DATA BREACH POLICY

Procedura gestione e notifica della violazione di dati personali
(Regolamento Europeo 679/2016)

INDICE

Premesse

Il Data Breach è una violazione della sicurezza, che comporta accidentalmente o in modo illecito la distruzione, perdita, modifica, divulgazione, accesso, copia o consultazione non autorizzate di dati personali trasmessi, conservati o comunque trattati. Tali criticità si realizzano a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB aziendali, etc.) o per la sottrazione di documenti con dati personali (furto, etc.).
In tali casi, il Regolamento Europeo 2016/679 (di seguito "GDPR"), impone al Titolare del trattamento di agire senza ritardo, prevedendo - ove ritenuto necessario - procedere alla notifica dell'evento al Garante per la protezione dei dati personali ed alla comunicazione ai soggetti interessati.
A riguardo, una specifica procedura di data breach è essenziale per poter gestire l'evento e se del caso valutare la necessità o meno di notificare la violazione dei dati personali al Garante e agli interessati qualora il rischio per gli stessi risulti elevato, al fine di consentirne la mitigazione attraverso l'adozione di precauzioni e rimedi

1. Definizioni

"Violazione dei dati personali" ***(c.d. Data breach)***: 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.
Nel dettaglio, la violazione dei dati personali può essere classificata come segue:

a) "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
b) "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
c) "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

(Cfr. Art 29 WG Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE (2016/679)

Una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché qualsiasi combinazione delle stesse.

"Dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

"Trattamento": qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

"Distruzione" dei dati personali: i dati personali non esistono più o non esistono più in una forma che sia di qualche utilità per il titolare del trattamento. (*Linee guida cit.*)

"Danno": i dati personali sono stati modificati, corrotti o non sono più completi. (*Linee guida cit.)*

“Perdita” dei dati personali: i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l’accesso, oppure non averli più in possesso. 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, o 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. *(Linee guida cit.)*

“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. *(Linee guida cit.)*

“Archivio”: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico.

“Titolare del trattamento”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

“Referente data breach”: la persona fisica che nell’ambito dell’azienda è incaricata come responsabile del processo di *data breach*, come disciplinato nella presente procedura.

“Data Protection Officer”: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR.

“Responsabile del trattamento”: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

2. Scopo del documento

Lo scopo del presente documento è disciplinare le attività di “reazione” della Federazione nei casi di “violazione dei dati personali”, andando ad individuare puntualmente le modalità e le responsabilità dei connessi adempimenti e, segnatamente:
- Gestione del *data breach* (comunicazioni interne; valutazione dell’evento, adozione di misure correttive e di contenimento)
- Notifica della violazione al Garante per la protezione dei dati personali
- Comunicazione della violazione all’interessato

3. Ambito di applicazione

Il presente documento è rivolto, e pertanto si applica, a tutti i soggetti che a qualsiasi titolo trattano dati personali di competenza dell’azienda e, segnatamente:

a) lavoratori dipendenti, della sede centrale e territoriale, nonché coloro che a qualsiasi titolo - e quindi a prescindere dal rapporto giuridico intercorrente - abbiano accesso ai dati personali trattati nell’ambito delle prestazioni rese in favore del Titolare del trattamento (di seguito “incaricati del trattamento”);
b) qualsiasi soggetto (persona fisica o persona giuridica) diverso dall’incaricato del trattamento che, in ragione del rapporto contrattuale intercorrente con il Titolare del trattamento abbia accesso ai dati richiamati, agisca quale Responsabile del trattamento ai sensi dell’art. 28

GDPR. Tra questi, come noto, si segnalano in particolare le Società affiliate e Sezioni provinciali.

Gli incaricati e i Responsabili del trattamento devono essere informati del presente documento, posto che il mancato rispetto delle relative previsioni legittimerà l'azienda all'adozione di provvedimenti disciplinari ovvero la risoluzione dei contratti in essere, salvo il risarcimento del maggior danno.

4. Rilevazione e segnalazione del data breach

La rilevazione e la segnalazione del *data breach* costituisce un obbligo per tutti i dipendenti della sede centrale e di quelle territoriali, collaboratori e fornitori della Federazione, ivi comprese Società affiliate e Sezioni provinciali.
4.1. Nel caso in cui si verifichi uno degli eventi di cui in premessa o, più in generale, in tutti gli altri casi in cui si sospetti il rischio per l'integrità e la protezione dei dati, i soggetti di cui al punto 3 lettera a) che precede sono tenuti a informare immediatamente il ***Referente data breach*** tramite il modello allegato (modello A) il quale provvede a darne tempestiva comunicazione al responsabile per la protezione dei dati personali (DPO), nonché al Titolare del trattamento.
4.2. I soggetti di cui al punto 3) lettera b), qualora vengano a conoscenza di un *data breach* che riguardi dati di cui l'Azienda è Titolare, ne danno avviso senza ingiustificato ritardo, e comunque non oltre 12 ore dalla conoscenza dell'incidente al *Referente data breach* tramite il modulo allegato (modello B)

5. Valutazione del data breach e del rischio conseguente

Il *Referente data breach* effettua una valutazione dell'evento avvalendosi del DPO, comunicando le sue conclusioni al Titolare del trattamento entro 36 ore dall'incidente.
Ai fini di una corretta classificazione dell'episodio, il *Referente data breach* utilizzerà il *Modulo di valutazione del Rischio connesso al Data Breach*, allegato alla presente procedura (modello B).
Laddove la violazione inerisca dati personali contenuti in un sistema informatico, il *Referente data breach* coinvolgerà nella presente procedura anche il Responsabile dell'Ufficio IT o, comunque, il soggetto interno o esterno competente IT.

La notifica al Garante dell'incidente è sempre obbligatoria a meno che sia improbabile che la violazione presenti UN RISCHIO per i diritti e le libertà delle persone fisiche, mentre la comunicazione agli interessati va effettutata solo quando il RISCHIO È *ELEVATO*.

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.

Di conseguenza, nel valutare il rischio per le persone fisiche derivante da una violazione, il Referente, nell'ambito dell'istruttoria conseguente al *data breach*, deve considerare le circostanze specifiche della violazione, inclusa la gravità dell'impatto potenziale e la probabilità che tale impatto si verifichi, adottando i seguenti criteri:

- ***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 e volume dei dati personali coinvolti***

Un elemento fondamentale della valutazione del rischio è rappresentato dalla natura dei dati personali compromessi dalla violazione. Ove questi rientrino nelle categorie particolari di dati, maggiore è il rischio di danni per gli interessati. Fermo quanto precede, ai fini di una puntuale valutazione occorre prendere in considerazione anche altri elementi, posto che anche la semplice violazione di dati comuni potrebbe comportare uno rischio rilevante ai fini della notifica e della comunicazione.

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.

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.

Ad esempio, 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 del GDPR 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 nei casi di furto o usurpazione di identità, danni fisici, disagio psicologico, umiliazione o danni alla reputazione. Parimenti, 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 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.

In buona sostanza, l fatto che il destinatario sia affidabile può neutralizzare la gravità delle conseguenze della violazione.

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.

- ***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.

Riassumendo:

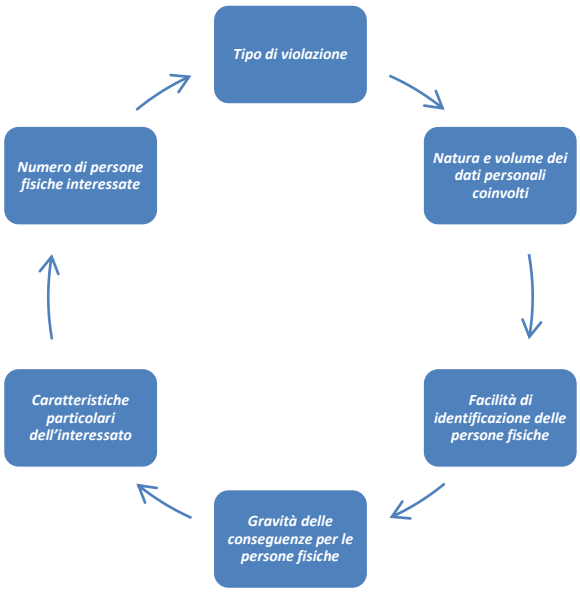

Figura 1 - Criteri di valutazione del rischio connesso all'incidente

Da ultimo, per quanto riguarda **la comunicazione dell'incidente all'interessato**, la stessa NON è dovuta nei seguenti casi:

a) L'Azienda ha adottato 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;

b) L'Azienda ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

In base all'esito della verifica che precede il Titolare:

a) se il data breach non risulta presentare alcun rischio per gli interessati, non provvede ad alcuna notifica né al Garante, né agli interessati.
Il *Referente data breach* annoterà comunque l'incidente nell'apposito registro.

b) Se il *data breach* presenta rischi per gli interessati, provvede alla notifica dell'incidente al solo Garante, nelle modalità di cui al successivo punto 7, ovvero anche alla comunicazione agli interessati se l'indicato rischia si presenta come elevato, nelle modalità di cui al punto 8.

In ogni caso tutti gli incidenti devono essere registrato in un apposito registro.

6. Contenimento del danno

A seguito della segnalazione della violazione il *Referente data breach*, con il supporto del DPO e – nei casi previsti – del responsabile IT, accertatane l'esistenza, dovrà porre in essere ogni azione possibile volta a limitare i danni che la violazione potrebbe causare (i.e. riparazione fisica di

strumentazione; utilizzo dei file di back up per recuperare dati persi o danneggiati; isolamento/chiusura di un settore compromesso della rete; cambio dei codici di accesso, ecc.).

7. Modalità di notifica al Garante per la protezione dei dati Personali

Sulla scorta delle determinazioni raggiunte, ovvero l'accertato rischio per i diritti e le libertà delle persone fisiche coinvolte nell'incidente, il *Referente data breach* predispone la comunicazione all'Autorità Garante - tramite il **modello D** - a firma del Titolare, da inviare senza ingiustificato ritardo e, comunque entro 72 ore, da determinarsi dal momento in cui il titolare ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo. E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di *follow-up (*c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del *Referente data breach*.

8. Modalità di comunicazione agli interessati

Nel caso in cui ne ricorrano i presupposti, il *Referente data breach* predispone la comunicazione all'interessato, a firma del titolare, da inviarsi senza ingiustificato ritardo attraverso il **modello E**. Detta comunicazione deve avvenire mediante un linguaggio semplice e di pronta comprensione per l'interessato.

9. Data breach e regimi particolari

Secondo le indicazioni del Garante per la protezione dei dati personali, sussistono quattro ipotesi di data breach in deroga alle disposizioni generali sopra richiamate, che richiedono una tempistica più stringente di attivazione da parte del Titolare, e segnatamente:

TIPOLOGIA DEL TRATTAMENTO	PROVVEDIMENTO DEL GARANTE	TIMING NOTIFICA
trattamento dati biometrici	Provvedimento n. 513 del 12 novembre 2014	Entro 24 ore dalla conoscenza del fatto
dossier sanitario elettronico	Provvedimento n. 331 del 4 giugno 2015	Entro 48 ore dalla conoscenza del fatto

MODELLO A – MODELLO DI COMUNICAZIONE DI DATA BREACH

RILEVAZIONE DELL'INCIDENTE	
Dati del segnalante (nome, cognome, dati di contatto)	
Data dell'incidente	[] Il ___/___/____ [] Tra il ___/___/____e il [] In un tempo non ancora determinato [] E' possibile che sia ancora in corso
Luogo dell'incidente *(Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)*	
Classificazione dell'incidente	[ ] violazione della riservatezza [ ] violazione dell'integrità [ ] violazione della disponibilità
Breve descrizione dell'incidente	
Categoria dei dati personali compromessi	[ ] Dati anagrafici/codice fiscale [ ] Dati di accesso e di identificazione (user name, password, customer ID, altro) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati personali idonei a rivelare lo stato di salute e la vita sessuale [ ] Dati giudiziari [ ] Copia per immagine su supporto informatico di documenti analogici [ ] Ancora sconosciuto [ ] Altro :
le categorie e il numero approssimativo degli interessati coinvolti nella violazione	
la descrizione di eventuali azioni già poste in essere	

MODELLO B MODELLO DI COMUNICAZIONE DEL DATA BREACH DAL RESPONSABILE AL TITOLARE TRATTAMENTO	
Azienda	[Ragione sociale, sede, contatti]
Responsabile della protezione trattamento	[nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni]
Data dell'incidente	[] Il ___/___/____ [] Tra il ___/___/____e il ___/___/____ [] In un tempo non ancora determinato [] E' possibile che sia ancora in corso
Luogo dell'incidente *(Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)*	
Classificazione dell'incidente	[ ] violazione della riservatezza [ ] violazione dell'integrità [ ] violazione della disponibilità
Breve descrizione dell'incidente	
Categoria dei dati personali compromessi	[ ] Dati anagrafici/codice fiscale [ ] Dati di accesso e di identificazione (user name, password, customer ID, altro) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati personali idonei a rivelare lo stato di salute e la vita sessuale [ ] Dati giudiziari [ ] Copia per immagine su supporto informatico di documenti analogici [ ] Ancora sconosciuto [ ] Altro :
Categorie e numero approssimativo degli interessati coinvolti nella violazione	
Descrizione delle probabili conseguenze del data breach	
Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del *data breach*	

MODELLO C – MODULO DI VALUTAZIONE DEL RISCHIO CONNESSO AL DATA BREACH

I seguenti esempi – suggeriti dal GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI nelle linee guida cit. - non esaustivi sono di ausilio nello stabilire se è necessaria la notifica in diversi scenari di violazione dei dati personali.

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 attacco tramite *ransomware* che provoca la cifratura di tutti i dati. Non sono disponibili backup e i dati non possono	Sì, effettuare la segnalazione all'autorità di controllo, se vi sono probabili conseguenze per le persone fisiche in quanto si tratta di una perdita di	Sì, effettuare la segnalazione alle persone fisiche, a seconda della natura dei dati personali interessati e del possibile effetto della mancanza di	Se fosse stato disponibile un backup e i dati avessero potuto essere ripristinati in tempo utile non sarebbe stato necessario segnalare la violazione all'autorità di controllo o alle persone

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.	disponibilità.	disponibilità dei dati, nonché di altre possibili conseguenze.	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	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

dall'autore dell'attacco.			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	Sì, la notifica all'autorità di controllo può essere obbligatoria	Sì, segnalare l'evento alle persone fisiche coinvolte in base alla	La notifica potrebbe non essere necessaria se non vengono rivelati dati

nei campi “a:” o “cc:”, consentendo così a ciascun destinatario di vedere l’indirizzo e-mail di altri destinatari.	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).	portata e al tipo di dati personali coinvolti e alla gravità delle possibili conseguenze.	sensibili e se viene rivelato soltanto un numero limitato di indirizzi di posta elettronica.

MODELLO D MODELLO DI NOTIFICA DEL *DATA BREACH* AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI	
Titolare del Trattamento	[Ragione sociale, sede, contatti]
Responsabile della protezione trattamento	[nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni]
Data dell'incidente	[] Il ___/___/____ [] Tra il ___/___/____e il ___/___/____ [] In un tempo non ancora determinato [] E' possibile che sia ancora in corso
Luogo dell'incidente *(Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)*	
Classificazione dell'incidente	[ ] violazione della riservatezza [ ] violazione dell'integrità [ ] violazione della disponibilità
Breve descrizione dell'incidente	
Categoria dei dati personali compromessi	[ ] Dati anagrafici/codice fiscale [ ] Dati di accesso e di identificazione (user name, password, customer ID, altro) [ ] Dati relativi a minori [ ] Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale [ ] Dati personali idonei a rivelare lo stato di salute e la vita sessuale [ ] Dati giudiziari [ ] Copia per immagine su supporto informatico di documenti analogici [ ] Ancora sconosciuto [ ] Altro :
Categorie e numero approssimativo degli interessati coinvolti nella violazione	
Descrizione delle probabili conseguenze del data breach	
Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del *data breach*	
La violazione è stata comunicata anche agli interessati	[ ] SI [ ] NO, perché_____
Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, descrivere dei motivi del ritardo.	

MODELLO E
MODELLO DI COMUNICAZIONE DEL DATA BREACH ALL'INTERESSATO

Gentile ...
La informiamo che in data_____ siamo venuti a conoscenza di un evento che potrebbe aver coinvolto i Suoi dati personali.

Inserire breve descrizione dell'incidente

Le possibili conseguenze dell'evento sono:

Inserire descrizione delle probabili conseguenze del data breach

In risposta all'evento, abbiamo adottato le seguenti misure:

Descrizione delle azioni già poste in essere o di cui si propone l'adozione per porre rimedio o attenuare gli effetti del data breach

Per maggiore garanzia, La invitiamo a:

Inserire descrizione delle eventuali azioni suggerite all'interessato

Per qualsiasi informazione o chiarimento, può contattare:

Inserire nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni

Data,

Il Titolare del Trattamento

_____

Il DPO

_____