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: 0000123

DATA: 24/04/2019 13:54

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)

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Cavalli Mario in qualità di Direttore Generale
Con il parere favorevole di Landini Maria Paola - Direttore Scientifico
Con il parere favorevole di Rolli Maurizia - 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:

- [02-05]
- [08-02]
- [02-07]
- [06-04]
- [04-08]

DESTINATARI:

- Collegio sindacale
- Clinical Trial Center
- Patrimonio ed Attivita' Tecniche
- Servizio Unico Metropolitano Amministrazione del Personale (SUMAP)
- Affari Legali e Generali
- Accesso ai Servizi
- Programmazione, Controllo e Sistemi di Valutazione
- ICT
- Servizio Prevenzione e Protezione
- Dipartimento Patologie Complesse
- Dipartimento Patologie Specialistiche
- Struttura di Supporto Direzionale

- Direzione Servizio di Assistenza Infermieristica, Tecnica e della Riabilitazione (DAITER)
- Farmacia
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)
- Servizio Bilancio e Coordinamento Processi Economici
- Dipartimento Rizzoli - Sicilia
- Direzione Scientifica
- Comunicazione e Relazione con i Media
- Marketing Sociale
- Dip. Rizzoli - RIT Research, Innovation & Technology
- Servizio Unico Metropolitano Economato (SUME)
- Amministrazione della Ricerca

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000123_2019_delibera_firmata.pdf	Cavalli Mario; Cilione Giampiero; Landini Maria Paola; Mandrioli Laura; Rolli Maurizia	7E8C4D80E6EE21BEDEF3291765D1D7EDCDD87F8C82AF44FE34A7E9CA8FA8F952
DELI0000123_2019_Allegato1.docx:		1EBA5772CF03ABFF69ABC91F3162B0B61FB9124ED89C0001B3F06A1E46B13342
DELI0000123_2019_Allegato2.pdf:		DDF03E14208D4052EA847B7F34D246122F4BCC245F429B0A925F0A22AB911799
DELI0000123_2019_Allegato3.pdf:		1BE3A93B7CEECCD3E29F8B356CBD1E48AA46EC47657B796D7F3CA7594725CE2A
DELI0000123_2019_Allegato4.pdf:		5D0702F8AB349CEC16C9333667D2DCB750D78EE2F085CD707726DF937443B93B
DELI0000123_2019_Allegato5.pdf:		2DC15E14FB2B3C16CF4D39C73F4B33CA8E362B5526A80C1291BD97A579B735F8

DELIBERAZIONE

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)

IL DIRETTORE GENERALE

Richiamati i seguenti 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 (c.d. GDPR) 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) – WP250, 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);

Atteso che:

- Il Regolamento generale per la protezione dei dati (UE) 2016/679 (c.d. GDPR) dispone che, in caso di violazione dei dati personali che presenti un rischio elevato per i diritti e le libertà delle persone fisiche (c.d. data breach), il Titolare del trattamento notifichi tale violazione all’Autorità Garante per la protezione dei dati personali senza ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza;

Ritenuto necessario

- al fine di dare attuazione alla suddetta disposizione normativa, predisporre ed adottare una procedura organizzativa che disciplini la gestione e successiva notifica all'Autorità Garante dei possibili casi di data breach e la tenuta del relativo registro delle violazioni;

Dato atto che:

- questo Ente, Azienda USL di Bologna, Azienda Ospedaliera Universitaria - Policlinico S. Orsola Malpighi, Azienda USL di Imola e Montecatone Rehabilitation Institute S.p.A. hanno nominato un Data Protection Officer condiviso con il compito, tra gli altri, di promuovere iniziative congiunte tra le Aziende/Enti affinché l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti;

- nella suddetta ottica, questo Ente, Azienda USL di Bologna, Azienda Ospedaliera Universitaria - Policlinico S. Orsola Malpighi, Azienda USL di Imola e Montecatone Rehabilitation Institute S.p.A. hanno predisposto, con la collaborazione e il coordinamento del loro DPO, un modello di procedura di data breach da condividere, salvo le specifiche organizzative in capo alle singole aziende, ed utilizzare in luogo delle diverse procedure di data breach precedentemente in uso;

Delibera

1) di approvare la procedura per la gestione di Data Breach (ex artt. 33 e 34 Regolamento (UE) 2016/679) dell'Istituto Ortopedico Rizzoli, comprensiva dei seguenti n.4 allegati:
- "Report interno per la comunicazione al Coordinatore del Gruppo Aziendale Privacy";
- "Fac simile registro violazioni";
- "Modello di report Responsabile del trattamento per la comunicazione del data breach al DPO";
- "Modello di notifica all'Autorità Garante";

2) di allegare, quale parte integrante e sostanziale del presente atto, il testo della procedura per la gestione di Data Breach e i relativi 4 documenti allegati descritti al punto che precede;
3) di dare adeguata e capillare diffusione alla procedura per la gestione di Data Breach di cui al punto 1).

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

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 interno per la comunicazione al Coordinatore del GAP**
2. **Fac simile Registro violazioni**
3. **Report Responsabile del trattamento per la comunicazione del Data Breach al DPO**
4. **Modello di notifica all'Autorità Garante**

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*) – WP250, 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).

2. Definizioni

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).

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

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.

Data Protection Officer: la persona fisica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (in particolare artt. 37, 38, 39).

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).

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).

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

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

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 i seguenti step del processo di notificazione:

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

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 Gruppo Aziendale Privacy con mail all'indirizzo privacy@ior.it o con eventuale altra modalità ritenuta idonea in rapporto ai mezzi di telecomunicazione o informatici a disposizione. A tal fine si può utilizzare il report di sintesi allegato al presente documento (**Allegato 1 - Report interno per la comunicazione del Data Breach al Coordinatore 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.

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 si 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 mettere il Titolare a conoscenza del potenziale caso di data breach.

Il Titolare assume le proprie determinazioni, disponendo la necessità o meno di notifica. Il Coordinatore del Gruppo Aziendale Privacy predispone l'eventuale comunicazione per l'Autorità Garante da sottoporre al DPO e al Titolare del trattamento. Il Titolare trasmette la comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui il Titolare da abbia un ragionevole grado di certezza della verifica di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.

È comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow up (c.d. notifica in fasi).

L'avvenuta notificazione al Garante viene documentata dal Coordinatore del Gruppo Aziendale Privacy nel **Registro delle violazioni** (**Allegato 2 – fac simile**) 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 con nota protocollata, ai fini della conservazione ai sensi di legge.

Si precisa che anche i casi segnalato e non ritenuti dal Titolare da notificare e le motivazioni sottese devono essere documentate nel medesimo registro.

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, il DPO all'indirizzo Pec protocollo@pec.ausl.bologna.it. o tramite raccomandata A/R all'indirizzo Via Castiglione, n. 29 – 40124 – Bologna utilizzando il modulo allegato **(Allegato 3 Report Responsabile del trattamento per la comunicazione del Data Breach al DPO)**.
Il DPO inoltra il modulo di segnalazione ricevuto di Data Breach al Coordinatore del Gruppo Aziendale Privacy e da questo momento vengono eseguiti i medesimi step della procedura illustrata al punto 3.1 (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, avvalendosi della funzione consulenziale del DPO.
In particolare, una volta verificato che l'evento segnalato si configuri effettivamente come un Data Breach (Analisi Preliminare), verranno svolte tutte le operazione necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante della privacy. Si sottolinea ulteriormente che nel caso in cui dall'Analisi Preliminare emerga che la segnalazione non ha i caratteri del Data Breach è comunque necessario registrarla nel Registro delle violazioni.
Durante l'Analisi Approfondita dovranno essere accertate le circostanze della violazione, le conseguenze e i relativi rimedi.
Si precisa che l'art. 33 paragrafo n. 4 del DGPR 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"*. Pertanto, sarà fondamentale raccogliere il maggior numero di informazioni e, anche nel caso in cui queste non siano] ritenute esaustive, effettuare la notificazione (c.d. notifica per fasi).
Nello specifico verrà effettuato:

- il riconoscimento della categoria della violazione (se di riservatezza, di integrità o di disponibilità) o altro evento (cfr. Linee Guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento UE 2016/79 – WP 250 Par. 1, punto 2);
- l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- l'identificazione degli interessati;

- il contenimento del danno come di seguito descritto:
    - limitazione degli effetti dell'incidente,
    - raccolta delle prove forensi nel caso sia ipotizzato un reato,
    - determinazione delle azioni possibili di ripristino,
    - valutazione delle eventuali vulnerabilità collegate con l'incidente,
    - individuazione delle azioni di mitigazione delle vulnerabilità individuate,
    - valutazione dei tempi di ripristino,
    - gestione della comunicazione con gli interessati, i media (se di impatto notevole),
    - ripristino dei dati, dei sistemi, dell'infrastruttura e delle configurazioni,
    - verifica dei sistemi recuperati.

L'art. 33 paragrafo n. 1 chiarisce che non vi è obbligo di notifica della violazione quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche, ovviamente 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.
Nella fase di Valutazione, 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 (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 si Data Breach si procedere con la notifica all'Autorità Garante.

6. Notifica all'Autorità Garante

La notifica, effettuata dal Titolare sulla falsariga del modello reso disponibile dal Garante della privacy (**Allegato 4 Modello di notifica all'Autorità Garante)** dovrà contenere i seguenti elementi:

1. la descrizione della violazione dei dati personali compresi, ove possibile le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
2. l'indicazione del nome e i relativi dati di contatto del DPO;
3. la descrizione delle probabili conseguenze della violazione;
4. l'indicazione 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, se del caso, per attenuare i possibili effetti negativi.

Nello specifico, la notifica al Garante sarà effettuata dal Titolare tramite PEC e per conoscenza al DPO, con indicazione del DPO come punto di contatto con il Garante.

7. ALTRE SEGNALAZIONI DOVUTE.

Il Coordinatore del Gruppo Aziendale Privacy e il DPO, con il 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 n. 3 dell'art. 34 del GDPR, non è richiesta quando:

- il Titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
- la comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece 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 l'Autorità Garante, il Coordinatore del Gruppo Aziendale Privacy e il DPO devono valutare se è il caso di notificare anche gli interessati. A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti.
Se il rischio è grave occorre individuare, la fattibilità di contattarli singolarmente oppure la necessità di procedere con pubblicazioni su diversi mezzi di comunicazione (sito web, quotidiani, radio, tv), le misure di contenimento che gli stessi interessati possano mettere in atto per minimizzare i rischi e le forme di comunicazione più comprensibili per gli interessati (mezzi, lingue, linguaggio) come indicato nelle Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679.

La forma di comunicazione prescelta dal Titolare verrà predisposta e curata dal DPO con la collaborazione del Coordinatore del Gruppo Aziendale Privacy.

9. INSERIMENTO DELL'EVENTO NEL REGISTRO DELLE VIOLAZIONI

L'art. 33 paragrafo n. 5 del GPR, prescrive al Titolare di documentare qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma. Pertanto, il Coordinatore del Gruppo Aziendale Privacy è responsabile dell'inserimento di tutte le attività indicate sopra nel registro delle violazioni, che devono essere documentate, tracciabili e in grado di fornire evidenza nelle sedi competenti.

10. MIGLIORAMENTO

Le azioni previste in questa fase sono:

Analisi della relazione dettagliata sull'incidente
Reiterazione del processo di Gestione del rischio informativo
Eventuale revisione di questo documento (se necessaria) e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza)
Individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi
Revisione del Sistema di Gestione della Privacy
Revisione delle relazioni con Clienti e Fornitori
Revisione annuale della procedura

ALLEGATO N. 1 - REPORT interno per la comunicazione al Coordinatore del GAP
(Da inviare al Coordinatore del GAP o suo delegato: inserire indirizzo)

U.O./Programma_____

DIRETTORE/RESPONSABILE (Referente privacy) _____

Indirizzo EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

BREVE DESCRIZIONE DELLA VIOLAZIONE DEI DATI PERSONALI

_____
_____
_____
_____

QUANDO SI È VERIFICATA LA VIOLAZIONE DEI DATI PERSONALI

☐ Il_____ ☐ Tra il _____ e il _____

☐ In un tempo non ancora determinato ☐ E' possibile che sia ancora in corso

DOVE È AVVENUTA LA VIOLAZIONE DEI DATI?

(ES. Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

_____
_____
_____
_____

MODALITÀ DI ESPOSIZIONE AL RISCHIO

TIPO DI VIOLAZIONE
☐ DISTRUZIONE
☐ PERDITA
☐ MODIFICA
☐ DIVULGAZIONE NON AUTORIZZATA
☐ ACCESSO NON AUTORIZZATO
☐ INDISPONIBILITA' DEL DATO
☐ Altro:

OGGETTO DELLA VIOLAZIONE
☐ Computer ☐ Dispositivo mobile ☐ Rete
☐ Apparecchiatura medicale
☐ File o parte di un file
☐ Strumento di backup
☐ Documento cartaceo
☐ Altro :

ALLEGATO N. 1 - REPORT interno per la comunicazione al Coordinatore del GAP
(Da inviare al Coordinatore del GAP o suo delegato: inserire indirizzo)

SINTETICA DESCRIZIONE DEI SISTEMI DI ELABORAZIONE O DI MEMORIZZAZIONE DEI DATI COINVOLTI, CON INDICAZIONE DELLA LORO UBICAZIONE:

_____
_____
_____
_____
_____

QUANTE PERSONE SONO STATE COLPITE DALLA VIOLAZIONE DEI DATI PERSONALI TRATTATI?

☐ N._____ persone

☐ Circa_____persone

☐ Un numero (ancora) sconosciuto di persone

CHE TIPO DI DATI SONO OGGETTO DI VIOLAZIONE?

☐ Dati anagrafici

☐ Indirizzo di posta elettronica

☐ Dati di accesso e di identificazione (user name, password, customer ID, altro)

☐ Dati relativi alla salute) _____

☐ Dati relativi a minori _____

☐ Dati ULTRASENSIBILI (es. HIV, IVG,….)_____

☐ Copie per immagine su supporto informatico di documenti analogici

☐ Ancora sconosciuto

☐ Altro :_____

LIVELLO DI GRAVITÀ DELLA VIOLAZIONE DEI DATI PERSONALI TRATTATI (SECONDO LE VALUTAZIONI DEL REFERENTE PRIVACY)?

☐ Basso/trascurabile ☐ Medio ☐ Alto ☐ Molto alto

MISURE TECNICHE E ORGANIZZATIVE APPLICATE AI DATI OGGETTO DI VIOLAZIONE

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Firma del Referente Privacy

_____

N. progressivo	Data della violazione	DESCRIZIONE sintetica della violazione (circostanze e causa).	Conseguenze della violazione	MISURE IMMEDIATE	VALUTAZIONE RISCHIO per i diritti e le libertà delle persone
	Momento in cui l'evento si è verificato.		Tipo e quantità dei dati personali oggetto della violazione. Numero dei soggetti coinvolti nella violazione.	Provvedimenti adottati per porre rimedio alla violazione.	Da valutare sempre. Se l'esito è di rischio "elevato": procedere con comunicazione agli interessati.

ALLEGATO N.2

PARERE del DPO	DATA di conoscenza della violazione da parte del DG	eventuale NOTIFICA al GPDP entro 72h	motivi dell'eventuale ritardo	eventuali ulteriori fasi di NOTIFICA	eventuale COMUNICAZIONE all'INTERESSATO
Determinazione del DPO a seguito dell'istruttoria del GAP.	Termine dal quale decorrono le 72 ore dalla notifica.	Estremi di protocollo e data.	Se la notifica della violazione è stata trasmessa al GPDP in un tempo >72h occorre giustificare il ritardo.	Se il titolare ha deciso di procedere alla "notifica per fasi" di cui alle LG del WP29	Se richiesta ai sensi dell'art.34 GDPR. Art.34 e Cons.86 ne descrivono condizioni, modalità e contenuti.

eventuale intervento del GPDP a seguito della notifica	ANNOTAZIONE casi non ritenuti da notificare al Garante
La notifica può aver dato luogo ad un intervento del GPDP nell'ambito dei suoi compiti e poteri.	

ALLEGATO N. 3

Modello per la segnalazione di un sospetto caso di *data breach*

Data

Al DPO
protocollo@pec.ausl.bologna.it
Via Castiglione, 29 40124
Bologna

Responsabile del trattamento (Ditta/Azienda…)
_____

Nome e Cognome e recapito telefonico del soggetto che trasmette l'episodio:
_____

Denominazione del Titolare

_____

Denominazione della/e banca/banche dati oggetto di *data breach* e breve descrizione della violazione dei dati personali ivi trattati:
_____

_____

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- Il _____
- Tra il _____ e il _____
- In un tempo che non è ancora stato possibile determinare

☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili): _____

_____

Modalità di esposizione al rischio (compilare solo se a conoscenza)**:**_____

_____

Tipo di violazione

- Distruzione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- Perdita
- Modifica
- Divulgazione non autorizzata
- Accesso non autorizzato
- Altro :

Dispositivo oggetto della violazione

Computer

- Rete
- Dispositivo mobile
- File o parte di un file

- Strumento di *backup*
- Documento cartaceo
- Campione
- Altro:

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione (compilare solo se a conoscenza)**:**

_____

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

N. persone
Circa persone
Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- Dati anagrafici/codice fiscale
- Dati di accesso e di identificazione (*username*, *password*, *customer ID*, altro)
- Dati relativi a minori
- Dati personali idonei a rivelare l'origine razziale o etnica, le convinzioni religiose o filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- Dati personali relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona
- Dati giudiziari
- Copia per immagine su supporto informatico di documenti analogici
- Ancora sconosciuto
- Altro:

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del delegato)?

- Basso/trascurabile
- Medio
- Alto
- Molto alto

Misure tecniche e organizzative applicate ai dati oggetto di violazione (compilare solo se a conoscenza)**:**

_____

_____

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future (compilare solo se a conoscenza)**?** _____

_____

Data **Firma**

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI

COMUNICAZIONE AL GARANTE

(art. 33 del Regolamento UE 2016/679)

Amministrazione titolare del trattamento

Denominazione o ragione sociale _____

Provincia _____ **Comune** _____

Cap _____ **Indirizzo** _____

Nome persona fisica addetta alla comunicazione _____

Cognome persona fisica addetta alla comunicazione _____

Funzione rivestita _____

Indirizzo PEC e/o EMAIL per eventuali comunicazioni _____

Recapito telefonico per eventuali comunicazioni _____

Eventuali Contatti (altre informazioni) _____

Allegato 1

Denominazione della/e banca/banche dati oggetto di data breach e breve descrizione della violazione dei dati personali ivi trattati

Quando si è verificata la violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ Il _____
- ☐ Tra il _____ e il _____
- ☐ In un tempo non ancora determinato
- ☐ E' possibile che sia ancora in corso

Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

Modalità di esposizione al rischio

Tipo di violazione

- ☐ Lettura (presumibilmente i dati non sono stati copiati)
- ☐ Copia (i dati sono ancora presenti sui sistemi del titolare)
- ☐ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
- ☐ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione)
- ☐ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione)
- ☐ Altro :

Allegato 1

Dispositivo oggetto della violazione

- ☐ Computer
- ☐ Rete
- ☐ Dispositivo mobile
- ☐ File o parte di un file
- ☐ Strumento di *backup*
- ☐ Documento cartaceo
- ☐ Altro :

Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

Quante persone sono state colpite dalla violazione dei dati personali trattati nell'ambito della banca dati?

- ☐ N. _____ persone
- ☐ Circa _____ persone
- ☐ Un numero (ancora) sconosciuto di persone

Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici/codice fiscale
- ☐ Dati di accesso e di identificazione (*user name*, *password*, *customer ID*, altro)
- ☐ Dati relativi a minori
- ☐ Dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
- ☐ Dati personali idonei a rivelare lo stato di salute e la vita sessuale
- ☐ Dati giudiziari
- ☐ Copia per immagine su supporto informatico di documenti analogici
- ☐ Ancora sconosciuto
- ☐ Altro :

Livello di gravità della violazione dei dati personali trattati nell'ambito della banca dati (secondo le valutazioni del titolare)?

- ☐ Basso/trascurabile
- ☐ Medio
- ☐ Alto
- ☐ Molto alto

Allegato 1

Misure tecniche e organizzative applicate ai dati oggetto di violazione

La violazione è stata comunicata anche agli interessati?

- ☐ Sì, è stata comunicata il
- ☐ No, perché _____

Qual è il contenuto della comunicazione resa agli interessati?

Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?