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

FRONTESPIZIO DELIBERAZIONE

AOO: ausl_fe

REGISTRO: Deliberazione

NUMERO: 0000045

DATA: 28/02/2020 09:59

OGGETTO: APPROVAZIONE DEL REGOLAMENTO "PROCEDURA PER LA GESTIONE DEI CASI DI VIOLAZIONE DEI DATI PERSONALI (C.D. DATA BREACH)"

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Vagnini Claudio in qualità di Direttore Generale
Con il parere favorevole di Natalini Nicoletta - Direttore Sanitario
Con il parere favorevole di Carlini Stefano - Direttore Amministrativo

CLASSIFICAZIONI:

- [01-01]

DESTINATARI:

- Collegio sindacale
- DIREZIONE DISTRETTO CENTRO NORD
- DIREZIONE GENERALE
- DIREZIONE SANITARIA
- UO DIREZIONE ATTIVITA VETERINARIE
- UO SERVIZIO COMUNE GESTIONE PERSONALE
- UO SERVIZIO COMUNE FORMAZIONE E AGGIORNAMENTO
- UO SERVIZIO COMUNE ECONOM E GEST CONTRATTI
- UO SERVIZIO COMUNE TECNICO E PATRIMONIO
- UO SERVIZIO COMUNE TECNOL DELLA COMUN E INFORM
- UO SERVIZIO ASSICURATIVO COMUNE E DEL CONTENZIOSO
- UO SERVIZI AMMINISTRATIVI DISTRETTUALI
- UO SERVIZI AMMINISTRATIVI PUO
- DIPARTIMENTO CURE PRIMARIE
- DIPARTIMENTO SANITA PUBBLICA
- DIPARTIMENTO ASS INT SALUTE MENTALE DP
- DIPARTIMENTO DIREZIONE ASS ZA OSPEDALIERA
- DAI - DIPARTIMENTO DI MEDICINA
- DAI - DIPARTIMENTO DI CHIRURGIA
- DAI - DIPARTIMENTO MATERNO INFANTILE
- DAI -DIPARTIMENTO DI EMERGENZA

- DAI - DIPARTIMENTO RADIOLOGIA
- DAI - DIPTO BIOTECNOLOGIE -TRASFUSIONALE E DI LABORATORIO
- MO AFFARI ISTITUZIONALI E DI SEGRETERIA
- UO COMUNICAZ ACCREDIT RISCHIO CLIN RIC INNOVAZIONE
- UO PREVENZIONE E SICUREZZA AMBIENTI DI LAVORO
- UO PROGRAM CONTR DELLA GESTIONE E DELLA MOB SAN E COMUN
- UO ECONOMICO FINANZIARIA
- DIREZIONE DISTRETTO OVEST
- DIREZIONE DISTRETTO SUD EST
- DIREZIONE AMMINISTRATIVA
- UO DIREZIONE INFERMIERISTICA E TECNICA
- DIREZIONE ATTIVITA SOCIO SANITARIE
- UO INGEGNERIA CLINICA
- UO ASSISTENZA FARMACEUTICA OSP E TERRITORIALE
- DIPARTIMENTO INT LE PREVENZIONE E PROTEZIONE (DIREZIONE STRATEGICA)

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000045_2020_delibera_firmata.pdf	Carlini Stefano; Natalini Nicoletta; Vagnini Claudio	D6147611F66A5B2023281285C9B4EAC3174525B9E89BB1629CF165B7E8C5CB72
DELI0000045_2020_Allegato1.doc:		BAA41DD3AD5BBB7A517D2C5FF36BBF4DD254B282228306ECB184841DDDB60C02
DELI0000045_2020_Allegato2.pdf:		F67A532D20FFAC3F8454EE436A7CF5F73DEDF22377A8B7E224F7A7CFA3B3DA99

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

DELIBERAZIONE

OGGETTO: APPROVAZIONE DEL REGOLAMENTO "PROCEDURA PER LA GESTIONE DEI CASI DI VIOLAZIONE DEI DATI PERSONALI (C.D. DATA BREACH)"

IL DIRETTORE GENERALE

Visti:
- il 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)”;
- il 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);
- il D.Lgs. 196/2003 Codice per la protezione dei dati personali;
- 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;
- le Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015;
- il D.Lgs. 82/2005 Codice dell’Amministrazione Digitale;
- gli artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale), di seguito anche denominato “c.p.p.”;
- il Decreto 9 gennaio 2008 del ministero degli interni in attuazione della Legge 155/2005 sulle infrastrutture critiche;
- il 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;
- l’Art. 13 del DPCM DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014 Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonchè dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376) (GU Serie Generale n.285 del 09-12-2014);

Dato atto che:
gli articoli 33 e 34 del Regolamento Generale sulla Protezione dei Dati (Reg. UE 2016/679, c.d. GDPR) prevedono che in caso di violazione dei dati personali (c.d. Data Breach) il Titolare dei dati personali (quindi, nel caso specifico, l'Azienda Usl di Ferrara") è tenuto:

(a) a procedere alla notifica del data breach al Garante per la protezione dei dati personali, entro 72 ore dal momento in cui ne è venuto a conoscenza;
(b) a comunicare ai singoli interessati la predetta violazione, senza ingiustificato ritardo;
(c) a registrare la violazione in un apposito Registro;

Vista la nota p.g. 10576 del 20.02.2020, con la quale il Data Protection Officer di questa Azienda ha trasmesso la bozza della procedura denominata “Linee Guida aziendali per la gestione della procedura per la notifica e la comunicazione delle violazioni di dati personali (c.d. Data Breach)”;

Ritenuto opportuno che la procedura per la gestione delle violazioni dei dati venga formalizzata, affinché tutti i Referenti Interni e i singoli soggetti autorizzati vengano messi a conoscenza degli adempimenti ai quali sono chiamati nel caso si verifichi un evento che sia sussumibile nel concetto di "violazione dei dati";

Richiamato il D. Lgs 33/2013 e s.m.i. recante "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni" e precisato che il presente provvedimento sarà posto in pubblicazione nella sezione "Atti amministrativi generali" di "Amministrazione Trasparente";

Ritenuto quindi di approvare la procedura denominata “Linee Guida aziendali per la gestione della procedura per la notifica e la comunicazione delle violazioni di dati personali (c.d. Data Breach)”, allegata al presente provvedimento a farne parte integrante e sostanziale;

Dato atto che il presente provvedimento risponde ai principi di legittimità, opportunità e convenienza;

Delibera

1) Di approvare la procedura denominata “Linee Guida aziendali per la gestione della procedura per la notifica e la comunicazione delle violazioni di dati personali (c.d. Data Breach)”, allegata al presente provvedimento a farne parte integrante e sostanziale;

2) Di dare al presente provvedimento la massima divulgazione all’interno delle Strutture aziendali, anche attraverso la pubblicazione sul sito web aziendale;

3) Di prevedere, a cura del M.O. Affari Istituzionali e di Segreteria, la pubblicazione nella sezione “Atti amministrativi generali” di “Amministrazione Trasparente” del sito istituzionale di questa Amministrazione;

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

Procedura per la gestione dei casi di Violazione dei dati personali (c.d. *Data Breach*)

Sommario

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)", di seguito anche denominato "D.Lgs. 101/18".
- 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), di seguito anche denominato "Regolamento".
- D.Lgs. 196/2003 Codice per la protezione dei dati personali, di seguito anche denominato "Codice".
- 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, di seguito anche denominate "Linee guida";
- Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche - 2 luglio 2015.
- D.Lgs. 82/2005 Codice dell'Amministrazione Digitale, di seguito anche denominato "CAD"
- artt. 331 e 361 del Codice di Procedura Penale (obbligo di denuncia da parte del pubblico ufficiale), di seguito anche denominato "c.p.p.".

- 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 DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 24 ottobre 2014 Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonchè dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese. (14A09376) (GU Serie Generale n.285 del 09-12-2014).

1. Definizione di "violazione dei dati personali" (c.d. "data breach").

L'art. 33 del Regolamento prevede 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".*
La violazione dei dati personali (in inglese "data breach") è un evento in conseguenza del quale si verifica, appunto, una violazione di sicurezza che comporta, o può comportare, accidentalmente o illecitamente, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
Una violazione di sicurezza comporta generalmente la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati e può quindi compromettere la riservatezza, l'integrità o la disponibilità di dati personali. A mero titolo esemplificativo costituisce una "violazione dei dati personali" l'accesso o l'acquisizione dei dati da parte di terzi non autorizzati, il furto o la perdita di dispositivi informatici contenenti dati personali, la deliberata alterazione di dati personali, l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni (virus, malware, ecc.), la perdita o la distruzione di dati personali a causa di incidenti, eventi avversi, incendi o altre calamità o la la divulgazione non autorizzata dei dati.
Secondo le Linee guida, le violazioni possono essere classificate in base ai seguenti tre principi ben noti 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.

L'**Allegato 1** contiene in maggior dettaglio alcuni esempi, non esaustivi, di possibili violazioni di dati personali, allo scopo di supportare i soggetti coinvolti nella procedura, nella valutazione in merito alla necessità di effettuare o meno la notifica di *data breach* all'Autorità Garante.

2. Gestione della violazione.

In caso di accertamento di violazione occorre procedere ai seguenti adempimenti, indicati nell'ordine:

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;
3. contenimento del danno;
4. valutazione della gravità dell'evento;
5. notifica al Garante per la protezione dei dati;
6. altre segnalazioni dovute;
7. comunicazione agli interessati, se necessario;
8. inserimento dell'evento nel Registro delle Violazioni;
9. azioni correttive specifiche e per analogia.

2.1. Gestione della violazione dei dati all'interno alla struttura.

Ogni operatore aziendale autorizzato a trattare dati (personale autorizzato), qualora venga a conoscenza di un potenziale caso di data breach, è tenuto ad avvisare tempestivamente, e comunque, entro tre ore da quanto ne è venuto a conoscenza, il Referente del trattamento dei dati della struttura a cui afferisce.
Il Referente, valutato l'evento, lo segnala tempestivamente al Dirigente ICT e al DPO secondo il mezzo più immediato (preferibilmente a mezzo email) compilando il modello allegato al presente documento (Allegato 2).
Il Dirigente ICT e il DPO, in accordo tra loro, effettuata una prima valutazione dell'evento, danno eventuali indicazioni al Referente per la completa compilazione del modello di cui all'Allegato. Il Referente ICT, in accordo con il DPO, alla luce della natura della violazione, può avocare a sé la compilazione del modello e la notifica al Garante.
Salvo diverso parere del DPO, il Referente ICT procede alla notifica al Garante secondo la procedura indicata nel sito della stessa Autorità, allo stato inviando il modello di cui all'Allegato 2 sottoscritto in forma digitale all'indirizzo PEC procotollo@pec.gpdt.it , il tutto entro 72 ore da quando il personale autorizzato ne era venuto a conoscenza.
Nel caso in cui la notifica venga eseguita oltre il termine delle 72 ore il Referente è tenuto a corredare la notifica delle ragioni del ritardo, da indicare nell'apposito riquadro.
Resta ferma la possibilità di fornire successivamente, all'Autorità Garante, le 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'evento che viene ritenuto costituire ipotesi di violazione dei dati, anche laddove non sia seguita la notifica al Garante, deve essere annotata nel Registro delle violazioni istituito dal Referente ICT.
Nell'ipotesi in cui non sia stata effettuata la notifica il Referente annota nel Registro delle violazioni anche detta circostanza, le ragioni per le quali non si è ritenuto di procedere e il parere del DPO.

2.2. Gestione della violazione dei dati esterno alla struttura

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 delle violazioni dei dati sia inclusa o allegata al suddetto contratto, e ciò allo scopo di fornire al responsabile designato la procedura e le istruzioni per informare il titolare del trattamento, senza ingiustificato ritardo, di ogni potenziale evento di violazione dei dati.
Il Responsabile del trattamento che venga a conoscenza di un potenziale caso di violazione dei dati è tenuto ad avvisare immediatamente, e comunque entro 12 ore, il Referente ICT (data-breach@ausl.fe.it) e il DPO dell'Azienda (dpo@ausl.fe.it) a mezzo posta elettronica (con indicato nell'oggetto: DATA BREACH) inviando contestualmente il modello di cui all'Allegato 2 già compilato.
Da questo momento dovranno essere eseguiti le medesime operazioni della procedura illustrata al punto 2.1 e il Referente competente è quello del Servizio che ha proceduto alla designazione del Responsabile esterno del trattamento o, in mancanza, il Referente ICT.
Resta fermo che l'onere di procedere alla sottoscrizione del modulo e alla notifica al Garante resta in carico al Referente ICT.

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

Laddove la violazione dei dati derivi da una violazione di natura tecnologica, il Referente ICT è tenuto a svolgere un'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 una violazione dei dati (Analisi Preliminare), verranno svolte tutte le operazioni necessarie a raccogliere gli elementi per una valutazione dell'evento (Analisi Approfondita) ai fini della notifica al Garante.
Si sottolinea ulteriormente che anche nel caso in cui dall'Analisi Preliminare emerga che la violazione dei dati non necessiti di notifica al Garante 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.
Alla luce del disposto di cui al l'art. 33 par. n. 4 del Regolamento (secondo il quale *"Qualora nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo"*), è essenziale raccogliere il maggior numero di informazioni e, laddove le stesse non siano ritenute esaustive, il Referente competente è tenuto a procedere alla 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;
- l'identificazione dei dati violati/distrutti/compromessi e relativi trattamenti;
- l'identificazione degli interessati;
-iI 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 di violazione dei dati, si procede con la notifica all'Autorità Garante.

4. Notifica all'Autorità Garante

La notifica effettuata dovrà contenere, oltre alle altre informazioni eventualmente richiesto dal modello di cui all'Allegato 2, 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 ed il numero approssimativo di registrazioni dei dati personali in questione;
2. l'indicazione del nominativo del Referente con i relativi dati di contatto;
3. l'indicazione del nome e dei dati di contatto del DPO nonché del numero di protocollo della comunicazione al Garante dello stesso (allo stato **20180048900**);
4. la descrizione delle probabili conseguenze della violazione;
5. 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 che, se del caso, per attenuare i possibili effetti negativi;

Nello specifico, la notifica al Garante dovrà essere effettuata dal Referente ICT a mezzo PEC (protocollo@pec.gpdp.it) e dovrà essere inviata per conoscenza anche al DPO.

5. Altre segnalazioni dovute.

Fermo restando l'eventuale obbligo di riferire all'autorità giudiziaria casi che costituiscano ipotesi di reato procedibili di ufficio, il Referente, avvalendosi della consulenza del DPO, e di altri eventuali Dirigenti compenti, dovrà valutare la necessità di informare altri organi quali:
- CERT-PA (in caso di incidenti informatici ai sensi della Circolare Agid n. 2/2017 del 18.04.2017);
- CNAIPC (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche).
- Gestore di Identità Digitale e ad Agid nel caso in cui si individui un uso anomalo di un'identità SPID (Sistema Pubblico di Identità Digitale).
In tale caso il Dirigente dovrà darne notizia al Direttore Generale.

6. Comunicazione agli interessati.

Nei casi previsti dall'art. 34 del Regolamento, il Referente è tenuto a comunicare gli interessati la violazione dei dati secondo le procedure previste della predetta norma.
Al fine di valutare la necessità di procedervi e, nel caso, il contenuto della comunicazione e le modalità per la comunicazione stessa, il Referente si avvale della consulenza del DPO.
In particolare, il Referente e il DPO dovranno valutare se è il caso di comunicare la violazione anche gli interessati, sulla base dei criteri previsti dall'art. 34 del Regolamento. A tale scopo va valutata la gravità del rischio per gli interessati e i loro diritti sulla base dei criteri di cui ai considerando n. 74 del Regolamento.
Se il rischio è grave occorre valutare la possibilità 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.
La forma di comunicazione prescelta verrà predisposta e curata dal Referente, sulla base delle indicazioni fornite dal DPO.

7. Inserimento dell'evento nel Registro delle Violazioni

Ai sensi di quanto disposte l'art. 33, par. 5 del Regolamento, al fine di consentire al Garante di verificare il rispetto della norma, il Referente è tenuto all'inserimento di tutte le attività sopra indicate nel Registro delle violazioni, che devono essere documentate, tracciabili, e in grado di fornire evidenza dello svolgimento di quanto prevede la presente procedura.
Al fine di consentire al Titolare e al DPO di valutare eventuali interventi correttivi sui trattamenti svolti, il Referente ICT, fino all'attivazione di un Registro automatizzato, è tenuto a trasmettere il Registro medesimo al Direttore Generale, ai Responsabili del trattamento (Direttore Amministrativo e Direttore Sanitario) e al DPO, oltre che ogni volta ciascuno di loro lo richieda, entro il 31 dicembre di ogni anno.

8. Miglioramento

La fase del "miglioramento" è una fase necessariamente successiva alla comunicazione agli interessati che interessa la singola ipotesi di violazione dei dati e, periodicamente, l'insieme delle violazioni accertate e registrate, e comprende:
- l'analisi della relazione dettagliata sull'incidente
- la reiterazione del processo di Gestione del rischio informativo
- l'eventuale revisione della presente procedura e di eventuali altri documenti collegati (es. Analisi del rischio, Misure di sicurezza, regolamento sull'uso dei sistemi informativi, regolamento aziendale sul trattamento dei dati);
- l'individuazione di controlli che diminuiscano la probabilità dell'incidente o i relativi impatti sul sistema colpito e su sistemi analoghi
- la revisione del Sistema di Gestione della Privacy
- la revisione delle relazioni con Clienti e Fornitori
- la revisione annuale della procedura.

Tale fase viene svolta, anche autonomamente, dal Referente, dal Referente ICT, dal DPO e/o dal Titolare il quale ultimo, in esito a ciascuna violazione esterna all'Azienda, anche su segnalazione del DPO, può avviare un controllo nei confronti del Responsabile del trattamento esterno.

Allegato 1

Tipo di Breach	Definizione	Estensione minima/Soglia di segnalazione	Esempi	Controesempi
Distruzione	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, né di altri. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	**Caratteristiche:** Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione	Rottura dell'ecografo prima di inviare al sistema centrale l'immagine. Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente Incendio di archivio cartaceo delle cartelle cliniche. Distruzione di campioni biologici	Rottura di una chiavetta USB che non contiene dati personali originali (in unica copia) Rottura di un PC che non contiene dati personali originali (in unica copia) Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
Perdita	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	**Caratteristiche:** Dati non recuperabili o provenienti da procedure non ripetibili Dati relativi a più assistiti, relativi a interi episodi o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato	Smarrimento di chiavetta USB contenente dati originali Smarrimento di fascicolo cartaceo personale dipendente	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa

		Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione		
Modifica	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	**Caratteristiche:** Modifiche sistematiche su più casi. Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Guasto tecnico che altera parte dei contenuti di un sistema clinico, compromettendo anche i backup Azione involontaria o fraudolenta, di un utente che porta alla alterazione di dati sanitari in modo non tracciato e irreversibile	Guasto tecnico che altera parte dei contenuti di un sistema clinico, rilevato e sanato tramite operazioni di recovery Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile Modifica di un documento non ancora validato dal proprio autore.
Divulgazione non Autorizzata	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Malfunzionamento del sistema di oscuramento del sistema dipartimentale che invia a SOLE Consegna di un CD con dati dei pazienti ad altra struttura senza autorizzazione	Il medico sul proprio sistema dipartimentale seleziona il paziente Mario Rossi ma visita il paziente Luca Bianchi. Inserisce anamnesi e gli altri valori di refertazione ed invia a SOLE. Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.

Accesso non Autorizzato	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche incaricati dal titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione.	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema clinico	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi Accesso non autorizzato di un documento non ancora validato dal proprio autore.
Indisponibilità temporanea del dato	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	Infezione da ransonware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup Cancellazione accidentale dei dati da parte di una persona non autorizzata Perdita della chiave di decrittografia di dati crittografati in modo sicuro Irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento nev	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in cors

Il *data breach* per eccellenza, generalmente, è un attacco informatico, ma può consistere anche in un accesso abusivo, in un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).

I casi di *data breach* per le casistiche già descritte si estendono ai documenti cartacei o su supporti analogici.

La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach,* ma è considerato un normale errore procedurale.

All. 2

Modello per la segnalazione di un sospetto caso di *violazione dei dati*

DIREZIONE GENERALE
Via Cassoli, 30 – 44100 FERRARA
Responsabile della Protezione dei Dati
T. +39.0532.235579 – F. +39.0532.235648
dpo@ausl.fe.it

Azienda Unità Sanitaria Locale di Ferrara
Sede legale Via Cassoli, 30 – 44100 Ferrara
T. +39.0532.235111 – F. +39.0532.235648
Partita IVA 01295960387

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

VIOLAZIONE DI DATI PERSONALI – MODELLO DI NOTIFICA AL GARANTE

I titolari di trattamento di dati personali sono tenuti a notificare al Garante le violazioni dei dati personali (*data breach*) che comportano accidentalmente o in modo illecito la distruzione, la perdita, la modificazione, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, anche nell'ambito delle comunicazioni elettroniche, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà degli interessati.

La notifica non deve includere i dati personali oggetto di violazione (es. non fornire i nomi dei soggetti interessati dalla violazione).
Si ricorda che chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice in materia di protezione dei dati personali (Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante), salvo che il fatto non costituisca più grave reato.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Notifica di una violazione dei dati personali

(art. 33 del Regolamento (UE) 2016/679 – RGPD e art. 26 del d.lgs. 51/2018)

Tipo di notifica

Preliminare[1]	Completa	Integrativa [2] rif.
Effettuata ai sensi del	art. 33 RGPD	art. 26 d.lgs 51/2018

Sez. A - Dati del soggetto che effettua la notifica

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B - Titolare del trattamento

Denominazione[3]:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Stato:
Indirizzo:
CAP : Città: Provincia:
Telefono:
E-mail:
PEC:

1 Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione con riserva di effettuare una successiva notifica integrativa. E' obbligatoria la compilazione delle sezioni A, B, B1 e C.
2 Il titolare del trattamento integra una precedente notifica (inserire il numero di fascicolo assegnato alla precedente notifica, se noto)
3 Indicare nome e cognome nel caso di persona fisica

Sez. B1- Dati di contatto per informazioni relative alla violazione

Indicare i riferimenti del soggetto da contattare per ottenere maggiori informazioni circa la violazione

o Responsabile della protezione dei dati[4] - prot. n.

o Altro soggetto[5]

Cognome Nome
E-mail:
Recapito telefonico per eventuali comunicazioni:
Funzione rivestita:

Sez. B2- Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare o responsabile del trattamento[6], rappresentante del titolare non stabilito nell'Ue)

Denominazione[7] *:
Codice Fiscale/P.IVA: Soggetto privo di C.F./P.IVA ☐
Ruolo: ◦ Contitolare ◦ Responsabile ◦ Rappresentante

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ◦ Contitolare ◦ Responsabile

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ◦ Contitolare ◦ Responsabile

Denominazione *: ……..……..……..
Codice Fiscale/P.IVA: ……..……..… Soggetto privo di C.F./P.IVA ☐
Ruolo: ◦ Contitolare ◦ Responsabile

[4] Qualora designato, indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD
[5] In assenza di un RPD, indicare i riferimenti di un punto di contatto designato per la notifica in questione
[6] In tale tipologia rientra anche il Responsabile individuato ai sensi art. 28, par. 4
[7] Indicare nome e cognome nel caso di persona fisica

Sez. C - Informazioni di sintesi sulla violazione

1. **Indicare quando è avvenuta la violazione**
   - o Il
   - o Dal (la violazione è ancora in corso)
   - o Dal al
   - o In un tempo non ancora determinato

   Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. **Momento in cui il titolare del trattamento è venuto a conoscenza della violazione**
   Data: Ora:

3. **Modalità con la quale il titolare del trattamento è venuto a conoscenza della violazione**
   - o Il titolare è stato informato dal responsabile del trattamento
   - o Altro[8]

4. **In caso di notifica oltre le 72 ore, quali sono i motivi del ritardo?[9]**

5. **Breve descrizione della violazione**

[8] Ad esempio: Segnalazione da parte di un interessato, comunicazione da parte di terzi, ecc.

[9] Da compilare solo per notifiche tardive.

6. **Natura della violazione**
   - ☐ a) Perdita di confidenzialità[10]
   - ☐ b) Perdita di integrità[11]
   - ☐ c) Perdita di disponibilità[12]

7. **Causa della violazione**
   - ☐ Azione intenzionale interna
   - ☐ Azione accidentale interna
   - ☐ Azione intenzionale esterna
   - ☐ Azione accidentale esterna
   - ☐ Sconosciuta
   - ☐ Altro (specificare)

8. **Categorie di dati personali 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 (numero di conto corrente, dettagli della carta di credito, altro…)
   - ☐ Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
   - ☐ Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza o di prevenzione
   - ☐ Dati di profilazione
   - ☐ Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
   - ☐ Dati di localizzazione
   - ☐ Dati che rivelino l'origine razziale o etnica
   - ☐ Dati che rivelino opinioni politiche
   - ☐ Dati che rivelino convinzioni religiose o filosofiche
   - ☐ Dati che rivelino l'appartenenza sindacale
   - ☐ Dati relativi alla vita sessuale o all'orientamento sessuale
   - ☐ Dati relativi alla salute
   - ☐ Dati genetici
   - ☐ Dati biometrici
   - ☐ Categorie ancora non determinate
   - ☐ Altro

[10] Diffusione/ accesso non autorizzato o accidentale
[11] Modifica non autorizzata o accidentale
[12] Impossibilità di accesso,perdita, distruzione non autorizzata o accidentale

9. Indicare il volume (anche approssimativo) dei dati personali oggetto di violazione[13]

- o N.
- o Circa n.
- o Un numero (ancora) non definito di dati

10. Categorie di interessati coinvolti nella violazione

- ☐ Dipendenti/Consulenti
- ☐ Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
- ☐ Associati,soci, aderenti, simpatizzanti, sostenitori
- ☐ Soggetti che ricoprono cariche sociali
- ☐ Beneficiari o assistiti
- ☐ Pazienti
- ☐ Minori
- ☐ Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
- ☐ Categorie ancora non determinate
- ☐ Altro (specificare)

☐ Ulteriori dettagli circa le categorie di interessati

11. Numero (anche approssimativo) di interessati coinvolti nella violazione

- o N. interessati
- o Circa n. interessati
- o Un numero (ancora) sconosciuto di interessati

[13] Ad esempio numero di referti, numero di record di un database, numero di transazioni registrate.

Sez. D - Informazioni di dettaglio sulla violazione

1. **Descrizione dell'incidente di sicurezza alla base della violazione**[14]

2. **Descrizione delle categorie di dati personali oggetto della violazione**[15]

3. **Descrizione dei sistemi e delle infrastrutture IT coinvolti nell'incidente, con indicazione della loro ubicazione**

4. **Misure di sicurezza tecniche e organizzative adottate per garantire la sicurezza dei dati, dei sistemi e delle infrastrutture IT coinvolti**[16]

[14] Segue punto 5, 6 e 7 della sez. C
[15] Segue punto 8 della sez. C
[16] Indicare le misure in essere al momento della violazione

Sez. E - Possibili conseguenze e gravità della violazione

1. Possibili conseguenze della violazione sugli interessati

a) In caso di perdita di confidenzialità: [17]

☐ I dati sono stati divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
☐ I dati possono essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
☐ I dati possono essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito
☐ Altro (specificare)

b) In caso di perdita di integrità:[18]

☐ I dati sono stati modificati e resi inconsistenti
☐ I dati sono stati modificati mantenendo la consistenza
☐ Altro (specificare)

c) In caso di perdita di disponibilità:[19]

☐ Mancato accesso a servizi
☐ Malfunzionamento e difficoltà nell'utilizzo di servizi
☐ Altro (specificare)

Ulteriori considerazioni sulle possibili conseguenze

[17] Da compilare solo nel caso in cui è stata selezionata l'opzione a) del punto 6, Sez. C
[18] Da compilare solo nel caso in cui è stata selezionata l'opzione b) del punto 6, Sez. C
[19] Da compilare solo nel caso in cui è stata selezionata l'opzione c) del punto 6, Sez. C

2. Potenziali effetti negativi per gli interessati

☐ Perdita del controllo dei dati personali
☐ Limitazione dei diritti
☐ Discriminazione
☐ Furto o usurpazione d'identità
☐ Frodi
☐ Perdite finanziarie
☐ Decifratura non autorizzata della pseudonimizzazione
☐ Pregiudizio alla reputazione
☐ Perdita di riservatezza dei dati personali protetti da segreto professionale
☐ Conoscenza da parte di terzi non autorizzati
Qualsiasi altro danno economico o sociale significativo (specificare)

3. Stima della gravità della violazione

- o Trascurabile
- o Basso
- o Medio
- o Alto

Indicare le motivazioni

Sez. F – Misure adottate a seguito della violazione

1. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione[20]) per porre rimedio alla violazione e ridurne gli effetti negativi per gli interessati**

2. **Misure tecniche e organizzative adottate (o di cui si propone l'adozione) per prevenire simili violazioni future**

[20] Nella descrizione distinguere le misure adottate da quelle in corso di adozione

Sez. G - Comunicazione agli interessati

1. **La violazione è stata comunicata agli interessati?**

- o Sì, è stata comunicata il
- o No, sarà comunicata
  il
  in una data da definire
- o No, sono tuttora in corso le dovute valutazioni[21]
- o No e non sarà comunicata perché:

a) il titolare del trattamento ritiene che la violazione dei dati personali non presenti un rischio elevato per i diritti e le libertà delle persone fisiche;
Spiegare le motivazioni

b) 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;

Descrivere le misure applicate

c) 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;

Descrivere le misure adottate

d) detta comunicazione richiederebbe sforzi sproporzionati.
Descrivere la modalità (comunicazione pubblica o misura simile) tramite la quale gli interessati sono stati informati

[21] Selezionando questa opzione, il titolare del trattamento si impegna a effettuare una integrazione alla presente notifica

2. **Numero di interessati a cui è stata comunicata la violazione**[22]

   N. interessati

3. **Contenuto della comunicazione agli interessati**

4. **Canale utilizzato per la comunicazione agli interessati**
   - ☐ SMS
   - ☐ Posta cartacea
   - ☐ Posta elettronica
   - ☐ Altro (specificare)

[22] Da compilare solo nel caso in cui al punto 1 venga scelta una delle prime due opzioni.

Sez. H - Altre informazioni

1. **La violazione coinvolge interessati di altri Paesi dello Spazio Economico Europeo[23]?**
   - o SI (indicare quali):
   - o NO
2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**
   - o SI (indicare quali):
   - o NO
3. **La violazione è stata notificata ad altre autorità di controllo[24]?**
   - o SI (indicare quali):
   - o NO
4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**
   - o SI (indicare quali):
   - o NO
5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**
   - o SI
   - o NO

[23] Fanno parte dello Spazio Economico Europeo tutti gli Stati membri della Unione Europea, nonchè l'Islanda, il Liechtenstein e la Norvegia
[24] Autorità di controllo così come definite ex art. 51 del Regolamento (UE) 2016/679
[25] Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

INFORMAZIONI SUL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'articolo 13 del Regolamento (UE) 2016/679 si rappresenta che il Garante per la protezione dei dati personali, in qualità di titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: garante@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterà i dati personali conferiti con il presente modulo, con modalità prevalentemente informatiche e telematiche, per le finalità previste dal Regolamento (UE) 2016/679 e dal Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003, n. 196 e s.m.i.), in particolare per l'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri attribuiti al Garante dalla disciplina vigente.

Il conferimento dei dati, fermo restando quanto previsto dall'art. 33, par. 4, del Regolamento (UE) 2016/679, è obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all'autorità di controllo. I dati acquisiti nell'ambito della procedura saranno conservati in conformità alle norme sulla conservazione della documentazione amministrativa.

I dati saranno trattati esclusivamente dal personale e da collaboratori del Garante o delle imprese espressamente designate come responsabili del trattamento. Al di fuori di queste ipotesi, i dati non saranno diffusi, né saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attività istruttoria e nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

Gli interessati hanno il diritto di ottenere dal Garante, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento UE 2016/679). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati presso il Garante (Garante per la protezione dei personali - Responsabile della Protezione dei dati personali, Piazza Venezia 11, 00187, Roma, email: rpd@gpdp.it).

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dalla disciplina in materia di protezione dei dati personali hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento (UE) 2016/679, o di adire le opportune sedi giudiziarie ai sensi dell'art. art. 79 del Regolamento citato.