

## FRONTESPIZIO DELIBERAZIONE

AOO: ASL\_BO  
REGISTRO: Deliberazione  
NUMERO: 0000005  
DATA: 11/01/2023 13:16  
OGGETTO: RECEPIMENTO DELLA PROCEDURA PER LA GESTIONE DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) REVISIONATA DAL DATA PROTECTION OFFICER (DPO)

### SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Roti Lorenzo in qualità di Direttore Generale, delegato ai sensi dell'art.3, comma 6, del D.Lgs. 30.12.1992 n.502, come modificato dal D.Lgs. 7.12.1993 n.517

In assenza di Bordon Paolo - Direttore Generale

Con il parere favorevole di Roti Lorenzo - Direttore Sanitario

Con il parere favorevole di Ferro Giovanni - Direttore Amministrativo

Su proposta di Gian Carla Pedrazzi - UO Affari Generali e Legali (SC) che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

### CLASSIFICAZIONI:

- [01-08-05]

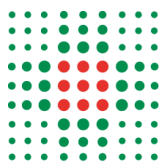
### DESTINATARI:

- Collegio sindacale
- DATeR - Direzione Assistenziale Tecnica e Riabilitativa
- UO Servizio Prevenzione e Protezione (SC)
- UO Anticorruzione e Trasparenza (SC)
- UO Libera Professione (SC)
- UO Affari Generali e Legali (SC)
- UO Ingegneria Clinica (SC)
- UO Governo Clinico, Ricerca, Formazione e Sistema Qualità (SC)
- UO Programmazione e Controllo (SC)
- UO Medicina Legale e Risk Management (SC)
- UO Governo dei Percorsi Specialistici (SC)
- UO Governo dei Percorsi di Screening (SC)
- Servizio Unico Metropolitan Contabilità e Finanza (SUMCF)
- Servizio Unico Metropolitan Economato (SUME)



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.



- Servizio Acquisti di Area Vasta - SAAV (SC)
- Servizio Unico Metropolitan Amministrazione Giuridica del Personale - SUMAGP (SC)
- Servizio Unico Metropolitan Amministrazione Economica del Personale - SUMAEP (SC)
- Distretto Savena Idice
- Distretto Pianura Ovest
- Distretto Pianura Est
- Distretto Citta' di Bologna
- Distretto dell'Appennino Bolognese
- Distretto Reno, Lavino e Samoggia
- Dipartimento Oncologico
- Dipartimento Chirurgie Specialistiche
- Dipartimento della Rete Medico Specialistica Ospedaliera e Territoriale
- Dipartimento interaziendale ad attivita' integrata di Anatomia Patologica - DIAP
- Dipartimento Farmaceutico Interaziendale - DFI
- Dipartimento Cure Primarie
- Dipartimento Emergenza Interaziendale - DEI
- Dipartimento Materno Infantile
- Dipartimento Chirurgie Generali
- Dipartimento Interaziendale per la Gestione Integrata del Rischio Infettivo - DIGIRI (IRCCS AOU)
- Dipartimento della Riabilitazione
- Dipartimento Medico
- Dipartimento Salute Mentale - Dipendenze Patologiche
- Dipartimento Tecnico-Patrimoniale
- Dipartimento della Diagnostica e dei Servizi di Supporto
- Dipartimento Sanita' Pubblica
- Dipartimento Attivita' Amministrative Territoriali e Ospedaliere - DAATO
- Dipartimento dell'Integrazione
- UO Direzione Attivita' Socio-Sanitarie - DASS (SC)
- IRCCS Istituto delle Scienze Neurologiche - Direzione Operativa
- UO Comunicazione (SS)
- UO Committenza e Governo dei Rapporti con il Privato Accreditato (SC)
- UO Sviluppo Organizzativo e Coordinamento Staff (SC)
- UO Sistemi Informativi Aziendali (SC)

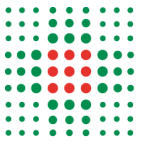
#### DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000005_2023_delibera_firmata.pdf	Ferro Giovanni; Pedrazzi Gian Carla; Roti Lorenzo	B537B26CA6C1347726F2F093B4C510342 055504FDD2776D1889DA4C3912A0CD0
DELI0000005_2023_Allegato1.pdf:		54B438E5F0FDFD04A76D1EE83EC588D6 401B2FDA9C91BFAD5B64590E680F527E



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: RECEPIMENTO DELLA PROCEDURA PER LA GESTIONE DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH) REVISIONATA DAL DATA PROTECTION OFFICER (DPO)

### IL DIRETTORE GENERALE

Su proposta del Direttore della U.O. Affari Generali e Legali Dr.ssa Gian Carla Pedrazzi, la quale esprime contestuale parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente provvedimento;

Visti:

- il Regolamento (UE) 2016/679 relativo alla Protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (in seguito “GDPR”, General Data Protection Regulation), applicabile in tutti gli Stati membri dell’Unione Europea a partire dal 25 maggio 2018, che nell’affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi per i diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento il compito di assicurare e di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure ritenute più idonee ed opportune (c.d. principio di responsabilizzazione o *accountability*);
- il Decreto Legislativo n.101 del 10 agosto 2018 recante disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo, in attuazione dell’art.13 della legge di delega europea 2016-2017 (legge 25 ottobre 2017, n.163), che ha introdotto disposizioni per l’adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il codice della privacy di cui al D.Lgs. n.196/2003;

Considerato che:

- il richiamato GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le Aziende Sanitarie, attribuendo al Titolare il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati;
- il “ *sistema privacy*’ delineato dal GDPR e confermato dal D.Lgs. n. 101/2018 di modifica ed integrazione del D.Lgs. n. 196/2003, implica la necessità di infondere nell’organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l’affermazione di una cultura della protezione dei dati, quale parte integrante dell’intero *asset* informativo di un’organizzazione, con particolare attenzione ai dati di salute (ivi compresi i dati biometrici e genetici);
- il nuovo approccio comporta il coinvolgimento di tutti i soggetti chiamati a trattare i dati personali all’interno della organizzazione aziendale, con assunzione delle relative responsabilità;



Richiamata la Deliberazione di Giunta Regionale - Emilia Romagna n. 919 del 10/4/2018, ad oggetto "Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l'anno 2018" la quale ha previsto fra gli obiettivi indicati al punto 4.6 dell'allegato B, oltre alla nomina del Responsabile della Protezione dei Dati (RPD) - Data Protection Officer (DPO) e all'adozione del Registro delle attività di trattamento, la ridefinizione e l'articolazione delle specifiche responsabilità privacy aziendali;

Richiamate le seguenti deliberazioni aziendali:

- n.146 del 19/04/2019 "*Regolamento UE 2016/679 in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR).Approvazione procedura per la gestione di violazione dei dati personali o Data Breach (artt.33 2 34 GDPR)*;
- n. 240 del 2/7/2021 "*Presenza d'atto della designazione del Responsabile della protezione dei dati dott.ssa Federica Filippini, ai sensi dell'art. 37 del Regolamento UE 2016/679*";
- n. 464 del 2/12/2021 "*Adeguamenti al Regolamento (UE) 2016/679. Definizione dell'organigramma delle responsabilità privacy aziendali e modalità di individuazione dei Referenti Privacy aziendali e dei Soggetti autorizzati al trattamento dei dati personali: aggiornamenti*";
- n. 400 del 2/11/2022 "*Presenza d'atto del documento di definizione dei rapporti tra il data protection officer (DPO) e le funzioni privacy aziendali*";

Richiamata la nota prot.144100 del 30/12/2022 ad oggetto "*Errata corrige del prot. n. 0044157/2022: invio documenti per la gestione di Data Breach e per la gestione dei diritti dell'interessato e relativi allegati*", con la quale il DPO dr.a Federica Filippini ha trasmesso i documenti revisionati concernenti, tra l'altro, la procedura per la gestione dei Data Breach, chiedendo alle funzioni privacy di procedere con quanto necessario per la conseguente applicazione a livello aziendale;

Ritenuto pertanto di recepire il suddetto documento allegato quale parte integrante alla presente deliberazione;

### **Delibera**

per le motivazioni espresse in premessa:

1) di recepire il documento concernente la revisione della procedura per la gestione di violazione dei dati personali (Data Breach) ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679, approvato dal DPO dr.a Federica Filippini il 3/11/2022, allegato quale parte integrante alla presente deliberazione;

2) di dare atto che a decorrere dall'adozione del presente atto cessano di avere efficacia le disposizioni di cui alla deliberazione n. 146 del 19/04/2019, come richiamata in premessa;

3) di precisare che il presente provvedimento verrà pubblicato alla pagina privacy policy del sito internet dell'Azienda USL di Bologna e che allo stesso dovrà essere fatto riferimento per ogni successiva



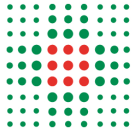
comunicazione di Data Breach (Allegati 1 e 3 alla procedura medesima) sia da parte dei Referenti privacy interni che da parte dei Responsabili di Trattamento ex art.28 GDPR (esterni);

4) di specificare che il Responsabile del Procedimento ai sensi della legge n.241/1990 e s.m.i. è la Dr.ssa Rosa Preiti, collaboratore amministrativo senior UO Affari Generali e Legali;

5) di trasmettere copia del presente provvedimento a tutti i Dipartimenti, Distretti e Strutture di Staff.

Responsabile del procedimento ai sensi della L. 241/90:

Rosa Preiti



## **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**
- 2. Fac-simile Registro violazioni**
- 3. Report Responsabile del trattamento per la comunicazione del Data Breach**

## 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).

**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).

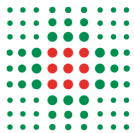
**Gruppo Aziendale Privacy (GAP):** il gruppo di professionisti individuato dal Titolare con il compito di presidiare a livello aziendale gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali.

**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).

**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, 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).

### 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 la 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 GPDR 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 al Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy (inserire la/le modalità ed i tempi adottata in Azienda/Istituto) A tal fine va utilizzato il report di sintesi allegato al presente documento (**Allegato 1 - 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 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 (Allegato 2 - Fac-simile 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 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/Istituto 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 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 4.1 (attraverso la necessaria collaborazione del Responsabile del trattamento).

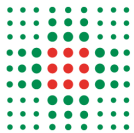
### **5. Analisi tecnica dell'evento e valutazione della gravità dell'evento**

Il Gruppo Aziendale Privacy, sotto la supervisione del Coordinatore o del 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 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 a 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

Il Coordinatore del Gruppo Aziendale Privacy/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 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

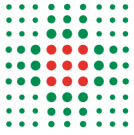
In caso di elevato rischio per la libertà e i diritti degli individui, si provvederà a informare gli interessati sul fatto avvenuto, sui dati violati e sulle procedure necessarie a ridurre il rischio.

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 la 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 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 all'Autorità Garante, il Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione 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 del Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy/U.O. 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.

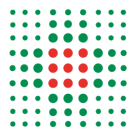
Pertanto, il Coordinatore del Gruppo Aziendale Privacy/Responsabile della Funzione Privacy è responsabile dell'inserimento di tutte le attività indicate sopra nel Registro delle violazioni (**Allegato 2 - Fac-simile Registro violazioni**), che devono essere documentate, tracciabili e in grado di fornire 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.gdpr.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/NOTIFICA DI UN DATA BREACH

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

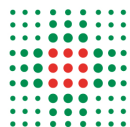
BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI:

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 ADOTTATE PER PORRE RIMEDIO ALLA VIOLAZIONE E ATTENUARE I POSSIBILI EFFETTI NEGATIVI DEGLI INTERESSATI:**

**MISURE TECNICHE E ORGANIZZATIVE ADOTTATE PER PREVENIRE SIMILI VIOLAZIONI FUTURE:**

Data \_\_\_\_\_

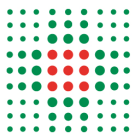
\_\_\_\_\_  
Firma referente privacy

AII. 2

Rev. 1 del 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	soggetti coinvolti: compreso tipologia dei dati e numero dei soggetti coinvolti	si/no	Riportare il nome della UO/struttura/ufficio coinvolta/o nella violazione	Indicare le misure atte a prevenire il rischio (procedure, linee guida, ecc), misure in uso presso le strutture sanitarie	Indicare le misure atte a contenere il danno eventuale, misure messe in campo al verificarsi della violazione	Misure messe in campo per prevenire il verificarsi/ripetersi di future violazioni	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)	si/no	Indicare se esistono motivi ostativi all'invio al AG	Indicare se si procedere alla "notifica per fasi"	Da attivare quando l'esito della valutazione del rischio è ELEVATO .Se richiesta ai sensi dell'art.34 GDPR. Art.34 e Cons.86 ne descrivono condizioni, modalità e contenuti	La notifica può aver dato luogo ad un intervento del AUTORITA' GARANTE nell'ambito dei suoi compiti e poteri	

x



ALLEGATO 3 alla PROCEDURA PER LA GESTIONE DI DATA BREACH

REPORT DEL RESPONSABILE DEL TRATTAMENTO PER LA COMUNICAZIONE DEL  
DATA BREACH

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

\_\_\_\_\_

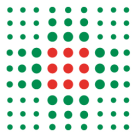
BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI:

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:**

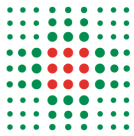
- Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale, altro...)  
 Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)  
 Dati di accesso e di identificazione (username, password, customer ID, altro.)  
 Dati di pagamento (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**