'integrità dei file nell'ambiente di produzione avrebbe potuto facilitare l'individuazione dell'iniezione del codice (un elenco delle misure consigliate figura nella sezione 3.7).

52. Nell'indagare sulla violazione, il titolare del trattamento dovrebbe sempre partire dall'identificazione della tipologia e della metodica dell'attacco, al fine di valutare le misure da adottare. Per garantire rapidità ed efficacia di tale valutazione, il titolare dovrebbe disporre di un piano di risposta agli incidenti che specifichi le misure necessarie da adottare rapidamente per assumere il controllo dell'incidente. In questo caso particolare, il tipo di violazione costituiva un fattore di incremento del rischio, in quanto non solo veniva compromessa la riservatezza dei dati, ma il soggetto infiltrato era anche in grado di apportare modifiche al sistema cosicché veniva messa in discussione anche l'integrità dei dati.

53. Si dovrebbe tenere conto della natura, della sensibilità e del volume dei dati personali colpiti dalla violazione per determinare in che misura quest'ultima abbia inciso sugli interessati. Sebbene non siano state

18 La sanificazione degli input dell'utente è una forma di convalida degli input finalizzata ad assicurare che solo dati adeguatamente formattati siano inseriti in un sistema IT.

compromesse categorie particolari di dati personali, i dati oggetto della violazione contengono importanti informazioni sulle persone che hanno compilato i moduli online e tali dati potrebbero essere utilizzati impropriamente in vari modi (marketing indesiderato, furto di identità, ecc.), per cui la gravità delle conseguenze dovrebbe aumentare il rischio per i diritti e le libertà degli interessati19.

3.1.2 Caso n. 05 — Misure di mitigazione e obblighi

54. Se possibile, una volta risolto il problema, la banca dati dovrebbe essere confrontata con quella memorizzata in un backup sicuro. Le esperienze tratte dalla violazione dovrebbero essere utilizzate per aggiornare l'infrastruttura informatica. Il titolare del trattamento dovrebbe riportare tutti i sistemi informatici interessati a uno stato pulito noto, porre rimedio alla vulnerabilità e attuare nuove misure di sicurezza per evitare analoghe violazioni dei dati in futuro, ad esempio controlli di integrità dei file e audit di sicurezza. Se i dati personali sono stati non solo esfiltrati, ma anche cancellati, il titolare del trattamento deve intraprendere un'azione sistematica per ripristinare i dati personali nello stato in cui si trovavano prima della violazione. Potrebbe essere necessario applicare backup completi, modifiche incrementali ed eventualmente ripetere il trattamento dall'ultimo backup incrementale, il che richiede che il titolare sia in grado di replicare le modifiche apportate dopo l'ultimo backup. Ciò potrebbe necessitare che il titolare del trattamento disponga di un sistema progettato per conservare i file di input giornalieri nel caso in cui questi debbano essere nuovamente elaborati; tutto ciò richiede una tecnica robusta di memorizzazione e un'adeguata politica di conservazione prolungata dei dati.

55. Alla luce di quanto precede, poiché la violazione può comportare un rischio elevato per i diritti e le libertà delle persone fisiche, gli interessati dovrebbero esserne informati (articolo 34, paragrafo 1), il che significa naturalmente che anche le autorità di controllo competenti dovrebbero essere coinvolte attraverso una notifica di violazione dei dati. Documentare la violazione è obbligatorio ai sensi dell'articolo 33, paragrafo 5, del regolamento generale sulla protezione dei dati e facilita la valutazione del caso specifico.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

3.2 Caso n. 06: Esfiltrazione da un sito web di password sottoposte ad hashing

Una vulnerabilità SQL Injection è stata sfruttata per accedere a un database sul server di un sito web dedicato alla cucina. Agli utenti è stato consentito di scegliere solo pseudonimi arbitrari come nomi utente. È stato scoraggiato l'uso di indirizzi di posta elettronica a tal fine. Le password memorizzate nella banca dati sono state sottoposte ad hashing con un algoritmo robusto e il *salt* non è stato compromesso. Dati interessati: password *hashed* di 1.200 utenti. Per motivi di sicurezza, il titolare del trattamento ha informato gli interessati della violazione tramite posta elettronica e ha chiesto loro di modificare le password, soprattutto se la stessa password è stata utilizzata per altri servizi.

3.2.1 Caso n. 06 — Misure in essere e valutazione del rischio

56. In questo caso particolare, la riservatezza dei dati è compromessa, ma le password nel database sono state sottoposte ad hashing con un metodo conforme allo stato dell'arte, il che ridurrebbe il rischio per quanto riguarda la natura, la sensibilità e il volume dei dati personali. Il caso non presenta rischi per i diritti e le libertà degli interessati.

57. Inoltre, non sono state compromesse le informazioni di contatto (ad esempio indirizzi di posta elettronica o numeri di telefono) degli interessati, il che significa che non vi è alcun rischio significativo per gli interessati di essere oggetto di tentativi di frode (ad esempio, messaggi di posta elettronica di phishing o telefonate e SMS fraudolenti). Non sono state coinvolte categorie particolari di dati personali.

19 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato"*, cfr. la nota 10.

58. Alcuni nomi utente potrebbero essere considerati dati personali, ma la materia trattata dal sito web non genera connotazioni negative. Tuttavia, si deve osservare che la valutazione del rischio può essere diversa20, se la natura del sito web e i dati consultati possono rivelare categorie particolari di dati personali (ad esempio il sito web di un partito politico o di un sindacato). L'uso di tecniche di cifratura conformi allo stato dell'arte potrebbe attenuare gli effetti negativi della violazione. Consentire un numero limitato di tentativi di login impedirà il successo degli attacchi di forza bruta sul login, riducendo in larga misura i rischi generati da i attaccanti che già conoscono i nomi utente.

3.2.2 Caso n. 06 — Misure di mitigazione e obblighi

59. In alcuni casi la comunicazione agli interessati potrebbe essere considerata un fattore di mitigazione del rischio, dal momento che anche gli interessati sono in grado di adottare le misure necessarie per evitare ulteriori danni derivanti dalla violazione, ad esempio modificando la loro password. In questo caso, la comunicazione non era obbligatoria, ma in molti casi può essere considerata una buona pratica.

60. Il titolare del trattamento dovrebbe correggere la vulnerabilità e implementare nuove misure di sicurezza per evitare in futuro analoghe violazioni dei dati, ad esempio attraverso audit sistematici di sicurezza sul sito web.

61. La violazione dovrebbe essere documentata conformemente all'articolo 33, paragrafo 5, ma non è necessaria alcuna notifica o comunicazione.

62. Inoltre, è fortemente consigliabile comunicare agli interessati una violazione che riguardi password anche se le password sono state memorizzate utilizzando un hash con l'impiego di *salt* attraverso un algoritmo conforme allo stato dell'arte. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server. Gli interessati dovrebbero avere la possibilità di adottare misure adeguate per quanto riguarda le proprie password.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

3.3 Caso n. 07: Attacco del tipo *credential stuffing* su un sito web bancario

Una banca ha subito un attacco informatico contro uno dei suoi siti web di servizi bancari online. L'attacco mirava a elencare tutti gli identificativi utente di accesso possibili utilizzando una banale password fissa. Le password sono composte da 8 cifre. A causa di vulnerabilità del sito web, in alcuni casi l'autore dell'attacco ha potuto accedere a informazioni riguardanti gli interessati (nome, cognome, sesso, data e luogo di nascita, codice fiscale, codici di identificazione dell'utente), anche se la password utilizzata non era corretta o il conto bancario non era più attivo. Ciò ha interessato circa 100.000 soggetti. Fra questi, l'autore dell'attacco si è connesso con successo a circa 2.000 account che utilizzavano la password banale da questi processata . Successivamente il titolare del trattamento è stato in grado di individuare tutti i tentativi illegittimi di log-on. Il titolare ha potuto verificare che, in base ai controlli antifrode, su tali account non è stata effettuata alcuna transazione durante l'attacco. La banca era a conoscenza della violazione dei dati in quanto il suo centro operativo di sicurezza ha individuato un numero elevato di richieste di login dirette verso il sito web. In risposta, il titolare del trattamento ha disattivato temporaneamente la possibilità di connettersi al sito web e ha forzato il cambio password degli account compromessi. Il titolare ha comunicato la violazione solo agli utenti con account compromessi, ossia agli utenti le cui password sono state compromesse o i cui dati sono stati divulgati.

3.3.1 Caso n. 07 — Misure in essere e valutazione del rischio

63. È importante ricordare che i titolari che trattano dati di natura estremamente personale21 hanno maggiori

20 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

21 Quali le informazioni degli interessati relative a metodi di pagamento come numeri di carta, conti bancari,

responsabilità in termini di garanzia di un'adeguata sicurezza dei dati, ad esempio predisponendo un centro operativo di sicurezza e attuando altre misure di prevenzione, rilevamento e risposta agli incidenti. Il mancato rispetto di questi standard più elevati comporterà certamente l'adozione di misure più severe durante l'indagine di un'autorità di controllo.

64. La violazione riguarda dati finanziari che vanno al di là dell'identità e delle informazioni identificative dell'utente, il che la rende particolarmente grave. Il numero di persone interessate è elevato.

65. Il fatto che una violazione possa verificarsi in un ambiente così sensibile segnala la presenza di notevoli lacune della sicurezza dei dati nel sistema del titolare del trattamento e può essere un indicatore della necessità di un riesame e di un aggiornamento delle misure in questione, in linea con gli articoli 24 (1), 25 (1) e 32 (1) del GDPR. I dati violati consentono l'identificazione univoca degli interessati e contengono altre informazioni su di essi (tra cui sesso, data e luogo di nascita); inoltre possono essere utilizzati dall'autore dell'attacco per ricavare le password dei clienti o per condurre una campagna di phishing mirata ai clienti della banca.

66. Per questi motivi, la violazione dei dati è stata ritenuta suscettibile di comportare un rischio elevato per i diritti e le libertà di tutti gli interessati22. Pertanto, è ipotizzabile il verificarsi di un danno materiale (ad esempio una perdita finanziaria) e immateriale (ad esempio furto d'identità o frode) in conseguenza della violazione.

3.3.2 Caso n. 07 — Misure di mitigazione e obblighi

67. Le misure del titolare del trattamento menzionate nella descrizione del caso sono adeguate. A seguito della violazione, ha inoltre corretto la vulnerabilità del sito web e ha adottato altre misure per prevenire analoghe violazioni dei dati in futuro, come l'aggiunta di un'autenticazione a due fattori al sito web interessato e il passaggio a un'autenticazione forte del cliente.

68. In questo scenario la documentazione della violazione a norma dell'articolo 33, paragrafo 5, del GDPR e la notifica all'autorità di controllo non sono lasciate alla discrezione del titolare. Inoltre, il titolare del trattamento dovrebbe informare tutti i 100.000 interessati (compresi gli interessati i cui account non sono stati compromessi) a norma dell'articolo 34 del GDPR.

Azioni necessarie sulla base dei rischi individuati		
Documentazione	Notifica all'autorità	Comunicazione agli interessati
✓	✓	✓

3.4 Misure organizzative e tecniche per prevenire/mitigare gli effetti degli attacchi di hacker

69. Come nel caso degli attacchi ransomware, indipendentemente dall'esito e dalle conseguenze dell'attacco, i titolari sono tenuti a riconsiderare le misure di sicurezza dei sistemi informativi in casi analoghi.

70. Misure consigliate:23

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Cifratura e gestione delle chiavi conformi allo stato dell'arte, in particolare quando si trattano password, dati sensibili o finanziari. L'hashing e l'utilizzo di salt crittografici sono sempre preferibili in caso di informazioni riservate (password) rispetto alla cifratura delle password. È preferibile utilizzare metodi di autenticazione che evitino la necessità di trattare password lato server.
- Aggiornamento del sistema (software e firmware). Garantire l'applicazione di tutte le misure di sicurezza

pagamenti online, cedolini degli stipendi, estratti conto bancari, studi economici o qualsiasi altro elemento che possa rivelare informazioni economiche relative agli interessati.

22 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato"*, cfr. la nota 10.

23 Per lo sviluppo sicuro di applicazioni web si veda anche: https://www.owasp.org/index.php/Main page.

informatica, garantirne l'efficacia e mantenerle regolarmente aggiornate quando il trattamento o le circostanze cambiano o evolvono. Per essere in grado di dimostrare la conformità all'articolo 5, paragrafo 1, lettera f), a norma dell'articolo 5, paragrafo 2, del GDPR, il titolare del trattamento dovrebbe conservare un registro di tutti gli aggiornamenti effettuati, compreso il momento in cui sono stati applicati.

- Uso di metodi di autenticazione forte quali autenticazione a due fattori e server di autenticazione, integrati da una politica aggiornata in materia di password.
- Gli standard sicuri di sviluppo comprendono l'applicazione di un filtro agli input utente (utilizzando per quanto possibile una *white list*), la sanificazione degli input utente e misure di prevenzione degli attacchi di forza bruta (come limitare il numero massimo di tentativi ripetuti). L'impiego di Web Application Firewall (WAF - firewall per le applicazioni web) può supportare l'implementazione efficace di questa tecnica.
- Politiche robuste per i privilegi utente e la gestione del controllo degli accessi.
- Uso di sistemi di protezione, di rilevamento delle intrusioni e di difesa perimetrale adeguati, aggiornati, efficaci e integrati.
- Audit sistematici della sicurezza informatica e valutazioni delle vulnerabilità (test di penetrazione).
- Revisioni e test periodici per garantire l'utilizzabilità dei backup al fine di ripristinare i dati la cui integrità o disponibilità siano state compromesse.
- Nessun identificativo di sessione nell'URL in chiaro.

4 FONTI DI RISCHIO INTERNE LEGATE AL FATTORE UMANO

71. Occorre evidenziare il ruolo dell'errore umano nelle violazioni dei dati personali a causa della sua frequenza. Poiché queste violazioni possono essere sia intenzionali che accidentali, è molto difficile per i titolari del trattamento individuare le vulnerabilità e adottare misure per evitarle. La Conferenza internazionale delle autorità per la protezione dei dati e la privacy ha riconosciuto l'importanza di affrontare tali fattori umani e ha adottato, nell'ottobre 2019, una risoluzione concernente il ruolo dell'errore umano nelle violazioni dei dati personali24. La risoluzione sottolinea la necessità di adottare misure di salvaguardia adeguate al fine di prevenire gli errori umani e fornisce un elenco non esaustivo di garanzie e approcci.

4.1 Caso n. 08: Esfiltrazione di dati aziendali da parte di un dipendente

Durante il suo periodo di preavviso, il dipendente di una società copia i dati aziendali dalla banca dati della società. Il dipendente è autorizzato ad accedere ai dati solo per svolgere le sue mansioni. Vari mesi dopo aver cessato il lavoro alle dipendenze della società, utilizza i dati così ottenuti (dati di contatto di base) per alimentare un nuovo trattamento dei dati per il quale è il titolare, al fine di contattare i clienti della società e invitarli a rivolgersi alla sua nuova impresa.

4.1.1 Caso n. 08 — Misure in essere e valutazione del rischio

72. Nel caso di specie non sono state adottate misure preventive per impedire al dipendente di copiare i dati di contatto della clientela della società, in quanto il dipendente aveva bisogno legittimamente di accedere – e di fatto accedeva – a tali informazioni per le sue mansioni. Poiché la gestione dei clienti richiede nella maggior parte dei casi un qualche tipo di accesso dei dipendenti ai dati personali, tali violazioni possono essere le più difficili da prevenire. Limitando la portata dell'accesso si rischia di limitare il lavoro che il dipendente è in grado di svolgere. Tuttavia, politiche di accesso ben concepite e un controllo costante possono contribuire a prevenire tali violazioni.

73. Come di consueto, durante la valutazione del rischio devono essere presi in considerazione il tipo di violazione e la natura, la sensibilità e il volume dei dati personali interessati. Queste violazioni sono generalmente

24 http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf

violazioni della riservatezza, in quanto la banca dati è solitamente lasciata intatta e il suo contenuto è "semplicemente" copiato in vista di un ulteriore utilizzo. La quantità di dati interessati è solitamente bassa o media. In questo caso particolare non sono state coinvolte categorie particolari di dati personali, il dipendente aveva bisogno soltanto delle informazioni di contatto dei clienti per essere in grado di contattarli dopo aver lasciato la società. Pertanto, i dati in questione non sono sensibili.

74. Sebbene l'unico obiettivo dell'ex-dipendente che ha copiato in modo fraudolento i dati possa consistere nell'ottenere le informazioni di contatto della clientela della società per i propri scopi di natura commerciale, il titolare del trattamento non può considerare basso il rischio per gli interessati poiché non dispone di alcuna certezza sulle intenzioni del dipendente. Pertanto, sebbene le conseguenze della violazione possano limitarsi all'esposizione alle attività di autopromozione svolte dall'ex-dipendente, non è escluso un ulteriore e più grave abuso dei dati copiati, a seconda della finalità del trattamento messo in atto dall'ex-dipendente25.

4.1.2 Caso n. 08 — Misure di mitigazione e obblighi

75. Nel caso di specie è difficile mitigare gli effetti negativi della violazione. Potrebbe essere necessario avviare un'azione legale immediata per impedire all'ex-dipendente di utilizzare impropriamente e diffondere ulteriormente i dati. In seconda battuta, l'obiettivo dovrebbe essere quello di evitare situazioni analoghe in futuro. Il titolare del trattamento potrebbe chiedere un'ingiunzione che imponga all'ex-dipendente di astenersi dall'utilizzo dei dati, ma le probabilità che ciò risulti efficace sono, nella migliore delle ipotesi, opinabili. Possono essere utili misure tecniche adeguate, come l'impossibilità di copiare o scaricare dati su dispositivi amovibili.

76. Non esiste una soluzione unica per tutti i casi di questo tipo, ma un approccio sistematico può contribuire a prevenirli. Ad esempio, l'impresa può prendere in considerazione, ove possibile, la limitazione degli accessi per i dipendenti che hanno segnalato l'intenzione di licenziarsi, oppure prevedere log degli accessi in modo da registrare e segnalare ogni accesso indesiderato. Il contratto firmato con i dipendenti dovrebbe includere clausole che vietino attività del genere descritto.

77. Nel complesso, poiché la violazione in questione non comporterà un rischio elevato per i diritti e le libertà delle persone fisiche, è sufficiente una notifica all'autorità di controllo. Tuttavia, informarne gli interessati potrebbe essere vantaggioso anche per il titolare del trattamento, in quanto sarebbe meglio che gli interessati ricevano la notizia della violazione dall'azienda piuttosto che apprenderla quando l'ex-dipendente cercherà di contattarli. La documentazione della violazione a norma dell'articolo 33, paragrafo 5, è un obbligo giuridico.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

4.2 Caso n. 09: Trasmissione accidentale di dati a un terzo fidato

Un agente assicurativo ha notato che — a causa dalle impostazioni difettose di un file Excel ricevuto per posta elettronica — era in grado di accedere alle informazioni relative a una ventina di clienti non appartenenti al suo portafoglio. Egli è vincolato dal segreto professionale ed è stato l'unico destinatario del messaggio di posta elettronica. L'accordo tra il titolare del trattamento e l'agente assicurativo obbliga quest'ultimo a segnalare senza ingiustificato ritardo una violazione dei dati personali al titolare stesso. Pertanto, l'agente ha immediatamente segnalato l'errore al titolare, che ha corretto il file e lo ha inviato nuovamente, chiedendo all'agente di cancellare il messaggio precedente. In base all'accordo di cui sopra, l'agente deve confermare la cancellazione per iscritto, cosa che ha fatto. Le informazioni raccolte non comprendono categorie particolari di dati personali, solo dati di contatto e dati relativi all'assicurazione stessa (tipo di assicurazione, importo). Dopo aver analizzato i dati personali interessati dalla violazione, il titolare del trattamento non ha individuato elementi particolari, sia per quanto riguarda gli interessati sia

25 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato"*, cfr. la nota 10.

per quanto riguarda lo stesso titolare, tali da incidere sul livello di impatto della violazione.

4.2.1 Caso n. 09 — Misure in essere e valutazione del rischio

78. In questo caso la violazione non deriva da un'azione deliberata di un dipendente, ma da un errore umano accidentale causato da disattenzione. Questo tipo di violazione può essere evitato o reso meno frequente: a) applicando programmi di formazione, istruzione e sensibilizzazione cosicché i dipendenti acquisiscano una migliore comprensione dell'importanza della protezione dei dati personali; b) riducendo lo scambio di file tramite posta elettronica, e utilizzando invece sistemi dedicati per il trattamento dei dati dei clienti; c) verificando due volte i file prima dell'invio; d) separando il momento della creazione da quello dell'invio di file.

79. La violazione riguarda solo la riservatezza dei dati, e l'integrità e l'accessibilità degli stessi non sono compromesse. La violazione dei dati riguardava solo una ventina di clienti, per cui è contenuto il volume dei dati interessati. Inoltre, non sono coinvolti dati sensibili. Il fatto che il responsabile del trattamento abbia contattato immediatamente il titolare dopo essere venuto a conoscenza della violazione dei dati può essere considerato un fattore di mitigazione del rischio. (Sarebbe da valutare anche l'eventualità che i dati siano stati trasmessi ad altri agenti assicurativi e, in caso di conferma, si dovrebbero adottare misure adeguate.) Grazie alle misure appropriate adottate successivamente alla violazione dei dati, probabilmente quest'ultima non avrà alcun impatto sui diritti e sulle libertà degli interessati.

80. Il basso numero di persone interessate, la rilevazione immediata della violazione e le misure adottate per minimizzarne gli effetti rendono il caso in questione privo di rischi.

4.2.2 Caso n. 09 — Misure di mitigazione e obblighi

81. Vi sono altri elementi di mitigazione del rischio nel caso in esame: l'agente è vincolato al segreto professionale; egli stesso ha segnalato il problema al titolare del trattamento e ha cancellato il file su richiesta. La sensibilizzazione ed eventualmente la previsione di ulteriori misure di controllo dei documenti contenenti dati personali potranno contribuire a evitare il ripetersi di situazioni simili in futuro.

82. Oltre a documentare la violazione a norma dell'articolo 33, paragrafo 5, non sono necessarie altre azioni.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

4.3 Misure organizzative e tecniche per prevenire/attenuare l'impatto delle fonti interne di rischio legate al fattore umano

83. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità di una recidiva analoga.

84. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Attuazione periodica di programmi di formazione, istruzione e sensibilizzazione per i dipendenti sugli obblighi in materia di privacy e sicurezza e sulla rilevazione e la segnalazione di minacce alla sicurezza dei dati personali26. Messa a punto di un programma di sensibilizzazione per ricordare ai dipendenti gli errori

26 Sezione 2) sottosezione i) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

più comuni che portano a violazioni dei dati personali e come evitarli.

- Istituzione di pratiche, procedure e sistemi solidi ed efficaci in materia di protezione dei dati e di tutela della vita privata27.
- Valutazione delle pratiche, delle procedure e dei sistemi in materia di tutela della vita privata per garantirne l'efficacia nel tempo28.
- Elaborazione di adeguate politiche di controllo dell'accesso e obbligo per gli utenti di rispettare le norme.
- Tecniche per forzare l'autenticazione dell'utente quando accede a dati personali sensibili.
- Disabilitazione dell'account aziendale non appena il dipendente lascia l'azienda.
- controllo dei flussi di dati insoliti tra il file server e le postazioni di lavoro dei dipendenti.
- impostazione della sicurezza dell'interfaccia I/O nel BIOS o mediante l'uso di software che controlla l'uso delle interfacce del computer (blocco o sblocco, ad esempio USB/CD/DVD, ecc.).
- revisione delle politiche in materia di accesso dei dipendenti (ad esempio, registrare l'accesso a dati sensibili chiedendo all'utente di inserire una motivazione di ordine aziendale, in modo che sia disponibile per gli audit).
- Disabilitazione dei servizi di cloud aperti.
- Vietare e impedire l'accesso a servizi di posta elettronica aperta noti.
- Disattivazione della funzione *print screen* [stampa schermata] nel sistema operativo (OS).
- Applicazione rigorosa di una politica della “scrivania sgombra” (c.d. *clean desktop*).
- Blocco automatico di tutti i computer dopo un certo periodo di inattività.
- Utilizzo di meccanismi (ad esempio token (wireless) per accedere a/aprire account bloccati) per cambi rapidi di utente in ambienti condivisi.
- Utilizzo di sistemi dedicati per la gestione dei dati personali che prevedano adeguati meccanismi di controllo dell'accesso e siano in grado di prevenire errori umani, come l'invio di comunicazioni al soggetto sbagliato. L'uso di fogli di calcolo e di altri documenti d'ufficio non è adeguato al fine di gestire i dati dei clienti.

5 SMARRIMENTO O FURTO DI DISPOSITIVI O DI DOCUMENTI CARTACEI

85. Un caso frequente è lo smarrimento o il furto di dispositivi portatili. In questi casi, il titolare del trattamento deve prendere in considerazione le circostanze del trattamento, quali le categorie dei dati conservati sul dispositivo, nonché le risorse di supporto, e le misure adottate precedentemente alla violazione per garantire un livello di sicurezza adeguato. Tutti questi elementi incidono sui potenziali impatti della violazione dei dati. La valutazione dei rischi potrebbe risultare difficile, in quanto il dispositivo non è più disponibile.

86. Questo tipo di violazione può essere classificato in tutti i casi come violazione della riservatezza. Tuttavia, se non esiste un backup per il database sottratto, può configurarsi anche una violazione della disponibilità e dell'integrità.

87. Gli scenari descritti di seguito illustrano in che modo le circostanze di cui sopra determinano la probabilità e la gravità della violazione dei dati.

5.1 Caso n. 10: Furto di supporti sui quali sono memorizzati dati personali cifrati

A seguito di un’effrazione compiuta in un asilo, sono stati rubati due tablet. Nei tablet era installata un'app contenente dati personali sui bambini che frequentano l’asilo: nome, data di nascita, dati personali relativi alle attività educative. Sia i tablet cifrati, che erano spenti al momento dell’effrazione, sia l'app erano protetti da una password robusta. Per il titolare era prontamente ed efficacemente disponibile il back-up. Subito

27 Sezione 2) sottosezione ii) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

28 Sezione 2) sottosezione iii) della risoluzione per affrontare il ruolo dell'errore umano nelle violazioni dei dati personali.

dopo essere venuto a conoscenza dell'effrazione, l'asilo ha inviato un comando a distanza per rimuovere il contenuto dei tablet.

5.1.1 Caso n. 10 — Misure in essere e valutazione del rischio

88. In questo caso particolare, il titolare del trattamento ha adottato misure adeguate per prevenire e mitigare gli effetti di una potenziale violazione dei dati utilizzando la cifratura dei dispositivi, introducendo un'adeguata protezione delle password e garantendo il back-up dei dati conservati sui tablet. (Un elenco delle misure consigliate figura nella sezione 5.7).

89. Dopo essere venuto a conoscenza di una violazione, il titolare del trattamento dovrebbe valutare la fonte di rischio, i sistemi a supporto del trattamento dei dati, il tipo di dati personali coinvolti e gli impatti potenziali della violazione sulle persone interessate. La violazione dei dati sopra descritta avrebbe riguardato la riservatezza, la disponibilità e l'integrità dei dati; tuttavia, grazie alle idonee misure adottate dal titolare precedentemente e successivamente alla violazione dei dati, nessuna di tali compromissioni si è verificata.

5.1.2 Caso n. 10 — Misure di mitigazione e obblighi

90. La riservatezza dei dati personali sui dispositivi non è stata compromessa grazie alla protezione delle password robuste sia sui tablet che sulle app. I tablet sono stati configurati in modo tale che la l'impostazione di una password comporti la cifratura dei dati nel dispositivo. A ciò si aggiunga il tentativo del titolare di cancellare da remoto tutte le informazioni nei tablet rubati.

91. Grazie alle misure adottate, anche la riservatezza dei dati non è stata compromessa. Inoltre, il backup garantiva la costante disponibilità dei dati personali, pertanto non si sarebbe potuto verificare alcun potenziale impatto negativo.

92. Ne deriva l'improbabilità che la violazione dei dati sopra descritta comporti un rischio per i diritti e le libertà degli interessati, pertanto non occorre alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione di questo tipo deve essere documentata, a norma dell'articolo 33, paragrafo 5.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	**X**

5.2 Caso n. 11: Furto di supporti sui quali sono memorizzati dati personali non cifrati

Il computer portatile di un dipendente di una società di servizi è stato rubato. Il notebook rubato conteneva nomi, cognomi, sesso, indirizzi e data di nascita di oltre 100.000 clienti. A causa dell'indisponibilità del dispositivo rubato non è stato possibile individuare se fossero interessate anche altre categorie di dati personali. L'accesso al disco rigido del notebook non era protetto da alcuna password. È possibile ripristinare i dati personali attraverso i backup giornalieri disponibili.

5.2.1 Caso n. 11 — Misure in essere e valutazione del rischio

93. Poiché il titolare del trattamento non ha adottato alcuna misura di sicurezza, i dati personali memorizzati nel notebook rubato erano facilmente accessibili all'autore del furto o a qualsiasi altra persona che successivamente entrasse in possesso del dispositivo.

94. Questa violazione riguarda la riservatezza dei dati conservati sul dispositivo rubato.

95. In questo caso il notebook contenente i dati personali era vulnerabile in quanto non disponeva di alcuna password di protezione né di cifratura. La mancanza di misure di sicurezza di base aumenta il livello di rischio per gli interessati. Un'ulteriore criticità è rappresentata dall'identificazione degli interessati, il che aumenta anche la gravità della violazione. Il numero considerevole di persone interessate comporta un incremento del

rischio; tuttavia, nella violazione non sono coinvolte categorie particolari di dati personali.

96. Nel corso della valutazione del rischio29, il titolare del trattamento dovrebbe prendere in considerazione le potenziali conseguenze e gli effetti negativi della violazione della riservatezza. A causa della violazione, gli interessati possono subire furti di identità sulla base dei dati disponibili nel notebook sottratto, per cui il rischio è da ritenersi elevato.

5.2.2 Caso n. 11 — Misure di mitigazione e obblighi

97. La cifratura del dispositivo e l'uso della protezione di una password robusta del database memorizzato nel dispositivo avrebbero potuto impedire che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati.

98. Alla luce di tali circostanze, è necessaria la notifica all'autorità di controllo competente nonché la comunicazione agli interessati.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

5.3 CASO n. 12 – FURTO DI FASCICOLI CARTACEI CONTENENTI DATI SENSIBILI

Un registro cartaceo è stato rubato da un centro per la riabilitazione dalle tossicodipendenze. Il registro conteneva dati identificativi e sanitari di base relativi ai pazienti del centro. I dati erano memorizzati solo sul supporto cartaceo e i medici che trattavano i pazienti non dispongono di un backup. Il registro non era conservato in un cassetto chiuso a chiave né in una stanza chiusa a chiave; il titolare non aveva previsto politiche per il controllo degli accessi né altre misure a protezione della documentazione cartacea.

5.3.1 Caso n. 12 — Misure in essere e valutazione del rischio

99. Poiché il titolare del trattamento dei dati non ha adottato alcuna misura di sicurezza, i dati personali conservati nel registro erano facilmente accessibili alla persona che lo ha trovato. Inoltre, la natura dei dati personali conservati nel registro rende la mancanza di un backup un fattore di rischio molto grave.

100. Questo caso esemplifica una violazione dei dati ad alto rischio. A causa della mancanza di adeguate precauzioni a, sono andati perduti dati sanitari sensibili a norma dell'articolo 9, paragrafo 1, del GDPR. Poiché in questo caso si trattava di una categoria particolare di dati personali, i rischi potenziali per gli interessati sono maggiori, e tale circostanza deve essere tenuta in considerazione anche dal titolare del trattamento nell'effettuare la valutazione del rischio30.

101. La violazione riguarda la riservatezza, la disponibilità e l'integrità dei dati personali in questione. La violazione compromette la segretezza del rapporto medico-paziente, e terzi non autorizzati possono accedere alle informazioni sanitarie riguardanti i pazienti, il che può avere gravi ripercussioni sulla loro vita. La violazione della disponibilità può anche compromettere la continuità delle cure prestate. Non potendosi escludere la modifica/cancellazione di parti del contenuto del registro, risulta compromessa anche l'integrità dei dati personali.

5.3.2 Caso n. 12 — Misure di mitigazione e obblighi

102. In fase di valutazione delle misure di salvaguardia dovrebbe essere presa in considerazione anche la natura del supporto utilizzato. Poiché il registro dei pazienti era un documento fisico, la sua protezione avrebbe dovuto essere organizzata in modo diverso rispetto a un dispositivo elettronico. La pseudonimizzazione dei nomi dei pazienti, la conservazione del registro in un locale protetto e in un cassetto o una stanza chiusi a

29 Per indicazioni sulle operazioni *di trattamento "che possono comportare un rischio elevato* ", cfr. la nota 10.
30 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

chiave, e un adeguato controllo degli accessi che prevedesse l'autenticazione al momento dell'accesso avrebbero potuto impedire la violazione dei dati.

103. La violazione dei dati di cui sopra può avere gravi ripercussioni sugli interessati; di conseguenza, la notifica dell'autorità di controllo e la comunicazione della violazione agli interessati sono obbligatorie.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

5.4 Misure organizzative e tecniche per prevenire/attenuare le conseguenze della perdita o del furto di dispositivi

104. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre la probabilità del ripetersi di incidenti analoghi.

105. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione)

- Attivare sistemi di cifratura del dispositivo (come BitLocker, Veracript o DM-Crypt).
- Utilizzare un codice di accesso/password su tutti i dispositivi. Cifrare tutti i dispositivi elettronici mobili prevedendo l'inserimento di una password complessa per la decifratura.
- Utilizzare l'autenticazione a più fattori.
- Attivare le funzionalità dei dispositivi ad alta mobilità che ne consentono la localizzazione in caso di perdita o smarrimento.
- Utilizzare software/app e localizzazione MDM (Mobile Devices Management). Utilizzare filtri antiriflesso. Chiudere tutti i dispositivi incustoditi.
- Se possibile e opportuno per il trattamento dei dati in questione, salvare i dati personali non su un dispositivo mobile, ma su un server centrale di back-end.
- Se la postazione di lavoro è collegata alla LAN aziendale, eseguire un backup automatico dalle cartelle di lavoro, a condizione che sia ineludibile che i dati personali siano ivi conservati.
- Utilizzare una VPN sicura (ad esempio, che richieda un secondo fattore di autenticazione separato per stabilire una connessione sicura) per collegare i dispositivi mobili ai server back-end.
- Fornire dispositivi di blocco fisico ai dipendenti per consentire loro di mettere fisicamente in sicurezza i dispositivi mobili che utilizzano quando rimangono incustoditi.
- Corretta regolamentazione dell'uso del dispositivo al di fuori dell'azienda.
- Corretta regolamentazione dell'uso dei dispositivi all'interno dell'azienda.
- Utilizzare software/app MDM (Mobile Devices Management) e attivare la funzione wipe da remoto.
- Utilizzare una gestione centralizzata dei dispositivi con diritti minimi per l'installazione di software da parte degli utenti finali.
- Installare controlli di accesso fisico.
- Evitare di conservare informazioni sensibili in dispositivi mobili o dischi rigidi. Se è necessario accedere al sistema interno dell'impresa, si dovrebbero utilizzare canali sicuri come indicato in precedenza.

6 ERRATO INVIO DI CORRISPONDENZA

106. Anche in questo caso la fonte di rischio è un errore umano interno, ma nessun atto doloso ha portato alla violazione. È il risultato di una disattenzione. Ben poco può fare il titolare del trattamento una volta che la violazione si sia verificata, pertanto la prevenzione in questi casi è ancora più importante.

6.1 Caso n. 13: Errore nella corrispondenza postale

Due ordini per l'acquisto di calzature sono stati evasi da una società di vendita al dettaglio. A causa di un errore umano, è stata fatta confusione con le due fatture per cui sia i prodotti che le relative fatture sono stati inviati alla persona sbagliata. Ciò significa che i due clienti hanno ricevuto gli ordini l'uno dell'altro, comprese le fatture contenenti i dati personali. Dopo essere venuto a conoscenza della violazione, il titolare del trattamento ha richiamato gli ordini e li ha inviati ai destinatari corretti.

6.1.1 Caso n. 13 — Misure in essere e valutazione del rischio

107. Le fatture contenevano i dati personali necessari per la consegna (nome, indirizzo, oltre all'articolo acquistato e il suo prezzo). È importante individuare in primo luogo come abbia potuto verificarsi l'errore umano e, se del caso, come avrebbe potuto essere evitato. Nel caso specifico, il rischio è basso, poiché non sono state coinvolte categorie particolari di dati personali o altri dati il cui abuso potrebbe avere effetti negativi rilevanti, la violazione non consegue a un errore sistemico da parte del titolare del trattamento e sono interessate solo due persone. Non sono stati rilevati effetti negativi sugli interessati.

6.1.2 Caso n. 13 — Misure di mitigazione e obblighi

108. Il titolare del trattamento dovrebbe prevedere la restituzione gratuita degli articoli e delle relative fatture, nonché chiedere ai destinatari errati di distruggere/cancellare tutte le eventuali copie delle fatture contenenti i dati personali dell'altro destinatario.

109. Anche se la violazione non comporta di per sé un rischio elevato per i diritti e le libertà delle persone interessate e, di conseguenza, la comunicazione agli interessati non è richiesta ai sensi dell'articolo 34 del GDPR, tale comunicazione di fatto è inevitabile in quanto è necessaria la cooperazione degli interessati per la mitigazione del rischio.

Azioni necessarie sulla base dei rischi individuati		
Documentazione	Notifica all'autorità	Comunicazione agli interessati
✓	X	X

6.2 Caso n. 14: Dati personali altamente riservati inviati erroneamente per posta elettronica

Il dipartimento risorse umane di una pubblica amministrazione ha inviato un messaggio di posta elettronica — sulle attività formative previste — alle persone registrate nel sistema come in cerca di occupazione. Per errore, all'e-mail è stato allegato un documento contenente tutti i dati personali di tali soggetti (nome, indirizzo e-mail, indirizzo postale, numero di previdenza sociale). Gli interessati coinvolti sono oltre 60.000. Successivamente, l'Ufficio ha contattato tutti i destinatari chiedendo loro di cancellare il messaggio precedente e di non utilizzare le informazioni in esso contenute.

6.2.1 Caso n. 14 — Misure in essere e valutazione del rischio

110. Per l'invio di messaggi di questo genere avrebbero dovuto essere applicate regole più rigorose. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

111. Il numero di persone interessate è considerevole e il coinvolgimento del loro numero di previdenza sociale, insieme ad altri dati personali più basilari, aumenta ulteriormente il rischio, che può essere classificato come elevato31. Il titolare non può implementare misure tese a contenere l'eventuale diffusione dei dati da parte di uno qualsiasi dei destinatari.

6.2.2 Caso n. 14 — Misure di mitigazione e obblighi

112. Come indicato in precedenza, sono pochi gli strumenti utili a mitigare efficacemente i rischi di una violazione analoga. Sebbene il titolare del trattamento abbia chiesto la cancellazione del messaggio, non può costringere

31 Per indicazioni sulle operazioni di trattamento *"che possono comportare un rischio elevato* ", cfr. la nota 10.

i destinatari a farlo e, di conseguenza, non può essere certo che essi adempiano a quanto richiesto.

113. In un caso del genere non dovrebbero esservi dubbi sulla necessità di tutte e tre le azioni indicate di seguito.

Azioni necessarie sulla base dei rischi individuati		
Documentazione	Notifica all'autorità	Comunicazione agli interessati
✓	✓	✓

6.3 Caso n. 15: Dati personali inviati per errore tramite posta elettronica

Un elenco dei partecipanti a un corso di inglese giuridico tenuto presso un albergo e della durata di 5 giorni è inviato per errore a 15 partecipanti a un precedente e analogo corso anziché all'albergo. L'elenco contiene nomi, indirizzi di posta elettronica e preferenze alimentari dei 15 partecipanti. Solo due partecipanti hanno indicato le loro preferenze alimentari, dichiarando di essere intolleranti al lattosio. Nessuno dei partecipanti ha un'identità protetta. Il titolare del trattamento scopre l'errore subito dopo l'invio dell'elenco e ne informa i destinatari chiedendo loro di cancellare l'elenco.

6.3.1 Caso n. 15 — Misure in essere e valutazione del rischio

114. Avrebbero dovuto essere applicate regole rigorose per l'invio di messaggi contenenti dati personali. Occorre prendere in considerazione l'introduzione di meccanismi di controllo supplementari.

115. I rischi derivanti dalla natura, dalla sensibilità, dal volume e dal contesto dei dati personali sono bassi. I dati personali comprendono dati sensibili sulle preferenze alimentari di due dei partecipanti. Anche se l' informazione relativa all'intolleranza al lattosio è un dato sanitario, il rischio che tali dati siano utilizzati in modo dannoso dovrebbe essere considerato relativamente basso. Mentre nel caso di dati relativi alla salute si presume solitamente che la violazione possa comportare un rischio elevato per l'interessato32, nel caso di specie non è possibile individuare il rischio che la violazione comporti danni fisici, materiali o immateriali all'interessato a causa della divulgazione non autorizzata di informazioni sull'intolleranza al lattosio. Contrariamente ad altre preferenze alimentari, l'intolleranza al lattosio non può di norma essere collegata a convinzioni religiose o filosofiche. Anche la quantità di dati violati e il numero di interessati coinvolti sono molto bassi.

6.3.2 Caso n. 15 — Misure di mitigazione e obblighi

116. In sintesi, si può affermare che la violazione non ha avuto effetti significativi sugli interessati. Il fatto che il titolare del trattamento abbia contattato immediatamente i destinatari dopo essere venuto a conoscenza dell'errore può essere considerato un fattore di mitigazione.

117. Se un messaggio di posta elettronica è inviato a un destinatario errato/non autorizzato, si raccomanda al titolare del trattamento di inviare un'e-mail di follow-up, in copia nascosta, ai destinatari non corretti, scusandosi per l'errore, invitando a cancellare l'e-mail inviata erroneamente e informando i destinatari che non hanno il diritto di utilizzare ulteriormente gli indirizzi di posta elettronica loro comunicati.

118. Alla luce delle circostanze descritte, era improbabile che la violazione dei dati comportasse un rischio per i diritti e le libertà degli interessati, pertanto non si è resa necessaria alcuna notifica all'autorità di controllo o agli interessati. Tuttavia, anche una violazione dei dati di questo tipo deve essere documentata a norma dell'articolo 33, paragrafo 5.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	X	X

6.4 Caso n. 16: Errore nell'invio di corrispondenza postale

Un gruppo assicurativo offre assicurazioni auto. A tal fine, invia per posta aggiornamenti periodici sulle

32 Cfr. le Linee-guida WP 250, pag. 23.

prestazioni assicurative. Oltre al nome e all'indirizzo dell'assicurato, la lettera contiene la targa del veicolo in chiaro, gli importi del premio assicurativo per l'anno in corso e per quello successivo, il chilometraggio annuo approssimativo e la data di nascita dell'assicurato. Non sono inclusi dati sanitari ai sensi dell'articolo 9 del GDPR, né dati relativi ai pagamenti (coordinate bancarie) o dati economici e finanziari.

Le lettere sono imbustate automaticamente. A causa di un errore meccanico, due lettere destinate a contraenti diversi sono inserite in una stessa busta e inviate per posta ordinaria a uno dei due. Il contraente apre la lettera a casa e legge la lettera a lui correttamente indirizzata nonché quella erroneamente consegnata e indirizzata a un diverso contraente.

6.4.1 Caso n. 16 — Misure in essere e valutazione del rischio

119. La lettera erroneamente consegnata contiene il nome, l'indirizzo, la data di nascita, il numero di immatricolazione in chiaro del veicolo e la classe attribuita per il premio assicurativo dell'anno in corso e dell'anno successivo. Gli effetti sulla persona interessata devono ritenersi di media entità, in quanto sono comunicate a una persona non autorizzata informazioni non accessibili al pubblico, quali la data di nascita o i numeri di immatricolazione in chiaro dei veicoli, nonché i dettagli relativi all'aumento del premio assicurativo. La probabilità di un uso improprio di questi dati è da valutarsi tra bassa e media. Tuttavia, mentre molti destinatari probabilmente cestineranno la lettera ricevuta per errore, non si può escludere del tutto che, in determinati casi, la lettera sia pubblicata sui social network o che l'assicurato sia contattato.

6.4.2 Caso n. 16 — Misure di mitigazione e obblighi

120. Il titolare del trattamento deve chiedere che, a sue spese, gli sia reinviato il documento originale. Inoltre, dovrebbe informare il destinatario errato del fatto che non può utilizzare in modo improprio le informazioni cui ha avuto accesso.

121. Probabilmente non sarà mai possibile prevenire del tutto errori di spedizione in una postalizzazione massiva effettuata in forma completamente automatizzata. Tuttavia, se tali errori avvengono con una certa frequenza, è necessario verificare se i dispositivi di imbustamento siano impostate e sottoposte a manutenzione in modo corretto o se vi siano altri problemi di natura sistemica alla base della violazione.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	X

6.5 Misure organizzative e tecniche per prevenire/attenuare gli effetti di un'errata postalizzazione

122. L'applicazione congiunta delle misure indicate di seguito, in funzione delle caratteristiche specifiche del caso, dovrebbe contribuire a ridurre le probabilità del ripetersi di eventi analoghi.

123. Misure consigliate:

(L'elenco delle seguenti misure non è da considerarsi assolutamente esaustivo né tassativo. L'obiettivo è piuttosto quello di fornire suggerimenti di prevenzione e possibili soluzioni. Ogni attività di trattamento è diversa, pertanto il titolare del trattamento dovrebbe decidere quali misure siano più idonee nella specifica situazione.)

- Definizione di standard specifici — che non lascino spazi all'interpretazione — per l'invio di lettere/e-mail.
- Formazione adeguata del personale sull'invio di lettere/e-mail.
- Quando si inviano messaggi di posta elettronica a più destinatari, questi sono inseriti nel campo "Ccn" per impostazione predefinita.
- Necessità di una conferma supplementare prima di inviare messaggi di posta elettronica a più destinatari senza inserirli nel campo "Ccn".
- Applicazione del principio del doppio livello di controllo.

- Inserimento automatico anziché manuale dei recapiti, con dati estratti da una banca dati disponibile e aggiornata; il sistema di inserimento automatico dovrebbe essere riesaminato periodicamente per verificare eventuali errori nascosti e impostazioni errate.
- Applicazione della funzionalità di invio ritardato (che consente di cancellare/modificare il messaggio entro un determinato periodo di tempo dopo aver premuto il pulsante "Invio").
- Disabilitazione del completamento automatico quando si digitano indirizzi e-mail.
- Sessioni di sensibilizzazione sugli errori più comuni che generano una violazione dei dati personali.
- Sessioni di formazione e manuali sulla gestione di incidenti che generano una violazione dei dati personali, compresa l'indicazione dei soggetti da informare (coinvolgimento del responsabile della protezione dei dati).

7 ALTRI CASI — INGEGNERIA SOCIALE (*Social Engineering*)

7.1 Caso n. 17: Furto d'identità

Il centro di contatto di un'impresa di telecomunicazioni riceve una telefonata da una persona che si presenta come cliente. Il presunto cliente chiede alla società di modificare l'indirizzo e-mail al quale inviare le informazioni di fatturazione. L'operatore convalida l'identità del cliente chiedendo alcuni dati personali, quali definiti dalle procedure dell'impresa. Il chiamante indica correttamente il codice fiscale e l'indirizzo postale del cliente (perché ha avuto accesso a tali informazioni). Dopo la convalida, l'operatore effettua la modifica richiesta e, successivamente, le informazioni di fatturazione sono inviate al nuovo indirizzo e-mail. La procedura non prevede alcuna notifica al precedente contatto e-mail. Il mese successivo il cliente legittimo contatta la società, chiedendo perché non riceva la fattura al suo indirizzo di posta elettronica, e nega qualsiasi richiesta da parte sua di modificare l'email di contatto. La società si rende conto che le informazioni sono state inviate a un utente illegittimo e annulla la modifica.

7.1.1 Caso n. 17 — Valutazione del rischio, misure di mitigazione e obblighi

124. Questo caso ben esemplifica l'importanza delle misure preventive. La violazione presenta un elevato livello di rischio33, in quanto i dati di fatturazione possono fornire informazioni sulla vita privata dell'interessato (ad esempio, abitudini, contatti) e potrebbero causare danni materiali (ad esempio stalking, rischio per l'integrità fisica). I dati personali ottenuti durante l'attacco possono essere utilizzati anche per facilitare l'acquisizione di account all'interno della specifica organizzazione o per testare ulteriori misure di autenticazione in altre organizzazioni. Tenuto conto di tali rischi, la soglia di "adeguatezza" delle misure di autenticazione dovrebbe essere fissata a un livello elevato in rapporto alla natura dei dati personali cui è possibile accedere una volta effettuata l'autenticazione.

125. Di conseguenza, sono necessarie sia una notifica all'autorità di controllo sia una comunicazione all'interessato da parte del titolare del trattamento.

126. È chiaro che il processo di convalida preventiva del cliente necessita di perfezionamenti, alla luce di questo caso. I metodi utilizzati per l'autenticazione non erano sufficienti. La parte malintenzionata è riuscita a fingere di essere l'utente legittimo utilizzando informazioni pubblicamente disponibili e altre informazioni cui aveva altrimenti accesso.5

127. Non si raccomanda l'uso di questa forma di autenticazione statica basata su elementi di conoscenza (in cui la risposta non cambia e non ci sono informazioni "segrete", come invece sarebbe nel caso di una password).

128. L'organizzazione dovrebbe invece utilizzare una forma di autenticazione altamente affidabile quanto alla dimostrazione che l'utente autenticato sia realmente chi afferma di essere, e non altri. L'introduzione di un metodo di autenticazione a più fattori fuori banda risolverebbe il problema, ad esempio per verificare

eventuali richieste di variazioni, attraverso l'invio di una richiesta di conferma al precedente indirizzo di contatto; oppure aggiungendo ulteriori domande di controllo e chiedendo informazioni presenti solo sulle fatture precedenti. Spetta al titolare del trattamento decidere quali misure introdurre, in quanto conosce meglio di chiunque altro i dettagli e le esigenze della sua operatività interna.

Azioni necessarie sulla base dei rischi individuati		
Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
✓	✓	✓

[33] Per indicazioni *sui trattamenti "che possono comportare un rischio elevato"*, cfr. la precedente nota 10.

7.2 Caso n. 18: Esfiltrazione di e-mail

Una catena di ipermercati ha rilevato, 3 mesi dopo la configurazione, che alcuni account di posta elettronica erano stati modificati attraverso la creazione di regole per cui ogni e-mail contenente determinate espressioni (ad esempio "fattura", "pagamento", "bonifico bancario", "autenticazione della carta di credito", "coordinate bancarie") veniva trasferita in una cartella non utilizzata e trasmessa anche a un indirizzo di posta elettronica esterno. Inoltre, a quella data, era già stato commesso un attacco di ingegneria sociale, vale a dire che l'attaccante, che fingeva di essere un fornitore, aveva modificato le coordinate bancarie di tale fornitore sostituendovi le proprie. Infine, a quella data, erano state inviate diverse fatture false che includevano i nuovi dati relativi alle coordinate bancarie. Il sistema di monitoraggio della piattaforma di posta elettronica aveva segnalato, in ultima istanza, un problema sulle cartelle. La società non è stata in grado di individuare in che modo l'attaccante fosse riuscito ad accedere agli account di posta elettronica, ma ha ritenuto che attraverso un'email infetta fosse avvenuto l'accesso al gruppo di utenti incaricati dei pagamenti.

A seguito della trasmissione di e-mail contenenti determinate parole-chiave, l'attaccante ha ricevuto informazioni su 99 dipendenti: nome e salario riferito a uno specifico mese per 89 soggetti; nome, stato civile, numero di figli, retribuzione, ore di lavoro e altre informazioni sulla retribuzione di 10 dipendenti il cui contratto era terminato. Il titolare ha comunicato la violazione soltanto ai 10 dipendenti appartenenti a quest'ultimo gruppo.

7.2.1 Caso n. 18 — Valutazione del rischio, misure di mitigazione e obblighi

129. Anche se l'attaccante non mirava probabilmente a raccogliere dati personali, la violazione potrebbe comportare sia un danno materiale (ad esempio, perdite finanziarie) che un danno immateriale (ad esempio furto o usurpazione di identità), e i dati potrebbero essere utilizzati per facilitare altri attacchi (ad esempio phishing); pertanto, la violazione potrebbe comportare un rischio elevato per i diritti e le libertà delle persone fisiche e dovrebbe essere comunicata a tutti i 99 dipendenti e non solo ai 10 dei quali sono state divulgate le retribuzioni.

130. Una volta venuto a conoscenza della violazione, il titolare del trattamento ha forzato la modifica della password per gli account compromessi, ha bloccato l'invio di e-mail all'account dell'attaccante, ha informato il fornitore del servizio di posta elettronica utilizzato dall'autore dell'attacco in merito alle azioni compiute da quest'ultimo, ha rimosso le regole stabilite dall'attaccante e perfezionato le segnalazioni del sistema di monitoraggio così da generare una segnalazione non appena venga creata una regola automatica. In alternativa, il titolare del trattamento potrebbe eliminare il diritto degli utenti di stabilire regole sull'inoltro dei messaggi di posta elettronica, prevedendo la necessità di un intervento del team del servizio informatico su specifica richiesta, oppure potrebbe introdurre una politica in base alla quale gli utenti dovrebbero verificare e comunicare le regole stabilite sui loro account una volta alla settimana o con maggiore frequenza, nei settori che trattano dati finanziari.

131. Il fatto che una violazione abbia potuto verificarsi e sfuggire al rilevamento per un periodo così prolungato, e la circostanza per cui, se la violazione fosse proseguita, le tecniche di ingegneria sociale avrebbero consentito di modificare un volume di dati ancora più consistente, evidenziano notevoli criticità nel sistema di sicurezza informatica del titolare del trattamento. Tali criticità dovrebbero essere affrontate senza indugio, ad esempio rivedendo le procedure automatizzate e le verifiche dei cambiamenti, le misure di rilevazione degli incidenti e di risposta agli incidenti. I titolari del trattamento di dati sensibili, informazioni finanziarie, ecc. hanno maggiori responsabilità nel garantire un'adeguata sicurezza dei dati.

Azioni necessarie sulla base dei rischi individuati			
	Documentazione interna	Notifica all'autorità di controllo	Comunicazione agli interessati
	✓	✓	✓

Ministero dell'Istruzione

Linee guida per la gestione operativa dei *data breach*

Agosto 2021

Sommario

PREMESSA

Il regolamento generale sulla protezione dei dati (in seguito "Regolamento") introduce l'obbligo di notificare una violazione dei dati personali all'autorità di controllo nazionale competente (oppure, in caso di violazione transfrontaliera, all'autorità capofila) e, in alcuni casi, di comunicare la violazione alle singole persone fisiche i cui dati personali sono stati interessati dalla violazione.

Il Regolamento rende la notifica obbligatoria per tutti i titolari del trattamento a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche.

Il Gruppo di lavoro ex articolo 29[1] ritiene che il nuovo obbligo di notifica presenti una serie di vantaggi. All'atto della notifica all'autorità di controllo, il Titolare può ottenere consulenza sull'eventuale necessità di informare le persone fisiche interessate. L'autorità di controllo, infatti, può ordinare al Titolare di informare le persone fisiche interessate dalla violazione. La comunicazione dell'avvenuta violazione alle persone fisiche interessate consente al Titolare di fornire loro informazioni sui rischi derivanti e sui provvedimenti che esse possono prendere per proteggersi dalle potenziali conseguenze della violazione stessa. Allo stesso tempo, va evidenziato come la mancata segnalazione di una violazione a una persona fisica o all'autorità di controllo possa comportare l'irrogazione di una sanzione al Titolare ai sensi dell'articolo 83 del Regolamento.

Il Regolamento in linea generale prevede che, mediante misure tecniche e organizzative adeguate, i dati personali siano trattati in maniera da garantire una loro adeguata sicurezza, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Pertanto, un aspetto fondamentale di qualsiasi politica di sicurezza dei dati è la capacità, ove possibile, di prevenire una violazione e, laddove essa si verifichi ciò nonostante, di reagire tempestivamente.

Definizione di violazione dei dati personali (*data breach*)

La violazione di dati personali è un particolare tipo di incidente di sicurezza.

Il dato personale oggetto della violazione può essere presente su archivi ed avere una rappresentazione sia digitale che cartacea[2].

Per porre rimedio a una violazione dei dati personali occorre innanzitutto che il Titolare sia in grado di riconoscerla. All'articolo 4, punto 12, il Regolamento definisce la "violazione dei dati personali" 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".

1 Il cosiddetto Gruppo di lavoro ex articolo 29 è un organismo consultivo e indipendente, istituito dall'articolo 29 della Direttiva 95/46 del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il Gruppo di lavoro ha trattato questioni relative alla protezione della vita privata e dei dati personali fino al 25 maggio 2018 (entrata in vigore del Regolamento). Con il nuovo Regolamento europeo il Gruppo di lavoro è stato sostituito dall'organismo europeo "European Data Protection Board".

2 Per data breach su archivi digitali s'intende qualsiasi violazione di dato personale presente sui componenti del sistema informatico. Ad esempio, il data breach digitale può verificarsi su dati presenti su piattaforme, sistemi in cloud, su dispositivi e supporti digitali (es. USB key, CD, DVD, …), nonché sulle postazioni di lavoro fisse e mobili.

Il significato di "distruzione" dei dati personali è chiaro: si ha distruzione dei dati quando gli stessi non esistono più o non esistono più in una forma che sia di qualche utilità per il Titolare. Anche il concetto di "danno" è evidente: si verifica un danno quando i dati personali sono stati modificati, corrotti o non sono più completi. Con "perdita" dei dati personali si intende il caso in cui i dati esistono, ma il Titolare può averne perso il controllo o l'accesso, oppure non averli più in possesso. Infine, un trattamento non autorizzato o illecito può includere la divulgazione di dati personali a (o l'accesso da parte di) destinatari non autorizzati a riceverli (o ad accedere a) oppure qualsiasi altra forma di trattamento in violazione del Regolamento.

Tipi di violazioni dei dati personali

Le violazioni di dati personali possono essere classificate in base a tre diverse tipologie connesse alla sicurezza delle informazioni:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale di dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

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.

Mentre stabilire se vi sia stata una violazione della riservatezza o dell'integrità è semplice, può essere meno ovvio determinare se vi è stata una violazione della disponibilità. Una violazione sarà sempre considerata una violazione della disponibilità se si è verificata una perdita o una distruzione permanente dei dati personali.

Ci si potrebbe chiedere se una perdita temporanea della disponibilità dei dati personali costituisca una violazione e, in tal caso, se si tratti di una violazione che richiede la notifica. L'articolo 32 del Regolamento ("Sicurezza del trattamento") spiega che nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".

Di conseguenza, un incidente di sicurezza che determina l'indisponibilità di dati personali per un certo periodo di tempo costituisce una violazione se la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche. Va precisato che l'indisponibilità dei dati personali dovuta allo svolgimento di un intervento di manutenzione programmata del sistema non costituisce una "violazione della sicurezza" ai sensi dell'articolo 4, punto 12, del Regolamento.

Come nel caso della perdita o distruzione permanente dei dati personali (o comunque di qualsiasi altro tipo di violazione), una violazione che implichi la perdita temporanea di disponibilità dovrebbe essere documentata in conformità all'articolo 33, paragrafo 5 del Regolamento. Tuttavia, a seconda delle circostanze in cui si verifica, la violazione può richiedere o meno la notifica all'autorità di controllo e la comunicazione alle persone fisiche coinvolte. Il Titolare dovrà

valutare la probabilità e la gravità dell'impatto dell'indisponibilità dei dati personali sui diritti e sulle libertà delle persone fisiche. Conformemente all'articolo 33 del Regolamento, il Titolare dovrà effettuare la notifica solo nel caso in cui la violazione dei dati personali comporta un probabile rischio per i diritti e le libertà delle persone fisiche. Questo aspetto dovrà essere valutato caso per caso.

Obblighi del responsabile del trattamento[3]

Sebbene il Titolare conservi la responsabilità generale per la protezione dei dati personali, il Responsabile del trattamento svolge un ruolo importante nel consentire al Titolare di adempiere ai propri obblighi, segnatamente in materia di notifica delle violazioni. L'articolo 28, paragrafo 3, del Regolamento dispone che il ruolo del Responsabile del trattamento è disciplinato da un contratto o da un altro atto giuridico e precisa, alla lettera f), che il contratto o altro atto giuridico deve prevedere che il Responsabile del trattamento "assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile del trattamento".

L'articolo 33, paragrafo 2, del Regolamento chiarisce che, se il Titolare ricorre a un Responsabile del trattamento e quest'ultimo viene a conoscenza di una violazione dei dati personali che sta trattando per conto del Titolare, il Responsabile del trattamento deve notificarla al Titolare "senza ingiustificato ritardo". Va evidenziato che il Responsabile del trattamento non deve valutare la probabilità di rischio sui diritti e le libertà delle persone fisiche derivante dalla violazione prima di notificarla al Titolare; spetta, infatti, a quest'ultimo effettuare tale valutazione nel momento in cui viene a conoscenza della violazione. Il Responsabile del trattamento deve soltanto stabilire se si è verificata una violazione e notificarla al Titolare.

La notifica al Garante per la protezione dei dati personali

La notifica ha la funzione di consentire all'autorità di controllo di applicare le misure correttive a sua disposizione (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ecc.) previste dall'articolo 58 del Regolamento e di adottare misure di tutela immediate a favore dei soggetti coinvolti. Elemento centrale della procedura di notificazione è la sua **tempestività**.

In generale, è necessario notificare **al Garante per la protezione dei dati personali, entro le 72 ore, l'avvenuto *data breach***. E' importante che sia dimostrabile il momento dell'asseverazione della violazione, poiché da quel momento decorrono le 72 ore per la notifica. Qualora la notifica al Garante per la protezione dei dati personali non sia effettuata entro 72 ore, dovrà essere corredata dei motivi del ritardo.

Il Garante per la protezione dei dati personali con il provvedimento n.209 del 27 maggio 2021, ha modificato il contenuto e le modalità della notifica della violazione dei dati personali individuati nel precedente provvedimento n. 157 del 30 luglio 2019 prevedendo l'adozione di un'apposita procedura telematica. L'articolo 33 del Regolamento prescrive al soggetto che esercita le funzioni di Titolare (ossia, Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) di documentare qualsiasi violazione dei dati personali, al fine di consentire al Garante per la protezione dei dati personali di verificare il rispetto della norma. Pertanto, tutte

3 Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare.

le generali attività di scoperta e di trattamento dell'incidente devono essere documentate, adeguate, tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Qualora il Titolare non sia in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva del *data breach*, il Regolamento (articolo 33, paragrafo 4) prevede che, le informazioni possano essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Gruppo di lavoro ex articolo 29 chiarisce come il Regolamento consente al Titolare di utilizzare alcune tecniche o modalità che permettono di bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza.

- La prima tecnica è l'utilizzo dell'**"approssimazione"**. Il Titolare che non sia ancora in grado di conoscere con certezza il numero di persone e di dati personali interessati dalla violazione può comunicarne in prima battuta un ammontare approssimativo, provvedendo a specificare il numero esatto a seguito di accertamenti.
- Secondo strumento previsto dal Regolamento è la **"notificazione in fasi"**. In questo caso il Titolare, per la complessità o estensione della violazione, potrebbe non essere in grado di fornire con immediatezza all'autorità tutte le informazioni necessarie, ma dopo una prima e rapida notifica di *allert*, può adempiere agli obblighi di notifica comunicando tutte le informazioni per fasi successive, aggiornando di volta in volta lo stesso Garante sui nuovi riscontri.
- Il Regolamento prevede la possibilità di effettuare una "notifica differita" dopo le 72 ore previste dall'articolo 33 nel caso in cui, ad esempio, si subiscano violazioni ripetute, ravvicinate e di simile natura che interessino un numero elevato di soggetti. Al fine di evitare un aggravio di oneri in capo al Titolare e l'invio dilazionato di un numero elevato di notificazioni tra loro identiche, il Titolare è autorizzato ad eseguire un'unica "notifica aggregata" di tutte le violazioni occorse nel breve periodo di tempo (anche se superi le 72 ore), purché la notifica motivi le ragioni del ritardo.

Se il Titolare omette di notificare una violazione dei dati all'autorità di controllo o agli interessati oppure a entrambi, nonostante siano soddisfatte le prescrizioni di cui agli articoli 33 e/o 34 del Regolamento, l'autorità di controllo dovrà effettuare una scelta e prendere in considerazione tutte le misure correttive a sua disposizione, tra cui l'irrogazione di una sanzione amministrativa pecuniaria appropriata in associazione a una misura correttiva ai sensi dell'articolo 58, paragrafo 2, del Regolamento oppure come sanzione indipendente.

La comunicazione agli interessati

Accanto agli obblighi di notifica al Garante per la protezione dei dati personali, l'articolo 34 del Regolamento prevede in capo ai Titolari un **obbligo di comunicazione** agli interessati, che consenta loro di attivarsi a tutela dei propri interessi.

Come evidenziato dalle Linee guida del Gruppo di lavoro ex art. 29, i due obblighi sono innescati dal superamento di soglie di rischio differenti: è sufficiente un rischio "semplice" per far scattare l'obbligo di notifica, mentre è necessario un rischio "elevato" per attivare quello di comunicazione.

L'adeguatezza di una comunicazione è determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione. Le Linee guida del Gruppo di lavoro ex art. 29, sulla base dell'art. 34 del Regolamento, ricordano che devono sempre essere privilegiate modalità di

comunicazione dirette con i soggetti interessati (quali email, SMS o messaggi diretti). Il messaggio dovrebbe essere comunicato in maniera chiara e trasparente, evitando di inviare le informazioni che potrebbero essere facilmente fraintese dai destinatari. Inoltre, dovrebbe tenere conto di possibili formati alternativi di visualizzazione del messaggio e delle diversità linguistiche dei soggetti riceventi (es: l'utilizzo della lingua madre dei soggetti riceventi rende il messaggio immediatamente comprensibile).

Anche in questo caso, il Regolamento è attento a non gravare i Titolari di oneri eccessivi prevedendo che, nel caso in cui la segnalazione diretta richieda sforzi sproporzionati, questa possa essere effettuata attraverso una comunicazione pubblica. Si sottolinea, però, che anche questo tipo di comunicazione deve mantenere lo stesso grado di efficacia conoscitiva del contatto diretto con l'interessato. Così, mentre può ritenersi adeguata la comunicazione fornita attraverso evidenti *banner* o notifiche disposte sul sito istituzionale, non lo sarà se questa sia limitata all'inserimento della notizia nella rassegna stampa.

La comunicazione, secondo quanto previsto dall'articolo 34 del Regolamento, deve contenere almeno le seguenti informazioni:

- la comunicazione del nome e dei dati di contatto del Responsabile della protezione dei dati previsto dall'articolo 37 del Regolamento o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze della violazione dei dati personali;
- la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali e alla gestione dei possibili effetti negativi.

La comunicazione all'interessato non è richiesta se:

- il Titolare ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- contattare gli interessati richiederebbe uno sforzo sproporzionato, ad esempio nel caso in cui i dati di contatto siano stati persi a causa della violazione o non siano mai stati noti. In tale circostanza, il Titolare deve invece effettuare una comunicazione pubblica o prendere una misura analoga, tramite la quale gli interessati vengano informati in maniera altrettanto efficace.

1. IL PROCESSO DI GESTIONE DEL *DATA BREACH* SU ARCHIVI DIGITALI

1.1 Attori del processo

1.1.1 CSIRT del Ministero dell'Istruzione

La responsabilità di gestire il processo generale degli **incidenti di sicurezza sui sistemi informativi del Ministero dell'Istruzione, di seguito Ministero o MI, gestiti a livello centrale** è affidata allo **CSIRT (Computer Security Incident Response Team) del Ministero**.

Lo CSIRT è una unità di presidio nominata con decreto del Direttore della Direzione generale per i sistemi informativi e la statistica (di seguito DGSIS) ed è costituita da referenti del Ministero che si occupano della sicurezza informatica.

Lo CSIRT ricopre un ruolo fondamentale nel processo del *data breach*, in quanto:

- gestisce il processo degli incidenti di sicurezza;
- elabora rapporti sulla gestione degli incidenti di sicurezza;
- analizza la vulnerabilità sui sistemi, sulle applicazioni e sulle infrastrutture IT;
- rappresenta il contatto operativo con le autorità esterne al Ministero in tema di sicurezza informatica (es. CERT-PA, CNAIPIC) e con gli altri enti afferenti al mondo MI (es. Indire, Invalsi, Cineca, ecc.);
- supporta il Titolare nella notifica del *data breach* asseverato a livello centrale al Garante per la protezione dei dati personali.

1.1.2 Unità di presidio regionale

La responsabilità della gestione degli **incidenti di sicurezza verificatisi sui sistemi informativi gestiti in via autonoma dagli Uffici scolastici regionali** è affidata all'unità di presidio regionale. Ciascun Dirigente preposto all'Ufficio scolastico regionale nomina con decreto il Responsabile e i componenti dell'unità di presidio regionale. L'unità di presidio regionale, qualora lo ritenga opportuno, può essere coadiuvata dallo CSIRT del Ministero nell'attività di analisi e gestione del *data breach.*

1.1.3 Altri attori coinvolti

- **Titolare -** il soggetto che esercita le funzioni di Titolare del trattamento (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) nella struttura i cui dati sono stati oggetto di violazione viene informato del sospetto *data breach*, notifica il *data breach* asseverato al Garante per la protezione dei dati personali e, ove necessario, comunica la violazione agli interessati senza ingiustificato ritardo;
- **Dirigente competente** – segnala il potenziale *data breach* e supporta lo CSIRT o l'unità di presidio regionale, fornendo utili elementi di valutazione;
- **Ufficio di Gabinetto del Ministro** – è informato, nei casi in cui la violazione è di particolare rilevanza in relazione alle attività del Ministero, del *data breach* asseverato e avvia, ove ritenuto necessario, le opportune attività di comunicazione;
- **Responsabile della protezione dei dati** - è costantemente informato a partire dal sospetto di *data breach*.

1.2 Fasi del processo

Il processo prevede tre fasi:

- Acquisizione del potenziale *data breach*;
- Asseverazione del *data breach*;

- Notifica e comunicazione del *data breach*.

Figura 1 – Fasi del processo di *data breach*

1.2.1 Acquisizione del potenziale *data breach*

La fase di "Acquisizione" rappresenta il momento nel quale il Ministero viene a conoscenza del sospetto che un *set* di dati personali sono stati esfiltrati o compromessi.

Nel caso di **incidenti di sicurezza sui sistemi informativi del Ministero gestiti a livello centrale**, si provvede a segnalare immediatamente il sospetto di violazione dati personali allo CSIRT.

Pertanto, i Dirigenti degli Uffici del Ministero, qualora rilevino, nel proprio contesto organizzativo, su segnalazione interna (dipendenti del proprio ufficio) o su segnalazione di terzi, la presenza di una possibile **violazione dei dati personali presenti sui sistemi informativi del Ministero gestiti a livello centrale,** ne danno immediata comunicazione allo CSIRT, tramite la casella di posta elettronica dedicata: CSIRT@istruzione.it, compilando e inviando il modulo allegato (Allegato A: "modello di comunicazione incidente violazione dati personali"). Tale comunicazione va inoltrata per conoscenza alla propria figura di vertice della struttura di riferimento (Capo di Gabinetto, Capo Dipartimento, Direttore Generale), alla DGSIS e al Responsabile della protezione dei dati.

Nel caso in cui l'incidente coinvolga dati personali presenti su **sistemi informativi gestiti in via autonoma dagli Uffici scolastici regionali** del Ministero la segnalazione dovrà essere effettuata dai dirigenti competenti all'unità di presidio regionale, dandone immediata comunicazione anche al Dirigente preposto all'Ufficio scolastico regionale e al Responsabile della protezione dei dati sulla base del modello di cui all' allegato A "modello di comunicazione incidente violazione dati personali". L'unità di presidio regionale valuterà l'opportunità di chiedere il supporto dello CSIRT.

Le segnalazioni da parte dei Responsabili del trattamento, di CERT-PA, di CNAIPIC o di altri enti esterni dovranno essere immediatamente inoltrate dagli uffici competenti allo CSIRT tramite la casella di posta elettronica dedicata: CSIRT@istruzione.it o all'unità di presidio regionale se non riguarda i sistemi informativi del Ministero gestiti a livello centrale.

1.2.2 Asseverazione del *data breach*

Nella fase di asseverazione del *data breach*, lo CSIRT o l'unità di presidio regionale, in collaborazione con la struttura di riferimento che ha segnalato l'incidente, analizza il sospetto incidente al fine di asseverare l'esistenza del *data breach*.

In particolare, lo CSIRT o l'unità di presidio regionale, supportati dal Dirigente del Ministero che ha segnalato l'incidente sia a livello centrale che periferico e dal relativo Referente privacy della struttura di riferimento, approfondiscono e analizzano la fattispecie nel rispetto dei termini previsti dall'articolo 33 del Regolamento, al fine di rilevare:

- la natura dell'eventuale violazione dei dati personali subita (tipologia di incidente, descrizione servizio impattato/banca dati/archivio fisico oggetto di *data breach*, intervallo temporale di riferimento, luogo dell'incidente, ecc.);
- il numero (anche approssimativo) e le categorie degli interessati e i dati personali oggetto di violazione;
- le possibili conseguenze della violazione sui diritti e sulle libertà dell'interessato e la valutazione della probabilità che le stesse si verifichino ai fini dell'eventuale notificazione al Garante per la protezione dei dati personali;
- le misure di sicurezza in essere e applicate ai dati violati;
- le eventuali misure adottate per porre rimedio alla violazione e/o per attenuarne gli effetti negativi.

Al termine dell'analisi, lo CSIRT o l'unità di presidio regionale elabora una scheda di valutazione del *data breach* (Allegato B) in cui indica la causa, lo scenario di emersione, il potenziale impatto, le azioni già compiute e altre informazioni ritenute utili.

In caso di *data breach* asseverato su sistemi informativi del Ministero gestiti a livello centrale, lo CSIRT trasmette la scheda di valutazione del *data breach* (Allegato B) al soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento) nella struttura i cui dati sono stati oggetto di violazione, nonché per conoscenza alla DGSIS, alla Direzione generale competente e, per *data breach* di particolare rilevanza, al Capo di Gabinetto.

In caso di *data breach* asseverato su sistemi informativi gestiti in via autonoma dagli Uffici scolastici regionali del Ministero, l'unità di presidio regionale trasmette la scheda di valutazione del *data breach* (Allegato B) al Dirigente preposto all'Ufficio scolastico regionale e allo CSIRT per le attività di competenza, nonché per conoscenza alla DGSIS e, per *data breach* di particolare rilevanza, al Capo di Gabinetto. Anche in caso di falso positivo, l'unità di presidio regionale trasmette la scheda allo CSIRT.

Lo CSIRT, sia in caso di asseverazione del *data breach* sia in caso di falso positivo, aggiorna il Registro degli incidenti di sicurezza (Allegato C).

1.2.3 Notifica e comunicazione del *data breach*

Entro 72 ore dal momento in cui lo CSIRT o l'unità di presidio regionale assevera la violazione, è necessario procedere alla **notifica del *data breach*** secondo quanto previsto dall'articolo 33 del Regolamento

In caso di violazione asseverata su sistemi informativi del Ministero gestiti a livello centrale, il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento) nella struttura i cui dati sono stati oggetto di violazione notifica il *data breach* al Garante per la protezione dei dati personali, utilizzando l'apposita procedura telematica disponibile al seguente link https://servizi.gpdp.it/databreach/s/ con la quale vengono richieste le informazioni contenute nel Modello - informazioni da fornire per la notifica *data breach* al Garante (Allegato D). La DGSIS supporta il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento) nell'individuazione delle informazioni da comunicare al Garante per la protezione dei dati personali per la notifica del *data breach*.

In caso di violazione asseverata su sistemi informativi gestiti in via autonoma dagli Uffici Scolastici Regionali, il Dirigente preposto all'Ufficio scolastico regionale notifica il *data breach* al Garante per la protezione dei dati personali, utilizzando l'apposita procedura telematica disponibile al seguente link https://servizi.gpdp.it/databreach/s/.

Il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) nella struttura i cui dati sono stati oggetto di violazione, ove necessario (cfr. par. La comunicazione agli interessati), **comunica la violazione** agli interessati senza ingiustificato ritardo utilizzando il modello "Template comunicazione all'interessato" (Allegato E) secondo quanto previsto dall'articolo 34 del Regolamento.

In relazione alla rilevanza del *data breach* possono essere coinvolti, ove necessario:

- **Ufficio di Gabinetto:** pianifica la comunicazione esterna al Ministero coinvolgendo l'Ufficio stampa;
- **CSIRT:** informa CNAIPIC e CERT-PA;
- **DGSIS:** pianifica la comunicazione interna al Ministero tramite l'ufficio competente.

2.PROCESSO DI GESTIONE *DATA BREACH* RELATIVI AD ARCHIVI CARTACEI

2.1 Tipologie di violazione di dati

La violazione di dati che si presenti in via esclusiva su archivi cartacei può aver luogo sia per eventi accidentali che per eventi dolosi.

Tra gli eventi accidentali rientrano gli eventi anomali avvenuti per:

- distruzione accidentale di documenti (incendio o allagamento dei locali dove sono presenti archivi cartacei);
- distruzione per errore di documenti originali, senza avere il possesso di una eventuale copia;
- smarrimento di documenti;
- fornitura involontaria di dati a persona diversa dal destinatario.

Gli eventi dolosi possono avvenire per comportamenti posti in essere dal personale interno o da soggetti esterni realizzati attraverso:

- distruzione dei documenti;
- accesso non autorizzato;
- furto.

2.2 Il processo di *data breach*

2.2.1 Gli attori del processo

- **Titolare -** il soggetto che esercita le funzioni di Titolare del trattamento (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) nella struttura i cui dati sono stati oggetto di violazione viene informato del sospetto *data breach*, notifica il *data breach* asseverato a livello centrale o regionale al Garante per la protezione dei dati

personali e, ove necessario, comunica la violazione agli interessati senza ingiustificato ritardo;

- **Dirigente competente** – segnala il potenziale *data breach*;
- **Ufficio di Gabinetto del Ministro** – è informato, nei casi in cui la violazione è di particolare rilevanza in relazione alle attività del Ministero, del *data breach* asseverato e avvia, ove ritenuto necessario, le opportune attività di comunicazione;
- **Responsabile della protezione dei dati** - è costantemente informato a partire dal sospetto di *data breach*;
- **CSIRT –** aggiorna, sia in caso di *data breach* asseverato che di falso positivo, il Registro degli incidenti di sicurezza (Allegato C).

2.2.2 Le fasi del processo

Il processo prevede tre fasi:

- Acquisizione del potenziale *data breach*;
- Asseverazione del *data breach*;
- Notifica e Comunicazione del *data breach*.

Figura 2 – Fasi del processo di *data breach* su archivi cartacei

2.2.3 Acquisizione del potenziale *data breach*

Il dirigente che viene a conoscenza dell'evento anomalo di violazione di dati personali deve comunicarlo, senza ingiustificato ritardo, con posta elettronica indicando come oggetto **"URGENTE: Potenziale *data breach* su archivi cartacei"**, alla propria figura di vertice della struttura i cui dati sono stati oggetto di violazione (Capo di Gabinetto, Capo Dipartimento, Direttore generale o Dirigente preposto all'Ufficio scolastico regionale) e, per conoscenza, al Responsabile della protezione dei dati, inviando il modulo "Modello di comunicazione incidente violazione dati personali presenti su archivi cartacei" (Allegato F).

2.2.4 Asseverazione del *data breach*

Il soggetto che ha ricevuto la segnalazione del potenziale *data breach*, coaudivato dal dirigente competente, approfondisce e analizza la fattispecie nel rispetto dei termini previsti dall'articolo 33 del Regolamento e, al fine di rilevare:

- la natura dell'eventuale violazione dei dati personali subita (tipologia di incidente, descrizione servizio impattato/banca dati/archivio fisico oggetto di *data breach*, intervallo temporale di riferimento, luogo dell'incidente, ecc.);
- il numero (anche approssimativo) e le categorie degli interessati e i dati personali oggetto di violazione;
- le possibili conseguenze della violazione sui diritti e sulle libertà dell'interessato e la valutazione della probabilità che le stesse si verifichino ai fini dell'eventuale notificazione al Garante per la protezione dei dati personali;
- le misure di sicurezza in essere e applicate ai dati violati;

- le eventuali misure adottate per porre rimedio alla violazione e/o per attenuarne gli effetti negativi.

Al termine dell'analisi, il soggetto che ha ricevuto la segnalazione del potenziale *data breach* elabora una scheda di valutazione del *data breach* (Allegato B) in cui indica la causa, lo scenario di emersione, il potenziale impatto, le azioni già compiute e altre informazioni ritenute utili e dichiara l'asseverazione o meno del *data breach*.

In caso di *data breach* asseverato, il soggetto che ha ricevuto la segnalazione del potenziale *data breach* trasmette la scheda di valutazione del *data breach* (Allegato B) al soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) e, per *data breach* di particolare rilevanza, informa per conoscenza il Capo di Gabinetto.

Sia in caso di *data breach* asseverato che di falso positivo, è necessario trasmettere la scheda di valutazione del *data breach* (Allegato B) allo CSIRT per l'aggiornamento del Registro degli incidenti di sicurezza (Allegato C).

2.2.5 Notifica e comunicazione del *data breach*

Entro 72 ore dal momento in cui il *data breach* è stato asseverato, il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) procede alla **notifica del *data breach*** secondo quanto previsto dall'articolo 33 del Regolamento e utilizzando l'apposita procedura telematica disponibile al seguente link https://servizi.gpdp.it/databreach/s/ con la quale vengono richieste le informazioni contenute nel Modello - informazioni da fornire per la notifica *data breach* al Garante (Allegato D).

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il soggetto che esercita le funzioni di Titolare (Capo di Gabinetto, Capo Dipartimento o Dirigente preposto all'Ufficio scolastico regionale) della struttura i cui dati sono stati oggetto di violazione, **comunica la violazione** agli interessati senza ingiustificato ritardo utilizzando il modello "Template comunicazione all'interessato" (Allegato E) secondo quanto previsto dall'articolo 34 del Regolamento.

In relazione alla rilevanza del *data breach* possono essere coinvolti, ove necessario:

- **Ufficio di Gabinetto:** pianifica la comunicazione esterna al Ministero coinvolgendo l'Ufficio stampa;
- **DGSIS:** pianifica la comunicazione interna al Ministero tramite l'ufficio competente.

3.ALLEGATI

3.1 Allegato A: "modello di comunicazione incidente violazione dati personali"

Allegato A modello di comunicazione incide

3.2 Allegato B: "scheda di valutazione del *data breach*"

Allegato B scheda di valutazione del data b

3.3 Allegato C: "Registro degli incidenti di sicurezza"

Allegato C Registro degli incidenti di sicur

3.4 Allegato D:" Modello - informazioni da fornire per la notifica *data breach* al Garante"

Allegato D Modello - informazioni da fornir

3.5 Allegato E "Template comunicazione all'interessato"

Allegato E Template comunicazione all'inte

3.6 Allegato F: "Modello di comunicazione incidente violazione dati personali presenti su archivi cartacei"

Allegato F Modello di comunicazione incide