Delibera del Direttore Generale n. 251 del 20/02/2020

OGGETTO: Regolamento UE 2016/679 (di seguito Regolamento Generale sulla Protezione dei Dati o RGPD). Approvazione della Procedura per la gestione di violazione dei dati personali o Data Breach (artt. 33 e 34 del RGPD)

NOTE TRASPARENZA: Con il presente provvedimento si approva la Procedura per la gestione di violazione dei dati personali o Data Breach (artt. 33 e 34 del RGPD).

Il Direttore della **UOC Affari Generali** riferisce:

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 "RGPD"), 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 dirittti 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 adeguate misure tecniche ed organizzative (c.d. principio di responsabilizzazione o accountability).
Il "sistema privacy" delineato dal RGPD e confermato a livello nazionale dal D.Lgs. n. 101/2018 di modifica ed integrazione del D.Lgs 196/2003 (Codice Privacy), 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 informativo dell'organizzazione aziendale con particolare attenzione ai dati di salute (ivi compresi i dati biometrici e genetici).
Il nuovo "sistema privacy" comporta, quindi, il coinvolgimento di tutti i soggetti autorizzati a trattare i dati personali all'interno dell'organizzazione aziendale, con assunzione delle relative responsabilità.
Questa Azienda, Titolare del Trattamento dei Dati Personali, nella persona del Suo Rappresentante Legale, il Direttore Generale, ha fatto proprio l'approccio del legislatore europeo relativo all'accountability ed alla compliance, adottando le deliberazioni di seguito riportate, per dare avvio alle azioni di carattere organizzativo, gestionale, tecnologico e documen-

tale, volte ad ottemperare, nel proprio ambito, ai precetti del Regolamento UE 2016/679:

- Deliberazione del Direttore Generale n. 537 del 24/04/2018 avente ad oggetto *"Adempimenti da attuare per dare corretta applicazione alla normativa del nuovo Regolamento Europeo 679/2016 sulla Data Protection (RGPD - General Data Protection Regulation). Approvazione Relazione Tecnica"*;
- Deliberazione del Direttore Generale n. 660 del 22/05/2018, avente ad oggetto "Atto di designazione del Responsabile della Protezione dei Dati personali (RPD), ai sensi dell 'art. 37 del Regolamento UE 2016/679 e successive deliberazioni del Direttore Generale n. 425 del 10/04/2019 e n. 1496 del 06/12/2019" ;
- Deliberazione del Direttore Generale n. 1501 del 10/12/2018, avente ad oggetto *"Regolamento Europeo 2016/679 in materia di Trattamento dei Dati Personali. Adempimenti di carattere documentale: approvazione modelli di informativa e di schema di accordo per la nomina del Responsabile Esterno del Trattamento Dati personali"*;
- Deliberazione del Direttore Generale n. 262 del 07/03/2019, avente ad oggetto *"Regolamento UE 2016/679 - ridefinizione dei profili di responsabilità in tema di protezione dei dati personali e nuove modalità di designazione dei soggetti Delegati Privacy (ex Responsabili) e Autorizzati al trattamento di dati personali (ex incaricati)"*.

Tra i molteplici adempimenti obbligatori ai sensi della normativa comunitaria in esame rientra quello previsto dagli artt. 33 e 34 del RGPD, e segnatamente quello relativo all'adozione di una specifica procedura disciplinante la gestione delle violazioni dei dati personali (c.d. "Data Breach").

L'art. 4 del succitato RGPD definisce quale violazione dei dati personali: *"Qualsiasi violazione di sicurezza che comporta anche 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"*.

La violazione dei dati personali conservati, trasmessi o trattati da questa Azienda Sanitaria possono, quindi, essere soggetti al rischio di perdita, distruzione o diffusione indebita, ad esempio, ma non solo, a seguito di attacchi informatici, accessi abusivi, incidenti (es. un incendio o altre calamità naturali), o consistenti nella semplice perdita di supporto informatico mobile (es. smartphone, notebook, pen-drive USB o hard disk aziendale) nella sottrazione di documenti con dati personali (es. perdita o furto, etc.).

Si tratta di situazioni che se non affrontate in modo adeguato e tempestivo, possono provocare gravi e ingenti danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazioni,

furto o usurpazione di identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita della riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
Va precisato che i casi di Data Breach si estendono anche ai documenti cartacei o su supporti analogici (es. perdita di fascicoli cartacei o altra documentazione aziendale), e possono riguardare anche la semplice consultazione degli stessi, se non autorizzata.

Dato atto, pertanto, che la corretta gestione della Data Breach assume un'importanza fondamentale nel pieno rispetto dei diritti, delle libertà e della dignità delle persone si è ravvisata la necessità, in aderenza al dettato normativo, di adottare la procedura interna, in materia di Data Breach, indicando ruoli, responsabilità tempistiche e modalità, con lo scopo di fornire, a ciascun soggetto aziendale autorizzato, a qualsiasi titolo, a trattare i dati personali nel corso della propria attività lavorativa, e a tutti i fornitori che trattino dati per conto dell'Azienda Ospedale – Università Padova, precise istruzioni operative per garantire un'efficace e tempestiva gestione di tutti i casi in cui si sia in presenza di un incidente di sicurezza che può determinare una violazione dei dati personali. Ciò al fine di consentire, come imposto dal RGPD, al Titolare del trattamento (Azienda Ospedale-Università Padova), che si avvale del supporto del Comitato aziendale di Valutazione della Data Breach, costituito ad hoc, di notificare all'Autorità Garante per la Protezione dei Dati Personali le violazioni dei dati personali di cui venga a conoscenza entro 72 ore e comunque senza "giustificato ritardo" ma soltanto se ritiene probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

La procedura, che si allega, è stata elaborata, tenendo conto anche delle linee di indirizzo e di coordinamento fornite, in materia, da Azienda Zero (Ente di governance della sanità veneta), dalla UOC Affari Generali con il supporto della UOS sistemi informativi, validata dal Responsabile per la Protezione dei Dati (RPD) e condivisa nel suo contenuto in data 28/11/2019 con la Direzione Generale e con il Gruppo Privacy aziendale e successivamente aggiornata alla luce delle indicazioni fornite durante la riunione del 28/11/2019 e dell'attuazione, a far data dal 01/01/2020 dell'Atto Aziendale e dell'annessione dell'Ospedale Sant'Antonio dall'AULSS 6 Euganea all'Azienda Ospedale-Università Padova.
Alla luce di quanto sopra esposto, si propone di approvare la procedura aziendale in materia di Data Breach per la gestione delle violazioni dei dati personali, allegata quale parte integrante e sostanziale al presente provvedimento.

Tutto ciò premesso

IL DIRETTORE GENERALE

PRESO ATTO della suestesa proposta e accertato che il Direttore della **UOC Affari Generali** ha attestato l'avvenuta regolare istruttoria della pratica, anche in ordine alla conformità con la vigente legislazione statale e regionale;
RITENUTO di dover adottare in merito i provvedimenti necessari;
VISTO il Decreto Legislativo n. 502/92 e successive modifiche ed integrazioni e le leggi regionali n. 55 e n. 56 del 1994 e successive modifiche ed integrazioni;
ACQUISITO il parere favorevole del Direttore Amministrativo e del Direttore Sanitario per quanto di rispettiva competenza;
IN BASE ai poteri conferitigli dal D.P.G.R.nr.92 del 01.08.2016.

DELIBERA

1) di approvare, per le motivazioni espresse in premessa, la Procedura aziendale, condivisa con il Gruppo Privacy aziendale e il Responsabile per la Protezione dei Dati, per la gestione delle violazioni di dati personali "Data Breach", ai sensi e per gli effetti degli artt. 33 e 34 del Regolamento UE 2016/679, allegata quale parte integrante e sostanziale del presente provvedimento;
2) di precisare che, qualora fosse necessario aggiornare la Procedura, di cui al punto 1), per renderla rispondente alla normativa tempo per tempo vigente, ai Provvedimenti che l'Autorità Garante provvederà ad emanare nonchè e non ultimo alle modifiche del nuovo Atto Aziendale, ciò avverrà con semplice comunicazione interna all'Azienda a prescindere dall'adozione di appositi atti deliberativi di modifica;
3) di incaricare la UOC Affari Generali a trasmettere il presente Provvedimento e l'allegata Procedura a tutti i Direttori delle Unità Operative Complesse e Semplici Dipartimentali sia Sanitarie che Amministrative affinché provvedano, in qualità di Delegati Privacy, a divulgare in modo capillare, all'interno delle rispettive strutture, la Procedura per la gestione di violazione dei dati personali o Data Breach, alla quale il proprio personale, che è autorizzato, a qualsiasi titolo, a trattare i dati, dovrà attenersi in caso ravvisi una potenziale violazione dei dati.
4) di stabilire che la succitata Procedura venga comunicata, a cura delle UOC/UOSD a tutti i fornitori, ove presenti, Responsabili del trattamento, ex art. 28 del RGPD, che trattino dati per conto dell'Azienda Ospedale – Università Padova;
5) Di stabilire, altresì, che venga fornita massima pubblicità e diffusione

del presente Provvedimento e dell'allegata Procedura, anche mediante la loro pubblicazione nel sito intranet aziendale.

Il Direttore Generale
F.to Dr.Luciano Flor

Procedura di
Gestione e Notifica di violazioni di dati personali
("Data Breach")

Rev.	Data	Redatto	Verificato	Approvato
00	13/02/2020	UOC Affari Generali UOS Sistemi Informativi	Gruppo Privacy aziendale Responsabile protezione dati	Direttore Generale
00				
00				

Rev.	Data Rev.	Descrizione della revisione

INDICE

1 Scopo e ambito di applicazione

Scopo della presente procedura è di fornire precise istruzioni operative in presenza di un incidente di sicurezza che determina una violazione dei dati personali (in linguaggio anglosassone "***Data Breach***"), per assicurare il sistematico trattamento di qualunque violazione dei dati personali, ai sensi degli artt. 33 e 34 del Regolamento Europeo 2016/679 (di seguito Regolamento Generale sulla Protezione dei Dati o "**RGPD**").

Per ***violazione dei dati personali*** (***Data Breach***) si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la **distruzione**, la **perdita**, la **modifica**, la **divulgazione non autorizzata o l'accesso non autorizzato** ai dati personali trasmessi, conservati o comunque trattati dall'Azienda Ospedale - Università Padova (di seguito "**AOUP**").

La presente procedura definisce le linee di comportamento da seguire, adottate da AOUP, e indica ruoli, responsabilità, tempistiche e modalità di comunicazione di eventuali violazioni di riservatezza, d'integrità e disponibilità dei dati personali all'Autorità di Controllo e, ove necessario, a tutti gli Interessati i cui dati personali sono oggetto di violazione.

Per la omessa notifica di Data Breach all'Autorità di Controllo o per l'omessa comunicazione agli interessati o per entrambi gli adempimenti, nei casi in cui siano soddisfatti i requisiti di cui agli artt. 33 e 34 del RGPD, sono previste, infatti, rilevanti sanzioni amministrative , il cui importo può arrivare fino ad euro 10.000.000 o al 2% del fatturato totale annuo dell'esercizio precedente, se superiore, in caso di imprese, nonché misure correttive di cui all'art. 58 del RGPD (avvertimenti, ammonimenti, ingiunzioni, imposizione di limiti al trattamento, ordine di rettifica, revoca di certificazioni, ordine di sospendere flussi dati).

È pertanto di fondamentale importanza rispettare la presente procedura organizzativa interna per la gestione di eventuali violazioni concrete, potenziali o sospette di dati personali per adempiere agli obblighi imposti dalla normativa applicabile ed evitare rischi per i diritti e le libertà degli interessati, nonché danni economici per l'AOUP, quale titolare del trattamento.

L'AOUP identifica la U.O.C. Affari Generali e la U.O.S. Sistemi Informativi, che agiranno con il supporto delle Unità Organizzative coinvolte, ognuno per la parte di propria competenza, quali strutture aziendali preposte alla gestione ed al coordinamento delle attività afferenti alla protezione dei dati personali ed alla gestione delle Data Breach.

1.1 Riferimenti normativi

La procedura è redatta tenendo in considerazione le disposizioni del RGPD e, nello specifico, gli articoli 33 e 34 (si veda l'Allegato 1 "*Riferimenti normativi*"), nonché le Linee Guida del Gruppo di Lavoro Articolo 29 adottate il 6 febbraio 2018 ed approvate dal Comitato Europeo per la Protezione dei dati il 25 maggio 2018 e le istruzioni fornite dall'Autorità Garante per la protezione dei dati personali con provvedimento n. 157 del 30 luglio 2019.

1.2 Definizioni

Autorità di Controllo: l'Autorità Garante per la protezione dei dati personali.

Autorizzati al trattamento: lavoratori dipendenti e terzi non dipendenti che trattano dati personali nel corso della propria attività lavorativa presso l'AOUP nel rispetto delle istruzioni operative e del profilo di autorizzazione consentito.

Comitato di Valutazione della Data Breach: Comitato di cui si avvale il Titolare, per la gestione e valutazione della Data Breach, composto dai seguenti soggetti: Responsabile della Protezione dei dati ("RPD"), Referente aziendale Privacy o suo delegato, Responsabile della U.O.S. Sistemi Informativi o un suo delegato, Dirigente della Direzione Medico Ospedaliera, Direttore della struttura presso cui è avvenuta la Data Breach o un suo delegato.

Comunicazione di una violazione dei dati personali all'interessato (Art. 34, RGPD): comunicazione della violazione/*DataBreach* al soggetto i cui dati sono stati violati.

Dato personale (Art. 4, n. 1, RGPD): 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 a 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.

Interessato: la persona fisica identificata o identificabile **(Art. 4, n. 1, RGPD)** a cui si riferisce il dato personale oggetto di trattamento.

Notifica di una violazione dei dati personali all'Autorità di Controllo (Art. 33, RGPD): comunicazione della violazione/*DataBreach* all'Autorità di Controllo.

Personale di competenza: soggetto delegato dal Titolare che collabora con il Referente Aziendale *Privacy* nella gestione della procedura, ovvero il Direttore di Unità Operativa Complessa, Direttore di Unità Operativa Semplice Dipartimentale e il Responsabile della U.O.S. Sistemi Informativi.

Referente Aziendale *Privacy*: soggetto preposto dal Titolare agli adempimenti aziendali in materia di protezione dei dati, con il supporto del Personale di competenza.

Responsabile del trattamento (Art. 4, n. 8, RGPD): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Responsabile della Protezione dei Dati (RPD): la persona fisica (o giuridica) nominata ai sensi dell'art. 37 del RGPD, che svolge i compiti previsti dall'art. 39 del RGPD o di altre disposizioni ivi contenute.

Responsabile U.O.S. Sistemi Informativi: Referente della struttura aziendale dei Sistemi Informativi.

Titolare del trattamento (Art. 4, n. 7, RGPD): 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 di 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.

Trattamento(Art. 4, n. 2, RGPD): 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.

Violazione dei dati personali o "*Data Breach*" (Art. 4. n. 12, RGPD): la 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**.**

2 Destinatari

La presente procedura interna è obbligatoria per tutti i soggetti:

➢**DESIGNATI** (Delegati Privacy) di specifici compiti e funzioni, ovvero, Direttore di Unità Operativa Complessa, Direttore di Unità Operativa Semplice Dipartimentale e il Responsabile della U.O.S. Sistemi Informativi

➢**AUTORIZZATI** al trattamento: lavoratori dipendenti e terzi non dipendenti che trattano dati personali nel corso della propria attività lavorativa presso l'AOUP nel rispetto delle istruzioni operative e del profilo di autorizzazione consentito;

➢**RESPONSABILI del trattamento** ex art. 28 del RGPD che, in ragione del rapporto contrattuale in essere con l'AOUP, trattano dati per conto della stessa.

La mancata conformità alle regole di comportamento previste dalla presente procedura può determinare provvedimenti disciplinari a carico dei dipendenti inadempienti, ovvero la risoluzione

dei contratti, accordi o convenzioni in essere con terze parti inadempienti, secondo le normative vigenti in materia.

3 Ruoli e responsabilità

La tabella propone una sintesi delle attività riconducibili a ciascuna risorsa, sia interna che esterna all'AOUP, coinvolta nel processo di gestione di una *Data Breach*.

Legenda di lettura della tabella (RD = Responsabilità Diretta del soggetto / PC = Per Conoscenza / C = Collaborazione / FI = Funzioni di indirizzo)

		Ruolo Aziendale				
Fasi attività		**Titolare del trattamento**	**Responsabile del trattamento (se ha subito la Data Breach)**	**Referente Aziendale Privacy e Responsabile della UOS Sistemi Informativi**	**Personale di competenza (coinvolto nella Data Breach)**	**Responsabile della protezione dei dati**
	Rilevazione/Valutazione	RD	RD	RD	RD	FI
	Gestione	RD	RD/C	RD	C	FI
	Notifica al Garante	RD	PC	C	PC	C
	Comunicazione agli interessati	RD	PC	C	PC	C
	Applicazione delle misure correttive	RD	RD	RD	RD	FI
	Archivio della documentazione: redazione verbale e registro delle data breach	RD	N/A	RD	PC	C

3.1 Comitato di Valutazione della Data Breach

Ai fini della gestione tempestiva di qualsiasi violazione di dati personali, è istituito un **Comitato di Valutazione della Data Breach** composto dalle seguenti funzioni:

- Responsabile della Protezione dei dati ("RPD"),
- Referente aziendale Privacy o suo delegato,
- Responsabile della U.O.S. Sistemi Informativi o un suo delegato,
- Dirigente della Direzione Medico Ospedaliera,
- Direttore della struttura presso cui è avvenuta la Data Breach o un suo delegato.

Il Comitato di valutazione della Data Breach è convocato con urgenza dal Referente aziendale Privacy, o suo delegato nel caso in cui si verifichi un incidente di sicurezza che possa determinare una Data Breach.

Il Comitato di Valutazione dovrà riunirsi, anche mediante teleconferenza o videoconferenza, entro 24 ore dalla convocazione, salvo, motivate, situazioni eccezionali per attivare tutte le necessarie azioni, raccogliere le informazioni e valutare se notificare la Data Breach al Garante e, se del caso, agli interessati.

Le attività di raccolta documentale ed informativa sono coordinate dal Referente Aziendale Privacy, o suo delegato.

Le valutazioni effettuate dal Comitato di Valutazione dovranno essere comunicate tempestivamente al Titolare del trattamento per consentire di procedere all'eventuale notifica all'Autorità di Controllo e/o agli interessati nei termini di legge.

4 Modalità operative

Il personale autorizzato al trattamento (sia esso in qualità di Delegato Privacy/Designato o Autorizzato), qualora venga a conoscenza, nell'espletamento delle attività di competenza o indirettamente nello svolgimento delle stesse, del verificarsi di eventuali violazioni dei dati personali o di incidenti informatici e non che possano esporre a rischio di violazione dei dati (data breach), deve tempestivamente informare il Titolare (nella persona del Referente aziendale privacy o suo delegato), anche attraverso il Responsabile della U.O.S. Sistemi Informativi, con il supporto del Responsabile della Protezione dei Dati.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione all'Autorità di Controllo. La notifica dovrà avvenire (possibilmente) entro 72 ore e comunque senza ingiustificato ritardo.

Anche l'eventuale Responsabile del trattamento designato dall'Azienda Ospedale - Università Padova ai sensi dell'art. 28 del RGPD è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione. Al riguardo, i contratti o convenzioni con i soggetti terzi che agiscono quali responsabili del trattamento dovranno prevedere uno specifico obbligo di tempestiva comunicazione delle Data Breach all'AOUP quale titolare del trattamento.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- *danni fisici, materiali o immateriali alle persone fisiche;*
- *perdita del controllo dei dati personali;*
- *limitazione dei diritti, discriminazione;*
- *furto o usurpazione d'identità;*
- *perdite finanziarie, danno economico o sociale.*
- *decifratura non autorizzata della pseudonimizzazione;*
- *pregiudizio alla reputazione;*
- *perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).*

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi.

I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- *coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;*
- *riguardare categorie particolari di dati personali;*
- *comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);*
- *comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);*
- *impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).*

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33, lett. b), c) e d).

I dati personali sono i dati personali trattati dall'AOUP, in qualsiasi formato (inclusi documenti cartacei) e con qualsiasi mezzo.

In particolare, essi si distinguono nelle seguenti categorie:

- *dati personali non appartenenti a categorie particolari o a condanne penali e reati che permettono l'identificazione diretta - come i dati anagrafici (ad esempio: nome e cognome) - e l'identificazione indiretta, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP);*
- *dati rientranti in categorie particolari: si tratta dei "dati che rivelino l'origine razziale od etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale di una persona" (art.9 GDPR);*
- *dati relativi a condanne penali e reati: si tratta dei dati c.d. "giudiziari", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. L'art. 10 del RGPD ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.*

Le fasi di attività connesse alla gestione di eventuali violazioni di riservatezza dei dati (*Data Breach*) si sostanziano in:

1. Rilevazione / Valutazione;
2. Gestione;
3. Notifica al Garante per la protezione dei dati personali;
4. Comunicazione agli Interessati (ove necessario);
5. Registro delle violazioni e archivio della documentazione;
6. Pianificazione di Audit Interni.

4.1 Rilevazione e valutazione della Data Breach

Come indicato in precedenza, per *Data Breach* si intende la 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.

Il Gruppo di Lavoro Articolo 29 per la protezione dei dati, nella *Opinion* 03/2014 richiamata nelle Linee Guida adottate in versione finale il 6 febbraio 2018, ha identificato le seguenti categorie di *Data Breach*.

In particolare, può trattarsi di:

- "***violazione della riservatezza***": in caso di divulgazione o accesso non autorizzato o accidentale ai dati personali, come ad esempio:
  - quando nella redazione di un atto non si redige la versione con omissione dei dati da non pubblicare e l'atto viene pubblicato nella sua interezza;
  - quando si inoltrano messaggi contenenti dati a soggetti non interessati o autorizzati al trattamento;
  - quando un operatore abbandona la propria postazione di lavoro senza prima prendere le opportune precauzioni (riporre la documentazione, lasciare attive procedure sulla risorsa informatica utilizzata, ecc..) e terze persone possono prendere visione di informazioni;

- quando un soggetto in malafede comunica dei dati non pubblici a terzi in modo non autorizzato;

- "***violazione dell'integrità***": in caso di alterazione non autorizzata o accidentale dei dati personali. L' "alterazione" è la situazione in cui i dati sono danneggiati, corrotti o non più completi. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale);
- "***perdita della disponibilità***": in caso di perdita o distruzione dei dati personali (accidentale o non autorizzata).
  La "perdita di dati" è la situazione in cui i dati, presumibilmente, esistono ancora, ma il titolare ne ha perso il controllo o la possibilità di accedervi, mentre la "distruzione" dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal titolare.
  La violazione dei dati può avvenire a seguito di un attacco informatico, di un accesso abusivo, di un incidente (es. incendio, allagamento, etc.) o per la perdita di un supporto informatico (smartphone, notebook, chiavetta USB, etc.) o per la sottrazione di documenti con dati personali (furto, etc.)

A seconda delle circostanze, una violazione può riguardare anche tutti gli aspetti sopra indicati o una combinazione di essi. La casistica è molto ampia.

A titolo esemplificativo, si riportano alcuni eventi di violazione dei dati personali per le quali è necessario avviare la procedura:

- perdita o furto di PC o Smartphone aziendali;
- perdita di supporti mobili quali pen-drive USB o hard disk aziendale;
- perdita di fascicoli cartacei o altra documentazione aziendale;
- dati cancellati accidentalmente o accessibili a soggetti non autorizzati;
- invio erroneo di comunicazioni/informazioni verso l'esterno;
- attacchi informatici ai sistemi aziendali;
- accesso a dati da parte di persona non autorizzata o accesso abusivo (ad esempio: accesso non autorizzato ai sistemi informatici con successiva divulgazione delle informazioni acquisite);
- interruzione significativa di un servizio ("black out" elettrico o attacchi di tipo "denial of service");
- virus o altri attacchi al sistema informatico o alla rete aziendale;
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo "owner";
- violazione di misure di sicurezza fisica (ad esempio: forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);
- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o sia loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono stati violati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;
- se sono stati violati dati afferenti alla valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se la violazione afferisce a un numero rilevante di dati;
- se l'evento riguarda il trattamento di dati personali di persone fisiche vulnerabili, in particolare minori.

Qualsiasi persona autorizzata al trattamento ogni qualvolta rilevi una avvenuta o potenziale *Data Breach* ha la responsabilità di informare immediatamente il Titolare del trattamento, anche per il tramite del Referente aziendale privacy o suo delegato e del RPD.

La comunicazione al Titolare del trattamento della violazione dei dati personali dovrà pervenire in forma scritta (**Allegato 2**).

Parimenti, qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione (es. Responsabile del trattamento), questi informa il Titolare del trattamento senza ingiustificato ritardo, ai sensi dell'art. 33 comma 2 del RGPD.

Il Titolare del trattamento, avuta notizia dell'avvenuta o potenziale *Data Breach*, per il tramite del Referente aziendale privacyo suo delegato, che convoca il Comitato di Valutazione della Data Breach, avvia l'istruttoria per l'identificazione e valutazione dell'evento.

In questa fase, il Titolare del trattamento deve consultare il RPD per funzioni di indirizzo.

4.2 Gestione della Data Breach

Il Comitato di Valutazione della Data Breach raccoglie le informazioni necessarie alla descrizione dell'evento, all'analisi delle misure tecniche e organizzative analogiche e/o digitali adottate e di quelle di possibile adozione per porre rimedio alla violazione e/o per attenuarne i possibili effetti negativi e valuta se notificare la Data Breach all'Autorità di Controllo e, se del caso, agli interessati.

Le valutazioni del Comitato di Valutazione della Data Breach sono comunicate tempestivamente al Titolare del trattamento.

Qualora il Titolare del trattamento dovesse ritenere non opportuno notificare la Data Breach all'Autorità di Controllo, è necessario che le motivazioni sottostanti a tale decisione siano documentate all'interno del *Registro Interno delle Violazioni*.

A tale proposito, occorrerà descrivere i motivi per cui il Titolare del trattamento ha ritenuto che la violazione non costituisse fattore di rischio per i diritti e le libertà degli individui.

Ai fini della gestione della *Data Breach* occorre considerare se:

- i dati siano stati in precedenza resi anonimi oppure pseudonimizzati;
- i dati siano stati oggetto di cifratura e se fosse garantita, al momento della violazione, la riservatezza della chiave di decifratura;
- i dati violati non siano riconducibili all'identità di persone fisiche;
- i dati siano già stati oggetto di pubblicazione;
- l'evento non costituisca una *Data Breach*.

4.3 Notifica all'Autorità di controllo

Ai sensi dell'art. 33 del RGPD, il Titolare ha sempre l'obbligo di notificare la *Data Breach* all'Autorità di Controllo, salvo i casi in cui sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Alla notificazione effettuata dal Titolare del trattamento utilizzando il modello dell'Autorità di controllo (**Allegato 4**) dovranno essere allegati tutti gli elementi informativi e le valutazioni in merito effettuate.

Qualora il Titolare del trattamento e il RPD abbiano opinioni discordanti circa l'insussistenza del rischio per i diritti e le libertà degli interessati, la decisione sull'opportunità di notificare la violazione dei dati personali all'Autorità di Controllo ricadrà unicamente sul Titolare del trattamento e dovrà essere debitamente motivata.

Laddove, invece, sia rilevato un rischio per i diritti e le libertà degli interessati, il Titolare del trattamento dovrà notificare la violazione all'Autorità di Controllo senza ingiustificato ritardo e, ove possibile, **entro 72 ore dal momento in cui ne sia venuto a conoscenza**.

Contestualmente è inoltrata dal Titolare del trattamento comunicazione scritta al RPD di avvenuta notifica al Garante, per mettere il medesimo a conoscenza dell'istruttoria in atto.

Qualora la notifica al Garante per la Protezione dei dati personali non sia effettuata entro 72 ore, essa dovrà essere corredata dei motivi del ritardo.

Se non fosse possibile fornire tutte le informazioni contestualmente, queste ultime potranno essere inviate in fasi successive senza ulteriore ingiustificato ritardo, avendo cura di dare evidenza delle motivazioni per cui tali informazioni non sono disponibili.

In questo caso sarà cura del Titolare del trattamento raccogliere le informazioni mancanti e procedere, senza ritardo, alle integrazioni eventualmente necessarie avvalendosi della collaborazione delle funzioni interessate che, a tal fine, dovranno prestare pronta, piena e fattiva disponibilità.

La mancata collaborazione delle risorse coinvolte assume rilevanza a fini disciplinari.

Ai sensi dell'art. 33 del Regolamento, la notifica all'Autorità di Controllo deve contenere almeno i seguenti contenuti:

a) descrizione della natura 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;
b) comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

4.4 Comunicazione agli Interessati

Nel caso in cui la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvede alla comunicazione di detta violazione a tutti gli interessati coinvolti, senza ingiustificato ritardo, dandone comunicazione per conoscenza al RPD.

La comunicazione agli interessati deve descrivere, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali e deve contenere almeno le seguenti informazioni:

a) la descrizione delle probabili conseguenze della violazione dei dati personali;
b) la descrizione delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibilieffetti negativi;
c) nome e dati di contatto del RPD.

Ai sensi dell'art. 34, comma 3, non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il Titolare del trattamento ha messo in atto misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
b) 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;
c) detta comunicazione richiederebbe sforzi sproporzionati; in tal caso, è necessario procedere a una comunicazione pubblica, ovvero a una misura simile alternativa, tramite la quale gli Interessati sono informati con analoga efficacia.

Nel caso in cui sia l'Autorità di Controllo a ordinare con provvedimento la comunicazione del *Data Breach* agli interessati, il Titolare del trattamento pone in essere tutte le attività necessarie per ottemperare al provvedimento.

4.5 Registro delle violazioni e archivio della documentazione

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate all'Autorità di Controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio e registrare.

A tal fine, con il supporto del Referente aziendale privacyo suo delegato, il Titolare registra nel Registro delle Violazioni (**Allegato 5**) qualsiasi tipologia di violazione e conserva con la massima cura e diligenza la documentazione a supporto, che può essere richiesta dall'Autorità di Controllo al fine di verificare il rispetto delle disposizioni del RGPD.

4.6 Pianificazione degli audit

Il Titolare del trattamento prevede, all'interno del proprio piano di *audit*, con cadenza almeno biennale, una verifica sulla tenuta del Registro interno delle violazioni e delle segnalazioni di violazione dei *Data Breach*.

5 Valutazione del rischio connesso alla violazione

Il livello di rischio è definito sulla base di due parametri, gravità e probabilità:

GRAVITA' rilevanza degli effetti pregiudizievoli che la violazione è in grado di produrre sui diritti e le libertà delle persone coinvolte	Impatto della violazione sui diritti e le libertà delle persone coinvolte: Basso: nessun impatto; Medio: impatto poco significativo, reversibile; Alto: impatto significativo, irreversibile.
PROBABILITA' grado di possibilità che si verifichino uno o più eventi temuti (es. la perdita di ogni traccia dei dati)	Possibilità che si verifichino uno o più eventi temuti Basso: l'evento temuto non si manifesta; Medio: l'evento temuto potrebbe manifestarsi; Alto: l'evento temuto si è manifestato.

Ai fini della identificazione dei valori da attribuire ai due parametri per la valutazione del rischio, occorre considerare anche i seguenti fattori:

- tipo di violazione;
- natura, sensibilità e volume dei dati personali;
- facilità di associare i dati violati ad una persona fisica;
- gravità delle conseguenze per gli interessati;
- particolarità degli interessati (es. minori);
- particolarità degli autorizzati al trattamento (es. personale sanitario);
- numero degli interessati esposti al rischio.

6 Fasi operative e flusso di gestione della Data Breach

Di seguito si descrivono le singole fasi operative di una Data Breach e le responsabilità dei singoli ruoli come sinteticamente individuati nel precedente par. 3.

Fase 1 – SEGNALAZIONE INCIDENTE

1.1.	Personale di competenza (Delegati Privacy) Personale Autorizzato Referente aziendale privacyo suo delegato Responsabile U.O.S. Sistemi Informativi o suo delegato Dirigente Medico della Direzione Medica Ospedaliera (se l'incidente si è verificato presso una UOC/UOSD sanitaria) RPD Responsabili del trattamento (se coinvolti)	Chiunque (Autorizzati e/o delegati) venga a conoscenza del verificarsi di eventuali incidenti che possono determinare violazioni dei dati personali (Data Breach)**deve immediatamente** informare il proprio Direttore di UOC/UOSD, il Referente aziendale privacy o suo delegato, il Responsabile della U.O.S. Sistemi Informativi, la Direzione Medica Ospedaliera (se l'incidente si è verificato presso una UOC/UOSD sanitaria)e il RPD ai seguenti indirizzi mail: rpd.aopd@aopd.veneto.it e protocollo.aopd@aopd.veneto.it. Il Direttore di UOC/UOSD o suo delegato tempestivamente, e comunque **entro e non oltre 24 ore dall'evento,**deve trasmettere ai predetti indirizzi email il modulo di "segnalazione di incidente di sicurezza"debitamente compilato. segnalare l'incidente mediante l'apposito modulo di "*Segnalazione incidente di sicurezza" (All. 2)* Qualora la rilevazione avvenga a cura di un soggetto terzo esterno all'organizzazione (es. Responsabile del trattamento, ex art. 28 del RGPD,) questi informa il Titolare del trattamento senza ingiustificato ritardo, ai sensi dell'art. 33, comma 2 del RGPD, con le medesime modalità di cui sopra.	*Modulo di "Segnalazione incidente di sicurezza" (**Allegato 2**)*

Fase2– RILEVAZIONE E VALUTAZIONE DELLA VIOLAZIONE

2.1	Referente aziendale privacy o suo delegato Responsabile U.O.S. Sistemi Informativi o suo delegato Dirigente Medico della Direzione Medica Ospedaliera (se l'incidente si è verificato presso una UOC/UOSD sanitaria	Il Referente aziendale privacy, o suo delegato convoca il Comitato di Valutazione della Data Breach che deve riunirsi entro 24 ore dalla comunicazione dell'incidente di cui al precedente Punto 1.1, salvo, situazioni eccezionali adeguatamente motivate, e coordina le attività di raccolta documentale ed informativa. Il Comitato di Valutazione della Data Breach esamina con la massima urgenza la segnalazione pervenuta e tutta la documentazione disponibile relativa all'incidente verificandone la relativa completezza, provvedendo ad avviare ulteriore attività istruttoria per ottenere completezza	*Modulo "Rilevazione e Valutazione della Violazione dei Dati personali (Data Breach)" (**Allegato 3**)*

	Direttore della struttura presso cui è avvenuta la Data Breach o un suo delegato RPD	informativa, individua le misure correttive e fornisce indicazioni per attuare tempestive le azioni correttive necessarie per gestire operativamente l'incidente.	
2.2	Referente aziendale privacy o suo delegato Responsabile U.O.S. Sistemi Informativi o suo delegato Dirigente Medico della Direzione Medica Ospedaliera (se l'incidente si è verificato presso una UOC/UOSD sanitaria Direttore della struttura presso cui è avvenuta la Data Breach o un suo delegato RPD Responsabili esterni del trattamento (se coinvolti)	Il Comitato di Valutazione della Data Breach effettua un'analisi dell'incidente per valutare la sussistenza di una violazione tenendo in considerazione: • la quantità dei dati personali; • la tipologia dei dati violati; • la quantità di soggetti interessati coinvolti; • la tipologia dei soggetti interessati coinvolti; • le aree coinvolte e l'impatto sulle persone fisiche a cui appartengono i dati. Dovranno anche essere desunte informazioni circa la natura dell'incidente occorso, le misure preventive poste in essere per evitarlo e le misure adottate per minimizzarne le conseguenze.	*Modulo "Rilevazione e Valutazione della Violazione dei Dati personali (Data Breach)"*
2.3	Referente aziendale privacy o suo delegato Responsabile U.O.S. Sistemi Informativio suo delegato Dirigente Medico della Direzione Medica Ospedaliera (se l'incidente si è verificato presso una UOC/UOSD sanitaria RPD	Il Comitato di Valutazione della Data Breach identifica i rischi conseguenti all'evento per i diritti e le libertà degli interessati, tenendo in considerazione le misure preventive logiche, fisiche ed organizzative attuate per far fronte ai danni. I rischi della violazione sono classificati in: • **NON PRESENTI** quando la violazione non ha alcuna conseguenza dimostrabile sui diritti e le libertà degli interessati • **PRESENTI** quando la violazione ha effetti negativi sui diritti e le libertà degli interessati, ma non sono elevati per la natura della violazione, per la quantità si soggetti o dati coinvolti, oppure sono state adottate misure preventive per limitarli (ad es. crittografia o pseudonimizzazione, esistenza di impianti antieffrazione etc.);	*Modulo "Rilevazione e Valutazione della Violazione dei Dati personali (Data Breach)"*

	Direttore della struttura presso cui è avvenuta la Data Breach o un suo delegato	• **ELEVATI** quando la violazione comporta rischi rilevanti per i diritti e le libertà degli interessati, coinvolge un elevato numero di interessati e dati e non sono state adottate misure preventive di protezione. Le valutazioni effettuate dal Comitato di Valutazione della Data Breach sono comunicate tempestivamente al Titolare del trattamento per poter effettuare la notifica all'Autorità di Controllo e/o agli interessati se ne sussistono i presupposti nelle tempistiche legislativamente previste.	

Fase 3 – NOTIFICA ALL'AUTORITA' GARANTE

3.1	Referente aziendale privacy o suo delegato Responsabile della U.O.S. Sistemi Informativio suo delegato personale di competenza (Delegati Privacy) RPD	Qualora dovesse risultare l'obbligo di notificare la Data Breach, il Referente aziendale privacy o suo delegato, con il supporto dell'RPD, del Responsabile della U.O.S. Sistemi Informativi e del personale di competenza, tempestivamente e comunque **entro e non oltre le 48 ore dal Punto 2.1**, salvo motivate situazioni eccezionali, raccoglie e rielabora le seguenti informazioni in merito alla violazione: • natura e breve descrizione della violazione dei dati; • data e ora in cui la violazione si è verificata; • data e ora in cui la violazione è stata rilevata; • luogo in cui si è verificata la violazione; • dispositivi oggetto della violazione; • breve descrizione dei sistemi di elaborazione o memorizzazione dei dati coinvolti nella violazione e relativa ubicazione; • categorie e numero approssimativo di soggetti interessati coinvolti; • tipologia e numero approssimativo di dati personali oggetto della violazione; • probabili conseguenze della violazione sui dati personali; • livello di rischio conseguente la violazione; • misure tecniche e organizzative adottate o che il AOUP quale Titolare intende adottare AOUP quale Titolare per limitare la violazione e gli effetti negativi; • se la violazione è stata o sarà comunicata ai soggetti interessati o, in caso contrario, le motivazioni per cui non sarà comunicata la violazione ai soggetti interessati; • contenuto della comunicazione agli interessati e il canale utilizzato per la comunicazione; • se la violazione coinvolge altri soggetti terzi; • se la violazione coinvolge altri Paesi dell'Unione Europea; • nome e dati di contatto del RPD o di altro punto di contatto per l'Autorità di Controllo.	

3.2	Referente aziendale privacy o suo delegato	Il Referente aziendale privacy, o suo delegato, con il supporto del RPD, tempestivamente, ***entro e non oltre 72 ore*** dal punto 2.1: • accede alla sezione del sito dell'Autorità di Controllo per la protezione dei dati personali dedicata alla notifica in caso di violazioni; • compila il modulo di notifica (seguendo l'eventuale procedura telematica o scaricando il modello inserito sul sito web dell'Autorità di Controllo) con le informazioni già raccolte in precedenza, sopra descritte; • sottopone il modulo al legale rappresentante di AOUP per la relativa verifica e sottoscrizione; • invia la notifica con le modalità indicate dall'Autorità di Controllo. Se entro il termine di cui sopra non si dispone di tutte le informazioni richieste per la notifica completa, dovrà essere effettuata una notifica preliminare da integrare tempestivamente con una successiva notifica non appena in possesso di tutti gli elementi utili.	*Modulo "Notifica della violazione dei dati personali (Data Breach)"(**Allegato 4**)*
3.3	Referente aziendale privacy o suo delegato RPD	Se per motivi organizzativi e tecnici, la notifica all'Autorità di Controllo non è stata effettuata entro e non oltre le 72 ore dal punto 2.1, il modulo di notifica dovrà specificare i motivi per cui del ritardo.	*Modulo "Notifica della violazione dei dati personali (Data Breach)")(**Allegato 4**)*
3.4	Referente aziendale privacy o suo delegato RPD	Monitorare eventuali disposizioni o richieste di informazioni che dovessero pervenire dall'Autorità di Controllo.	

Fase 4– NOTIFICA AGLI INTERESSATI

4.1	Referente aziendale privacy o suo delegato RPD Responsabile	Qualora i rischi individuati dal Comitato di Valutazione della Data Breach o dall'Autorità stessa siano ritenuti "elevati", il Referente aziendale privacy o suo delegato, con il supporto del RPD, del Responsabile della U.O.S. Sistemi Informativi e del personale di competenza, deve: • coinvolgere le aree impattate dalla violazione; • stabilire se la notifica agli interessati possa in qualche modo compromettere eventuali indagini in corso relative alla violazione e, in tal caso,	

	Sistema Informativo o suo delegato Personale di competenza (Delegati Privacy)	attendere per la notifica agli interessati; • rispettare eventuali indicazioni che l'Autorità di Controllo potrebbe fornire in tali circostanze; • individuare il mezzo più opportuno per la notifica agli interessati (posta elettronica, sito internet, comunicati stampa, media, etc.), consultandosi eventualmente con l'Autorità di Controllo, tenendo in considerazione: o la quantità di soggetti interessati coinvolti da raggiungere; o il contesto aziendale; o i mezzi normalmente utilizzati per comunicare con gli interessati; o i costi.	
4.2	Referente aziendale privacy o suo delegato RPD	Il Referente aziendale privacy o suo delegato, con il supporto del RPD, predispone la comunicazione agli interessati con un linguaggio semplice e chiaro indicando: • natura della violazione dei dati • probabili conseguenze della violazione • misure tecniche e organizzative adottate e/o da adottare per limitare la violazione; • eventuali raccomandazioni per imitare gli eventuali danni.	
4.3	Referente aziendale privacy o suo delegato	Il Referente aziendale privacy, o suo delegato deve condividere il testo di comunicazione con il titolare e provvedere, per suo conto, ad inviare la comunicazione agli interessati ed a monitorare i riscontri da parte degli stessi.	

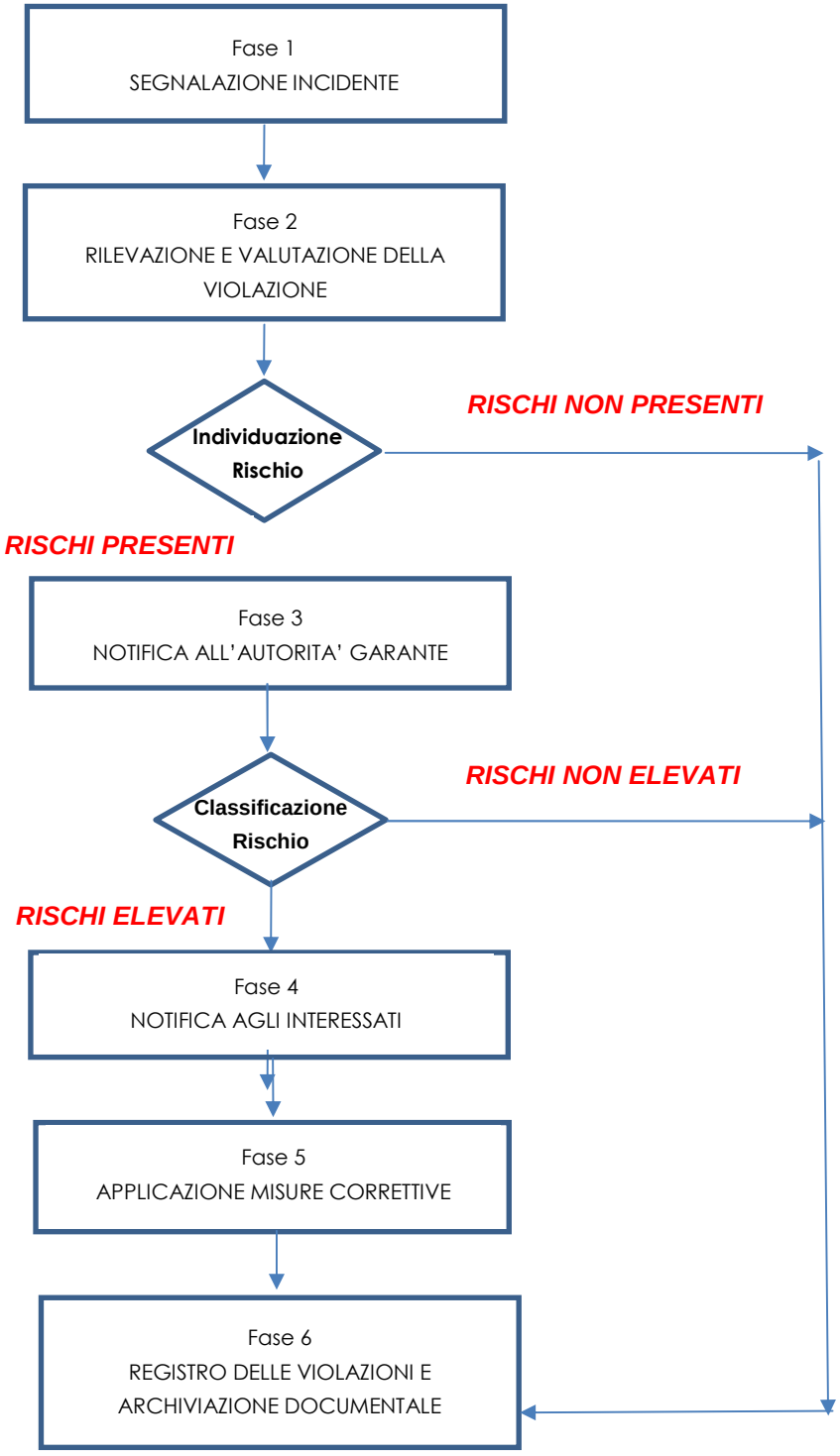
Fase 5 – INDIVIDUAZIONE ED APPLICAZIONE DELLE MISURE CORRETTIVE

5.1	Referente aziendale privacy o suo delegato Responsabile U.O.S. Sistemi Informativi o suo delegato RPD Personale di competenza (Delegati Privacy)	Il Referente aziendale privacy, o suo delegato, con il supporto dell'RPD e del Responsabile della U.O.S. Sistemi Informativi, documenta le misure correttive individuate ed applicate coordinando tutte le funzioni aziendali coinvolte. Tutte le funzioni aziendali, coordinate dal Personale di competenza, devono collaborare affinché le misure correttive siano tempestivamente applicate. L'applicazione delle misure correttive è un processo che può procedere per livelli di implementazione il primo dei quali è, evidentemente, quello necessario ad eliminare la "causa" primaria che ha ingenerato il data breach.	

Fase 6– REGISTRO DELLE VIOLAZIONI E ARCHIVIO DELLA DOCUMENTAZIONE

6.1	Referente aziendale privacy o suo delegato RPD	Il Referente aziendale privacy, o suo delegato con il supporto del RPD, a conclusione di tutte le fasi precedenti, documenta la violazione dei dati personali, anche nel caso in cui la stessa risultasse non soggetta all'obbligo di notificazione all'Autorità di Controllo o non dovesse essere comunicata agli interessati, all'interno di un apposito registro (**Allegato 5**), in cui riportare: • le circostanze della violazione; • le date di riferimento; • le conseguenze della violazione; • le misure adottate per porvi rimedio; • copia della eventuale notifica all'Autorità di Controllo; • se avvenuta, attestazione della notifica ai soggetti interessati (comunicazione di esempio, email, comunicato stampa, etc.)	*Modulo "Registro violazioni dati personali" (**Allegato 5**)*
5.2	Referente aziendale privacy o suo delegato RPD	Il Referente aziendale privacy, o suo delegato con il supporto del RPD, conserva il Registro delle violazioni e lo mette a disposizione dell'Autorità di Controllo o di chi la rappresenta, in caso di accertamenti	*Modulo "Registro violazioni dati personali"*

FLUSSO DI GESTIONE DELLA DATA BREACH



7 Allegati

Allegato 1 - Normativa di riferimento
Allegato 2 - Segnalazione incidente di sicurezza
Allegato 3 - Rilevazione e Valutazione della Violazione dei Dati personali (Data Breach)
Allegato 4 - Notifica della violazione dei dati personali *(Data Breach)*
Allegato 5 - Registro delle violazioni di dati personali.

8 Diffusione della procedura

La presente procedura dovrà essere divulgata in modo capillare e dovrà essere pubblicata nella intranet aziendale, comunicata a tutto il personale dipendente e a tutti i fornitori che trattino dati per conto dell'Azienda Ospedale – Università Padova.

9 Modifichedella procedura

Eventuali modifiche al presente documento avranno efficacia dal momento della loro pubblicazione e si applicheranno alle nuove fattispecie di *Data Breach* che si manifesteranno, eventualmente, dopo tale efficacia, salva diversa disposizione.

ALLEGATO 1
RIFERIMENTI NORMATIVI

REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI
Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016

Articolo 33
Notifica di una violazione dei dati personali all'autorità di controllo
(C85, C87, C88)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 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.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
    a) descrivere la natura 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;
    b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
    c) descrivere le probabili conseguenze della violazione dei dati personali;
    d) descrivere le 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.
4. 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.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Articolo 34
Comunicazione di una violazione dei dati personali all'interessato (C86-C88)

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
    a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
    b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
    c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

Considerando

(85) Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

(86) Il titolare del trattamento dovrebbe comunicare all'interessato la violazione dei dati personali senza indebito ritardo, qualora questa violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà della persona fisica, al fine di consentirgli di prendere le precauzioni necessarie. La comunicazione dovrebbe descrivere la natura della violazione dei dati personali e formulare raccomandazioni per la persona fisica interessata intese ad attenuare i potenziali effetti negativi. Tali comunicazioni agli interessati dovrebbero essere effettuate non appena ragionevolmente possibile e in stretta collaborazione con l'autorità di controllo e nel rispetto degli orientamenti impartiti da questa o da altre autorità competenti quali le autorità incaricate dell'applicazione della legge. Ad esempio, la necessità di
attenuare un rischio immediato di danno richiederebbe che la comunicazione agli interessati fosse tempestiva, ma la necessità di attuare opportune misure per contrastare violazioni di dati personali ripetute o analoghe potrebbe giustificare tempi più lunghi per la comunicazione.

(87) È opportuno verificare se siano state messe in atto tutte le misure tecnologiche e organizzative adeguate di protezione per stabilire immediatamente se c'è stata violazione dei dati personali e informare tempestivamente l'autorità di controllo e l'interessato.
È opportuno stabilire il fatto che la notifica sia stata trasmessa senza ingiustificato ritardo, tenendo conto in particolare della natura e della gravità della violazione dei dati personali e delle sue conseguenze e effetti negativi per l'interessato.
Siffatta notifica può dar luogo a un intervento dell'autorità di controllo nell'ambito dei suoi compiti e poteri previsti dal presente regolamento.

(88) Nel definire modalità dettagliate relative al formato e alle procedure applicabili alla notifica delle violazioni di dati personali, è opportuno tenere debitamente conto delle circostanze di tale violazione, ad esempio stabilire se i dati personali fossero o meno protetti con misure tecniche adeguate di protezione atte a limitare efficacemente il rischio di furto d'identità o altre forme di abuso. Inoltre, è opportuno che tali modalità e procedure tengano conto dei legittimi interessi delle autorità incaricate dell'applicazione della legge, qualora una divulgazione prematura possa ostacolare inutilmente l'indagine sulle circostanze di una violazione di dati personali.

Compilazione a cura dell'autorizzato/addetto al trattamento				
Segnalazione	**N°**	**Data**		
Rilevazione a seguito di:	❑ **Incidente**	❑ **Terzi**	❑**Audit interno**	❑**Altro**

Dati del segnalatore

Nome	
Cognome	
Area appartenenza/esterno	
Indirizzo PEC o email per eventuali comunicazioni	
Recapito telefonico	

Segnalazione incidente

Descrizione dell'incidente (cosa è successo)	
Modalità dell'incidente (come è successo)	
Cause dell'incidente (perché è successo)	
Come è stato rilevato l'incidente	
Sistemi e supporti interessati	
Aree aziendali interessate	
Evidenze oggettive allegate	

Modello compilato da	
Segnalato a:Referente aziendale privacy/ RPD / Referente Sistemi Informativi	

Data:

Titolare del trattamento

Ragione sociale				
Indirizzo	*Prov:*		*Comune*	
	Cap		*Indirizzo*	
Persona addetta alla comunicazione				
Funzione rivestita				
Indirizzo PEC o email per eventuali comunicazioni				
Recapito telefonico				

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?

[ ] Il giorno _____
[ ] 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?

a) Tipo di violazione

[ ] Lettura (presumibilmente i dati non sono stati copiati) (Riservatezza)
[ ] 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:

b) Dispositivo oggetto della violazione

[ ] Postazione di lavoro / 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

Quali categorie di interessati ha riguardato la violazione di dati?

[ ] Dipendenti
[ ]Pazienti
[ ] Cittadini / Consumatori
[ ] Altro specificare: ……
[ ] Altro specificare: ……

Quante persone sono state colpite dalla violazione di dati?

[ ] Nr. _____ di persone
[ ] Circa _____ persone
[ ] Un numero (ancora) sconosciuto di persone

Quante registrazioni sono state interessate dalla violazione di dati?

[ ] Nr. _____ di registrazioni
[ ] Circa _____ registrazioni
[ ] Un numero (ancora) indeterminato

Altri dati coinvolti nella 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 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

Misure tecniche ed organizzativeapplicate ai dati colpiti dalla violazione

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

Valutazione dei rischi conseguenti l'evento per i diritti e le libertà degli interessati, tenendo in considerazione le misure preventive attuate per far fronte ai danni

[ ] NON PRESENTI [ ] PRESENTI [ ] ELEVATI

Natura della comunicazione

[ ] Nuova comunicazione

[ ] Inserimento ulteriori informazioni sulla precedente comunicazione (numero di riferimento) _____

La violazione è stata comunicata anche agli interessati?

[ ] Sì, è stata comunicata il _____

[ ] Si sta provvedendo ad effettuare la comunicazione nelle prossime ore

[ ] No, perché _____

La violazione coinvolge interessati che si trovano in altri Paesi UE?

[ ] Sì [ ] No

La comunicazione è stata effettuata alle competenti autorità di controllo?

[ ] No, perché _____

[ ] Sì

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

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

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

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

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

○ 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**
   - (•) Il
   - ( ) Dal (la violazione è ancora in corso)
   - ( ) Dal al
   - ( ) 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**
   - ( ) Il titolare è stato informato dal responsabile del trattamento
   - ( ) 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 razzialeo 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]

- ◯ N.
- ◯ Circa n.
- ◯ 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

- ◯ N. interessati
- ◯ Circa n. interessati
- ◯ 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

○ Trascurabile
○ Basso
○ Medio
○ 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

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Sez. G - Comunicazione agli interessati

1. La violazione è stata comunicata agli interessati?

- ○ Sì, è stata comunicata il
- ○ No, sarà comunicata il
  in una data da definire
- ○ No, sono tuttora in corso le dovute valutazioni[21]
- ◉ 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]?**

   ◉ SI (indicare quali):

   ○ NO

2. **La violazione coinvolge interessati di Paesi non appartenenti allo Spazio Economico Europeo?**

   ○ SI (indicare quali):

   ○ NO

3. **La violazione è stata notificata ad altre autorità di controllo[24]?**

   ○ SI (indicare quali):

   ○ NO

4. **La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[25]?**

   ○ SI (indicare quali):

   ○ NO

5. **E' stata effettuata una segnalazione all'autorità giudiziaria o di polizia?**

   ○ SI
   ○ 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 qualitàdi titolare del trattamento (con sede in Piazza Venezia 11, IT-00187, Roma; Email: garante@gpdp.it; PEC: protocollo@pec.gpdp.it; Centralino: +39 06696771), tratterài dati personali conferiti con il presente modulo, con modalitàprevalentemente informatiche e telematiche, per le finalitàpreviste 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, Ł obbligatorio e la loro mancata indicazione non consente di ritenere adempiuto il dovere di notificazione della violazione all autorità di c ontrollo. I dati acquisiti nell'ambito della procedura saranno conservati in conformitàalle norme s ulla 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, nØ saranno comunicati a terzi, fatti salvi i casi in cui si renda necessario comunicarli ad altri soggetti coinvolti nell'attivitàistruttoria 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 Ł 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.

Numero incidente	Data evento	Descrizione evento	Rimedi	Notifica interessati?	Notifica Autorità?	Note

ATTESTAZIONE DI PUBBLICAZIONE

La presente deliberazione e' stata pubblicata in copia all Albo di questa Azienda Ospedaliera di Padova per 15 giorni consecutivi dal

Il Direttore
UOC AFFARI GENERALI
(Avv.Maria Grazia Cali)

CERTIFICAZIONE DI ESECUTIVITA'

La presente deliberazione e' divenuta esecutiva il 20/2/2020

Il Direttore
UOC AFFARI GENERALI
(Avv.Maria Grazia Cali)

Copia composta di n°46 fogli (incluso il presente) della delibera n. 251 del 20/2/2020 firmata digitalmente dal Direttore Generale e conservata secondo la normativa vigente presso Infocert S.p.a.

Padova, li

Il Direttore
UOC AFFARI GENERALI
(Avv.Maria Grazia Cali)
