SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Imola

FRONTESPIZIO DELIBERAZIONE

AOO: AS_BO66

REGISTRO: Deliberazione

NUMERO: 0000102

DATA: 15/05/2019 10:16

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

SOTTOSCRITTO DIGITALMENTE DA:

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

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

CLASSIFICAZIONI:

- [07-05]

DESTINATARI:

- Collegio sindacale
- UO SEGRETERIA GENERALE E AFFARI LEGALI

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000102_2019_delibera_firmata.pdf	Donattini Maria Teresa; Fiorentini Sabrina; Neri Andrea; Rossi Andrea	1CEAEB391EB191E1CC3A8637B9E2B5B2 299E2844F0484715D3F98F9AE4DA21C2
DELI0000102_2019_Allegato1.docx:		F03F6592562EA7A81D24B957EC62761D2 0BAA92FB6816AF67D379B2836660546
DELI0000102_2019_Allegato2.docx:		F094546E1D625B414292BDBD74A3E31E6 7B79ECFDEB24F29D3E9D5DC6C71542D
DELI0000102_2019_Allegato3.xlsx:		6441CE3C91DF8A965A8DCAF0DF86FF70 10D7FAC8B2DF0DD8B771A6810167665D
DELI0000102_2019_Allegato4.docx:		289553F4CFEAF29E8DA4E9E435D22C6C 2CE3FEA57F0A159EDF980D19F0D11B37
DELI0000102_2019_Allegato5.pdf:		2DC15E14FB2B3C16CF4D39C73F4B33CA 8E362B5526A80C1291BD97A579B735F8

DELIBERAZIONE

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

IL DIRETTORE GENERALE

- richiamati i seguenti riferimenti normativi:
- 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);
- D. Lgs. 196/2003 (Codice per la protezione dei dati personali) e il D. Lgs. 10 agosto 2018 n. 101 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 207/679;

- visti in particolare gli artt. 33 e 34 del regolamento UE 2016/679 che disciplinano gli adempimenti a carico del Titolare del trattamento in caso di violazioni dei dati personali;

- richiamata la deliberazione n. 142 del 29.6.2018 di nomina del DPO condiviso con Azienda USL di Bologna, Azienda ospedaliero universitaria di Bologna, IOR e Montecatone Spa e dato atto che è compito del DPO, tra gli altri, la promozione di iniziative congiunte tra le Aziende/enti, affinchè l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti;

- richiamata inoltre la deliberazione n. 275 del 21.12.2018 "Regolamento (UE) 2016/679. Definizione dell'organigramma aziendale: referenti privacy (e relative funzioni), soggetti autorizzati al trattamento dei dati personali e gruppo aziendale privacy. Approvazione istruzioni operative generali";

- dato atto che gli uffici competenti delle richiamate amministrazioni, con il coordinamento e la supervisione del DPO, hanno condiviso un modello di procedura di gestione delle violazioni di dati personali (salve le specifiche organizzative in capo ai singoli enti), da utilizzare in luogo delle procedure in uso;

- ritenuto pertanto di approvare la procedura per la gestione delle violazioni dei dati personali, ai sensi degli artt. 33 e 34 del regolamento UE 2016/679, conforme al modello condiviso in ambito metropolitano, visto il parere del DPO in atti al prot. n. 12504 del 18.4.2019;

Delibera

1. di approvare la procedura per la gestione di violazioni dei dati personali o Data Breach ai sensi degli artt. 33 e 34 del Regolamento UE 2016/679, nel testo condiviso in ambito metropolitano e con il DPO, procedura allegata alla presente deliberazione quale parte integrante unitamente agli allegati (n. 4) della medesima;

2. di trasmettere la presente deliberazione ai Referenti privacy nominati ai sensi della deliberazione n. 275 del 21.12.2018 (Direttori di Unità operativa complessa, semplice dipartimentale e di programma gestionale, oltre che Responsabili delle Tecnostrutture in staff alla Direzione), per gli adempimenti di competenza e per la diffusione della procedura ai collaboratori;

3. trasmettere la deliberazione ai componenti del Gruppo aziendale privacy;

4. di pubblicare, al fine di garantire la massima diffusione e la pronta disponibilità della procedura, la presente deliberazione completa di tutti gli allegati, nella intranet aziendale sezione privacy, nonché nel sito internet dell'Azienda, sezione privacy;

5. di trasmettere il presente atto al Collegio Sindacale ai sensi dell'art. 18, comma 4, della L.R. 16.7.2018 n. 9.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Imola

Procedura per la gestione di violazione dei dati personali o Data Breach (artt. 33 e 34 Regolamento Europeo 679/2016)

La presente 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

Sommario

Allegati

1) **Report interno per la comunicazione del Data Breach al Coordinatore del GAP**
2) **Registro delle violazioni**
3) **Report Responsabile del trattamento per la comunicazione del Data Breach al DPO**
4) **Modello di notifica del Titolare 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, RGPD o *General Data Protection Regulation*, *GDPR*), 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. 7 marzo 2005, n.82, Codice dell'Amministrazione Digitale (CAD), e ss.mm. ed ii.
- Codice di Procedura Penale, artt.331 (Denuncia da parte di pubblici ufficiali e incaricati di pubblico servizio) e 361 (Omessa denuncia di reato 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 (Adesione ed obblighi dei fornitori di servizi) 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).

Si richiama inoltre la deliberazione n. 275 del 21.12.2018 "Regolamento UE 2016/679. Definizione dell'organigramma aziendale: referenti privacy (e relative funzioni), soggetti autorizzati al trattamento dei dati personali e gruppo aziendale privacy. Approvazione istruzioni operative generali"

2. Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera *identificabile* la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, un numero di identificazione, 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 (GDPR art.4, punto 1).
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 (GDPR, 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 (GDPR, art. 4, punto 7). In questo contesto, sono Titolari del trattamento le Aziende sanitarie, in persona del legale rappresentante (Direttore generale).

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 e svolge specifici compiti e funzioni connessi al trattamento dei dati personali (GDPR, 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 (GDPR, 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.

Coordinatori del GAP: i Dirigenti aziendali deputati a coordinare le attività, gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali.

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, paragrafo 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. Violazione dei dati personali o 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 conferma le valutazioni di potenziale Data Breach, lo segnala tempestivamente ai Coordinatori del Gruppo Aziendale Privacy indirizzando la mail a “gap@ausl.imola.bo.it” (lista di distribuzione che comprende tutto il GAP e relativa segreteria nonché Direttore UOTIR e Direttore DAT). A tal fine si può utilizzare il report di sintesi allegato al presente documento (**Allegato 1 – Report interno per la comunicazione del Data Breach ai Coordinatori del GAP**). Anche nel caso in cui sia il referente privacy a venire direttamente a conoscenza del potenziale caso di Data Breach, la procedura da seguire è la medesima.
I Coordinatori del Gruppo Aziendale Privacy, effettuano una prima valutazione dell’evento, avvalendosi dei componenti del Gruppo Aziendale Privacy competenti alla trattazione del caso specifico e di eventuali altre professionalità necessarie per la corretta analisi del caso e comunicano l’esito dell’analisi preliminare effettuata al DPO, al fine di avvalersi della sua consulenza.
I Coordinatori del Gruppo Aziendale Privacy, completata l’istruttoria avvertono inoltre il Direttore Generale, nonché il Direttore Sanitario ed il Direttore Amministrativo comunicando 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, in persona del Direttore Generale, assume le proprie determinazioni, disponendo la necessità o meno di notifica.

Nel caso in cui il Direttore Generale disponga la notifica i Coordinatori del Gruppo Aziendale Privacy predispongono la comunicazione all'Autorità Garante da sottoporre al DPO e al Titolare del trattamento.

Il Titolare, in persona del Direttore generale, trasmette la comunicazione all'Autorità Garante, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore da determinarsi dal momento in cui lo stesso, informato all'esito dell'istruttoria, 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 dalle 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 dell'effettuazione di ulteriori indagini e attività di follow up (c.d. notifica in fasi).

L'avvenuta notificazione al Garante viene documentata dai Coordinatori del Gruppo Aziendale Privacy nel **Registro delle violazioni** (**Allegato 2**) dagli stessi curato e tenuto. Tale registro ha durata annuale, contiene tutte le segnalazioni ricevute e gestite durante l'anno ed entro il 31 dicembre deve essere chiuso. Entro il 31 gennaio dell'anno successivo i Coordinatori del Gruppo Aziendale Privacy provvedono ad inviarlo al Titolare del trattamento e al DPO con nota protocollata, ai fini della conservazione ai sensi di legge.

Si precisa che anche i casi segnalati e non ritenuti dal Titolare da notificare insieme alle motivazioni sottese devono essere documentate nel medesimo Registro.

Nel caso di assenza o impedimento del Coordinatore del GAP per la parte informatica, le relative funzioni sono svolte dal Direttore dell'UOTIR (o dirigente delegato) e in caso di assenza o impedimento dell'ulteriore Coordinatore del GAP, le relative funzioni sono svolte dal Direttore del Dipartimento Amministrativo e tecnico (o dirigente delegato). Restano fermi i compiti dei componenti del Gruppo.

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 quello 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 di Data Breach ricevuto ai Coordinatori del Gruppo Aziendale Privacy (mail: gap@ausl.imola.bo.it) e da questo momento

vengono eseguiti i medesimi step della procedura illustrata al punto 4.1 (attraverso la necessaria collaborazione del Responsabile del trattamento).

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

Il Gruppo Aziendale Privacy, sotto la supervisione dei Coordinatori, è responsabile, sulla base delle rispettive competenze, in base alla tipologia della violazione e dell'analisi tecnica dell'evento, della individuazione 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 eventuale notifica al Garante della privacy e della eventuale comunicazione agli interessati. Si sottolinea 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 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"*. 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 paragrafo n. 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, eventuale ricorso ai media (quando l'impatto è 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 affermativa 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 di Data Breach con "probabile" rischio per i diritti e le libertà delle persone fisiche si procede 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

I Coordinatori del Gruppo Aziendale Privacy e il DPO, con il supporto dei componenti del Gruppo Aziendale Privacy, sulla base delle rispettive competenze, dovranno 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 secondo le prassi aziendali.

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 n. 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:

- la natura della violazione;
- 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, i Coordinatori 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 250), 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 GDPR, prescrive al Titolare di documentare qualsiasi violazione di dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma.

Pertanto, i Coordinatori del Gruppo Aziendale Privacy sono responsabili dell'inserimento di tutte le attività indicate sopra nel registro delle violazioni, 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
- 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 delle relazioni con Clienti e Fornitori

Allegato alla procedura per la gestione di violazioni dei dati personali o Data Breach

REPORT interno per la comunicazione ai Coordinatori del GAP

(da inviare ai Coordinatori del GAP o loro delegati: gap@ausl.imola.bo.it)

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 _____ e il _____

☐ Tra 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

Allegato alla procedura per la gestione di violazioni dei dati personali o Data Breach

REPORT interno per la comunicazione ai Coordinatori del GAP

(da inviare ai Coordinatori del GAP o loro delegati: gap@ausl.imola.bo.it)

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

Allegato alla procedura per la gestione di violazioni dei dati personali o Data Breach

REPORT interno per la comunicazione ai Coordinatori del GAP

(da inviare ai Coordinatori del GAP o loro delegati: gap@ausl.imola.bo.it)

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

_____

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Imola

Allegato alla procedura per la gestione del Data Breach

Registro delle violazioni

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	PARERE del DPO	DATA di conoscenza della violazione da parte del DG
	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.	Determinazione del DPO a seguito dell'istruttoria del GAP.	Termine dal quale decorrono le 72 ore dalla notifica.

Eventuale NOTIFICA al GPDP entro 72h	MOTIVI dell'eventuale ritardo	Eventuali ulteriori fasi di NOTIFICA	Eventuale COMUNICAZIONE all'INTERESSATO	Eventuale intervento del GPDP a seguito della notifica	ANNOTAZIONE casi non ritenuti da notificare al Garante
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.	La notifica può aver dato luogo ad un intervento del GPDP nell'ambito dei suoi compiti e poteri.	

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Imola

Allegato alla procedura per la gestione di violazioni dei dati personali o Data Breach

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?