POLICY SULLA GESTIONE DELLE VIOLAZIONI DI DATI PERSONALI

INFORMAZIONI DOCUMENTO:

Titolo	Policy sulla gestione delle violazioni di dati personali		
Data di emissione	25/5/2018	**Versione**	1.0

Il **GDPR** disciplina il **Data Breach**, ovvero le procedure che un'organizzazione pubblica o privata deve adottare in caso di incidente di sicurezza in cui dati sensibili, protetti o riservati vengono consultati, copiati, trasmessi, rubati o utilizzati da un soggetto non autorizzato.

Si verifica un caso di data breach se si verifica una divulgazione o un accesso non autorizzato o accidentale, se si verifica un'alterazione o la perdita, l'impossibilità di accesso o la distruzione, accidentale o non autorizzata, di dati personali.

Ovviamente in questi casi non rientra solamente il furto o il danno provocato da soggetti terzi malintenzionati, ma **anche la perdita accidentale**, quindi la cancellazione di dati per un errore umano o di sistema, o semplicemente l'impossibilità di accesso al dato, per esempio la perdita della password di accesso ad un archivio protetto, o la criptazione provocata da un'infezione da ramsonware.

L'autorità di controllo a cui segnalare il Data Breach è il **Garante della Privacy**, come definito dall'articolo 55 del General Data Protection Regulation.

Assenza di rischi

In caso non ci fosse alcun rischio connesso all'attacco verso i dati personali immagazzinati, è necessario registrare la violazione e successivamente conservare il registro. **La notifica al Garante della Privacy non è obbligatoria ed è comunque necessario comprovare l'assenza dei rischi.**

Presenza di rischi

In presenza di rischi per gli interessati è necessaria la **notifica entro 72 ore** al **Garante della Privacy**, il quale rilascia un apposito modulo (Modello di segnalazione Data Breach).

La procedura da seguire è:

1. Raccogliere tutte le informazioni inerenti al **Data Breach** per la notifica al **Garante della Privacy**
2. Inviare la notifica al **Garante della Privacy**
3. Registrare la violazione
4. Conservare il registro delle violazioni

Presenza di un elevato rischio

La procedura da seguire è:

1. Raccogliere tutte le informazioni inerenti al **Data Breach** per la notifica al **Garante della Privacy** e ai diretti interessati del trattamento
2. Inviare la notifica al **Garante della Privacy** e **agli interessati**
3. Gestione dei riscontri da parte degli interessati
4. Registrare la violazione
5. Conservare il registro delle violazioni

Per un rischio elevato si intende per esempio una violazione che interessa un rilevante quantitativo di dati personali e/o di soggetti interessati, piuttosto che un **Data Breach** che impatta su soggetti vulnerabili per le loro condizioni o categorie particolari di dati personali.

Dossier Sanitario Elettronico

Provvedimento n. 331 del 4 giugno 2015 [doc. web n. 4084632]

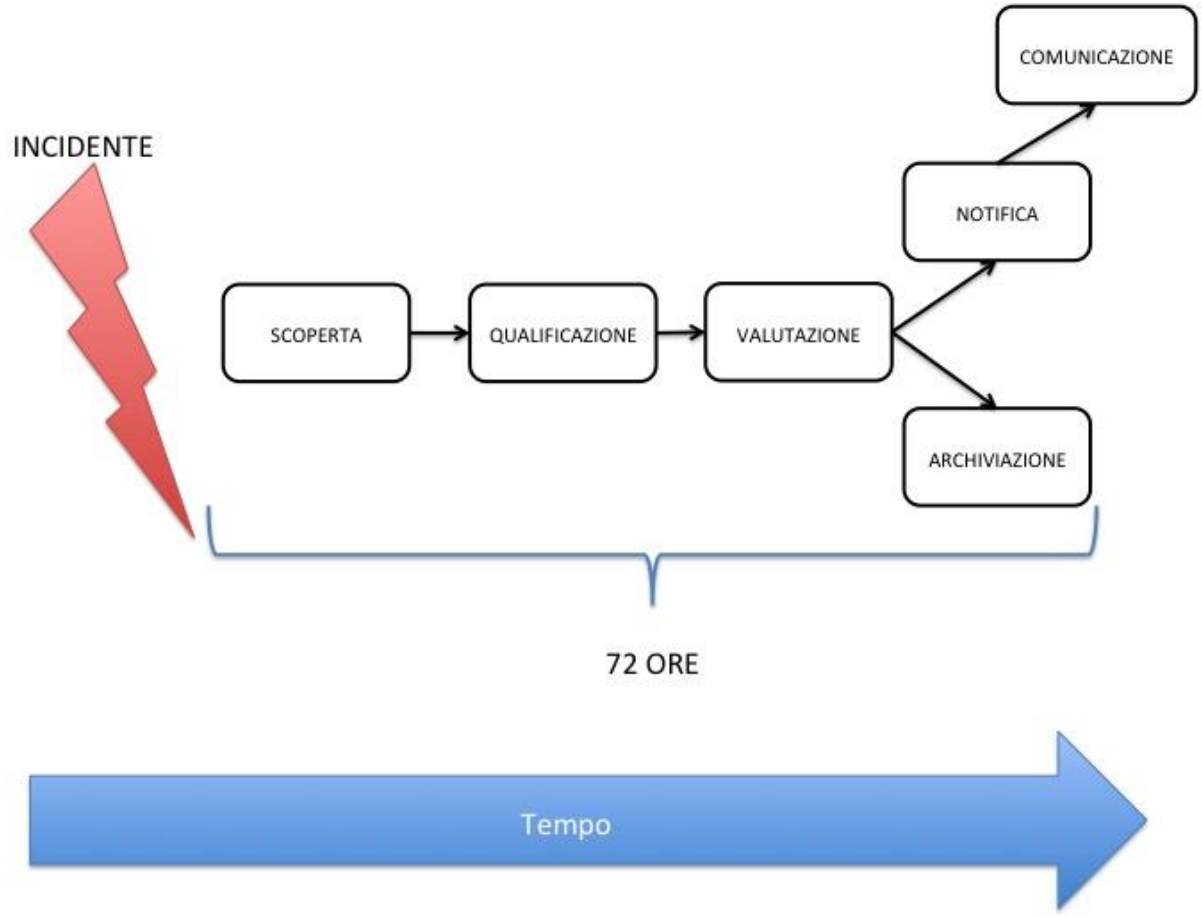
Entro 48 ore dalla conoscenza del fatto, le strutture sanitarie pubbliche o private sono tenute a comunicare al Garante tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali trattati attraverso il dossier sanitario.

Amministrazioni pubbliche

Provvedimento n. 392 del 2 luglio 2015 [doc. web n. 4129029]

Entro 48 ore dalla conoscenza del fatto, le amministrazioni pubbliche sono tenute a comunicare al Garante tutte le violazioni dei dati o gli incidenti informatici che possano avere un impatto significativo sui dati personali contenuti nelle proprie banche dati.

COME NOTIFICARE UNA VIOLAZIONE



Rilevazione del Data Breach

A. Canali interni

Le segnalazioni interne di eventi anomali possono:

- pervenire dal personale dell'Ente;
- essere inoltrate dal DPO.

B. Canali esterni

Le segnalazioni possono pervenire anche da fonti esterne, o anche dall'analisi di informazioni presenti sul Web, ovvero dai Responsabili.

Inoltre, ogni Interessato può segnalare, anche solo in caso di sospetto, che i propri Dati Personali siano stati utilizzati abusivamente o fraudolentemente da un terzo; in tal caso, l'Interessato può richiedere all'azienda la verifica dell'eventuale violazione.

Per la segnalazione è necessario compilare la Scheda Evento, allegato alla presente procedura, contenente tutte le informazioni raccolte:

- Data evento anomalo;
- Data presunta di avvenuta violazione;
- Data e ora in cui si è avuto conoscenza della violazione;
- Fonte segnalazione;
- Tipologia violazione e di informazioni coinvolte;
- Descrizione evento anomalo;
- Numero Interessati coinvolti;
- Numerosità di Dati Personali di cui si presume una violazione;
- Indicazione del luogo in cui è avvenuta la violazione dei dati, specificando altresì se essa sia avvenuta a seguito di smarrimento di Device Mobili;
- Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione.

La Scheda Evento viene consegnata al Titolare che può farsene carico o designare un delegato.

Le segnalazioni, a qualunque soggetto/funzione pervengano, devono essere tempestivamente comunicate al DPO comunque non oltre 12 ore dalla conoscenza della violazione, ove possibile a mezzo PEC.

La presa in carico di tutte le segnalazioni è di responsabilità del Direttore Generale, che provvederà a gestirle coinvolgendo le altre funzioni interessate secondo quanto specificato nella presente procedura.

La consapevolezza del titolare è considerato il momento in cui iniziano a decorrere i termini della notifica: è importante avere un "ragionevole grado di certezza" dato da indagini approfondite, quando necessarie.

Se l'incidente di sicurezza richiede maggiori controlli e verifiche, non è possibile ancora ritenere sufficiente la conoscenza dei fatti tanto da dover notificare l'accaduto.

Tuttavia sarà un'azione tempestiva, anche se solo di indagine, a rendere corretto il comportamento del titolare che quindi non dovrà prorogare troppo a lungo la fase investigativa.

Quando il titolare, anche quando ha appurato con ragionevole certezza l'esistenza di una violazione, non è già in possesso di tutti gli elementi utili per effettuare una descrizione completa ed esaustiva dell'infrazione, può adottare alcune tecniche o modalità che permettono di bilanciare le esigenze di celerità del messaggio con quelle di una sua sostanziale accuratezza e completezza.

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.

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. Potrà allora ottemperare agli obblighi di notifica comunicando, dopo una prima e rapida notifica di *alert*, tutte le informazioni per fasi successive, aggiornando di volta in volta l'autorità sui nuovi riscontri.

Notifica differita: dopo le 72 ore previste dall'art. 33. È il caso in cui, per esempio, un'impresa subisca 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 scaglionato 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.

Anche il responsabile del trattamento potrà notificare la violazione per conto del titolare, anche se a lui restano le responsabilità a essa collegate.

Analizzare la violazione e valutarne i rischi connessi

L'analisi consente al titolare di individuare con prontezza adeguate misure per arginare o eliminare l'intrusione e di valutare la necessità di attivare le procedure di comunicazione e di notifica (che si ricorda si attivano solo al superamento di determinate soglie di rischio).

Obiettivo dell'analisi di primo livello è quella di verificare che la segnalazione non si tratti di un cd. "falso positivo".

Nel caso la violazione su dati personali venga accertata il Titolare o il suo delegato recupera le informazioni di dettaglio sull'evento necessarie alle analisi di secondo livello, e le riporta nella Scheda Evento.

Nel caso in cui l'evento segnalato risulti essere un falso positivo, si chiude l'incidente e la funzione IT/Security si attiva per effettuare un raffinamento delle regole di rilevazione dei falsi positivi, comunicando via e-mail l'esito dell'analisi al Titolare.

L'evento viene comunque inserito a cura del Titolare o del suo delegato nel Registro dei Data Breach nell'apposita sezione dedicata agli "eventi falsi positivi".

Per l'analisi di secondo livello vengono analizzate congiuntamente tutte le informazioni raccolte e redige una Scheda Violazione Dati per le conseguenti valutazioni.

L'evento viene classificato tra i seguenti casi:

1) violazione di riservatezza, ovvero quando si verifica una divulgazione o un accesso a dati personali non autorizzato o accidentale.
2) Violazione di integrità, ovvero quando si verifica un'alterazione di dati personali non autorizzata o accidentale.
3) Violazione di disponibilità, ovvero quando si verifica perdita, inaccessibilità, o distruzione, accidentale o non autorizzata, di dati personali.

In particolari circostanze le violazioni potrebbero essere combinate tra loro.

La violazione deve essere valutata secondo i livelli di rischio:

- NULLO
- BASSO
- MEDIO
- ALTO

Il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'Interessato a cui si riferiscono i dati, a causa della violazione dei Dati Personali:

1. discriminazioni

2. furto o usurpazione d'identità

3. perdite finanziarie

4. pregiudizio alla reputazione

5. perdita di riservatezza dei dati personali protetti da segreto professionale

6. decifratura non autorizzata della pseudonimizzazione

7. danno economico o sociale significativo

8. privazione o limitazione di diritti o libertà

9. impedito controllo sui dati personali all'interessato

10. danni fisici, materiali o immateriali alle persone fisiche.

Saranno inoltre valutate, come variabili qualitative dell'impatto temuto, le seguenti eventuali condizioni:

a) che si tratti di dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché di 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;

b) che si tratti di dati relativi a valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;

c) che si tratti di dati di persone fisiche vulnerabili, in particolare minori;

d) che il trattamento riguardi una notevole quantità di Dati Personali;

e) che il trattamento riguardi un vasto numero di Interessati.

Il Titolare deve provvedere affinché vengano tempestivamente adottate misure che consentano di minimizzare le conseguenze negative della violazione.

Contenuto della notifica al Garante (Art. 33 p.3 GDPR)

La Comunicazione al Garante della violazione dei dati deve avere questi contenuti:

- Descrizione della 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.
- Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Contenuto della Comunicazione agli interessati (Art. 34 p.3 GDPR)

In primo luogo il GDPR determina l'essenzialità della **notifica della violazione** dei dati all'autorità e della **comunicazione** ai soggetti interessati quando il data breach mette a rischio le **libertà** e i **diritti** di un individuo quali:

- Danni fisici, materiali o morali
- Danni economici o sociali
- Perdita del controllo dei dati
- Limitazione dei diritti
- Discriminazione
- Furto o usurpazione d'identità
- Perdite finanziarie
- Decifratura non autorizzata della Pseudoanimizzazione
- Pregiudizio alla reputazione
- Perdita di riservatezza dei dati protetti da segreto professionale (sanitari, giudiziari)

Mentre per far scattare l'obbligo di notifica è sufficiente che sussista una violazione di dati personali che presenti un rischio per i diritti e le libertà delle persone fisiche, per la comunicazione occorre che tale rischio sia indicato come ALTO nella Scheda Violazione Dati.

La comunicazione all'interessato non è tuttavia richiesta se si ravvisano una serie di circostanze specifiche:

- quando il titolare del trattamento ha messo in atto, e applicato ai dati che sono stati oggetto di violazione, tutte le necessarie misure tecniche e organizzative di protezione, comprese quelle destinate a rendere i dati personali incomprensibili ai soggetti non autorizzati (come, ad esempio, la cifratura delle informazioni).
- quando il titolare del trattamento abbia successivamente adottato misure per scongiurare il verificarsi di un rischio elevato per i diritti e le libertà degli interessati.
- quando la comunicazione stessa richiederebbe sforzi sproporzionati e, in tal caso, si può procedere a una comunicazione pubblica o ad altra soluzione analoga, così da informare gli interessati in maniera ugualmente efficace.

In sostanza, dunque, è opportuno procedere a un duplice controllo: da un lato, occorre verificare che siano state adottate le misure di protezione adeguate, così da poter stabilire se c'è stata violazione dei dati personali e informare, di conseguenza, l'autorità di controllo e gli interessati. Dall'altro, si

deve stabilire se la notifica è stata trasmessa senza ingiustificato ritardo, tenendo conto, in particolare, della natura e della gravità della violazione, nonché delle sue conseguenze ed effetti negativi per l'interessato.

Devono sempre essere **privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS o messaggi diretti).** Il messaggio dovrebbe essere comunicato in maniera evidente e trasparente, evitando quindi di inviare le informazioni nel contesto di *update* generali o *newsletter*, che potrebbero essere facilmente fraintesi dai lettori. 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 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 sui siti web, non lo sarà se questa sia limitata all'inserimento della notizia in un blog o in una rassegna stampa.

La comunicazione agli interessati deve avere questi contenuti:

- Descrizione con un linguaggio semplice e chiaro della natura della violazione dei dati personali.
- Data e ora della violazione, anche solo presunta, e data e ora in cui si è avuto conoscenza della stessa;
- Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni.
- Descrizione delle probabili conseguenze della violazione dei dati personali.
- Descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Il registro dei data breach

L'art. 33 p.5 del GDPR, prescrive al titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'autorità di controllo di verificare il rispetto della norma.

Ne discende che le generali attività di scoperta dell'incidente, come le successive di trattamento, devono essere documentate, adeguate (devono riportare le violazioni, le circostanze, le conseguenze ed i rimedi), tracciabili, replicabili ed essere in grado di fornire evidenza nelle sedi competenti.

Il **registro dei data breach** è una documentazione che, ai sensi dell'art. 33 del GDPR, il titolare del trattamento è tenuto a conservare per tenere traccia di tutti i data breach avvenuti.

I titolari del trattamento sono tenuti a conservare un registro dei data breach che deve contenere le seguenti informazioni:

- i dettagli relativi al data breach, ovvero informazioni inerenti le cause della violazione, il luogo nel quale essa è avvenuta e la tipologia dei dati personali violati
- gli effetti e le conseguenze della violazione
- il piano di intervento predisposto dal titolare
- la motivazione delle decisioni assunte a seguito del data breach nei casi in cui:
    - il titolare ha deciso di non procedere alla notifica
    - il titolare ha ritardato nella procedura di notifica
    - il titolare ha deciso di non notificare il data breach agli interessati

Il registro dei data breach deve essere continuamente aggiornato e messo a disposizione del Garante qualora l'Autorità chieda di accedervi.

Il titolare del trattamento dovranno registrare nel registro il data breach che ha coinvolto la Struttura contestualmente alla comunicazione al Garante, avendo cura di inserire tempestivamente gli elementi che dovessero emergere all'esito di ulteriori verifiche.

Il registro dei data breach dovrà inoltre essere strutturato in modo da garantire l'integrità e l'immodificabilità delle registrazioni in esso contenute.

Ecco alcuni esempi commentati di violazione

Un supporto (cd/dvd/cassetta/ecc.) contenente un backup criptato con dati personali viene perso o rubato.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Se i dati vengono crittografati con un algoritmo di ultima generazione, esistono dei backup dei dati e la chiave privata non è compromessa, non è necessario notificare la violazione. Tuttavia, se venisse compromessa anche successivamente, la notifica diverrà necessaria.

Durante un cyber-attacco al sito web vengono rubati dati personali.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e se è alto il livello di gravità dei potenziali danni.

Commento: Se il rischio non è elevato, consigliamo al titolare del trattamento di informare l'interessato, a seconda delle circostanze del caso. Ad esempio, la notifica potrebbe non essere necessaria in caso di violazione della riservatezza per una newsletter relativa ad un programma televisivo, mentre la notifica può essere richiesta se questa newsletter può portare a conoscenza del punto di vista politico del soggetto interessato.

Una breve interruzione dell'alimentazione del call center del titolare del trattamento, che comporta l'impossibilità dei clienti di chiamare il titolare del trattamento e di accedere ai propri dati.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: No.

Commento: Questa non è una violazione dei dati personali da notificare, ma solo un incidente di cui tenere nota ai sensi dell'art. 33, paragrafo 5.
Il titolare del trattamento dovrà redigere un apposito registro.

Un titolare del trattamento subisce un attacco ransomware che causa la crittografia di tutti i dati. Nessun back-up è disponibile e i dati non possono essere ripristinati. Al momento dell'indagine, risulta evidente che l'unico scopo del ransomware era quello di crittografare i dati e che nessun altro malware veniva rilevato nel sistema.

- Comunicazione al Garante: Sì, la notifica è necessaria in caso di potenziali danni ai soggetti interessati, visto che questo attacco comporta una perdita di disponibilità dei dati.
- Comunicazione agli interessati: Sì, la notifica dipende dalla natura dei dati violati e dal possibile effetto della perdita di disponibilità dei dati, così come altre probabili conseguenze.

Commento: Se fosse disponibile un backup e se i dati potessero essere ripristinati in tempo utile, non sarebbe necessario segnalare al Garante o agli interessati poiché non ci sarebbe stata perdita

permanente di disponibilità o riservatezza. Tuttavia, il Garante potrebbe considerare di verificare la conformità dei requisiti di sicurezza più ampi previsti dall'art. 32.

Un interessato denuncia all'Ente una violazione di dati. Il soggetto ha ricevuto un documento contenente dati di qualcun altro.
Il titolare del trattamento intraprende una breve indagine (che va completata entro 24 ore) e stabilisce con ragionevole certezza che si è verificata una violazione dei dati personali e se ciò è stato causato da un difetto sistemico che comporti il potenziale interessamento di altri soggetti.

- Comunicazione al Garante: No.
- Comunicazione agli interessati: Vengono notificati i soggetti interessati solo se esiste un rischio elevato ed è chiaro che altri soggetti non sono stati coinvolti.

Commento: Se, dopo ulteriori indagini, si è stabilito che sono interessati più soggetti, sarà necessario aggiornare il Garante ed il titolare del trattamento dovrà intraprendere, come azione supplementare, la notifica ad altri soggetti, in caso di loro rischio elevato.

Una società di hosting web individua un errore nel codice che controlla l'accesso da parte degli utenti. L'anomalia comporta che qualunque utente possa accedere ai dettagli dell'account di qualsiasi altro utente.

- Comunicazione al Garante: Come responsabile del trattamento, la società di hosting web deve notificare tempestivamente al Garante quali suoi clienti (titolari del trattamento) sono coinvolti. Supponendo che la società di hosting web abbia effettuato una propria indagine, i titolari coinvolti dovrebbero essere ragionevolmente sicuri di sapere o meno di aver subito una violazione. Pertanto è da considerarsi "avvisato" una volta è stato oggetto di notifica dalla società di hosting (il responsabile del trattamento). Il titolare dovrà in seguito notificare la violazione all'autorità di vigilanza.
- Comunicazione agli interessati: Se non esiste un rischio elevato per i soggetti interessati, la notifica non è necessaria.

Commento: La società di hosting web (responsabile) deve considerare tutti gli altri obblighi di notifica (ad esempio, nell'ambito della direttiva NIS).
Se non vi è alcuna prova che questa vulnerabilità sia stata sfruttata da un particolare soggetto titolare, una notifica di violazione non può aver luogo ma è probabile che sia registrabile o che rientri nei casi di non conformità, ai sensi dell'art. 32.

Un attacco informatico causa la non disponibilità dei registri medici in un ospedale per il periodo di 30 ore.

- Comunicazione al Garante: Sì, l'ospedale è tenuto a notificare al paziente che potrebbe verificarsi un alto rischio per il suo benessere e la sua privacy.
- Comunicazione agli interessati: Sì, la notifica è necessaria.

I dati personali di 5000 studenti sono inviati per errore ad una mailing list sbagliata con più di 1000 destinatari.

- Comunicazione al Garante: Sì, la notifica è necessaria.
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda dell'ambito e tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Una e-mail di marketing diretto viene inviata ai destinatari nel campo "a:" o "cc:", consentendo così a ciascun destinatario di visualizzare l'indirizzo di posta elettronica di altri destinatari.

- Comunicazione al Garante: Sì, la notifica all'autorità di vigilanza può essere obbligatoria se è coinvolto un numero elevato di soggetti, se vengono rivelati dati sensibili (ad esempio una mailing list di un psicoterapeuta) o se altri fattori presentano rischi elevati (ad esempio, la mail contiene le password iniziali).
- Comunicazione agli interessati: Sì, la notifica è necessaria ai soggetti interessati, a seconda del tipo dei dati personali coinvolti e della gravità delle possibili conseguenze.

Commento: La notifica potrebbe non essere necessaria se non vengono rivelati dati sensibili o se viene rivelato solo un numero ristretto di indirizzi di posta elettronica.

SCHEDA EVENTO

CODICE	
Data evento e ora della violazione anche solo presunta (specificando se è presunta);	
Data e ora in cui si è avuto conoscenza della violazione;	
Fonte di segnalazione	
Tipologia evento anomalo	
Descrizione evento anomalo	
Numero interessati coinvolti	
Numerosità dei dati personali di cui si presume la violazione	
Data, anche presunta, della violazione e del momento in cui se ne è avuta conoscenza	
Luogo in cui è avvenuta la violazione dei dati (specificare se è avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)	
Descrizione dei sistemi di elaborazione e/o memorizzazione dei dati coinvolti, con indicazione della loro ubicazione	

SCHEDA VIOLAZIONE DATI

CODICE EVENTO[1]	CLASSIFICAZIONE[2]	RISCHIO[3]

[1] Inserire il CODICE della scheda evento

[2] L'Evento viene classificato tra i seguenti casi:

- distruzione di dati illecita,
- perdita di dati illecita,
- modifica di dati illecita,
- distruzione di dati accidentale,
- perdita di dati accidentale,
- modifica di dati accidentale,
- divulgazione non autorizzata
- accesso ai dati personali illecito.

[3] Il rischio deve essere valutato secondo i seguenti livelli di rischio:

- NULLO
- BASSO
- MEDIO
- ALTO

il rischio va riferito alla probabilità che si verifichi una delle seguenti condizioni a danno di persone fisiche anche diverse dall'interessato a cui si riferiscono i dati, a causa della violazione dei dati personali:

- discriminazioni
- furto o usurpazione d'identità
- perdite finanziarie
- pregiudizio alla reputazione
- perdita di riservatezza dei dati personali protetti da segreto professionale
- decifratura non autorizzata della pseudonimizzazione
- danno economico o sociale significativo
- privazione o limitazione di diritti o libertà
- impedito controllo sui dati personali all'interessato
- danni fisici, materiali o immateriali alle persone fisiche.

REGISTRO DEI DATA BREACH

Evento				Conseguenze	Provvedimenti adottati	Notifica all'autorità di controllo		Comunicazione all'interessato	
Codice[4]	Falso Positivo	Irrilevante	Rilevante			SI/NO	Data	SI/NO	Data

[4] Inserire codice scheda evento

MODELLO DI COMUNICAZIONE AGLI INTERESSATI DELLA VIOLAZIONE DEI DATI

G.mo Utente,

Secondo quanto prescritto dall'art. 34 del Regolamento Generale in materia di protezione dei dati personali RE (UE) 679/2016, L'Ente _____, titolare del trattamento, con la presente è a comunicarLe, l'intervenuta violazione dei Suoi dati personali (data breach) che si è verificata in data _____[5], alle ore_____;[6] data_____alle ore_____;

NATURA DELLA VIOLAZIONE

_____

_____

_____

TIPO DI VIOLAZIONE:

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ _____

DISPOSITIVO OGGETTO DI VIOLAZIONE:

- ☐ Computer,
- ☐ Rete,
- ☐ Dispositivo mobile
- ☐ Strumento di backup
- ☐ Documento cartaceo
- ☐ _____

[5] A. Tra il __e il____
B. In un tempo non ancora determinato
C. È possibile che sia ancora in corso

[6] Indicare l'ora se nota, altrimenti indicare l'ora in cui si viene a conoscenza della violazione.

CHE TIPO DI DATI SONO OGGETTO DI VIOLAZIONE PER ESEMPIO:

- ☐ Dati anagrafici (nome, cognome, numero di telefono, e mail, CF, indirizzo ecc..)
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica
- ☐ Dati personali idonei a rivelare le convinzioni religiose
- ☐ Dati personali idonei a rivelare filosofiche o di altro genere
- ☐ Dati personali idonei a rivelare le opinioni politiche
- ☐ Dati personali idonei a rivelare l'adesione a partiti
- ☐ Dati personali idonei a rivelare sindacati,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere religioso,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere filosofico,
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere politico
- ☐ Dati personali idonei a rivelare associazioni od organizzazioni a carattere sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute
- ☐ Dati personali idonei a rivelare la vita sessuale
- ☐ Dati giudiziari
- ☐ Dati genetici
- ☐ Dati biometrici
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ _____

NOME E DEI DATI DI CONTATTO DEL DPO O UN ALTRO PUNTO DI CONTATTO PRESSO CUI OTTENERE PIÙ INFORMAZIONI:

_____

_____

DESCRIZIONE DELLE PROBABILI CONSEGUENZE DELLA VIOLAZIONE

_____

_____

_____

DESCRIZIONE DELLE MISURE ADOTTATE O DI CUI SI PROPONE L'ADOZIONE PER PORRE RIMEDIO ALLA VIOLAZIONE DEI DATI PERSONALI[7]

_____

_____

_____

Scusandoci per quanto avvenuto rimaniamo a Sua disposizione per eventuali chiarimenti.

Firma Ente

[7] e anche, se del caso, per attenuarne i possibili effetti negativi