# FRONTESPIZIO DELIBERAZIONE

AOO: ASL_BO

REGISTRO: Deliberazione

NUMERO: 0000146

DATA: 19/04/2019 16:26

OGGETTO: REGOLAMENTO UE 2016/679 IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (GDPR). APPROVAZIONE PROCEDURA PER LA GESTIONE DI VIOLAZIONE DEI DATI PERSONALI O DATA BREACH (ARTT. 33 E 34 GDPR).

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Gibertoni Chiara in qualità di Direttore Generale
In assenza di Novaco Francesca Caterina - Direttore Sanitario
Con il parere favorevole di Petrini Anna Maria - Direttore Amministrativo

Su proposta di Grazia Matarante - UO Anticorruzione, Trasparenza e Privacy (SC) che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [01-01-02]

DESTINATARI:

- Collegio sindacale
- Dipartimento Cure Primarie
- Dipartimento Salute Mentale - Dipendenze Patologiche
- Dipartimento Chirurgico
- Dipartimento Emergenza
- Dipartimento Medico
- Dipartimento Servizi
- Dipartimento Farmaceutico
- UO Anticorruzione, Trasparenza e Privacy (SC)
- Direzione Attivita' Socio-Sanitarie - DASS (SC)
- UO Presidio Ospedaliero Unico Aziendale (SC)
- UO Governo Clinico e Sistema Qualita' (SC)
- UO Controllo di Gestione e Flussi Informativi (SC)
- UO Sviluppo Organizzativo, Professionale e Formazione (SC)
- UO Medicina Legale e Risk Management (SC)
- Distretto di Committenza e Garanzia di San Lazzaro di Savena

- DATeR - Direzione Assistenziale Tecnica e Riabilitativa
- Servizio Unico Metropolitano Amministrazione del Personale (SUMAP)
- UO Libera Professione (SC)
- UO Amministrativa DSP (SC)
- Dipartimento Sanita' Pubblica
- Dipartimento Materno Infantile
- Dipartimento Oncologico
- Dipartimento Amministrativo
- DAAT - Dipartimento Attivita' Amministrative Territoriali
- UO Servizio Prevenzione e Protezione (SC)
- UO Servizi Amministrativi Ospedalieri (SC)
- UO Funzioni HUB (SC)
- UO Committenza e Specialistica Ambulatoriale (SC)
- UO Ingegneria Clinica (SC)
- Distretto di Committenza e Garanzia dell'Appennino Bolognese
- Distretto di Committenza e Garanzia della Citta' di Bologna
- Distretto di Committenza e Garanzia Pianura Ovest
- Distretto di Committenza e Garanzia Reno, Lavino e Samoggia
- Distretto di Committenza e Garanzia Pianura EST
- UOC Direzione Amministrativa IRCCS
- Dipartimento Tecnico-Patrimoniale
- IRCCS Istituto delle Scienze Neurologiche - Direzione Scientifica
- IRCCS Istituto delle Scienze Neurologiche - Direzione Operativa
- UO Amministrativa DCP (SC)
- UO Amministrativa DSM - DP (SC)
- Servizio Unico Metropolitano Economato (SUME)
- UO Amministrativa e Segreteria DATeR (SSD)
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)
- UO Affari Generali e Legali (SC)
- Direzione Generale

DOCUMENTI:

| File | Firmato digitalmente da | Hash |
|---|---|---|
| DELI0000146_2019_delibera_firmata.pdf | Gibertoni Chiara; Matarante Grazia; Petrini Anna Maria | 5EE156051F28B6C1DDFFD2CF3AC15190FF14F0F2C90761398147521DB6BC2A0B |
| DELI0000146_2019_Allegato1.pdf: | | 62A62A7A9D73A66E734898BA1F8D2272494AD2A455AB81D8D6D73FB1F6834DB1 |

**DELIBERAZIONE**

OGGETTO: REGOLAMENTO UE 2016/679 IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (GDPR). APPROVAZIONE PROCEDURA PER LA GESTIONE DI VIOLAZIONE DEI DATI PERSONALI O DATA BREACH (ARTT. 33 E 34 GDPR).

**IL DIRETTORE GENERALE**

Su proposta della Dr.ssa Grazia Matarante, Dirigente Amministrativo a tempo indeterminato, Direttore UO Anticorruzione, Trasparenza e Privacy (SC), la quale esprime contestuale parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente provvedimento;

Premesso:

- che il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (in seguito per brevità "GDPR", General Data Protection Regulation), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi sui diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento il compito di assicurare e di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure che ritiene a ciò più idonee ed opportune (c.d. principio di responsabilizzazione o *accountability*);

- che il richiamato GDPR detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le Aziende Sanitarie, attribuendo al titolare il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati;

- che il Decreto Legislativo n. 101 del 10 agosto 2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo, in attuazione dell'art.13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n.163) ha introdotto disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR, novellando il codice della privacy di cui al D.Lgs. n. 196/2003;

- che il " *sistema privacy*" delineato dal GDPR e confermato a livello nazionale dal D.Lgs. n. 101/2018 di modifica ed integrazione del D.Lgs. n. 196/2003, implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati, quale parte integrante dell'intero *asset* informa tivo di un'organizzazione, con particolare attenzione ai dati di salute (ivi compresi i dati biometrici e genetici);

- che il nuovo approccio comporta il coinvolgimento di tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione aziendale, con assunzione delle relative responsabilità;

- che la Regione Emilia-Romagna con DGR n.919 del 10/4/2018, avente ad oggetto: "Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l'anno 2018" ha previsto, fra gli obiettivi indicati al punto 4.6 dell'allegato B, oltre alla nomina del DPO e all'adozione del registro delle attività di trattamento, la ridefinizione e l'articolazione delle specifiche responsabilità privacy aziendali;

Richiamate le deliberazioni dell'Azienda USL di Bologna:

- n.372 del 28/12/2015, avente per oggetto: "Ridefinizione della struttura organizzativa delle Aree di attività amministrative territoriali, ospedaliere e di anticorruzione, trasparenza e privacy", con la quale si è provveduto, tra l'altro, ad individuare la UO Anticorruzione, Trasparenza e Privacy (SC);

- n. 12 del 29.01.2016, ad oggetto:"Provvedimenti conseguenti alla ridefinizione della struttura organizzativa delle aree di attività amministrative territoriali, ospedaliere e di anticorruzione, trasparenza e privacy di cui alla deliberazione n.372/2015", con la quale si è tra l'altro conferito, con decorrenza dalla data del 1.2.2016, l'incarico di Direzione della Struttura Complessa UO Anticorruzione, Trasparenza e Privacy (SC) alla Dr.ssa Grazia Matarante, Dirigente Amministrativo a tempo indeterminato di questa Azienda USL con trasferimento delle funzioni Privacy dalla UO Affari Generali e Legali (SC) alla UO Anticorruzione, Trasparenza e Privacy (SC);

- n. 47 del 13 febbraio 2017 con la quale sono state attribuite le deleghe all'adozione di atti amministrativi ai dirigenti responsabili di articolazioni organizzative aziendali con la quale sono state attribuite deleghe all'adozione di specifici atti amministrativi al Direttore della UO Anticorruzione, Trasparenza e Privacy (SC)

Vista la nota prot. n. 66887 del 25 maggio 2018 con la quale è stato adottato il Registro delle Attività di Trattamento dell'Azienda USL di Bologna;

Richiamata la nota prot. n. 61715 del 16 maggio 2018 con la quale, in conformità al GDPR sopra richiamato, è stata designata, in via temporanea, la dott.ssa Gian Carla Pedrazzi, quale Responsabile della Protezione dei dati personali a decorrere dal 25 maggio 2018 e fino alla conclusione delle procedure avviate per il conferimento dell'incarico di Responsabile della protezione dei dati (RDP o DPO);

Preso atto della Deliberazione n. 220 del 29/06/2018, recante "Designazione del Responsabile della Protezione dei Dati (RPD) ai sensi dell'art. 37 del Regolamento UE 2016/679", con la quale la Dr.ssa Federica Banorri è stata designata, a decorrere dal 1 luglio 2018, Responsabile della Protezione dati (RPD) dell'Azienda Usl di Bologna;

Considerato che il GDPR - con riferimento ai soggetti - disciplina espressamente, oltre al Responsabile della Protezione dei Dati (RPD) - Data Protection Officer (DPO), le figure del " **titolare del trattamento**" e del " **responsabile del trattamento**", riferendosi con quest'ultima espressione ai soli soggetti esterni alla organizzazione che trattano dati personali per conto del titolare del trattamento e delinea la categoria delle «persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare[...]» (art. 4, n. 10);

Preso atto che - in attuazione dell'art. 39 del GDPR ("Compiti del responsabile della protezione dei dati") - al DPO spettano le funzioni e i compiti di seguito riportati:

- informare e fornire consulenza alle Aziende/Enti, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- assicurare in collaborazione con i referenti Privacy attività di informazione/consulenza ai Responsabili del trattamento nonché ai dipendenti che, in qualità di autorizzati al trattamento, eseguono operazioni di trattamento dati;
- sorvegliare l'osservanza della normativa in materia di protezione dei dati personali e delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti aziendali individuati dalle singole Aziende/Enti dell'area metropolitana;
- fornire, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
- cooperare con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;

- supportare le strutture aziendali deputate alla tenuta del Registro del trattamento delle singole Aziende/Enti, al fine di uniformarne la predisposizione;
- garantire il corretto livello di interlocuzione con gli altri DPO delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE, ARA, GRU, GAAC);
- promuovere 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 nelle singole Aziende/Enti;
- favorire il coordinamento dei DPO delle altre aziende sanitarie regionali relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna, nota PG/2018/0482475 del 5 luglio 2018;

Considerato inoltre che l'Autorità Garante per la protezione dei dati personali, a sua volta, nel Documento Guida all´applicazione del Regolamento europeo in materia di protezione dei dati personali, *«ritiene opportuno che titolari […..] del trattamento mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento, così come delineatesi negli anni»;*

Rilevato che, ai sensi dell'art. 32 del GDPR, al titolare del trattamento competono le decisioni atte a garantire il profilo di sicurezza del trattamento dei dati personali, « *tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, […] mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio »*;

Rilevato, inoltre, che ai sensi degli artt.29 e 32 del GDPR chiunque agisca sotto l'autorità del titolare del trattamento e abbia accesso a dati personali possa trattare tali dati solo se adeguatamente istruito;

Richiamata la deliberazione n. 11 in data 14 gennaio 2019 ad oggetto: "Adeguamenti al Regolamento UE 2016/679, definizione dell'organigramma delle Responsabilità Privacy aziendali e modalità di individuazione dei referenti privacy aziendali e dei soggetti autorizzati al trattamento dei dati personali", tramite la quale si sono ridefinite l'organizzazione dei profili di responsabilità, la gestione degli adempimenti connessi al trattamento dei dati e si è provveduto alla costituzione di un Gruppo Aziendale Privacy (GAP), composto da: Direttore UO Anticorruzione, Trasparenza e Privacy (SC) con funzioni di coordinamento; Direttore UO Tecnologie Informatiche e di Comunicazione (SC) o suo delegato; Direttore Sanitario di Presidio o suo delegato; Direttore del Dipartimento di Cure Primarie o suo delegato; Direttore del Dipartimento di Sanità Pubblica o suo delegato; Direttore Direzione Assistenziale Tecnica e Riabilitativa o suo delegato; Direttore Operativo IRCSS o suo delegato; Direttore Amministrativo o suo delegato;

Osservato che una delle principali novità introdotte dal GDPR consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su meri adempimenti formali;

Dato atto che, già dal mese di luglio 2018, è stato attivato un Tavolo Privacy in ambito metropolitano composto dai Referenti Privacy delle Aziende Sanitarie dell'Area Metropolitana di Bologna, coordinato dal DPO, Dr.ssa Banorri, Tavolo al quale è stato affidato, tra gli altri compiti, quello di predisporre una procedura – da condividere in area metropolitana - per la gestione di violazione dei dati personali o Data Breach (artt. 33 e 34 del GDPR);

Atteso che, nell'ambito delle attività svolte dal suddetto Tavolo Privacy, è stata redatta una procedura per le gestione di violazione dei dati personali o Data Breach ex art. 33 e 34 del GDPR, procedura a disposizione dell'Autorità Garante per la Protezione dei dati Personali;

Ritenuto pertanto di approvare la procedura per la gestione di violazione dei dati personali o Data Breach ex artt. 33 e 34 del GDPR, condivisa in sede di Tavolo Privacy di ambito metropolitano;

Preso atto che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico del bilancio dell'Azienda Usl di Bologna;

**Delibera**

per le motivazioni esposte in premessa e che si intendono tutte integralmente riportate:

1. di approvare la procedura per la gestione di violazione dei dati personali o Data Breach ex artt. 33 e 34 del GDPR - condivisa in sede di Tavolo Privacy di ambito metropolitano -a disposizione dell'Autorità Garante per la Protezione dei dati Personali, Allegato 1 alla presente deliberazione;
2. di prendere atto che dall'adozione del presente provvedimento non derivano oneri aggiuntivi a carico del bilancio dell'Azienda Usl di Bologna;
3. di specificare che il Responsabile del Procedimento ai sensi della legge n.241/1990 e s.m.i. è la Dr.ssa Grazia Matarante, Dirigente Amministrativo a tempo indeterminato, Direttore della UO Anticorruzione, Trasparenza e Privacy (SC);
4. di trasmettere copia del presente atto a tutti i Referenti Privacy (Direttori di UOC-UOSD-UOSI e Programmi gestionali) e a tutti i componenti del Gruppo Aziendale Privacy:
5. di trasmettere copia del presente atto a:

- Direttori di Dipartimenti di Produzione Ospedaliera e Territoriale;
- Direttore Scientifico IRCCS;
- Direttore Operativo IRCCS;
- Direttore UO Amministrativa IRCCS;
- Direttore Dipartimento Amministrativo;
- Direttori di UO del Dipartimento Amministrativo;
- Direttore Dipartimento Tecnico Patrimoniale;

- Direttore Dipartimento Farmaceutico;
- DAAT – Dipartimento Attività Amministrative Territoriali;
- Direttori UO Staff specifico del DG-DS-DA;
- Direttori UO Staff di Direzione aziendale;
- Direttori di Distretto;
- DATeR – Direzione Assistenziale Tecnica e Riabilitativa
- Direttore UO Amministrativa DCP;
- Direttore UO Amministrativa DSM;
- Direttore UO Amministrativa DSP;
- Direttore UO Amministrativa DATeR
- DPO
- Collegio Sindacale.

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

# Procedura per la gestione di violazione dei dati personali o *data breach* (artt.33 e 34 Regolamento UE 2016/679)

La presente procedura deve essere diffusa a tutti i soggetti autorizzati al trattamento dei dati personali che, a diverso titolo, potranno e dovranno essere di ausilio al Titolare del trattamento.

Sommario



Allegati

1. **Report Referente Privacy (interno all'Azienda) per la comunicazione del Data Breach al Coordinatore del GAP o suo sostituto.**
2. **Registro aziendale delle violazioni.**
3. **Report Responsabile del trattamento (esterno all'Azienda) per la comunicazione del Data Breach al DPO**
4. **Modello di notifica del Titolare all'Autorità Garante.**

## 1. Normativa e documentazione aziendale di riferimento

- 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 artt.33 (Notifica all'Autorità di Controllo), 34 (Notifica agli interessati) e 28 (Responsabile del trattamento).
- D. Lgs. 30 giugno 2003, n.196, "Codice per la protezione dei dati personali" e ss.mm. ed ii..
- Garante per la protezione dei dati personali, "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679" (WP250), adottate il 3 ottobre 2017 ed emendate il 6 febbraio 2018.
- Garante per la protezione dei dati personali, "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati", provvedimento del 15 maggio 2014,di cui al doc. web n.3134436, attualmente in corso di aggiornamento;
- Garante per la protezione dei dati personali, "Misure di sicurezza e modalità di scambio dei dati personali tra Amministrazioni Pubbliche", provvedimento del 2 luglio 2015, di cui al doc. web n.4129029;
- 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. Serie Generale n. 144 del 21 giugno 2008).
- 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 9 dicembre 2014), art.13 (Adesione ed obblighi dei fornitori di servizi).
- Deliberazione aziendale n.11 del 14 gennaio 2019, "Adeguamenti al Regolamento (UE) 2016/679. Definizione dell'organigramma elle responsabilità privacy aziendali e modalità di individuazione dei referenti privacy aziendali e dei soggetti autorizzati al trattamento dei dati personali".
- Regolamento organizzativo aziendale aggiornato.

## 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 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 e che determina specifiche modalità organizzative rispetto ad uno o più trattamenti.
***Data Protection Officer (DPO) o Responsabile della Protezione dei Dati (RPD)***: 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 o del Responsabile del trattamento secondo le istruzioni del Titolare di trattamento, e che svolge specifici compiti e funzioni connessi al trattamento dei dati personali (GDPR art. 4 punto 10, art.29, art.32 punto 4).
***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 nel rispetto delle 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.
***Violazione dei dati personali*** o ***Data breach:*** si veda il §3.

## 3. Violazione dei dati personali o *Data Breach*

L'art.33 del GDPR recita: *"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 **violazione dei dati personali** o **Data Breach** si intende un evento in conseguenza del quale si verifica una 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 (GDPR art.4, punto 12).
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 principî 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.

A seconda dei casi, una violazione può riguardare contemporaneamente la riservatezza, l'integrità e la disponibilità dei dati personali, nonché una loro qualsiasi combinazione. Si precisa che una violazione avrà interessato la sfera della disponibilità se si sarà verificata una perdita o una distruzione permanente dei dati personali.

## 4. Gestione del Data Breach

In caso di segnalazione di violazione che rientri nella definizione di Data Breach, occorre seguire i seguenti steps del processo di accertamento ed eventuale notificazione:

1. acquisizione della notizia da parte dei soggetti preposti al ricevimento 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, nel caso in cui, a seguito di analisi dell'evento ravvisi una potenziale violazione, la segnala tempestivamente al Coordinatore del Gruppo Aziendale Privacy o al Gruppo Aziendale Privacy mediante l'invio all'indirizzo di posta elettronica del GAP gap@ausl.bologna.it. A tal fine si può utilizzare il report di sintesi allegato al presente documento (**Allegato 1 - Report Referente Privacy (interno all'Azienda) 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 o il vice Coordinatore del GAP, individuato nella figura del Direttore della UO Tecnologie Informatiche e di Comunicazione effettua una prima valutazione dell'evento, per accertarsi che l'incidente di sicurezza si sia effettivamente verificato. Per l'accertamento potrà avvalersi dei componenti del Gruppo Aziendale Privacy competenti alla trattazione del caso specifico e di eventuali ulteriori professionalità ritenute

necessarie per la corretta analisi del caso. Gli esiti della preliminare analisi saranno comunicati al DPO, al fine di ricorrere alla sua consulenza.

Completata l'istruttoria, il Coordinatore del Gruppo Aziendale Privacy o il suo sostituto trasmette al Titolare del trattamento l'esito della valutazione eseguita dal GAP in collaborazione con il DPO. Il Titolare viene così messo "a conoscenza" del potenziale caso di data breach. Infatti, nel caso in cui l'istruttoria abbia dato esito positivo, il Titolare raggiunge la ragionevole certezza che si sia verificato un incidente di sicurezza.
Il Titolare assume le proprie determinazioni, disponendo la necessità o meno di notifica sulla base di un giudizio di probabilità che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Nel caso in cui il Titolare disponga la notifica dà mandato al Coordinatore del Gruppo Aziendale Privacy o al suo sostituto di predisporre la comunicazione da inviare all'Autorità Garante. Predisposta la comunicazione, il Coordinatore del GAP provvederà a sottoporla al DPO e al Titolare del trattamento per la trasmissione all'Autorità Garante.
L'invio all'Autorità Garante dovrà effettuarsi senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il Titolare sia venuto *a conoscenza* del data breach, avendo raggiunto un ragionevole grado di certezza della verifica dell'incidente di sicurezza.
Oltre il termine delle 72 ore la notifica deve essere corredata delle ragioni del ritardo.

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

L'intero iter di gestione della segnalazione, compresa l'avvenuta notificazione al Garante, viene documentato dal Coordinatore del Gruppo Aziendale Privacy nel **Registro aziendale delle violazioni** (**Allegato 2**), da questi curato e tenuto. Tale Registro ha durata annuale, contiene tutte le segnalazioni ricevute e gestite durante l'anno e deve essere chiuso entro il 31 dicembre. Il Coordinatore del Gruppo Aziendale Privacy provvede ad inviarlo al Titolare del trattamento e al DPO con nota protocollata entro il 31 gennaio dell'anno successivo, ai fini della conservazione ai sensi di legge.

Si precisa che anche i casi segnalati e non ritenuti dal Titolare da notificare, unitamente alle motivazioni sottese, devono essere documentati 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, o altro atto giuridico, 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 di ogni potenziale evento di Data Breach il Titolare del trattamento, senza ingiustificato ritardo.
Pertanto, il Responsabile del trattamento, qualora venga a conoscenza di un potenziale caso di Data Breach, deve avvisare il DPO, senza ingiustificato ritardo e nel rispetto dei tempi previsti dall'atto di nomina, all'indirizzo pec protocollo@pec.ausl.bologna.it. oppure tramite raccomandata A/R all'indirizzo Via Castiglione, n.29 – 40124 – Bologna, utilizzando il modulo allegato **(Allegato 3 - Report Responsabile del trattamento (esterno all'Azienda) per la comunicazione del Data Breach al DPO)**.
Il DPO inoltra il modulo di segnalazione di Data Breach ricevuto al Coordinatore del Gruppo Aziendale Privacy e al vice Coordinatore del GAP individuato nella figura del Direttore della UO Tecnologie Informatiche e di Comunicazione e da questo momento vengono eseguiti i medesimi steps della procedura illustrata al punto 4.1 (attraverso la necessaria collaborazione del Responsabile del trattamento).

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

Il Gruppo Aziendale Privacy, sotto la supervisione del Coordinatore ed avvalendosi della funzione consulenziale del DPO, è responsabile, in base alla tipologia della violazione e delle specifiche competenze, dell'analisi tecnica dell'evento nonché dell'individuazione delle azioni da mettere in atto tempestivamente per il contenimento del danno.
Pertanto, una volta verificato che l'evento segnalato si configuri effettivamente come un Data Breach (a seguito di analisi preliminare), verranno svolte tutte le operazioni necessarie a raccogliere gli elementi per una valutazione della rischiosità dell'evento (analisi approfondita), ai fini della eventuale notifica al Garante della privacy, e del grado di rischiosità dell'evento, ai fini della eventuale comunicazione agli interessati.
Si sottolinea che, anche nel caso in cui dall'analisi preliminare emerga che la segnalazione non abbia i caratteri del Data Breach, è comunque necessario annotarla nel Registro aziendale delle violazioni.
Durante l'analisi approfondita dovranno essere accertate le circostanze della violazione, le conseguenze ed i relativi rimedi.
Si precisa che l'art.33, paragrafo n.4 del GDPR, recita: *"Qualora e 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, verranno effettuati:

- 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 agli interessati, con eventuale ricorso ai media (se sussistono i presupposti),
- 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 all'Autorità Garante quando è "improbabile" che questa comporti un rischio per i diritti e le libertà delle persone fisiche. Ne consegue che il giudizio che determina l'improbabilità del rischio deve essere riportato nel Registro delle violazioni.
I Garanti europei, nelle linee guida, precisano che la mancata notifica 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 siano coinvolti dati personali. In caso affermativo 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, presenza di algoritmo di cifratura o di 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, in quanto 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 ed inviata per conoscenza al DPO, con indicazione del DPO come punto di contatto con il Garante.

## 7. Altre segnalazioni dovute

Il Coordinatore o il vice Coordinatore del Gruppo Aziendale Privacy e il DPO, con il supporto dei componenti del Gruppo Aziendale Privacy e consultandosi con gli Uffici aziendali coinvolti, sulla base delle rispettive competenze, dovranno verificare 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);
- 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 di Suo delegato procedere con le segnalazioni dovute.

## 8. Comunicazione agli interessati

In caso di elevato rischio per la libertà e i diritti delle persone fisiche si provvederà ad 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 abbia messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure fossero state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non fosse autorizzato ad accedervi, quali la cifratura;
- il Titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- la comunicazione richieda sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati siano informati con analoga efficacia.

La comunicazione deve contenere, ai sensi dell'art.34 paragrafo 2 del GDPR, 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 probabili conseguenze nonché 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 la violazione all'Autorità Garante, il Coordinatore del Gruppo Aziendale Privacy e il DPO devono valutare se sia 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 valutato di grado grave occorre individuare la modalità di comunicazione adeguata, considerando la fattibilità di contattare gli interessati 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 e ss.mm. ed ii.) definite in base alle previsioni del Regolamento (UE) 2016/679.

Una volta che il Titolare abbia indicato la forma prescelta, il DPO curerà la predisposizione della comunicazione 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 che il Titolare documenti qualsiasi violazione dei dati personali, al fine di consentire all'Autorità di controllo di verificare il rispetto della norma. Il Coordinatore del Gruppo Aziendale Privacy è responsabile dell'inserimento di tutte le attività indicate sopra nel Registro delle violazioni, così che siano documentate, tracciabili e in grado di fornire evidenza nelle sedi competenti.

## 10. Azioni di 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.

**Allegato 1 Procedura data breach REPORT interno per la comunicazione al Coordinatore del GAP**

da inviare al Coordinatore del GAP o suo delegato all'indirizzo gap@ausl.bologna.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 .....
- ☐ Tra il ..... e il .....
- ☐ E' possibile che sia ancora in corso .....
- ☐ In un tempo non ancora determinato .....

**DOVE È AVVENUTA LA VIOLAZIONE DEI DATI?**

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

_____
_____
_____
_____

## MODALITA' 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 : |

## All. 2 - PROCEDURA DATA BREACH

| 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 | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 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. | 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. | |

## Allegato 3 Procedura Data Breach Modulo 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?**