SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Ortopedico Rizzoli di Bologna
Istituto di Ricovero e Cura a Carattere Scientifico

FRONTESPIZIO DELIBERAZIONE

AOO: DA

REGISTRO: Deliberazione

NUMERO: 0000107

DATA: 13/04/2023 16:20

OGGETTO: AGGIORNAMENTO DELLA PROCEDURA DI SEGNALAZIONE DEGLI EVENTI DI VIOLAZIONE DEI DATI PERSONALI (C.D. DATA BREACH) AI SENSI DEGLI ARTICOLI 33 e 34 DEL REGOLAMENTO (UE) 2016/679 (c.d. GDPR)

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Campagna Anselmo in qualità di Direttore Generale
Con il parere favorevole di Fini Milena - Direttore Scientifico
Con il parere favorevole di Damen Viola - Direttore Sanitario
Con il parere favorevole di Cilione Giampiero - Direttore Amministrativo

Su proposta di Laura Mandrioli - Affari Legali e Generali che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [06-04]

DESTINATARI:

- Collegio sindacale
- ICT
- Servizio Prevenzione e Protezione
- Dipartimento Patologie Complesse
- Dipartimento Patologie Specialistiche
- SAITER - Servizio di Assistenza Infermieristica, Tecnica e Riabilitazione
- Farmacia
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)
- Dipartimento Rizzoli - Sicilia
- Comunicazione e Relazione con i Media
- Marketing Sociale
- Clinica Ortopedica e Traumatologica I
- Ortopedia - Traumatologia e Chirurgia protesica e dei reimpianti d'anca e di ginocchio
- Anestesia e Terapia Intensiva post operatoria e del dolore
- Banca del tessuto muscoloscheletrico (BTM)
- Anatomia e Istologia Patologica

- Laboratorio di Analisi del Movimento
- Laboratorio BIC
- Servizio Unico Metropolitano Amministrazione Giuridica del Personale - SUMAGP (SC)
- Direzione Generale
- Direzione Amministrativa
- Direzione Sanitaria
- Direzione Scientifica
- Affari Legali e Generali
- Laboratorio di Tecnologia Medica
- Laboratorio RAMSES
- Ortopedia Bentivoglio
- Chirurgia della Spalla e del Gomito
- Medicina Fisica e Riabilitativa
- Controllo Qualita' secondo GMP
- Laboratorio di Biologia Cellulare Muscoloscheletrica
- Lab. Immunoreumatologia e rigenerazione tissutale
- Patrimonio ed Attivita' Tecniche
- Accesso ai Servizi
- Programmazione, Controllo e Sistemi di Valutazione
- Dipartimento Rizzoli RIT Research, Innovation Technology
- Servizio Unico Metropolitano Economato (SUME)
- Amministrazione della Ricerca
- Clinica Ortopedica e Traumatologica II
- Clinica Ortopedica e Traumatologica III a prevalente Indirizzo Oncologico
- Ortopedia Generale Rizzoli-Sicilia
- Ortopedia e Traumatologia Pediatrica
- Chirurgia Vertebrale
- Reumatologia
- Genetica Medica - Malattie Rare Ortopediche
- Radiologia Diagnostica ed Interventistica
- Pronto Soccorso
- Radiologia interventistica Angiografica
- Laboratorio di Oncologia Sperimentale
- Patologia delle Infezioni Associate all'Impianto

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000107_2023_delibera_firmata.pdf	Campagna Anselmo; Cilione Giampiero; Damen Viola; Fini Milena; Mandrioli Laura	8C28033DDCC9F9CD8CF80814F2D34E30E853B6A245212788C39C324F6B1A7C59
DELI0000107_2023_Allegato1.pdf:		7478096F5EFE12CFAB09194083085E5BE4FD1C7CC683AC8538296E8FB909ACAF
DELI0000107_2023_Allegato2.pdf:		C5AA0D87F919B67855745AA57694E59F9C2AA9BDB38590ED857BCCB049878567
DELI0000107_2023_Allegato3.pdf:		647493160C53FDEF0E0BA646E4456D9C7502DB577110548CC1EDB5AD4EFE7B06

File	Firmato digitalmente da	Hash
DELI0000107_2023_Allegato4.pdf:		F5F4B22953075243168AB2BACDE52B032 78345FE639CCEBCAFC041F59CE14FF9

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Ortopedico Rizzoli di Bologna
Istituto di Ricovero e Cura a Carattere Scientifico

DELIBERAZIONE

OGGETTO: AGGIORNAMENTO DELLA PROCEDURA DI SEGNALAZIONE DEGLI EVENTI DI VIOLAZIONE DEI DATI PERSONALI (C.D. DATA BREACH) AI SENSI DEGLI ARTICOLI 33 e 34 DEL REGOLAMENTO (UE) 2016/679 (c.d. GDPR)

IL DIRETTORE GENERALE

Richiamati:

- Il 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), c.d. GDPR;
- Il Decreto Legislativo 30 giugno 2003 n. 196 "Codice in materia di protezione dei dati personali", come modificato e integrato dal D.Lgs. 101/2018 recante disposizioni per l'adeguamento dell' ordinamento nazionale al Regolamento (UE) 2016/679;
- Il Provvedimento dell'Autorità Garante per la protezione dei dati personali sulla notifica delle violazioni dei dati personali (data breach) del 30 luglio 2019;
- 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.

Richiamati i seguenti provvedimenti aziendali:

Deliberazione n. 123 del 24.04.2019, ad oggetto "APPROVAZIONE DELLA PROCEDURA DI SEGNALAZIONE DEGLI EVENTI DI VIOLAZIONE DEI DATI PERSONALI (C.D. DATA BREACH) AI SENSI DEGLI ARTICOLI 33 e 34 REGOLAMENTO (UE) 2016/679 (c.d. GDPR)" con la quale, al fine di dare attuazione alla suddetta normativa, l'Istituto ha adottato una procedura organizzativa che disciplina la gestione e la notifica all'Autorità Garante degli eventi di data breach e la tenuta del registro delle violazioni;

Deliberazione n. 212/2021, ad oggetto "Presa d'atto dell'accordo tra l'Istituto Ortopedico Rizzoli, l'Azienda Ospedaliero Universitaria di Bologna Policlinico Sant'Orsola-Malpighi, l'Azienda USL di Bologna e l' Azienda USL di Imola per la gestione unificata delle funzioni di Data Protection Officer";

Deliberazione n. 235/2021, "Presa d'atto della designazione del Responsabile della protezione dei dati (detto anche Data Protection Officer), dott.ssa Federica Filippini, ai sensi dell'art. 37 del Regolamento (UE) 2016/679" con decorrenza dell'incarico dal 01.07.2021, per la durata di cinque anni.

Visti:

Il Provvedimento del Garante Privacy n. 209 del 27 maggio 2021 sulla notifica delle violazioni dei dati personali (*data breach*), con il quale l'Autorità ha previsto, a decorrere dal 1° luglio 2021, una procedura telematica per la notifica di una violazione dei dati personali;

La nota ad oggetto: "Trasmissione comunicazione del Garante per la protezione dei dati personali: Nuovo servizio online per la notifica di una violazione dei dati personali (data breach)", prot. IOR n. 0009692 del 24/06/2021, con cui l'allora DPO dott.ssa Federica Banorri ha trasmesso ai Referenti Privacy delle Aziende dell'area metropolitana tale Provvedimento e comunicato le nuove modalità di notifica.

Considerato che in seguito alla designazione del DPO interaziendale dott.ssa Filippini, si rende necessario aggiornare la "Procedura per la gestione di Data Breach (artt. 33 e 34 Regolamento Europeo 679/2016)" dell'Istituto Ortopedico Rizzoli adottata con Deliberazione n. 123 del 24.04.2019, comprensiva dei due allegati:

- "Report interno per la comunicazione al Coordinatore del Gruppo Aziendale Privacy" (All. 1)
- "Modello per la segnalazione di un sospetto caso di data breach" (All. 3)

con i dati di contatto del nuovo Responsabile della Protezione dei Dati.

Considerata altresì la necessità di aggiornare la "Procedura per la gestione di Data Breach (artt. 33 e 34 Regolamento Europeo 679/2016)" approvata con la richiamata Deliberazione IOR n. 123 del 24.04.2019, e relativi allegati nn. 1, 2 ("Fac simile registro violazioni") e 3, con riferimento alla nuova procedura telematica per la notifica di una violazione dei dati personali di cui al Provvedimento del Garante Privacy n. 209 del 27 maggio 2021.

Dato atto che il DPO ha elaborato l'aggiornamento e la revisione della "Procedura per la gestione di Data Breach (artt. 33 e 34 Regolamento Europeo 679/2016)", e relativi allegati nn. 1, 2 e 3, con riferimento alla nuova procedura telematica per la notifica di una violazione dei dati personali introdotta dal Garante Privacy con il Provvedimento sopra richiamato.

Precisato che con nota prot. IOR n. 0018748 del 19.12.2022, il DPO ha trasmesso ai competenti Uffici aziendali, la procedura e i relativi allegati nei modelli definitivi revisionati e condivisi in ambito metropolitano, per i successivi passaggi finalizzati alla loro adozione nell'ambito di ciascuna Azienda;

Ritenuto pertanto di approvare l'aggiornamento della procedura nel testo allegato alla presente, condiviso in ambito metropolitano, comprensiva dei relativi allegati nn. 1, 2 e 3.

Acquisito il parere favorevole del DPO.

Delibera

1) di approvare la “Procedura per la gestione di Data Breach (artt. 33 e 34 Regolamento Europeo 679/2016)” dell’Istituto Ortopedico Rizzoli, comprensiva dei seguenti allegati:

- "Report per la comunicazione interna/notifica di un Data Breach” (All. 1)
- “Fac-simile Registro delle violazioni” (All. 2)
- “Report del Responsabile del trattamento per la comunicazione del Data Breach” (All. 3)

quale aggiornamento della precedente procedura e dei corrispondenti allegati n. 1 ("Report interno per la comunicazione al Coordinatore del Gruppo Aziendale Privacy”) n. 2 (“Fac simile registro violazioni”), n. 3 (“Modello per la segnalazione di un sospetto caso di data breach”) e n. 4 (“Modello di notifica all’Autorità Garante”) approvati con Deliberazione IOR n. 123 del 24.04.2019;

2) di allegare, quale parte integrante e sostanziale del presente atto, il testo della “Procedura per la gestione di Data Breach (artt. 33 e 34 Regolamento Europeo 679/2016)”, comprensiva degli allegati:

- "Report per la comunicazione interna/notifica di un Data Breach” (All. 1)
- “Fac-simile Registro delle violazioni” (All. 2)
- “Report del Responsabile del trattamento per la comunicazione del Data Breach” (All. 3)

quale aggiornamento della precedente procedura e corrispondenti allegati nn. 1, 2, 3 e 4 approvati con Deliberazione IOR n. 123 del 24.04.2019;

3) di stabilire che la procedura e i relativi allegati di cui al presente provvedimento sostituiscono integralmente la precedente procedura e corrispondenti allegati nn. 1, 2, 3 e 4 approvati con Deliberazione IOR n. 123 del 24.04.2019;

4) di pubblicare nell’apposita sezione della intranet aziendale e nel sito web dell’Istituto la procedura e i relativi allegati di cui al presente provvedimento, in sostituzione della precedente procedura e corrispondenti allegati nn. 1, 2, 3 e 4 approvati con Deliberazione IOR n. 123 del 24.04.2019.

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

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

Allegati

1. **Report per la comunicazione interna/notifica di un Data Breach**
2. **Fac-simile Registro delle violazioni**
3. **Report del 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 perso - nali, 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 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 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 con mail all'indirizzo privacy@ior.it

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 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, 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 AziendalePrivacy nel **Registro delle violazioni** (**Allegato 2 - Fac-simile Registro delle 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 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 del 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 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, 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, avva- lendosi della funzione consulenziale del DPO.

Si precisa che l'art. 33 paragrafo 4 del GDPR recita: "Qualora nella misura in cui non sia possibile fornire le infor-mazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustifi- cato 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 de - termina 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 comuni- cazione 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.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.

7. Altre segnalazioni dovute

Il Coordinatore 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 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 e il DPO devono valutare se sia il caso di notificare anche agli inte-ressati. 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.

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 è responsabile 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 compe-tenti.

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/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 medicale, file, documento cartaceo, ecc.):

MISURE TECNICHE E ORGANIZZATIVE, <u>IN ESSERE AL MOMENTO DELLA VIOLAZIONE</u>, 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 <u>ADOTTATE PER PORRE RIMEDIO</u> ALLA VIOLAZIONE E ATTENUARE I POSSIBILI EFFETTI NEGATIVI DEGLI INTERESSATI:

MISURE TECNICHE E ORGANIZZATIVE <u>ADOTTATE PER PREVENIRE</u> SIMILI VIOLAZIONI FUTURE:

Data _____ _____

Firma referente privacy

ALLEGATO 2 alla PROCEDURA PER LA GESTIONE DI DATA BREACH

FAC-SIMILE REGISTRO DELLE VIOLAZIONI

n. progressivo	DATA DELLA VIOLAZIONE	DATA DI INFORMAZIONE DELLA VIOLAZIONE E MEZZO DI COMUNICAZIONE	DESCRIZIONE VIOLAZIONE DATI PERSONALI	INTERESSATI
n. progressivo del registro	Momento in cui l'evento si è verificato	Data di ricevimento della 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

AVVIO ISTRUTTORIA	U.O. INTERESSATA	MISURE PREVENTIVE	AZIONI E/O MISURE IMMEDIATE ADOTTATE
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

AZIONI E/O MISURE DI MIGLIORAMENTO STRUTTURALI E NON	VALUTAZION EDEL RISCHIO per i diritti e le libertà dellepersone	Eventuale NOTIFICA al GPDP entro 72h
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

Motivi dell'eventuale ritardo	Eventuali ulteriori fasi di NOTIFICA	Eventuale COMUNICAZIONE all'INTERESSATO	Eventuale intervento del GPDP a seguito della notifica	NOTE
Indicare se esistono motivi ostativi all'invio al AG	Indicare se si procede 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	

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 medicale, 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 <u>ADOTTATE PER PORRE RIMEDIO</u> ALLA VIOLAZIONE ATTENUARNE I POSSIBILI EFFETTI NEGATIVI DEGLI INTERESSATI (se si conoscono):

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

_____
Firma del Responsabile del trattamento