



FRONTESPIZIO DELIBERAZIONE

AOO: AS_BO66
REGISTRO: Deliberazione
NUMERO: 0000030
DATA: 31/01/2023 15:23
OGGETTO: Regolamento UE 2016/679 (art. 33 e 34). Approvazione della procedura per la gestione di eventi di violazione dei dati personali o data breach. AGGIORNAMENTO.

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Rossi Andrea in qualità di Direttore Generale
Con il parere favorevole di Neri Andrea - Direttore Sanitario
Con il parere favorevole di Donattini Maria Teresa - Direttore Amministrativo

Su proposta di Sabrina Fiorentini - UO SEGRETERIA GENERALE E AFFARI LEGALI che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [07-05]

DESTINATARI:

- Collegio sindacale
- DIREZIONE GENERALE
- DIREZIONE ATTIVITA' SOCIO SANITARIE
- DISTRETTO
- DIPARTIMENTO CURE PRIMARIE
- DIPARTIMENTO SALUTE MENTALE
- INFORMAZIONE E COMUNICAZIONE
- SERVIZIO PREVENZIONE E PROTEZIONE
- UO SEGRETERIA GENERALE E AFFARI LEGALI
- GOVERNO CLINICO
- FORMAZIONE
- UO AMMINISTRAZIONE DEI SERVIZI SANITARI OSPEDALIERI E TERRITORIALI
- Servizio Unico Metropolitan Amministrazione Giuridica del Personale - SUMAGP (SC)
- Servizio Unico Metropolitan Amministrazione Economica del Personale - SUMAEP (SC)
- PROGRAMMAZIONE E CONTROLLO DIREZIONALE
- MEDICINA LEGALE
- UO CONTABILITA' E FINANZA



L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.

Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.



- UO ECONOMATO E LOGISTICA
- UO PATRIMONIO E TECNOLOGIE IMPIANTISTICHE
- ATTIVITA' AMMINISTRATIVE TRASVERSALI DAT/DIREZIONE GENERALE
- DIREZIONE ASSISTENZA FARMACEUTICA
- DIREZIONE SANITARIA
- DIREZIONE AMMINISTRATIVA
- TECNOLOGIE SANITARIE E INFORMATICHE SANITARIE E DI RETE
- DIREZIONE INFERMIERISTICA E TECNICA
- DIREZIONE MEDICA DI PRESIDIO
- DIPARTIMENTO DI SANITA' PUBBLICA

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000030_2023_delibera_firmata.pdf	Donattini Maria Teresa; Fiorentini Sabrina; Neri Andrea; Rossi Andrea	B38CBB65BA25A9825E2C83B5460E871D 6C286350E52809A45BF22E2EACE501A6
DELI0000030_2023_Allegato1.pdf:		4BAB6AD310665C3A116B2708D8D4102C B0FC68C9E20897C3C178C13494F3D5C0
DELI0000030_2023_Allegato2.pdf:		C539F7F627A541761D34AE10D79268FA0 4677F8D162AAF0B26FCD24622C89A9E
DELI0000030_2023_Allegato3.pdf:		1B67D87AFE702C3122A25EE3D8B06DB2 6D20403B9B13D4FC2F3F9C27A8FF9B17
DELI0000030_2023_Allegato4.pdf:		CA3946EEB2D5B49CAA9E6CD1327988FF 8FDE9A4AB1C437115ED477A8886B7756



L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.

Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.



DELIBERAZIONE

OGGETTO: Regolamento UE 2016/679 (art. 33 e 34). Approvazione della procedura per la gestione di eventi di violazione dei dati personali o data breach. AGGIORNAMENTO.

IL DIRETTORE GENERALE

- Richiamata la deliberazione n. 102 del 15.05.2019 ad oggetto "Regolamento UE 2016/679 (art. 33 e 34). Approvazione della procedura per la gestione di eventi di violazione dei dati personali o data breach";

- richiamate altresì le deliberazioni dell'Azienda USL di Imola:

- n. 275 del 21/12/2018 ad oggetto: "Regolamento (UE) 2016/679. Definizione dell'organigramma aziendale: Referenti privacy (e relative funzioni), soggetti autorizzati al trattamento dei dati personali e gruppo aziendale privacy. Approvazione istruzioni operative generali", con la quale si sono ridefinite l'organizzazione dei profili di responsabilità, la gestione degli adempimenti connessi al trattamento dei dati e si è provveduto alla costituzione di un Gruppo Aziendale Privacy (GAP) e - in attuazione dell'art. 39 del GDPR ("Compiti del responsabile della protezione dei dati") richiamati funzioni e compiti del DPO;
- n. 285 del 31/12/2019 ad oggetto: "Adozione del documento "Linee guida per l'applicazione del Regolamento UE 2016/679 e del D. Lgs. 30.6.2003 n. 196";
- n. 241 del 30/11/2022 ad oggetto: "Regolamentazione dei rapporti tra il Data Protection Officer (DPO) ed i Coordinatori del Gruppo Aziendale Privacy (GAP). Aggiornamento".
- n. 24 del 24/01/2023 ad oggetto: "Procedura per la gestione dei diritti in materia di protezione dei dati personali dell'interessato ai sensi degli artt. 12-22 del Regolamento EU 2016/679 (GDPR). Aggiornamento";

- richiamata altresì la deliberazione n. 139 del 2.7.2021 "Preso d'atto della designazione del Responsabile della protezione dei dati, Dott.ssa Federica Filippini, ai sensi dell'art. 37 del Regolamento UE 2016/679";

- dato atto che il Capo IV del GDPR disciplina agli artt. 33 (Notifica di una violazione dei dati personali all'Autorità di controllo), 34 (Comunicazione di una violazione dei dati personali all'interessato) e 28 (Responsabile del trattamento) le modalità e le responsabilità per la gestione di eventi di violazione dei dati personali (o *data breach*);

- dato atto altresì che sono stati elaborati l'aggiornamento e la revisione della procedura per la gestione di *data breach*, approvata con la richiamata deliberazione n. 102 del 15/05/2019;

- precisato che la procedura in questione è stata condivisa con i competenti uffici delle Aziende di area metropolitana;



- ritenuto pertanto di approvare l'aggiornamento della procedura per la gestione di *data breach* ai sensi degli artt. 33 e 34 del Regolamento EU 2016/679, nel testo allegato, conforme a quanto trasmesso dal DPO con nota prot. n. 42112 del 19/12/2022;

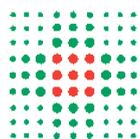
- acquisito il parere favorevole del DPO;

Delibera

per le motivazioni esposte in premessa e che si intendono tutte integralmente riportate:

1. di approvare l'aggiornamento della procedura per la gestione di *data breach* ai sensi degli artt. 33 e 34 del Regolamento EU 2016/679, nel testo allegato al presente provvedimento quale parte integrante e sostanziale;
2. di dare mandato ai Coordinatori del Gruppo Aziendale Privacy di pubblicare nell'apposita sezione della intranet aziendale e sul sito web, la procedura di cui al punto 1, per garantirne la più ampia diffusione;
3. di trasmettere la presente deliberazione ai Referenti privacy per gli adempimenti di competenza e per la diffusione della stessa ai collaboratori;
4. di prendere atto che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico del bilancio dell'Azienda Usl di Imola;
5. di trasmettere il presente atto al Collegio Sindacale ai sensi dell'art. 18, comma 4, della L.R. 16.7.2018 n. 9.

Responsabile del procedimento:
Sabrina Fiorentini



Procedura per la gestione di Data Breach (artt. 33 e 34 Regolamento Europeo 679/2016)

Tale procedura deve essere diffusa a tutti i soggetti deputati al trattamento dei dati personali che, a diverso titolo, potranno e dovranno essere di ausilio al Titolare del trattamento.

Sommario

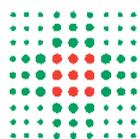
1. Riferimenti normativi
2. Definizioni
3. Data Breach
4. Gestione del Data Breach
 - 4.1. Gestione del Data Breach da parte del Titolare del trattamento
 - 4.2. Gestione del Data Breach da parte del Responsabile del trattamento
5. Analisi tecnica dell'evento e valutazione della gravità dell'evento
6. Notifica all'Autorità Garante
7. Altre segnalazioni dovute
8. Comunicazione agli interessati
9. Inserimento dell'evento nel Registro delle violazioni
10. Azioni di miglioramento

Allegati

1. Report per la comunicazione interna di Data Breach ai Coordinatori del GAP
2. Fac-simile Registro delle violazioni
3. Report del Responsabile del trattamento per la comunicazione del Data Breach al DPO

1. Riferimenti normativi

- Decreto Legislativo 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).
- D.Lgs. 196/2003 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.



- D.Lgs. 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 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 7 marzo 2005, n. 82, recante il "Codice dell'amministrazione digitale". G.U. 21 giugno 2008, n. 144.
- Art. 13 del DPCM 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 27.05.2021: Procedura telematica per la notifica di violazioni di dati personali (Data Breach)

2. 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).

Coordinatori del GAP: i Dirigenti aziendali deputati 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).

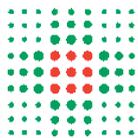
Gruppo Aziendale Privacy (GAP): il gruppo di professionisti individuato dal Titolare con il compito di presidiare a livello aziendale gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali.

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 ai sensi della Deliberazione n. 275 del 21/12/2018 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).

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). In questo contesto, è titolare del trattamento l'Azienda USL di Imola.



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).

3. 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.

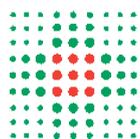
Le Linee guida in materia di notifica delle violazioni di dati personali (Data Breach notification) – WP250, definite in base alle previsioni del Regolamento (UE) 2016/679 precisano la nozione di violazione come di seguito riportata. Le violazioni possono essere classificate in base ai seguenti tre principi 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.

4. 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 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



4.1 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 ai Coordinatori del Gruppo Aziendale Privacy indirizzando l'e-mail a: gap@ausl.imola.bo.it. A tal fine va utilizzato il report di sintesi allegato al presente documento (**Allegato 1 - Report per la comunicazione interna di Data Breach ai Coordinatori del GAP**). Se è il referente privacy a venire direttamente a conoscenza del potenziale caso di Data Breach, la procedura da seguire è la medesima.

I Coordinatori del Gruppo Aziendale Privacy effettuano 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 comunicano l'esito dell'analisi preliminare effettuata al DPO, al fine di avvalersi della sua consulenza.

I Coordinatori del Gruppo Aziendale Privacy completata l'istruttoria avvertono 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 e in conformità alle determinazioni dello stesso notifica la violazione all'Autorità Garante (secondo le modalità descritte nel paragrafo 6).

L'avvenuta notificazione al Garante viene documentata dai Coordinatori del Gruppo Aziendale Privacy nel **Registro delle violazioni (Allegato 2 – Fac-simile Registro delle violazioni)** dagli stessi 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 i Coordinatori del Gruppo Aziendale Privacy provvedono ad inviarlo al Titolare del trattamento e al DPO con nota protocollata, ai fini della conservazione ai sensi di legge.

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

4.2 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 dall'atto di nomina/accordo/convenzione/contratto, il DPO all'indirizzo PEC: dpo@pec.aosp.bo.it utilizzando il modulo allegato (**Allegato 3 – Report del Responsabile del trattamento per la comunicazione del Data Breach al DPO**).

Il DPO inoltra il modulo di segnalazione di Data Breach ricevuto ai Coordinatori del Gruppo Aziendale Privacy e da questo momento vengono eseguite le medesime fasi della procedura illustrata al punto 4.1 (attraverso la necessaria collaborazione del Responsabile del trattamento).

5. Analisi tecnica dell'evento e valutazione della gravità dell'evento

Il Gruppo Aziendale Privacy, sotto la supervisione dei Coordinatori, 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 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. Notifica all'Autorità 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.gdpd.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.

7. Altre segnalazioni dovute

I Coordinatori del Gruppo Aziendale 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 aziendali 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 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.

8. Comunicazione agli interessati

In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà a 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 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 a una comunicazione pubblica o a una misurazione simile, tramite la quale gli interessati sono informati con analoghi 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 all'Autorità Garante, i Coordinatori del Gruppo Aziendale Privacy e il DPO devono valutare se sia il caso di notificare anche agli 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 dei Coordinatori del Gruppo Aziendale Privacy e dello Staff Informazione e Comunicazione aziendale.

9. Inserimento dell'evento nel Registro delle violazioni

L'art. 33 paragrafo 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.

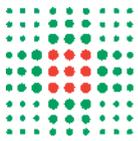
Pertanto, i Coordinatori del Gruppo Aziendale Privacy sono responsabili dell'inserimento di tutte le attività indicate sopra nel Registro delle violazioni (**Allegato 2 – Fac-simile Registro delle violazioni**), che devono essere documentate, tracciabili e in grado di fornire evidenza nelle sedi competenti.

10. Azioni di 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)
- Revisione 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.



ALLEGATO 1 alla PROCEDURA PER LA GESTIONE DI DATA BREACH

**REPORT PER LA COMUNICAZIONE INTERNA DI DATA BREACH AI COORDINATORI
DEL GAP**

da inviare via e-mail a: gap@ausl.imola.bo.it

U.O. _____

DIRETTORE/RESPONSABILE struttura (Referente privacy) _____

Indirizzo EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

QUANDO SI È VERIFICATA LA VIOLAZIONE DEI DATI PERSONALI:

- Il _____ Dal _____ (la violazione è ancora in corso)
 Dal _____ al _____ In un tempo non ancora determinato

CAUSA DELLA VIOLAZIONE:

- Azione intenzionale interna Azione accidentale interna
 Azione intenzionale esterna Azione accidentale esterna Sconosciuta

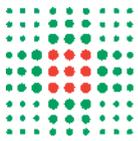
BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI:

DESCRIZIONE DEI SISTEMI, SOFTWARE, SERVIZI, INFRASTRUTTURE IT COINVOLTE NELLA VIOLAZIONE, CON INDICAZIONE DELLA LORO UBICAZIONE (ad es. PC, dispositivo mobile, apparecchiatura medica, file, documento cartaceo, ecc.):

MISURE TECNICHE E ORGANIZZATIVE, IN ESSERE AL MOMENTO DELLA VIOLAZIONE, ADOTTATE PER GARANTIRE LA SICUREZZA DEI DATI PERSONALI COINVOLTI

NATURA DELLA VIOLAZIONE:

- PERDITA DI RISERVATEZZA** (diffusione/accesso non autorizzato o accidentale)
 PERDITA DI INTEGRITÀ (modifica non autorizzata o accidentale)
 PERDITA DI DISPONIBILITÀ (impossibilità di accesso, indisponibilità del dato, distruzione, perdita, modifica non autorizzata o accidentale)



Altro

NUMERO DI INTERESSATI COINVOLTI NELLA VIOLAZIONE:

- N. _____ interessati Circa _____ interessati
 Non determinabile Non ancora determinato

CATEGORIE DI DATI OGGETTO DI VIOLAZIONE:

- Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
 Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
 Dati di accesso e di identificazione (username, password, customer ID, altro...)
 Dati di pagamento (n. conto corrente, dettagli della carta di credito, altro...)
 Dati relativi alla salute
 Dati relativi alla vita sessuale o orientamento sessuale
 Dati relativi a minori (specificare la tipologia di dato)
 Dati genetici
 Dati biometrici
 Altro

GRAVITÀ DEL POTENZIALE IMPATTO DELLA VIOLAZIONE SUGLI INTERESSATI (secondo le valutazioni del referente privacy):

- Trascurabile Bassa Media Alta Non ancora definita

Motivazioni:

MISURE TECNICHE E ORGANIZZATIVE ADOPTATE PER PORRE RIMEDIO ALLA VIOLAZIONE E ATTENUARE I POSSIBILI EFFETTI NEGATIVI DEGLI INTERESSATI:

MISURE TECNICHE E ORGANIZZATIVE ADOPTATE PER PREVENIRE SIMILI VIOLAZIONI FUTURE:

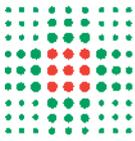
Data _____

Firma referente privacy

ALLEGATO 2 alla PROCEDURA PER LA GESTIONE DI DATA BREACH
FAC-SIMILE REGISTRO DELLE VIOLAZIONI

Rev1 03.11.2022

n. progressivo	DATA DELLA VIOLAZIONE	DATA DI INFORMAZIONE DELLA VIOLAZIONE E MEZZO DI COMUNICAZIONE	DESCRIZIONE VIOLAZIONE DATI PERSONALI	INTERESSATI	AVVIO ISTRUTTORIA	U.O. INTERESSATA	MISURE PREVENTIVE	AZIONI E/O MISURE IMMEDIATE ADOTTATE	AZIONI E/O MISURE DI MIGLIORAMENTO STRUTTURALI E NON	VALUTAZIONE DEL RISCHIO per i diritti e le libertà delle persone	Eventuale NOTIFICA al GDPR entro 72h	Motivi dell'eventuale ritardo	Eventuali ulteriori fasi di NOTIFICA	Eventuale COMUNICAZIONE all'INTERESSATO	Eventuale intervento del GDPR a seguito della notifica	NOTE
n. progressivo del registro	Momento in cui l'evento si è verificato	Data di ricevimento delle segnalazione da parte della funzione Privacy e mezzo con cui è pervenuta (es. PG, segnalazione utente, come da procedura del DB, ecc...)	Descrizione dettagliata dei fatti di violazione	<p>oggetti coinvolti:</p> <p>compreso tipologia dei dati e numero dei soggetti coinvolti</p>	si/no	Riportare il nome della UO/Struttura/Ufficio coinvolto/a nella violazione	<p>Indicare le misure atte a prevenire il rischio di procedure, linee guida, ecc), misure in uso presso le strutture sanitarie</p>	<p>Indicare le misure atte a contenere il danno eventuale, misure messe in campo al verificarsi della violazione</p>	<p>Misure messe in campo per prevenire il verificarsi/ripetersi di future violazioni</p>	<p>Da valutare sempre. Se l'esito è di rischio "elevato", procedere con comunicazione agli interessati. Riportare anche la data di parere del DPO (notificare o non notificare)</p>	si/no	Indicare se esistono motivi giustificati per l'invio al AG	Indicare se si procederà alla "notifica per fasi"	<p>Da attivare quando l'esito della valutazione del rischio è ELEVATO. Se richiesta ai sensi dell'art.34 GDPR, Art.34 e Cans.36 ne descrivono condizioni, modalità e contenuti</p>	<p>La notifica può aver dato luogo ad un intervento dell'AUTORITA' GARANTE nell'ambito dei suoi compiti e poteri</p>	x



ALLEGATO 3 alla PROCEDURA PER LA GESTIONE DI DATA BREACH

<p align="center">REPORT DEL RESPONSABILE DEL TRATTAMENTO PER LA COMUNICAZIONE DEL DATA BREACH AL DPO</p>
--

Data _____

Al DPO

dpo@pec.aosp.bo.it

Responsabile del trattamento (Ditta/Azienda)

Nome, cognome e recapito telefonico del soggetto che trasmette l'episodio:

Denominazione del Titolare

BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI:

DESCRIZIONE DEI SISTEMI, SOFTWARE, SERVIZI, INFRASTRUTTURE IT COINVOLTE NELLA VIOLAZIONE, CON INDICAZIONE DELLA LORO UBICAZIONE (ad es. PC, dispositivo mobile, apparecchiatura medica, file, documento cartaceo, ecc.):

MISURE TECNICHE E ORGANIZZATIVE, IN ESSERE AL MOMENTO DELLA VIOLAZIONE, ADOTTATE PER GARANTIRE LA SICUREZZA DEI DATI PERSONALI COINVOLTI

QUANDO SI È VERIFICATA LA VIOLAZIONE DEI DATI PERSONALI:

Il _____ Dal _____ (la violazione è ancora in corso)

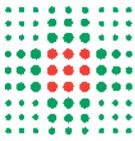
Dal _____ al _____ In un tempo non ancora determinato

CAUSA DELLA VIOLAZIONE:

- Azione intenzionale interna Azione accidentale interna
 Azione intenzionale esterna Azione accidentale esterna Sconosciuta

NATURA DELLA VIOLAZIONE:

- PERDITA DI RISERVATEZZA** (diffusione/accesso non autorizzato o accidentale)
 PERDITA DI INTEGRITÀ (modifica non autorizzata o accidentale)
 PERDITA DI DISPONIBILITÀ (impossibilità di accesso, indisponibilità del dato, distruzione, perdita, modifica non autorizzata o accidentale)



Altro _____

NUMERO DI INTERESSATI COINVOLTI NELLA VIOLAZIONE:

- N. _____ interessati Circa _____ interessati
 Non determinabile Non ancora determinato

CATEGORIE DI DATI SONO OGGETTO DI VIOLAZIONE:

- Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)
 Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
 Dati di accesso e di identificazione (username, password, customer ID, altro...)
 Dati di pagamento (n. conto corrente, dettagli della carta di credito, altro...)
 Dati relativi alla salute
 Dati relativi alla vita sessuale o orientamento sessuale
 Dati relativi a minori (specificare la tipologia di dato) _____
 Dati genetici
 Dati biometrici
 Altro

GRAVITÀ DEL POTENZIALE IMPATTO DELLA VIOLAZIONE SUGLI INTERESSATI (secondo le valutazioni del delegato):

- Trascurabile Bassa Media Alta Non ancora definita

Motivazioni:

**MISURE TECNICHE E ORGANIZZATIVE ADOTTATE PER PORRE RIMEDIO ALLA VIOLAZIONE
ATTENUARNE I POSSIBILI EFFETTI NEGATIVI DEGLI INTERESSATI** (se si conoscono):

MISURE TECNICHE E ORGANIZZATIVE ADOTTATE PER PREVENIRE SIMILI VIOLAZIONI FUTURE (se si conoscono):

Firma del Responsabile del trattamento