SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Ospedaliero - Universitaria di Ferrara

Università degli Studi di Ferrara

Linee Guida per la gestione dei casi di Violazione dei dati personali (c.d. Data Breach)

Sommario

1. Premessa.

L'art. 33 del RGPD prevede che:

> *In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente [...] 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*

La violazione dei dati personali (in inglese: "*data breach*") è un evento in conseguenza del quale si verifica, appunto, una violazione di sicurezza che comporta, o può comportare, accidentalmente o illecitamente, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Secondo le Linee guida WP250 adottate dal Gruppo di Lavoro ex Articolo 29, , costituisce una "violazione dei dati personali", a mero titolo esemplificativo, l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati, il furto o la perdita di dispositivi informatici contenenti dati personali, la deliberata alterazione di dati personali, l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni (virus, malware, ecc.), la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità o la divulgazione non autorizzata dei dati.

Secondo le medesime Linee guida, le violazioni di sicurezza possono essere classificate in tre macro-categorie:

- "violazioni della **riservatezza**", in caso di accesso accidentale o abusivo a dati personali o divulgazione degli stessi;
- "violazioni dell'**integrità**", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazioni della **disponibilità**", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

L'Allegato B delle predette Linee guida contiene alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella valutazione sulla necessità di effettuare o meno la notifica di *data breach* all'Autorità Garante.

Il Garante per la Protezione dei Dati Personali, con provvedimento 27 maggio 2021 n. 209 emesso ai sensi dell'art. 57, par. 1, lett. d) del RGPD, modificando il contenuto e le modalità della notifica della violazione dei dati personali fino all'epoca vigente, che prevedeva l'invio a mezzo PEC di apposita modulistica , ha adottato un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, attraverso la quale, dal 1° luglio 2021, i titolari del trattamento sono tenuti a fornire all'Autorità le informazioni ivi richieste.

La predetta procedura prevede, in particolare, che debba procedere alla compilazione e all'invio del *form* on line il legale rappresentante del titolare del trattamento o anche uno o più delegati del medesimo legale rappresentante.

A tal fine, il Direttore Generale dell'Azienda conferisce delega al Direttore dell'U.O. Interaziendale Affari Generali (cfr. art. 20, comma 1, Regolamento per il trattamento dei dati personali dell'Azienda Ospedaliero - Universitaria di Ferrara) il quale potrà a sua volta subdelegare detto potere.

Il presente documento viene elaborato sulla base delle normative di seguito tenute in considerazione:

- Regolamento (UE) 2016/679 del Parlamento Europeo 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 (Regolamento generale sulla protezione dei dati), in particolare gli articoli 33 (Notifica all'Autorità di Controllo), 34 (notifica agli interessati) e 28 (Responsabile del trattamento), **di seguito anche denominato "RGPD"**.
- D.Lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali ((, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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", di **seguito anche denominato "Codice"**.
- D.Lgs. 7 marzo 2005, n. 82, recante Codice dell'Amministrazione Digitale, **di seguito anche denominato "CAD"**.

- Linee guida in materia di notifica delle violazioni di dati personali - WP250 rev.01, adottate il 3 ottobre 2017 Versione emendata e adottata in data 6 febbraio 2018, **di seguito anche denominate "Linee Guida 2018"**;
- Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021, ver. 1.0, di seguito anche denominate "**Linee Guida 2021**"
- Provvedimento n. 393 del 2 luglio 2015 del Garante per la Protezione dei Dati Personali recante "**Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche**", pubblicato in Gazzetta Ufficiale n. *179 del 4 agosto 2015*.
- Provvedimento n. 157 del 30 luglio 2019 del Garante per la Protezione dei Dati Personali sulla notifica delle violazioni dei dati personali (*data breach*).
- Provvedimento n. 209 del 27 maggio 2021 del Garante per la Protezione dei Dati Personali, in cui sono descritte le funzionalità e i flussi della nuova procedura telematica adottata per la notifica della violazione dei dati personali, effettuate ai sensi dell'art. 33 del RGPD.

2. Definizioni.

Ai fini delle presenti Linee Guida si applicano le definizioni di cui all'art. 2 del Regolamento Aziendale, e le seguenti:

- **REGOLAMENTO AZIENDALE**: il Regolamento per il Trattamento dei dati personali dell'Azienda Ospedaliero – Universitaria di Ferrara.
- **ICT**: Servizio Comune ICT;
- **INGEGNERIA CLINICA**: Servizio Comune di Ingegneria Clinica.
- **DIRETTORE COMPETENTE:** Direttore dell'U.O. Interaziendale Affari Generali.

3. Gestione della violazione.

In caso di accertamento di violazione occorre procedere, nell'ordine, ai seguenti adempimenti:

1. Fase di acquisizione o comunicazione della notizia dell'evento che si sospetta costituisca *"data breach"*;
2. Fase istruttoria finalizzata all'acquisizione delle informazioni necessarie per gli adempimenti successivi;
3. Fase dell'analisi tecnica dell'evento comunicato;
4. Fase dell'individuazione e implementazione delle misure finalizzate al contenimento del danno, laddove possibile;
5. Fase di valutazione della gravità dell'evento e dell'eventuale esclusione dell'obbligo di procedere alla notifica al Garante;
6. Fase di notifica al Garante per la protezione dei dati, se necessario (art. 33 del RGPD);
7. Fase delle altre segnalazioni dovute;
8. Fase di comunicazione agli interessati, se necessario (art. 34 del RGPD);
9. Fase di registrazione dell'evento nel Registro delle Violazioni;
10. Fase delle azioni correttive.

4. Acquisizione e/o comunicazione della notizia dell'evento.

Avviso al Referente Privacy: ogni soggetto autorizzato al trattamento, qualora venga a conoscenza di eventi, fatti o comportamenti, propri o altrui, che rappresentino un potenziale caso di *data breach*, **è tenuto ad avvisare tempestivamente il Referente Interno della struttura a cui afferisce**.

Inoltro della notizia del Data Breach: Il **Referente, valutato l'evento, lo segnala,** descrivendo sommariamente l'evento, alla casella data-breach@ospfe.it, che garantisce l'inoltro contemporaneo della segnalazione sia al Direttore Competente sia al DPO. In mancanza o in caso di indisponibilità del Referente Interno l'evento può essere segnalato anche direttamente dal soggetto autorizzato.

Il Direttore Competente, ricevuta la notizia dell'avvenuta violazione nelle modalità di cui sopra o attraverso qualsiasi altra fonte (ad es. dal DPO, dalla stampa, direttamente in esito alla segnalazione di un interessato, ecc.) procede con le fasi successive, descritte ai successivi paragrafi (6 e seguenti).

5. Gestione della violazione dei dati esterno alla struttura.

L'articolo 33, par. 2, RGPD prevede che:

> "*Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione*."

Al fine di fornire al Responsabile le istruzioni per la corretta e regolare comunicazione al titolare delle violazioni di dati, nell'atto di designazione a Responsabile del trattamento previsto dall'articolo 3 del Regolamento Aziendale sono allegate le presenti Linee Guida o, comunque, alle stesse deve essere fatto rinvio, anche mediante indicazione del link del sito internet aziendale ove sono pubblicate.

Il Responsabile del trattamento che venga a conoscenza di un potenziale caso di violazione dei dati è tenuto ad avvisare immediatamente, e comunque entro 12 ore, il **Direttore Competente** all'indirizzo email dedicato (data-breach@ospfe.it), indicando nell'oggetto "*DATA BREACH del xx/xx/xxxx*" e inviando contestualmente il modello di cui all'Allegato 2 già compilato.

Da questo momento dovranno essere eseguite le medesime operazioni della procedura illustrata nei paragrafi seguenti.

6. Istruttoria.

Il Direttore Competente, anche tramite delegato, ricevuta la notizia di una ipotesi di violazione dei dati, provvede a svolgere l'istruttoria necessaria alla comprensione dell'ipotesi di *data breach*, allo scopo di

- valutare la necessità di procedere alla notifica al Garante;
- valutare la necessità di procedere alla comunicazione agli interessati;
- individuare eventuali azioni correttive e/o di miglioramento necessarie;
- conoscere tutti gli elementi previsti dagli articoli 33 e 34 RGPD e/o di tutti gli elementi che, nel caso, dovranno essere oggetto di notificazione al Garante, di comunicazione agli interessati e/o di Registrazione.

Tale istruttoria potrà essere svolta chiedendo informazioni al Referente Interno, direttamente al soggetto autorizzato, o a chiunque altro sia a conoscenza dei fatti comunicati. Le informazioni potranno essere acquisite chiedendo a detti soggetti la compilazione del modulo di cui all'Allegato 2 in formato editabile oppure chiedendo ai medesimi soggetti, anche per le vie brevi, specifiche informazioni e/o chiarimenti nonché la trasmissione di eventuali documenti ritenuti necessari ai predetti fini.

Alla luce del disposto di cui all'art. 33 par. 4 del RGPD, secondo cui,

> "*[q]ualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.*"

si avrà cura di raccogliere il maggior numero di informazioni e, laddove le stesse non siano ritenute esaustive, il Direttore Competente è tenuto a procedere alla c.d. notifica per fasi.

All'esito della Fase istruttoria il Direttore Competente comunica al DPO (all'indirizzo email dpo@ospfe.it) le risultanze dell'istruttoria stessa, al fine di ottenere la sua consulenza sulla qualificazione dell'evento come *data breach* e sulle determinazioni di cui alle Fasi di seguito descritte.

7. Analisi tecnica dell'evento.

Laddove il Data Breach derivi da una violazione di natura tecnologica, il Direttore Competente trasmette la segnalazione dell'evento, unitamente all'istruttoria fino a quel momento compiuta, al Direttore ICT e/o al Direttore Ingegneria Clinica, secondo le rispettive competenze.

I predetti Direttori svolgeranno l'analisi tecnica dell'evento, svolgendo essi stessi l'istruttoria di cui alla Fase istruttoria (par. 6), nonché delle azioni da mettere in atto tempestivamente allo scopo di contenere il danno, anche avvalendosi della consulenza del DPO.

Gli stessi, inoltre, collaboreranno con il Direttore Competente, o con suo delegato, se ritenuto necessario, per la compilazione del modulo di cui all'Allegato 2. In particolare, una volta qualificato l'evento segnalato come una violazione dei dati personali, verranno raccolti tutti gli elementi utili ai fini della notifica al Garante, anche mediante compilazione, da parte del Direttore ICT e/o del Direttore Ingegneria Clinica, per le parti di competenza, del modello di cui all'Allegato 2.

8. Individuazione e implementazione delle misure finalizzate al contenimento del danno.

Nel caso in cui sia stato valutato che le misure implementate siano insufficienti alla tutela degli interessati, il Direttore Competente, sentito il DPO e, se necessario alla luce della natura del Data Breach, i Direttori ICT o INGEGNERIA CLINICA, secondo le rispettive competenze, provvede a identificare le possibili azioni correttive da implementare, selezionandole tra quelle di cui sia valutata la fattibilità immediata e il miglior esito ai fini della minimizzazione del possibile danno agli interessati.

9. Fase di valutazione della gravità dell'evento.

L'art. 33 RGPD chiarisce che la notifica all'Autorità Garante può non essere fatta

> "*ove sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.*"

Pertanto, nella fase di valutazione, sulla base delle informazioni acquisite, occorre innanzitutto stabilire, avvalendosi della consulenza del DPO, espressa anche per le vie brevi:

- se l'evento è astrattamente inquadrabile in una ipotesi di *data breach* (ad es. se nell'incidente sono effettivamente coinvolti i dati personali);
- in caso affermativo, in quale delle tre ipotesi di violazione rientra l'evento segnalato.

In esito alla predetta valutazione il Direttore Competente deve valutare, avvalendosi della consulenza del DPO, espressa anche per le vie brevi, l'impatto sugli interessati.

Se si tratta di una **violazione di riservatezza** occorre verificare che le misure di sicurezza (es.: cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note) nonché se l'ipotesi del Data Breach rientra o sia analogo ad uno dei casi esemplificati nelle Linee Guida 2021.

In caso di perdita di **violazione di integrità** o di **violazione di disponibilità** di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.

Se, dalle predette valutazioni, emerge che:

- in caso di **violazione della riservatezza**, le misure di sicurezza precedenti il Data Breach impediscono o rendono altamente improbabile l'effettivo accesso ai dati da parte di terzi oppure,
- in caso di **violazione dell'integrità** o della **disponibilità**, è possibile il recupero dei dati in tempi ragionevoli, entro i quali gli interessati non subiscono alcun pregiudizio, o comunque sono stati violati dati che non sono di alcun interesse per gli interessati stessi, oppure
- in ogni caso, laddove il Data Breach rientra in uno dei casi, o è analogo ad uno dei casi per i quali le Linee Guida 2021 prevedono che non sia necessari la Notifica e la Comunicazione,

la procedura può terminare, e si potrà passare alle Fasi di cui ai successivi paragrafi 12, 13 e 14.

Se la valutazione si conclude con evidenza di un caso di violazione dei dati e/o con l'evidenza della necessità di procedere alla Notifica, si procede con la Fase della Notifica al Garante (paragrafo 10).

10. Notifica all'Autorità Garante e casi di esclusione.

Notifica al Garante. In esito alla Fase dell'istruttoria e della Fase della Valutazione il Direttore Competente, o suo delegato, anche avvalendosi della consulenza del DPO, procede alla notifica al Garante attraverso il portale messo a disposizione dalla medesima autorità (https://servizi.gpdp.it/databreach/s/scelta-auth), seguendo le istruzioni ivi presenti, **entro 72 ore dalla ricezione della email del Referente Interno, del Responsabile del Trattamento o, comunque, dalla conoscenza**, comunque avvenuta, dalla violazione dei dati.

Nel caso in cui la notifica venga eseguita oltre il termine delle 72 ore il Direttore Competente è tenuto a indicare, nell'apposito campo, le specifiche ragioni del ritardo.

Resta ferma la possibilità di procedere con la c.d. **Notifica per fasi**, quindi, nella procedura informatica del Garante, spuntando la casella "Notifica Preliminare" e fornendo successivamente le informazioni aggiuntive o dettagli rilevanti sulla violazione all'esito della ricezione in epoca successiva alla notifica preliminare delle informazioni richieste.

La notifica effettuata dovrà contenere, oltre alle altre informazioni richieste dalla procedura del Garante, i seguenti elementi:

1. 'indicazione del nominativo del Direttore Competente, con i relativi dati di contatto diretti;
2. l'indicazione del numero di protocollo della comunicazione al Garante del nominativo del DPO lo stesso (allo stato: **20180048881**).

Protocollazione della notifica. In esito alla notifica, e alla ricezione della comunicazione di protocollazione da parte del Garante, il Delegato alla notifica provvederà a trasmettere al DPO, attraverso il Sistema di Protocollo Aziendale, l'atto Notificato (ovvero il file sottoscritto digitalmente e uploadato nel portale del Garante), da inserire come atto principale, e, in allegato, le due Email ricevute in esito alla notifica dall'Ufficio del Garante, attestanti:

- la ricezione della Notifica da parte del Garante (Email con oggetto "**Notifica di violazione dei dati personali - Ricezione notifica completa - Fascicolo xxxxxxxx - Protocollo xxxxxxx**");
- il PIN dell'atto di Notifica attribuito dal Garante (Email con oggetto "**Notifica di violazione dei dati personali - Invio PIN - Fascicolo xxxxxxxx**").

I medesimi atti dovranno essere conservati in una cartella condivisa nel cloud aziendale tra il Direttore Competente, e suo delegato, e il DPO, al fine delle successive ed eventuali attività, anche di riscontro ad eventuali richieste di chiarimenti da parte del Garante.

11. Altre segnalazioni dovute.

Fermo restando l'eventuale **obbligo di riferire all'autorità giudiziaria casi che costituiscano ipotesi di reato procedibili di ufficio**, nonché di informare il Direttore Generale laddove l'evento costituisca ipotesi di reato procedibile a querela, il **Direttore Competente**, ricevuta la comunicazione di cui al precedente paragrafo 7, ne dà notizia al Direttore competente a procedere, a mero titolo esemplificativo alle notifiche:

- CSIRT (in caso di incidenti di sicurezza NIS, ai sensi degli articoli 12 e 14 del D.Lgs. 18 maggio 2018, n. 65 recante Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione;
- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Gestore di Identità Digitale e AGID nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

In tale caso il Direttore che vi provveda dovrà darne notizia al Direttore Generale, e per conoscenza al DPO, anche ai fini della registrazione di cui al successivo paragrafo 11, allegando copia dell'atto inviato.

12. Comunicazione agli interessati.

Nei casi previsti dall'art. 34 del Regolamento, il Dirigente Competente è tenuto a comunicare gli interessati la violazione dei dati secondo le procedure previste della predetta norma.

Il predetto art. 34, tuttavia, prevede che la Comunicazione è necessaria

> "[q]*uando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche*"

Nel caso risulti, pertanto, che la violazione è suscettibile di presentare tale rischi, il **Direttore Competente comunica la violazione all'interessato senza ingiustificato ritardo**.

Al fine di valutare la necessità di procedervi e, nel caso, il contenuto della comunicazione e le modalità per la comunicazione stessa, il **Dirigente Competente si avvale della consulenza del DPO**.

A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti sulla base dei criteri di cui ai considerando n. 74 del Regolamento e, comunque, sulla base delle indicazioni contenute nelle Linee Guida 2018 e nelle Linee Guida 2021, in particolare valutando se il Data Breach rientra in uno dei casi esemplificati in tali ultime Linee Guida (o se è analogo a uno di essi) e, nel caso, applicando gli stessi criteri suggeriti dal EDPB.

Se il rischio è grave occorre valutare la possibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web aziendale, quotidiani, radio, tv), le

misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi e le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida.

La forma di comunicazione prescelta verrà predisposta e curata dal Dirigente Competente, sulla base delle indicazioni fornite dal DPO.

Si segnala l'opportunità che il Direttore Compente valuti se:

- sono erano state poste in essere, prima della violazione, misure tecniche e organizzative adeguate di protezione;
- successivamente al data breach sono state adottate misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al par. 1;
- se detta comunicazione richiederebbe sforzi sproporzionati. In tal caso si procederà a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

In tali casi la comunicazione agli interessati, infatti, non è obbligatoria.

13. Inserimento dell'evento nel Registro delle Violazioni.

L'art. 33, par. 5, del RGDP prevede che:

> "[i]*l 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.*"

Al fine di consentire il rispetto di tale norma, l'evento che viene ritenuto costituire ipotesi di violazione dei dati, anche laddove non sia seguita la Notifica o la Comunicazione, deve essere annotata, a cura del Direttore Competente, o di suo delegato, nel Registro delle Violazioni compilando, in particolare, tutti i campi previsti dal Registro istituito.

Sino all'eventuale attivazione di un Registro delle Violazioni web-based, il Registro è conservato in forma elettronica dal Direttore Competente nella cartella condivisa tramite cloud aziendale con il DPO.

Al fine di consentire al Titolare e al DPO di valutare e/o suggerire eventuali interventi correttivi sui trattamenti svolti, il **Direttore Competente trasmette copia elettronica del Registro medesimo al Direttore Generale e al DPO, tramite il Sistema di Protocollo Aziendale, entro il 15 dicembre di ogni anno (v. art. 20, comma 2, del** REGOLAMENTO AZIENDALE**)**.

14. Miglioramento.

La gestione del Data Breach non costituisce unicamente un insieme di attività di tipo reattivo rispetto ad eventi potenzialmente dannosi, ma anche di tipo proattivo.

La gestione dei casi di Data Breach occorsi nel passato rappresentano la base per indirizzare nella maniera più efficace possibile il trattamento di violazioni future.

A valle della risoluzione della violazione dei dati personali, il Direttore Competente, unitamente al DPO e, se di competenza, ai Direttori ICT e Ingegneria Clinica, conducono una analisi della singola violazione, per individuare i fattori che ne hanno determinato l'accadimento, in particolare considerando i seguenti elementi:

- numero totale di segnalazioni/rilevazioni strumentali riconducibili all'evento occorso;

- comunicazioni da più referenti della stessa rispondenza di violazione, anche in tempi diversi;
- anomalie riscontrate da altri strumenti di monitoraggio, da considerare in aggiunta alla rilevazione dell'evento;

- momento esatto dell'accadimento della violazione, ovvero se riconducibile ad altra evidenza antecedente rispetto alla segnalazione/rilevazione;
- eventuale vulnerabilità sfruttata;
- verifica della presenza dei controlli preventivi necessari ed efficacia di quelli effettivamente implementati, tra qui analisi log, opportuna configurazione apparati di protezione, hardening dei sistemi, patching dei sistemi, attuazione corretta delle istruzioni operative;
- dettaglio ex-post della tipologia di dati coinvolti e dei sistemi/infrastrutture tecnologiche impattati;
- eventuali azioni inibitorie alle attività di contrasto o alla loro tempestività, tra cui l'eventuale indisponibilità temporanea o permanente delle risorse tecnologiche per il contenimento e/o impedimenti di natura organizzativa;
- indicazione della codifica di eventuali eventi pregressi con analoghe caratteristiche (e.g. data/ora accadimento, sistema/piattaforma target).

Il Direttore Competente, anche su indicazione del DPO, verificate le risultanze della attività di cui sopra, indirizza le azioni di natura correttiva/evolutiva del singolo evento, atte a:

- ottimizzare e velocizzare la gestione di occorrenze di eventi e violazioni di dati personali future;
- migliorare la gestione dei Data Breach;
- affinare i sistemi di rilevazione e segnalazione eventi;
- migliorare i processi atti a proteggere i dati personali (e.g. nuovi controlli correttivi e/o preventivi, ridefinizione processi e procedure, ridefinizione istruzioni operative, definizione piani di formazione, eventuale revisione della presente procedura e di eventuali altri documenti collegati [es. analisi del rischio, misure di sicurezza, disciplinare SIA, regolamento aziendale sul trattamento dei dati, istruzioni operative in materia di protezione dei dati, ecc..]);
- individuare controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi;
- revisionare le relazioni con Clienti e Fornitori.

In aggiunta alla predetta verifica, il Direttore Competente e/o il DPO, congiuntamente o singolarmente e, comunque, se di competenza, unitamente al Direttore ICT e al Direttore Ingegneria Clinica, entro il 30 aprile di ogni anno, procedono all'analisi dei Data Breaches verificatisi nell'anno precedente mediante analisi del Registro delle Violazioni e, in esito, procedono alle valutazioni e agli atti di cui ai capoversi precedenti.

Allegato 1 – Esempi di casi di Data Breach.

Tipo di Breach	Definizione	Estensione minima/Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	**Caratteristiche:** Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente Incendio di archivio cartaceo delle cartelle cliniche. Distruzione di campioni biologici	Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) Rottura di un PC che non contiene dati personali originali (in unica copia) Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	**Caratteristiche:** Dati non recuperabili o provenienti da procedure non ripetibili Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla	Smarrimento di chiavetta USB contenente dati originali Smarrimento di fascicolo cartaceo personale dipendente	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

		perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione		
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	**Caratteristiche:** Modifiche sistematiche su più casi. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup Azione involontaria o fraudolenta, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile	Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile Modifica di un documento non ancora validato dal proprio autore.
Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Malfunzionamento del sistema di oscuramento del sistema dipartimentale che invia a SOLE Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione. Invio di una email e/o di un file a soggetto diverso dal reale destinatario.	Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione ed invia a SOLE. Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet

				Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi Accesso non autorizzato di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	Infezione da ransonware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup Cancellazione accidentale dei dati da parte di una persona non autorizzata Perdita della chiave di decrittografia di dati crittografati in modo sicuro Irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento nev	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in cors

Il Data Breach per eccellenza, generalmente, è un attacco informatico, ma può consistere anche in un accesso abusivo, in un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).

Nella prassi esaminata dall'entrata in vigore del Regolamento nell'ambito delle Aziende Sanitarie italiane i casi più frequenti di *data breach* sono stati rappresentati

- dagli scambi di identità (per lo più determinati da casi di omonimia -stesso nome ma dati di nascita differenti- o, addirittura, omocodia -stesso codice fiscale-);
- dall'invio di comunicazioni (via email o via posta) a soggetti non legittimati (soggetti diversi dai reali destinatari).

I casi di data breach per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato data breach, ma è considerato un normale errore procedurale.

Allegato 2 – Modulo per l'acquisizione di informazioni sull'evento.

Notifica di una violazione dei dati personali

(art. 33 del Regolamento UE 2016/679)

Questo modulo, finalizzato a raccogliere informazioni per la notifica e la comunicazione di una violazione dei dati personali, deve essere utilizzato al solo fine di fornire al Responsabile della Protezione dei Dati (DPO) e/o al Direttore dell'U.O. Interaziendale Affari Generali le informazioni necessarie per valutare la violazione e, in particolare, per:

- valutare la necessità, o meno, di procedere alla notifica della violazione al Garante (art. 33 del RGPD);
- valutare la necessità, o meno, di procedere alla comunicazione della violazione agli interessati (art. 34 del RGPD);
- fornire al soggetto deputato le informazioni per la registrazione della violazione nel Registro delle Violazioni.

A tal fine si invita il Referente Interno a compilare le sezioni di seguito indicate in ogni sua parte.

La notifica verrà successivamente inoltrata al Garante, se necessario, a cura del predetto Direttore sulla base delle informazioni fornite. Si evidenzia che dette informazioni devono essere veritiere in quanto, ai sensi di legge, il soggetto che effettua la Notifica è responsabile penalmente in caso di falsità.

Si segnala che **nei campi liberi non ci sono limiti di caratteri: è però essenziale, per consentire la lettura del modulo, che lo stesso venga compilato informaticamente, e salvato in formato PDF** (non stampato in cartaceo e scansionato).

Si segnala che è possibile inviare al Garante ogni documento ritenuto opportuno ai fini della descrizione dei fatti. In tale caso si potranno inviare in allegato all'invio del presente modulo.

Si segnala che è essenziale e indispensabile che il presente modulo venga inviato in risposta all'email con la quale è stato ricevuto, così da mantenere il thread dell'evento.

Il modulo non può essere inoltrato al Garante in quanto, ai fini della notifica, può procedersi solo attraverso la procedura prevista e raggiungibile al link https://servizi.gpdp.it/databreach/s/scelta-auth.

Maggiori informazioni sono disponibili sul sito istituzionale del Garante Privacy (https://servizi.gpdp.it/databreach/s/) o, comunque, possono essere chieste rispondendo alla stessa email con la quale è stato ricevuto il presente modulo.

1. Struttura aziendale presso la quale è avvenuta la violazione

La compilazione di questa sezione è obbligatoria. In mancanza non è possibile per il Direttore Competente avere le informazioni utili per procedere alla notifica.

Indicare le informazioni relative alla struttura presso la quale è avvenuta la violazione (es. U.O. Urologia, Direzione delle Professioni, ecc.).

Si segnala che, in ogni caso, il soggetto notificante della violazione è sempre e comunque l'Azienda e, quindi, verrà indicata dal Direttore Competente alla Notifica.

Denominazione[1]

Telefono[2] E-mail3

Direttore[4] Recapiti Direttore[5]

Altro Soggetto Autorizzato informato sui fatti[6]

Recapiti di Altro Soggetto Autorizzato informato sui fatti[7]

2. Ulteriori soggetti coinvolti nel trattamento

La compilazione di questa sezione non è obbligatoria: potrebbero non esserci ulteriori soggetti coinvolti.

In questa sezione è necessario inserire i dati di **eventuali** altri soggetti coinvolti nel Data Breach (ad es. società informatiche che gestiscono la piattaforma dove è avvenuta la violazione, soggetto terzi che gestivano e/o trattavano dati per conto della Struttura indicata al punto 1, ecc..).

Denominazione[8]
Codice Fiscale[9]
CAP Comune[10]

---

[1] Indicare la struttura aziendale dove si è verificato il Data Breach;
[2] Indicare il numero di telefono presso il quale sia reperibile un soggetto che abbia informazioni utili ai fini del data breach. Non indicare un numero di telefono generico (tipo il centralino) ma il numero di un soggetto che potrebbe essere contattato dal Direttore Competente o direttamente dal DPO.
[3] Indicare come in nota 2.
[4] Indicare il Direttore della Struttura, che potrebbe essere contattato dal Direttore Competente sia direttamente dal DPO.
[5] Indicare i recapiti del Direttore, sia telefono sia email;
[6] Indicare il nominativo di chi è a conoscenza dell'evento verificatosi, che potrebbe essere contattato dal Direttore Competente sia direttamente dal DPO;
[7] Indicare i recapiti del predetto soggetto;
[8] Indicare il nominativo del "soggetto" (società, professionista esterno, ecc.) nell'ambito della quale, o attraverso il quale, è avvenuto il Data Breach.
[9] Indicare il codice fiscale del soggetto di cui alla nota precedente.

Indirizzo[11]

Telefono[12] E-mail13 PEC14

Legale Rappresentante[15]

Referente[16] Recapiti Referente17

3. Informazioni sulla violazione

In questa sezione è necessario fornire la maggior parte delle indicazioni necessarie per poter ricostruire quanto accaduto e le modalità in cui si è verificato il data breach.

3.1. Momento in cui è avvenuta la violazione

3.2. Modalità con la quale si è venuti a conoscenza della violazione

3.3. Momento si è venuti a conoscenza della violazione

Data ___ Ora

3.4. Motivi del ritardo[18]:

3.5. Descrizione della violazione[19]:

3.6. Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione[20]:

3.7. Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti[21]:

---

[10] Indicare il comune (non la frazione) in cui ha sede il soggetto indicato alla nota 8.

[11] Indicare la sede principale (non quella in cui è avvenuta la violazione) del soggetto indicato alla nota 8.

[12] Indicare il numero di telefono presso il quale sia reperibile un soggetto che abbia informazioni utili ai fini del Data Breach. Non indicare un numero di telefono generico (tipo il centralino) ma il numero di un soggetto che potrebbe essere contattato dal Direttore Competente e/o dal DPO

[13] Indicare come in nota 12.

[14] Indicare la PEC del soggetto indicato al punto 8, se esistente.

[15] Indicare cognome e nome del Legale Rappresentante del soggetto di cui alla nota 8, se noto.

[16] Indicare cognome e nome di una persona a conoscenza del Data Breach presso il soggetto di cui alla nota 8.

[17] Indicare i recapiti del soggetto di cui alla nota 16.

[18]Compilare solo se la data di cui al punto precedente è anteriore alle 72 ore.

[19]Descrivere analiticamente cosa è acceduto, ovvero come è avvenuto il Data Breach, dove, ad opera di chi, attraverso quali modalità.

[20]Paragrafo da compilare solo se trattasi di violazione di natura informatica. Nel caso, indicare specificamente il sistema informativo, il software, la piattaforma attraverso la quale è avvenuto il Data Breach.

[21]Indicare specificamente le misure che erano state adottate per evitare la violazione poi in realtà verificatasi. Se esistente, allegare la valutazione di impatto.

3.8. Categorie di interessati coinvolti nella violazione

3.9. Numero (anche approssimativo) di interessati coinvolti nella violazione:

3.10. Categorie di dati personali oggetto di violazione[22]:

3.11. Numero (anche approssimativo) di registrazioni[23] dei dati personali oggetto di violazione

4. Misure adottate a seguito della violazione

4.1. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per porre rimedio alla violazione e attenuarne i possibili effetti negativi per gli interessati[24]:

4.2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future[25] (c.d. azioni di miglioramento):

5. Comunicazione della violazione agli interessati

Si evidenzia che, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Azienda è tendenzialmente tenuta a comunicare la violazione agli interessati coinvolti.

Di seguito vengono richieste le informazioni necessarie per valutare se ed in che misura sia da ritenersi necessaria la comunicazione agli interessati e, nel caso, per poter procedere alla Comunicazione.

5.1. Con riferimento alla specifica violazione e al trattamento svolto:

5.1.1. La struttura, **prima** del verificarsi del *Data Breach* in analisi, aveva messo in atto misure tecniche e/o organizzative che rendevano i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi (es. cifratura dell'HD, criptazione dei dati, ecc.)?

In caso di risposta affermativa, indicare quali misure erano state applicate:

5.1.2. La struttura, **dopo** il verificarsi del *data breach*, ha applicato misure finalizzate a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati (con riferimento, quindi, agli specifici dati oggetto del *data breach*)?

---

[22]Laddove la violazione abbia ad oggetto dati personali distinti per interessato, nel campo libero descrivere nel dettaglio le categorie di dati personali e distinguerli per ciascuna categoria di interessati.

[23]Ad esempio, numero di moduli compilati, fatture, ordini, referti, immagini, record di un database o numero di transazioni.

[24]In questo paragrafo è necessario evidenziare cosa si è fatto per tentare di porre rimedio a quanto accaduto o per mitigare il danno subito o subendo dalla violazione, sia per la Struttura sia per le persone I cui dati sono stati violati. Si segnala che, in ogni caso, eventuali indicazioni potranno essere suggerite anche dal Direttore Competente e/o dal DPO.

[25]In questo paragrafo è necessario evidenziare quali misure di sicurezza verranno adottate, in futuro, per evitare che si verifichino nuovamente eventi simili e/o di cui si ritiene opportuno proporre l'adozione. Si segnala che, in ogni caso, eventuali misure potranno essere suggerite anche dal Direttore Competente e/o dal DPO.

In caso di risposta affermativa, indicare quali misure sono state applicate:

6. Altre informazioni

6.1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[26]?

In caso di risposta affermativa, indicare l'autorità alla quale è stata fatta la notifica e la norma di riferimento:

6.2. È stata effettuata la segnalazione[27] all'autorità giudiziaria o di polizia?

[26] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

[27] Denuncia, Esposto, Querela. Nel caso sia stata fatta è necessario allegarne copia.