SOMMARIO

STATO	DATA	FIRMA
Verificato	06.02.2023	Dott.ssa Rita La Cioppa
Approvato	09.02.2023	Dott.ssa Chiara Gibertoni
Approvato	07.02.2023	Dott.ssa Federica Banorri
Approvato	08.02.2023	Ing. Luca Capitani
Data di applicazione: 13.02.2023		

1. OGGETTO E SCOPO

Il documento descrive il percorso aziendale per la **notifica di violazione dei dati personali** all'Autorità di controllo (art. 33 del GDPR) e **comunicazione della violazione dei dati personali** all'interessato (art. 34 del GDPR), nonché i casi non oggetto di notifica all'Autorità di controllo, ma comunque annotati nel *Registro delle Violazioni.*
Scopo del documento è garantire la sicurezza dei dati personali.

2. CAMPO DI APPLICAZIONE

La presente procedura si applica all'interno della IRCCS AOSP Policinico S. Orsola di Bologna nei casi in cui si verifica una "violazione dei dati personali".

3. RESPONSABILITA'

Gli aggiornamenti e le revisioni periodiche sono di responsabilità del Responsabile della Funzione Privacy e del Responsabile ICT, previo parere del DPO.
Le responsabilità delle attività specifiche sono descritte nella procedura.
Il documento è stato redatto dalla Funzione Privacy e dal Servizio ICT e validato da F. Filippini Data Protection Officer (DPO) dell'Azienda al fine di garantire la coerenza con quanto definito in ambito AVEC.

4. RIFERIMENTI NORMATIVI E DOCUMENTALI

- Decreto Legislativo del 10 agosto 2018 n. 101 "Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)";
- 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);
- Decreto Legislativo n. 196/2003 *e s.m.i* "Codice per la protezione dei dati personali";
- Linee guida in materia di notifica delle violazioni di dati personali (*Data Breach notification*) – WP 250, definite in base alle previsioni del Regolamento (UE) 2016/679;
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche – 2 luglio 2015;
- Decreto Legislativo n. 82/2005 "Codice dell'Amministrazione Digitale (CAD)" artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale);
- Decreto del 9 gennaio 2008 del Ministero degli Interni in attuazione della Legge 155/2005 sulle infrastrutture critiche;
- Decreto del Presidente del Consiglio dei Ministri 1 aprile 2008 "Regole tecniche e di sicurezza per il funzionamento del Sistema pubblico di connettività" previste dall'articolo 71, comma 1-bis del Decreto Legislativo del 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale". G.U. 21 giugno 2008, n. 144;
- Art. 13 del DPCM del 24 ottobre 2014 "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese (G.U. Serie Generale n. 285 del 09/12/2014);

- *Provvedimento del Garante per la protezione dei dati personali n. 209 del 27 /05/2021 "Procedura telematica per la notifica di violazioni di dati personali (Data Breach)".*

5. DEFINIZIONI

- **Autorizzato al trattamento**: la persona fisica, espressamente designata, che opera sotto l'autorità del Titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali (art. 4, punto 10 *del GDPR*).
- **Coordinatore del GAP**: il Dirigente aziendale deputato a coordinare le attività, gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali.
- **Data Protection Officer**: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39 *del GDPR*).
- **Gruppo Aziendale Privacy (GAP)**: il gruppo di professionisti individuato dal Titolare con il compito di presidiare a livello aziendale gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali.
- ***Interessato**: È la persona fisica identificata o identificabile a cui si riferiscono i dati personali. 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, i 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.*
- **Referente privacy**: la persona fisica che, secondo l'organizzazione aziendale, ricopre un ruolo gestionale e di responsabilità all'interno dell'azienda sanitaria che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.
- **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 (art. 4, punto 8 *del GDPR*).
- **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 (art. 4, punto 7 *del GDPR*). In questo contesto, sono titolari del trattamento le Aziende Sanitarie afferenti ad AVEC.
- **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 (art. 4, punto 2 *del GDPR*).

6. CONTENUTO

6.1 DATA BREACH

L'art. 33 del GDPR recita che: "In caso di violazione dei dati personali, il Titolare del trattamento notifica la violazione all'Autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'Autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Per "**Data Breach**" si intende un evento in conseguenza del quale si verifica una "violazione dei dati personali". Nello specifico, l'articolo 4 p.12 del GDPR definisce la violazione dei dati personali come 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.
Le Linee guida in materia di notifica delle violazioni di dati personali (*Data Breach notification*) - WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione come di seguito riportata. Le violazioni possono essere classificate in base ai seguenti tre principi ben noti della sicurezza delle informazioni:

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

6.2 GESTIONE DEL DATA BREACH

In caso di accertamento di violazione che rientra nella definizione di Data Breach, *occorre seguire le seguenti fasi del processo* di notificazione:

1. acquisizione della notizia da parte dei soggetti preposti al ricevimento/raccolta della violazione (di seguito indicati) che provvederanno ad attivare i passi successivi;
2. analisi tecnica dell'evento, contenimento del danno, valutazione della gravità dell'evento (*istruttoria*);
3. *eventuale* notifica al Garante Privacy;
4. *eventuali* altre segnalazioni dovute;
5. comunicazione agli interessati, dove necessario;
6. inserimento dell'evento nel Registro delle Violazioni;
7. azioni correttive specifiche.

6.3 GESTIONE DEL DATA BREACH DA PARTE DEL TITOLARE DEL TRATTAMENTO

Ogni operatore aziendale autorizzato a trattare dati (personale autorizzato), qualora venga a conoscenza di un potenziale caso di Data Breach, anche tramite segnalazioni esterne dei cittadini, **deve avvisare tempestivamente** il Referente privacy della struttura a cui afferisce. Quest'ultimo, valutato l'evento, se confermate le valutazioni di potenziale Data Breach, lo segnala tempestivamente *al Coordinatore del Gruppo Aziendale Privacy / Responsabile della Funzione Privacy (tramite e-mail al seguente indirizzo: ufficio.privacy@aosp.bo.it)*.
A tal fine *va* utilizzato il report di *sintesi allegato al presente documento (**R01-IOA98** "REPORT PER LA COMUNICAZIONE INTERNA/NOTIFICA DI UN DATA BREACH").* Se è il referente privacy a venire direttamente a conoscenza del potenziale caso di data breach la procedura di comunicazione da seguire è la medesima.
Il Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy effettua una prima valutazione dell'evento, avvalendosi dei componenti del Gruppo Aziendale Privacy competenti alla trattazione del caso specifico e di eventuali altre professionalità necessarie per la corretta analisi del caso e comunica l'esito dell'analisi preliminare effettuata al DPO, al fine di avvalersi della sua consulenza.
Il Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy, completata l'istruttoria, avverte *inoltre* il Titolare del trattamento comunicandogli l'esito della valutazione, eseguita dal GAP in collaborazione con il DPO, al fine di metterlo a conoscenza del potenziale caso di Data Breach.
Il Titolare assume le proprie determinazioni, disponendo la necessità o meno di notifica.
Il DPO su delega del Titolare notifica la violazione all'Autorità Garante (secondo le modalità descritte nel paragrafo 6).

L'avvenuta notificazione al Garante viene documentata dal *Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy* nel Registro delle violazioni *(**R02-IOA98** "*REGISTRO *VIOLAZIONI")* dallo stesso curato e tenuto. Tale registro ha durata annuale, contiene tutte le segnalazioni ricevute e gestite durante l'anno ed entro il 31 dicembre deve essere chiuso. Entro il 31 gennaio dell'anno successivo il *Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy* provvede ad inviarlo al Titolare del trattamento ed al DPO con nota protocollata, ai fini della conservazione ai sensi di legge.

Si precisa che *tutte le violazioni compresi* i casi non ritenuti dal Titolare da notificare devono essere *comunque* documentati nel Registro *delle violazioni*.

6.4 GESTIONE DEL DATA BREACH DA PARTE DEL RESPONSABILE DEL TRATTAMENTO

Ogni qualvolta l'Azienda si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuta a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati.

A tal fine è necessario che la presente procedura di segnalazione di Data Breach sia resa nota a tutti i Responsabili del trattamento. *L'obiettivo è di fornire al Responsabile del trattamento la procedura e le istruzioni* per informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di Data Breach.

Pertanto il Responsabile del trattamento, qualora venga a conoscenza di un potenziale caso di Data Breach, deve avvisare, senza ingiustificato ritardo, e nel rispetto dei tempi previsti nell'atto di nomina/*accordo/convenzione/contratto,* il DPO all'indirizzo PEC: *dpo@pec.aosp.bo.it utilizzando il modulo allegato (**R03-IOA98** "REPORT RESPONSABILE DEL TRATTAMENTO PER LA COMUNICAZIONE DEL DATA BREACH").*

Il DPO inoltra *il modulo di segnalazione di Data Breach ricevuto al Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy* e da questo momento vengono *eseguite le medesime fasi* della procedura illustrata al punto 4.3 (attraverso la necessaria collaborazione del Responsabile del trattamento).

6.5 ANALISI TECNICA DELL'EVENTO E VALUTAZIONE DELLA GRAVITÀ DELL'EVENTO

Il Gruppo Aziendale Privacy, *sotto la supervisione del Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy,* è responsabile *sulla base delle rispettive competenze, in base alla tipologia della violazione*, dell'analisi tecnica dell'evento, delle azioni da mettere in atto tempestivamente per il contenimento del danno, avvalendosi della funzione consulenziale del DPO.

Si precisa che l'art. 33 paragrafo 4, GDPR recita "Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo". *Quindi è possibile effettuare la **notifica per fasi** nel caso in cui non si possiedono di tutti gli elementi necessari ad una notifica completa.*

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche.

Ne consegue che il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle Violazioni.

A questo proposito, i Garanti europei nelle loro linee guida, precisano che la mancata comunicazione può essere sanzionata, ma che nessuna sanzione è prevista nel caso di comunicazione incompleta o di comunicazione non necessaria.

Nell'esecuzione dell'istruttoria, sulla base delle informazioni acquisite, occorre innanzitutto stabilire se nell'incidente sono coinvolti i dati personali. In caso di risposta positiva occorre valutare l'impatto sugli interessati.

*Se si tratta di una **violazione di riservatezza** occorre verificare che le misure di sicurezza (ad es. cifratura dei dati) in vigore rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note).*

*In caso di **perdita di integrità o disponibilità** di dati occorre valutare se è possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati. Se in tale modo i rischi per gli interessati sono trascurabili, la procedura può terminare, dopo aver documentato il processo e le scelte operate: le misure messe in atto sono state adeguate alla minaccia. Se la valutazione si conclude con evidenza di un caso di Data Breach si procede con la notifica all'Autorità Garante.*
Per semplificare gli adempimenti previsti per i Titolari del trattamento, il Garante ha progettato e messo disposizione un apposito strumento di autovalutazione (self assessment) che consente di individuare le azioni da intraprendere a seguito di una violazione dei dati personali derivante da un incidente di sicurezza.

6.6 NOTIFICA ALL'AUTORITA' GARANTE

La notifica all'Autorità Garante, effettuata dal DPO su delega del Titolare , dal 01.07.2021 deve essere inviata tramite un'apposita procedura telematica, resa disponibile nel portale dei servizi online dell'Autorità, e raggiungibile all'indirizzo https://servizi.gpdp.it/databreach/s/
Nella stessa pagina è disponibile un fac-simile che permette di vedere in anteprima i contenuti che saranno comunicati al Garante. È opportuno non utilizzare il fac-simile per l'invio della notifica al Garante.

6.7 ALTRE SEGNALAZIONI DOVUTE

Il responsabile della Funzione Privacy e il DPO, con *l'eventuale* supporto dei componenti del Gruppo Aziendale Privacy, sulla base delle rispettive competenze, dovrà verificare la necessità di informare altri organi, consultandosi con gli Uffici aziendale competenti quali:

- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- Organi di Polizia (in caso di violazioni di dati conseguenza di comportamenti illeciti o fraudolenti);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Gestore di Identità Digitale e ad AGID nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).

All'esito delle valutazioni sarà cura del titolare o suo delegato procedere con le segnalazioni dovute.

6.8 COMUNICAZIONE AGLI INTERESSATI

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà ad informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.
La comunicazione agli interessati, secondo quanto previsto dal paragrafo n. 3 dell'art. 34 del GDPR, non è richiesta quando:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati *di cui al paragrafo 1*;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece ad una comunicazione pubblica o a una misurazione simile, tramite la quale gli interessati sono informati con analoga efficacia.

La comunicazione deve contenere, ai sensi dell'art. 34, le seguenti informazioni:

- il nome e i dati di contatto del DPO o di altro punto di contatto;
- la descrizione *delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento* per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Pertanto a valle della decisione di notificare l'Autorità Garante, il *Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy* e il DPO devono valutare se sia il caso di notificare anche gli interessati. A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti.
Se il rischio è grave occorre individuare, la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, 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 elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679.
La *modalità* di comunicazione *decisa* dal Titolare verrà *curata* dal DPO con la collaborazione del *Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy /U.O. Comunicazione Aziendale.*

6.9 INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

L'art. 33 paragrafo n. 5 del GPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.
Pertanto, il *Responsabile della Funzione Privacy* è responsabile *dell'inserimento di tutte le attività indicate sopra nel Registro delle violazioni (**R02-IOA98 "REGISTRO VIOLAZIONI"**)*, che devono essere documentate, tracciabili e in grado di fornire evidenza nelle sedi competenti.

6.10 MIGLIORAMENTO

Il Titolare, sulla base dell'analisi delle violazioni riportate nel Registro delle violazioni documenta una serie di azioni di miglioramento che a titolo di esempio si riporta di seguito:

- *individuazione di verifiche e audit mirati alla riduzione delle probabilità di violazione;*
- revisione del Sistema di Gestione della Privacy *(organigramma privacy);*
- *r*evisione delle relazioni con Clienti e Fornitori *(nomina Responsabile del trattamento);*
- revisione annuale della procedura di gestione *delle violazioni*

A supporto dell'esecuzione di valutazioni e semplificazioni delle fasi, l'Autorità Garante ha istituito una sezione dedicata (https://servizi.gpdp.it/databreach/s/) con gli strumenti da utilizzare (ad es. simulazione, ecc.) a cui è possibile fare riferimento.

7. ALLEGATI E MODULI UTILIZZABILI

R01/IOA98 *"REPORT PER LA COMUNICAZIONE INTERNA/NOTIFICA DI UN DATA BREACH"*
R02/IOA98 *"REGISTRO VIOLAZIONI"*
R03/IOA98*" REPORT RESPONSABILE DEL TRATTAMENTO PER LA COMUNICAZIONE DEL DATA BREACH"*