REGIONE DEL VENETO
ULSS7 PEDEMONTANA
Via dei Lotti, n. 40
36061 Bassano del Grappa (VI)
Codice fiscale e partita IVA 00913430245

N. 1474 DEL 08/08/2025

DELIBERAZIONE
del

DIRETTORE GENERALE

Nominato con D.P.G.R. n. 13 del 26/02/2024

Coadiuvato dai sigg.:

DIRETTORE AMMINISTRATIVO dott.ssa MICHELA CONTE

DIRETTORE SANITARIO dr. ANTONIO DI CAPRIO

DIRETTORE DEI SERVIZI SOCIO – SANITARI dott. EDDI FREZZA

OGGETTO: AGGIORNAMENTO DEGLI STRUMENTI DI GESTIONE DELLA PRIVACY AZIENDALE

IL DIRETTORE GENERALE
DELL'AZIENDA ULSS 7 PEDEMONTANA
dott. Carlo Bramezza

Documento informatico firmato digitalmente ai sensi del D. Lgs n. 82/2005, del T.U. n. 445/2000 e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa; il documento informatico è conservato digitalmente negli archivi informatici dell'Azienda.

Proponente: UOC AFFARI GENERALI
Anno Proposta: 2025 Numero Proposta: 1302/25

Il Direttore dell'U.O.C Affari Generali nonché Responsabile del procedimento, attesta che la presente proposta di deliberazione è stata regolarmente istruita nel rispetto della vigente normativa nazionale, regionale e regolamentare: f.to Cristiano Galizian

---

Il Direttore dell'UOC Affari Generali relaziona quanto segue.

Premesso che:

- il Regolamento (UE) 2016/679 (General Data Protection Regulation – GDPR), in vigore dal 25 maggio 2018, ha introdotto nuovi obblighi in materia di protezione dei dati personali, rafforzando i diritti degli interessati e imponendo misure organizzative e tecniche adeguate per garantire la conformità del trattamento dati;
- il Codice in materia di protezione dei dati personali (D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018) ha adeguato la normativa nazionale al GDPR, specificando ulteriori obblighi per i titolari del trattamento, in particolare per le aziende sanitarie;
- l'Azienda ULSS, in qualità di titolare del trattamento, è tenuta a garantire che tutte le attività di gestione dei dati personali, con particolare riguardo ai dati relativi alla salute (rientranti nelle categorie particolari di dati personali tutelate ai sensi dell'Art. 9 del GDPR), siano svolte nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione e limitazione delle finalità
- gli adempimenti di cui sopra rendono necessario un costante adeguamento delle politiche e degli strumenti aziendali per la gestione privacy, anche alla luce di eventuali nuovi indirizzi del Garante per la Protezione dei Dati Personali e dell'evoluzione giurisprudenziale in materia;

Dato atto che:

- con deliberazione del Direttore Generale n 1696 del 27/11/2019 l'Azienda ULSS 7 Pedemontana ha istituito la propria procedura aziendale per la gestione dei Data Breach;
- con deliberazione del Direttore Generale 2322 del 24/12/2021 l'Azienda ULSS 7 Pedemontana ha adottato il Modello Organizzativo Aziendale in materia di Privacy;
- con deliberazione del Direttore Generale n. 790 del 14/12/2023 sono stati affidati da Azienda Zero, per una durata di 5 anni con decorrenza 15/12/2023, alla ditta TIM SpA, i servizi di posta elettronica e *collaboration tools* in SaaS Google Workspace, per le Aziende del SSR Veneto.

Considerato che:

- l'attuale Modello Organizzativo Privacy aziendale necessita di un aggiornamento per recepire le modifiche normative, le linee guida europee e nazionali, nonché le migliori pratiche in materia di sicurezza e tutela dei dati;
- occorre prevedere disposizioni specifiche creando un vero e proprio Regolamento Privacy aziendale ed un correlato regolamento di coordinamento e di accesso alle funzioni dell'Ufficio Privacy aziendale e del Responsabile della Protezione dei Dati al fine di garantire un approccio uniforme e conforme alla normativa privacy in tutti i processi aziendali in ossequio al principio di *Accountability* (Responsabilizzazione e Rendicontazione);
- è necessario aggiornare la procedura aziendale di gestione dei Data Breach prevedendo la figura del Responsabile della stessa;
- per i servizi di posta elettronica e *collaboration tools* in SaaS Google Workspace è essenziale garantire che siano utilizzati in modo sicuro, etico e conforme alle normative sulla protezione dei dati (come il GDPR), da tutto il personale.

Dato atto che nella riunione della Direzione Strategica del 04/08/2025 sono stati illustrati i temi e i principali contenuti che, per corrispondere alle esigenze sopra evidenziate e in aggiornamento e ad integrazione delle deliberazioni su citate, vengono proposti con i regolamenti sotto specificati e già in precedenza condivisi con il *Data Protector Officer* aziendale;

Tutto ciò premesso, si propone di adottare:

a. il "Regolamento per la protezione dei Dati Personali - Sistema Privacy" così come predisposto dall'Ufficio Privacy in collaborazione con il Data Protector Officer aziendale,

b. il "Regolamento di coordinamento e di accesso alle funzioni dell'Ufficio Privacy aziendale e del Responsabile della Protezione dei Dati" così come predisposto dall'Ufficio Privacy in collaborazione con il Data Protector Officer aziendale,

c. la "Procedura Data Breach" aggiornata con la figura del Responsabile della procedura stessa;

d. il "Regolamento sull'utilizzo degli strumenti "Google Workspace", così come predisposto dall'UOC Sistemi Informativi in collaborazione con Ufficio Privacy aziendale,

e di dare atto che con l'adozione del presente provvedimento cessano di avere effetto le deliberazioni del Direttore Generale n 1696 del 27/11/2019 (procedura Data Breach) e n.2322 del 24/12/2021 (Modello Organizzativo Aziendale in materia di Privacy).

IL DIRETTORE GENERALE

Vista la relazione e la proposta del Responsabile del procedimento;

Dato atto che il responsabile dell'Ufficio competente ha attestato l'avvenuta regolare istruttoria della pratica, in ordine alla compatibilità con la vigente legislazione statale, regionale e regolamentare;

Acquisito il parere favorevole dei Direttori Amministrativo, Sanitario e dei Servizi Socio-Sanitari, per quanto di rispettiva competenza;

DELIBERA

1. di approvare:
   a) il "Regolamento per la protezione dei Dati Personali - Sistema Privacy" (All. 1),
   b) il "Regolamento di coordinamento e di accesso alle funzioni dell'Ufficio Privacy aziendale e del Responsabile della Protezione dei Dati" (All. 2),
   c) la "Procedura Data Breach" (All. 3),
   d) il "Regolamento sull'utilizzo degli strumenti "Google Workspace" (All. 4),

   i cui testi costituiscono parti integranti e sostanziali del presente provvedimento;

2. di dare atto che con l'adozione del presente provvedimento cessano di avere effetto le deliberazioni del Direttore Generale n 1696 del 27/11/2019 (procedura Data Breach) e n.2322 del 24/12/2021 (Modello Organizzativo Aziendale in materia di Privacy);

3. di incaricare l'UOC Affari Generali di dare la più ampia diffusione dei Regolamenti di cui ai punti precedenti 1.a), 1.b) e 1.c);

4. di incaricare l'UOC Sistemi Informativi di dare la più ampia diffusione del nuovo Regolamento di cui al precedente punto 1.d);

5. di dare atto che la presente deliberazione viene pubblicata all'albo del sito istituzionale dell'Azienda per 10 gg. continuativi, inviata contestualmente al Collegio Sindacale e diventa esecutiva il giorno stesso della sua pubblicazione, come da norma regolamentare approvata con deliberazione n. 1386 del 22/7/2022.

All. 1

REGIONE DEL VENETO

ULSS7 PEDEMONTANA

REGOLAMENTO

PER LA PROTEZIONE DEI DATI PERSONALI

"SISTEMA PRIVACY"

ENTE:

Azienda ULSS n. 7 Pedemontana

Via dei Lotti, 40

36061 Bassano del Grappa (VI)

Tel. 0424 888111

CF e P. I.V.A. n. 00913430245

PEC protocollo.aulss7@pecveneto.it

in persona del Direttore Generale *pro tempore*

Indice

1. Definizioni

"GDPR": il Regolamento (UE) 2016/679 del Parlamento 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 (RGPD), meglio conosciuto come General Data Protection Regulation (GDPR);

"Codice Privacy": il decreto legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679, come riformato dal decreto legislativo 10 agosto 2018 n. 101 e ss.mm.ii.;

"Garante": Autorità Garante per la Protezione dei Dati Personali, con sede in Roma, che rappresenta l'Autorità di controllo prevista dal GDPR per l'Italia;

"EDPB": European Data Protection Board o Comitato Europeo per la Protezione dei Dati, organismo di consultazione e di indirizzo previsto dal GDPR;

"Disciplina Privacy": l'intero quadro che disciplina la materia della protezione dei dati personali ("privacy") come composto dal GDPR, dal Codice Privacy, dai provvedimenti del Garante, dalle linee guida dell'EDPB, nonché da ogni altro atto normativo, di indirizzo, giurisprudenziale o simile in materia;

"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 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;

"Categorie particolari di dati personali": i particolari dati personali, già definiti come "dati sensibili", che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, disciplinati all'art. 9 GDPR;

"Dati penali": i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, disciplinati all'art. 10 GDPR;

"Dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

"Dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

"Dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

"Trattamento di dati personali": 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;

“Interessato”: la persona fisica, identificata o identificabile, cui si riferiscono i dati personali trattati;

"Titolare del trattamento" o **“Titolare”**: 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;

"Responsabile del trattamento" o **“Responsabile”**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

"Autorizzato al trattamento": la persona fisica autorizzata a compiere operazioni di trattamento sotto l’autorità del Titolare o del Responsabile e che a tale fine riceve istruzioni;

“Delegato del trattamento”: particolare Autorizzato al trattamento con funzioni specifiche di coordinamento, sub-designazione ed altre disciplinate con la designazione;

“Sub-Delegato del trattamento”: particolare Autorizzato al trattamento con funzioni specifiche di coordinamento, sub-designazione ed altre disciplinate con la sub-designazione da parte del Delegato del trattamento;

“Punto di Contatto”: il soggetto autorizzato, eventualmente nominato presso varie Unità, che funge, in collaborazione con l’Ufficio Privacy, da punto di coordinamento privacy specifico per una o più Unità;

“Unità”: ciascuna area organizzativa dell’Ente, quale un settore, un’unità, un dipartimento o simile che abbia una propria struttura organizzativa;

“Responsabile della protezione dei dati” o **“Data Protection Officer”** o **“RPD”** o **“DPO”**: il soggetto dotato di competenze specialistiche in materia, che svolge funzioni consultive e formative, di sorveglianza, di parere sulle valutazioni di impatto, di punto di contatto con il Garante e le altre funzioni ivi previste, designato dall’Ente ai sensi degli artt. 37-39 GDPR;

“Destinatario”: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

“Terzo”: la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che non sia l’interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l’autorità diretta del Titolare o del Responsabile;

“Informativa”: l’insieme delle informazioni che il Titolare rende all’Interessato ai sensi degli articoli

13 e/o 14 GDPR;

“Basi Giuridiche”: le condizioni di liceità del trattamento ai sensi dell’art. 6 GDPR;

"Consenso": la prima delle basi giuridiche di cui all’art. 6 GDPR, consistente in qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell’interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

“Altre Condizioni di Liceità”: le ulteriori condizioni di liceità del trattamento, quali ad esempio quelle stabilite dall’art. 9 GDPR per il trattamento delle categorie particolari di dati personali; altre condizioni sono dettate dal Codice Privacy, ad esempio attraverso il rinvio a regole deontologiche o misure di garanzia, o direttamente dal Garante, ad esempio attraverso prescrizioni;

“Diritti dell’Interessato”: i diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR;

“Regolamento Privacy”: il presente documento comprensivo di eventuali allegati;

“Sistema Privacy”: l’insieme del Regolamento Privacy, delle misure ivi previste, degli eventuali allegati e di tutte le ulteriori disposizioni applicabili che costituiscono la concreta adozione ed attuazione della Disciplina Privacy presso l’Azienda ULSS 7 Pedemontana;

“Ente”: il soggetto che adotta ed attua il presente Regolamento, come tale **Azienda ULSS n. 7 Pedemontana**, Via dei Lotti, 40 - 36061 Bassano del Grappa (VI), Tel. 0424 888111, CF e P. I.V.A. n. 00913430245, PEC protocollo.aulss7@pecveneto.it, in persona del Direttore Generale *pro tempore*.

Per ogni ulteriore definizione si fa riferimento alla Disciplina Privacy nonché al Sistema Privacy adottato dall’Ente.

2. Il Sistema Privacy dell'Azienda ULSS 7 Pedemontana

Il Regolamento (UE) 2016/679 (GDPR) detta la disciplina comunitaria sulla protezione delle persone fisiche con riferimento al trattamento dei loro dati personali (c.d. "privacy") nonché alla loro libera circolazione.

Il GDPR è un regolamento comunitario e si applica automaticamente in tutta l'Unione Europea, a decorrere dal 25 maggio 2018.

Il GDPR si applica a tutti i trattamenti di dati personali svolti in territorio europeo o da soggetti europei o verso soggetti europei, intendendosi per "europei" il riferimento all'Unione Europea.

Il GDPR riguarda solo il trattamento dei dati personali delle persone fisiche, facendo però salve le altre discipline che coinvolgono anche le persone giuridiche, gli enti e le associazioni.

Sono esenti dalla disciplina solo rari ambiti oggettivi di trattamento, ad esempio quelli svolti per l'esercizio di attività a carattere esclusivamente personale o domestico.

In vari ambiti, ad esempio in materia di dati sulla salute o di consenso dei minori in relazione ai servizi della società dell'informazione, il GDPR demanda ai singoli Stati Membri la facoltà di adottare particolari adeguamenti nazionali nel rispetto del principio di compatibilità con la normativa europea.

In Italia, salva l'applicazione automatica del GDPR nella sua natura di regolamento comunitario, vige altresì il Decreto Legislativo 196/2003 (Codice Privacy), come riformato dal Decreto Legislativo 101/2018 con decorrenza dal 19 settembre 2018; altri adeguamenti sono seguiti e seguono ulteriormente nel tempo mediante ulteriori interventi sul Codice.

Nel corso del tempo, sia l'EDPB che il Garante, al pari delle altre Autorità di controllo previste dal GDPR, sono intervenute con proprie linee guida, di indirizzo, provvedimenti ed ogni altro atto a guidare il migliore adeguamento alla Disciplina Privacy.

Anche la giurisprudenza, sia comunitaria della Corte di Giustizia, che nazionale, ha statuito sulla materia, aggiungendo ulteriori elementi al quadro complessivo della Disciplina Privacy.

Per tendere al massimo rispetto della disciplina in materia di privacy e soddisfare la migliore *accountability*, ossia la capacità di dimostrare tale rispetto, l'Azienda ULSS 7 Pedemontana provvede ad adottare ed attuare presso la propria organizzazione un impianto di adeguamento che definisce il "Sistema Privacy" aziendale, il quale si compone del presente Regolamento e di un insieme di documenti, linee guida, istruzioni, prassi, disciplinari, misure di sicurezza ed ogni altra misura idonea alla migliore protezione dei diritti e delle libertà fondamentali delle persone fisiche in relazione ai propri dati personali, nel rispetto della libera circolazione per l'assolvimento delle funzioni dell'Ente.

3. Oggetto

Con il presente Regolamento l'Azienda ULSS 7 Pedemontana disciplina le misure adottate in materia di protezione dei dati personali e di libera circolazione dei dati, al fine di adeguare alla vigente Disciplina Privacy i trattamenti dei dati personali da sé svolti.

Il presente Regolamento si applica solo ai trattamenti di dati personali, come definiti dalla Disciplina Privacy.

4. Dati personali oggetto di trattamento

Considerata la natura e la conformazione istituzionale dell'Azienda ULSS 7 Pedemontana, questi tratta:

- dati personali comuni quali, a mero titolo esemplificativo, dati anagrafici e simili;

nonché, al ricorrere delle specifiche condizioni previste dalla Disciplina Privacy e nei limiti in cui ciò sia necessario per la gestione dei trattamenti nel proprio ambito, si riserva di trattare:

- categorie particolari di dati ai sensi dell'art. 9 GDPR, come tali i dati che rivelino l'origine razziale o etnica, le convinzioni religiose o l'appartenenza sindacale, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, dati relativi alla vita sessuale ed all'orientamento sessuale della persona;

- dati penali e relativi a reati o a connesse misure di sicurezza ai sensi dell'art. 10 GDPR.

I dati possono provenire dal conferimento diretto da parte dell'Interessato o da fonti previste dalla vigente disciplina.

I dati personali sono trattati in specifici archivi, nel rispetto delle disposizioni vigenti.

I dati sono oggetto di uno o più dei trattamenti previsti dal GDPR ed in genere dalla Disciplina Privacy, che siano conformi alle funzioni dell'Azienda ULSS 7 Pedemontana o con esse compatibili.

5. Principi applicati

L'Azienda ULSS 7 Pedemontana si impegna a trattare i dati personali in conformità alla Disciplina Privacy.

L'Azienda ULSS 7 Pedemontana garantisce in particolare che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati.

La tutela dei predetti diritti e libertà è attuata cercando di dare, al contempo, piena attuazione anche al principio di operatività, non solo mediante la redazione del presente Regolamento che detta disposizioni appropriate al contesto, ma anche attraverso una capillare sensibilizzazione alla protezione dei dati personali che mira a diffondere presso tutta la struttura organizzativa l'Azienda ULSS 7 Pedemontana.

A tale proposito l'Azienda ULSS 7 Pedemontana promuove al suo interno ogni migliore strumento di sensibilizzazione, anche attraverso idonee attività formative ed informative, al fine di consolidare una mentalità attenta al pieno rispetto della protezione dei dati ed ai principi dettati dalla Disciplina Privacy.

5.1 Principi fondamentali

In conformità ai principi fondamentali dettati dall'art. 5 GDPR, l'Azienda ULSS 7 Pedemontana si impegna affinché i dati personali siano:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principio di "liceità, correttezza e trasparenza");

- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di

archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'art. 89 par. 1 GDPR non è considerato incompatibile con le finalità iniziali (principio di "limitazione della finalità");

- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
- esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di "esattezza");
- conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'art. 89.1 GDPR, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato (principio di "limitazione della conservazione");
- trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di "integrità e riservatezza").

5.2 Responsabilizzazione (c.d. accountability)

L'Azienda ULSS 7 Pedemontana si impegna a rispettare i suddetti principi fondamentali applicando tutte le necessarie misure di protezione e restando in grado di documentarlo (principio di "responsabilizzazione" o "accountability").

A tale proposito, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, l'Azienda ULSS 7 Pedemontana si impegna a mettere in atto - e tenere costantemente aggiornate - misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al GDPR.

L'Azienda ULSS 7 Pedemontana si riserva peraltro di aderire a codici di condotta ai sensi dell'art. 40 GDPR o a meccanismi di certificazioni ai sensi dell'art. 43 GDPR, per dimostrare il rispetto degli obblighi di legge.

5.3 Privacy by design e Privacy by default

Tenuto conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, l'Azienda ULSS 7 Pedemontana si impegna a mettere in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, nonché integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del GDPR e tutelare i diritti degli interessati (principio di "*privacy by design*").

L'Azienda ULSS 7 Pedemontana si impegna altresì a mettere in atto misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica (principio di "*privacy by default*").

6. Ruoli che coinvolgono l'Azienda ULSS 7 Pedemontana nel trattamento dei dati personali

Ciascun trattamento di dati personali coinvolge almeno un Interessato ed almeno un Titolare e può coinvolgere anche uno o più Responsabili del trattamento.

Possono verificarsi anche situazioni di Contitolarità.

Possono altresì verificarsi comunicazioni verso Destinatari, nei casi previsti ed autorizzati, così come diffusioni di dati, alle condizioni e con i limiti ed i divieti di legge.

L'Azienda ULSS 7 Pedemontana regola il proprio ruolo in relazione a tali diverse ipotesi.

6.1 L'Azienda ULSS 7 Pedemontana come Titolare

L'Azienda ULSS 7 Pedemontana opera come Titolare del trattamento in tutti i casi in cui determina le finalità ed i mezzi del trattamento ovvero, quale soggetto pubblico, ove detta titolarità sia definita dal diritto applicabile o dai fini istituzionali che l'Azienda ULSS 7 Pedemontana persegue.

In tale contesto, l'Azienda ULSS 7 Pedemontana assume il ruolo di Titolare del trattamento nella sua integrale personalità giuridica, come rappresentata dal Vertice Gerarchico.

Quale Titolare, l'Azienda ULSS 7 Pedemontana si impegna ad adottare tutte le misure richieste espressamente a tale ruolo, tra cui la resa delle informazioni agli Interessati ("informative") ed il riscontro ai diritti esercitati da costoro ai sensi degli artt. 12 e seguenti GDPR, lo svolgimento di una Valutazione di Impatto (DPIA) ai sensi dell'art. 35 GDPR, l'eventuale notifica al Garante e l'eventuale comunicazione agli Interessati delle violazioni di dati personali ("*data breach*") ai sensi degli articoli 33 e 34 GDPR ed ogni altra misura in capo a tale figura.

6.2 L'Azienda ULSS 7 Pedemontana come Contitolare

Nei casi in cui le finalità e/o i mezzi del trattamento siano definiti congiuntamente da due o più Titolari, anche in forma asimmetrica e/o non paritaria, ovvero detta contitolarità sia prevista o derivi dalla disciplina vigente cui l'Azienda ULSS 7 Pedemontana è soggetta, l'Azienda ULSS 7 Pedemontana sarà considerata Contitolare rispetto agli altri Contitolari e si impegna, a tale fine, a definire le rispettive responsabilità, compiti ed attribuzioni mediante un accordo ai sensi dell'art. 26 GDPR.

6.3 l'Azienda ULSS 7 Pedemontana come Responsabile

In tutti i casi in cui operi trattamenti per conto di altri Titolari, l'Azienda ULSS 7 Pedemontana è individuata come Responsabile del trattamento.

In tali casi, l'Azienda ULSS 7 Pedemontana si impegna a sottoscrivere con il Titolare un apposito contratto o altro atto equipollente ai sensi dell'art. 28 GDPR, secondo cui, quale Responsabile del

trattamento:

a) si impegna a trattare i dati personali soltanto su istruzione documentata del Titolare, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvi gli obblighi di legge cui sia soggetto il Responsabile; in tal caso, il Responsabile informa il Titolare circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisce che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotta tutte le misure richieste dall'art. 32 GDPR;

d) qualora intenda avvalersi di uno o più Sub-Responsabili, chiede previa autorizzazione del Titolare ed impegni tali Sub-Responsabili con un contratto o altro atto equipollente di tenore analogo a quello sottoscritto con il Titolare;

e) tenendo conto della natura del trattamento, assiste il Titolare nella soddisfazione dei diritti esercitati dagli interessati;

f) assiste il Titolare nel garantire il rispetto degli obblighi previsti dagli artt. da 32 a 36 GDPR in termini dunque di misure di sicurezza (art. 32 GDPR), eventuali *data breach* (artt. 33 e 34 GDPR), DPIA ed eventuale consultazione preventiva del Garante (art. 35 e 36 GDPR);

g) su scelta del Titolare, cancella o gli restituisce tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto preveda la conservazione dei dati;

h) metta a disposizione del Titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal Titolare o da suoi delegati; a tale fine, il Responsabile deve informare immediatamente il Titolare qualora, a suo parere, un'istruzione violi la disciplina privacy.

Il contratto può essere stipulato anche sulla base di clausole generali standard (art. 28 par.7 GDPR), quali quelle emanate dalla Commissione Europea con provvedimento del 4 giugno 2021 ("SCCs": *Standard Contractual Clauses*).

6.4 Responsabili del trattamento dell'Azienda ULSS 7 Pedemontana

Qualora altri soggetti esterni trattino dati personali per conto dell'Azienda ULSS 7 Pedemontana, l'Azienda ULSS 7 Pedemontana si impegna a permettere tale trattamento solo a seguito espressa nomina a Responsabile di detti soggetti. La nomina dovrà avvenire mediante apposito contratto o altro atto equipollente ai sensi dell'art. 28 GDPR, il quale dovrà prevedere impegni del Responsabile analoghi a quelli sopra descritti.

L'Azienda ULSS 7 Pedemontana individua tali Responsabili del trattamento tra i soggetti che offrono garanzie sufficienti alla migliore protezione dei dati personali.

6.5 Autorizzati al trattamento

Salva la nomina di uno o più Responsabili del trattamento per i trattamenti effettuati per conto

dell'Azienda ULSS 7 Pedemontana da parte di soggetti esterni, l'Azienda ULSS 7 Pedemontana compie in proprio le operazioni di trattamento attraverso persone fisiche sotto la propria autorità, che designa come Autorizzati al trattamento ed a cui sono conferite istruzioni, ai sensi degli artt. 29 GDPR e 2-quaterdecies Codice Privacy.

Tali istruzioni vertono principalmente sulle misure di sicurezza organizzative, fisiche e tecniche che devono essere rispettate per ciascun trattamento, nonché possono consistere in linee guida ed altre regole di buona condotta.

Rinviando alla disciplina specifica dettata nell'ambito dell'Organigramma Privacy dell'Azienda ULSS 7 Pedemontana, salvo diversamente disposto tutto il personale dell'Azienda ULSS 7 Pedemontana che esegue operazioni di trattamento sotto la sua autorità è designato quale Autorizzato al trattamento per gli ambiti di propria competenza.

Specifici Autorizzati possono altresì assumere la veste di Referenti o di Delegati o Sub-Delegati o di Punti di Contatto, con compiti di coordinamento.

6.6 Comunicazioni di dati verso Destinatari e diffusione di dati

L'Azienda ULSS 7 Pedemontana si riserva di comunicare dati personali verso quei Destinatari per cui sussistano idonee Basi Giuridiche ed Altre Condizioni di Liceità, nonché ogni altra condizione di legge.

Tra i Destinatari, rientrano i Responsabili del trattamento, previo contratto o altro atto equipollente ai sensi dell'art. 28 GDPR, nonché gli Autorizzati al trattamento debitamente designati ai sensi degli artt. 29 GDPR e 2-quaterdecies Codice Privacy, oltre ad altri Titolari o eventuali Contitolari del trattamento nell'ambito di accordi ai sensi dell'art. 26 GDPR.

I dati possono essere diffusi solo in presenza di idonee Basi Giuridiche e delle Altre Condizioni di Liceità applicabili, nonché delle altre condizioni di legge, salvi i divieti espressi, ad esempio per i dati sulla salute.

6.7 Trasferimenti transfrontalieri verso Paesi terzi o organizzazioni internazionali

L'Azienda ULSS 7 Pedemontana si riserva di eseguire trasferimenti transfrontalieri di dati personali verso Paesi terzi, localizzati al di fuori dell'Unione Europea e dello Spazio Economico Europeo, oppure verso organizzazioni internazionali, ma solo al ricorrere di una o più delle condizioni di adeguatezza di cui agli artt. da 44 a 49 GDPR.

7. Il Responsabile della Protezione dei Dati / *Data Protection Officer* (RPD/DPO)

L'Azienda ULSS 7 Pedemontana designa un proprio Responsabile della Protezione dei Dati (RPD) o, con accezione inglese, *Data Protection Officer* (DPO), al ricorrere di una o più delle condizioni di cui all'art. 37 GDPR, il quale prevede l'obbligatorietà di tale designazione ove:

a) il trattamento sia effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali dell'Ente consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;

c) le attività principali dell'Ente consistono in trattamenti, su larga scala, di categorie particolari di dati personali (art. 9 GDPR) o di dati relativi a condanne penali e a reati (art. 10 GDPR).

Come disciplinato anche dagli artt. 38 e 39 GDPR, il RPD/DPO è un importante presidio del sistema di protezione dei dati personali, in quanto si prefigura quale figura autonoma ed indipendente che svolge i seguenti compiti essenziali:

a) informa e fornisce consulenza di indirizzo all'Ente nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dalla Disciplina Privacy;
b) sorveglia l'osservanza della Disciplina Privacy nonché delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornisce, se richiesto, un parere in merito alla Valutazione d'Impatto sulla protezione dei dati (DPIA) e ne sorveglia lo svolgimento ai sensi dell'art. 35 GDPR;
d) coopera con l'Autorità di controllo;
e) funge da punto di contatto per l'Autorità di controllo (il Garante, per l'Italia) per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il RPD/DPO considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

L'Azienda ULSS 7 Pedemontana si riserva di designare il RPD/DPO nella persona di un soggetto esterno (persona fisica o giuridica) sulla base di un contratto di servizi oppure di un soggetto interno, nell'ambito del proprio personale; in ambo i casi, garantisce che il profilo del soggetto individuato sia dotato di particolari competenze nella materia e offra autonomia ed indipendenza nell'assolvimento dei propri compiti.

L'Azienda ULSS 7 Pedemontana si impegna ad avvisare tempestivamente e adeguatamente il RPD/DPO con riferimento a tutte le questioni riguardanti la protezione dei dati personali ed a sostenerlo nell'assolvimento delle proprie funzioni, mediante assicurazione delle risorse necessarie, anche di collaborazione da parte del personale interno.

Il RPD/DPO mantiene il massimo segreto e la massima riservatezza in merito all'adempimento dei propri compiti e, in genere, alle informazioni assunte nello svolgimento del ruolo.

L'assunzione del ruolo di RPD/DPO non implica vincolo di esclusiva con l'Azienda ULSS 7 Pedemontana, ad eccezione degli obblighi di esclusiva nel caso di designazione di persona interna, salvo in ogni caso il limite del conflitto di interessi. Laddove fossero ravvisati dall'Azienda ULSS 7 Pedemontana casi di potenziale conflitto di interessi, l'Azienda ULSS 7 Pedemontana medesima potrà evidenziare la questione al RPD/DPO in opportuno contraddittorio affinché siano discusse ed apportate le opportune soluzioni.

Nell'ambito delle proprie funzioni il RPD/DPO non è in ogni caso responsabile per gli adempimenti imposti dalla Disciplina Privacy, che sono e restano a cura e carico esclusivi dell'Azienda ULSS 7 Pedemontana anche ai sensi delle linee guida "WP-243" del 13 dicembre 2016 del Gruppo di Lavoro art. 29 ("WP29").

La designazione ed i dati di contatto sono comunicati al Garante e pubblicati a disposizione degli Interessati, ad esempio sul sito internet l'Azienda ULSS 7 Pedemontana, nonché inseriti nelle informative.

8. Organigramma Privacy dell'Azienda ULSS 7 Pedemontana

L'Azienda ULSS 7 Pedemontana ha strutturato un proprio Modello Organizzativo per la protezione dei dati personali secondo un Organigramma Privacy che rispecchia da un lato i ruoli previsti dalla Disciplina Privacy e dall'altro la propria organizzazione.

L'Azienda ULSS 7 Pedemontana, a prescindere che operi quale Titolare o Contitolare o Responsabile, ha adottato un proprio Organigramma Privacy con i seguenti ruoli e funzioni:

1) **Figure privacy e soggetti a cui rispondono.**

1) **Direttore Generale**: è il legale rappresentante dell'Azienda ULSS 7 Pedemontana, la quale, a seconda delle circostanze, assume il ruolo di Titolare, Contitolare o Responsabile/Sub Responsabile del trattamento (di seguito "Azienda"); in tale veste, svolge i compiti precisati *sub* 2.1.
2) **Ufficio Privacy**: afferisce alla U.O.C. Affari Generali, svolge i compiti precisati *sub* 2.2 e risponde al Direttore Generale.
3) **Delegati Privacy**: sono i Direttori di Unità Operativa Complessa, i responsabili di Unità Operativa Semplice Dipartimentale, i responsabili degli uffici in staff al Direttore Generale, gli sperimentatori e i responsabili di istituti clinici, svolgono i compiti precisati *sub*. 2.3, sono nominati dal Direttore Generale.
4) **Sub Delegati**: sono i responsabili di Unità Operativa Semplice, sono individuati dai Direttori di Unità Operativa Complessa, nella loro qualità di Delegati Privacy, svolgono i compiti da questi attribuiti e rispondono al soggetto che li ha nominati.
5) **Punti di Contatto Privacy**: svolgono i compiti precisati *sub* 2.4, sono individuati dai Delegati Privacy o dai Sub Delegati Privacy, laddove presenti, tra i rispettivi collaboratori e rispondono al soggetto che li ha nominati.
6) **Autorizzati**: Tutte le persone che funzionalmente svolgono operazioni di trattamento su dati di cui l'Azienda ha la titolarità, nonché prestano attività all'interno dell'Azienda stessa a qualsiasi titolo, con o senza retribuzione, compresi gli allievi e i docenti dei corsi di formazione e di aggiornamento professionale, anche in convenzione con le università, gli specializzandi, i tirocinanti e i volontari, qualora in occasione della loro attività vengano a conoscenza di dati personali trattati dall'Azienda sono autorizzati dai competenti Delegati ed assumono gli stessi obblighi. I dirigenti che svolgono attività libero professionale intramuraria sono autorizzati direttamente dal Direttore Generale.
7) **U.O.C. Sistemi Informativi**: svolge i compiti precisati *sub* 2.5 e risponde al Direttore Generale;
8) **Responsabile della Protezione dei Dati (RPD/DPO)**: svolge in autonomia i compiti a sé attribuiti dalla disciplina in materia di protezione dei dati personali - richiamati e integrati *sub* 2.6 - e risponde al Direttore Generale.
9) **Sperimentatore Principale:** svolge i compiti precisati *sub* 2.7 si tratta di medici qualificati ai fini delle sperimentazioni, responsabili del gruppo di sperimentatori e dell'esecuzione delle sperimentazioni cliniche nell'AULSS 7 Pedemontana. Sono nominati dal Direttore Generale.

2) **Individuazione dei compiti/funzioni.**

2.1) Il Direttore Generale:
- ✓ approva il Modello Organizzativo Privacy e la revisione dello stesso, oltre che i documenti volti a dare atto delle specifiche scelte compiute in materia di protezione dei dati personali, al fine di dare concreta attuazione al principio di *accountability ex* art. 5, par. II, Reg. (UE) 2016/679 (di seguito "GDPR");
- ✓ sottoscrive le nomine a Responsabile del trattamento *ex* art. 28 GDPR in relazione ai contratti di propria pertinenza;
- ✓ sottoscrive gli accordi di contitolarità *ex* art. 26 GDPR in relazione ai contratti di propria pertinenza;

2.2) Nelle forme ritenute opportune caso per caso, l'Ufficio Privacy:
- ✓ fornisce supporto nella predisposizione e nell'aggiornamento dei registri delle attività di trattamento;
- ✓ predispone i modelli documentali, le istruzioni operative per la relativa applicazione e le procedure utili ai fini dell'osservanza della disciplina in materia di protezione dei dati personali;
- ✓ fornisce il materiale di cui al punto precedente a ciascun Delegato Privacy;
- ✓ fornisce supporto a ciascuna delle Figure Privacy in caso di questioni particolari (es. pareri su nuove schede dei registri delle attività di trattamento, predisposizione di nuova modulistica, pareri su Valutazione d'impatto, ecc.);
- ✓ coinvolge il R.P.D. nei casi previsti dalla disciplina in materia di protezione dei dati personali;
- ✓ coinvolge l'U.O.C. Sistemi Informativi in merito a ogni questione inerente alla disciplina in materia di protezione dei dati personali che ne richieda l'intervento.

2.3) Con riguardo ai trattamenti di dati personali effettuati nell'ambito di appartenenza (U.O.C., U.O.S.D. e A.F.), ciascun Delegato Privacy:
- ✓ svolge i compiti attribuiti dal Direttore Generale o dal Coordinatore Privacy che lo ha nominato;
- ✓ sottoscrive le nomine a Responsabile del trattamento *ex* art. 28 GDPR in relazione ai contratti di propria pertinenza;
- ✓ sottoscrive gli accordi di contitolarità *ex* art. 26 GDPR in relazione ai contratti di propria pertinenza;
- ✓ individua gli Autorizzati al trattamento dei dati personali, specificandone i compiti e impartendo le istruzioni per il trattamento conseguentemente necessarie;
- ✓ dà impulso alla predisposizione e all'aggiornamento del registro delle attività di trattamento del Titolare e del Responsabile;
- ✓ se necessario, individua uno o più Punti di Contatto Privacy, affidando i compiti previsti nel presente documento;
- ✓ in mancanza di Punti di Contatto, svolge i compiti ad essi assegnati nel presente documento;
- ✓ fornisce il materiale predisposto dall'Ufficio Privacy ai Punti di Contatto Privacy;
- ✓ verifica periodicamente che la documentazione adottata in materia di protezione dei dati personali rispecchi i trattamenti effettivamente svolti;
- ✓ verifica periodicamente la compatibilità, fra loro, dei documenti adottati in materia di protezione dei dati personali;

- ✓ vigila sul corretto utilizzo dei modelli documentali e delle relative istruzioni fornite dall'Ufficio Privacy;
- ✓ vigila sulla corretta applicazione delle procedure fornite dall'Ufficio Privacy;
- ✓ collabora con l'Ufficio Privacy e con l'U.O.C. Sistemi Informativi nella definizione delle misure di sicurezza tecniche e organizzative adeguate, vigilando sulla loro applicazione;
- ✓ affida in tutto o in parte i propri compiti a un Sub Delegato Privacy, laddove previsto;
- ✓ il Delegato Privacy afferente all'U.O.S.D. Innovazione e Sviluppo Organizzativo svolge i compiti di cui al presente elenco anche in relazione alle segreterie del Direttore Generale e dei Direttori Sanitario, dei Servizi Socio Sanitari, Amministrativo.

2.4) Con riguardo ai trattamenti di dati personali effettuati nel rispettivo ambito di afferenza, ciascun Punto di Contatto Privacy:

- ✓ funge da referente per il personale afferente al proprio ambito nei confronti del Delegato Privacy, del Sub Delegato privacy, dell'Ufficio Privacy e dell'U.O.C. Sistemi informativi;
- ✓ predispone e mantiene aggiornato il registro delle attività di trattamento del Titolare/Contitolare e del Responsabile/Sub-Responsabile, dandone tempestivamente avviso all'Ufficio Privacy;
- ✓ supporta il Delegato Privacy o il Sub Delegato Privacy, laddove previsto, nelle sue funzioni di vigilanza;
- ✓ segnala all'Ufficio Privacy la necessità di predisporre nuova modulistica o di aggiornare quella esistente, collaborando con lo stesso a tale scopo;
- ✓ segnala all'Ufficio Privacy la necessità di predisporre una valutazione d'impatto sulla protezione dei dati personali e/o collabora nella predisposizione della stessa e nell'espletamento degli obblighi correlati (es. consultazione preventiva);
- ✓ collabora con l'Ufficio Privacy e con l'U.O.C. Sistemi informativi nell'effettuazione dell'analisi dei rischi;
- ✓ conserva e mette a disposizione del personale afferente al proprio ambito i modelli documentali, le istruzioni operative per la relativa applicazione e le procedure forniti dall'Ufficio Privacy;
- ✓ funge da punto di riferimento del personale afferente al proprio ambito per l'applicazione dei modelli documentali, delle istruzioni operative per la relativa applicazione e delle procedure forniti dall'Ufficio Privacy;
- ✓ interpella l'Ufficio Privacy laddove le proprie conoscenze e/o la documentazione in suo possesso non fossero sufficienti in relazione a specifiche questioni.

2.5) l'U.O.C. Sistemi Informativi:

- ✓ collabora con le Figure Privacy che la interpellano in merito alle questioni in materia di protezione dei dati personali riguardanti il rispettivo ambito di afferenza;
- ✓ coinvolge l'Ufficio Privacy in merito alle questioni in materia di protezione dei dati personali che non possano essere risolte in tutto o in parte all'interno dell'ambito in cui le stesse sono sorte;
- ✓ collabora con l'Ufficio Privacy quando richiesto;
- ✓ partecipa alle attività necessarie all'analisi dei rischi e alla valutazione d'impatto.

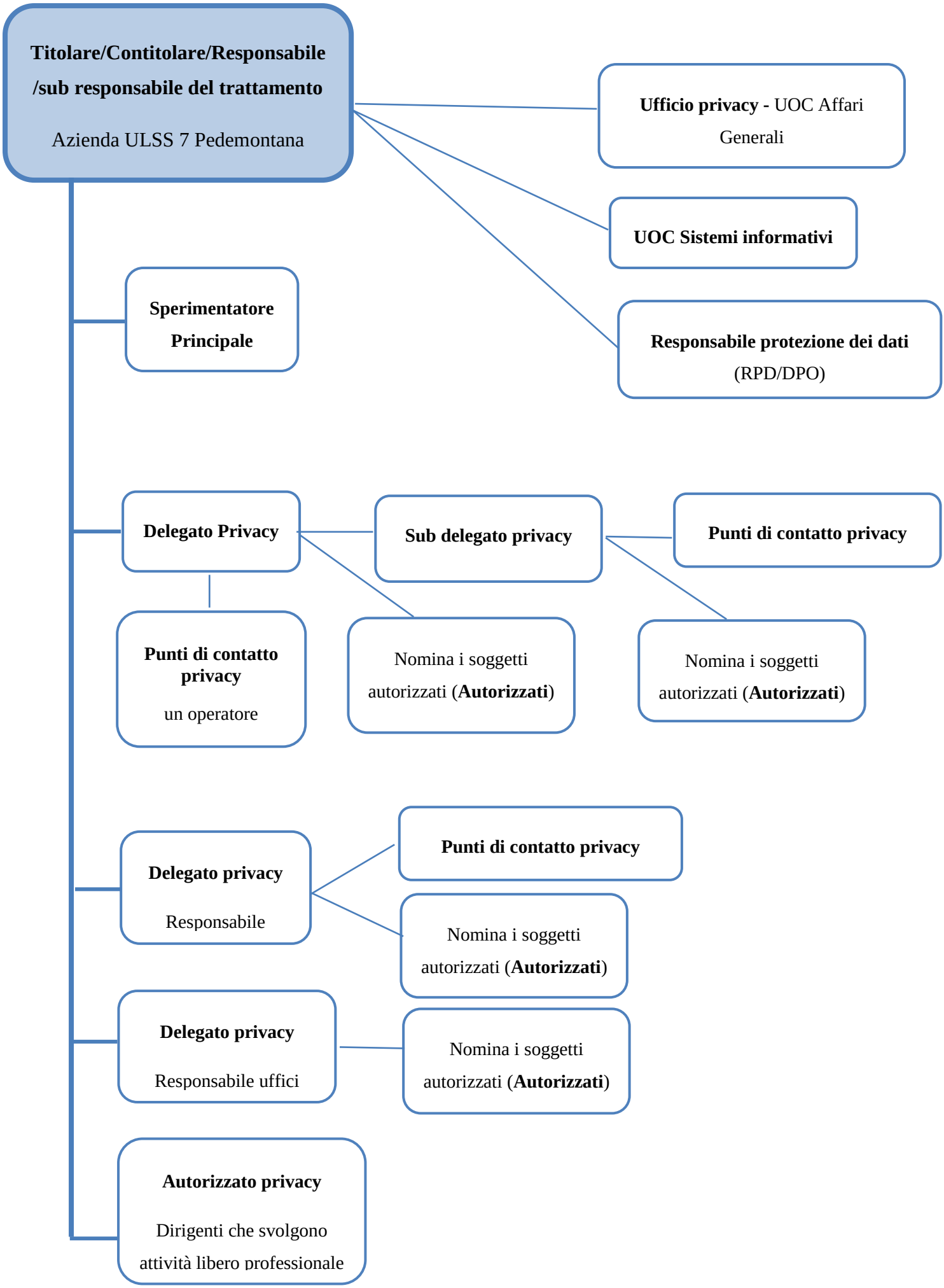
2.6) ferma restando la propria autonomia, nei termini sopra richiamati, il Responsabile della Protezione dei Dati (R.P.D.) con l'Ufficio Privacy per fornire i pareri eventualmente necessari a questi ultimi e può invece rivolgersi a ciascuna delle Figure Privacy in sede di verifica o, comunque, qualora altrimenti necessario.

Il R.P.D. svolge inoltre i compiti e le funzioni di cui all'art. 39 del Regolamento (UE) 2016/679, di seguito riassunte:

- ✓ **funzione consultiva**: informa e fornisce consulenza all'Azienda; se richiesto, fornisce parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento;
- ✓ **funzione di sorveglianza e garanzia**: sorveglia l'osservanza, da parte dell'Azienda, della disciplina in materia di protezione dei dati personali, nonché delle politiche del trattamento definite dall'Azienda stessa;
- ✓ **funzione di contatto**: coopera con l'Autorità di controllo e funge da punto di contatto con la stessa; può essere contattato dagli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

2.7) Lo Sperimentatore Principale è individuato dall'Azienda ULSS 7 Pedemontana quale persona autorizzata al trattamento ai sensi dell'art. 29 del GDPR e quale soggetto designato ai sensi dell'art. 2 quaterdecies del Decreto Legislativo n. 196/2003.

- ✓ Lo Sperimentatore Principale, deve informare in modo chiaro e completo, prima che abbia inizio lo Studio (incluse le relative fasi prodromiche e di screening) ogni paziente circa natura, finalità, risultati, conseguenze, rischi e modalità del trattamento dei dati personali; in particolare il paziente deve inoltre essere informato che Autorità nazionali e straniere, nonché il Comitato Etico, potranno accedere, nell'ambito di attività di monitoraggio, verifica e controllo sulla ricerca, alla documentazione relativa allo Studio così come anche alla documentazione sanitaria originale del paziente, e che ad esse potranno anche eccedere in visione, nell'ambito delle rispettive competenze, Monitor e Auditor.
- ✓ Lo Sperimentatore Principale deve acquisire dal paziente debitamente informato il documento di consenso oltre che alla partecipazione allo Studio, anche al trattamento dei dati. L'Azienda ULSS 7 Pedemontana è responsabile della conservazione di tale documento.
- ✓ Qualora uno dei Titolari del trattamento accerti una violazione dei dati personali, si impegna a comunicarlo all'altro Titolare del trattamento entro 48 ore dall'accertamento della violazione, ferma restando l'autonomia di ognuno dei Titolari del trattamento nella valutazione della sussistenza delle condizioni e nell'adempimento degli obblighi previsti dagli artt. 33 e 34 del GDPR.


Titolare/Contitolare/Responsabile /sub responsabile del trattamento
Azienda ULSS 7 Pedemontana
Ufficio privacy - UOC Affari Generali
UOC Sistemi informativi
Responsabile protezione dei dati (RPD/DPO)
Sperimentatore Principale
Delegato Privacy
Sub delegato privacy
Punti di contatto privacy
Punti di contatto privacy un operatore
Nomina i soggetti autorizzati (Autorizzati)
Nomina i soggetti autorizzati (Autorizzati)
Delegato privacy Responsabile
Punti di contatto privacy
Nomina i soggetti autorizzati (Autorizzati)
Delegato privacy Responsabile uffici
Nomina i soggetti autorizzati (Autorizzati)
Autorizzato privacy Dirigenti che svolgono attività libero professionale

Per l'accesso alle funzioni proprie del Referente/Ufficio Privacy e del RPD/DPO, l'Azienda ULSS 7 Pedemontana ha previsto uno specifico Regolamento di accesso alle funzioni di tali organi privacy al quale si rimanda interamente.

9. Registro dei trattamenti

L'Azienda ULSS 7 Pedemontana registra i trattamenti svolti nel ruolo di Titolare (e/o di Contitolare) in apposito Registro dei trattamenti del Titolare, ai sensi dell'art. 30 par. 1 GDPR, nonché quelli svolti nel ruolo di Responsabile in apposito Registro del Responsabile, ai sensi dell'art. 30 par. 2 GDPR.

Il Registro delle attività di trattamento o Registro dei trattamenti è quel documento previsto e disciplinato dall'art. 30 GDPR, sia per il Titolare, che per il Responsabile del trattamento, che contiene le principali informazioni relative alle operazioni di trattamento svolte.

Il Registro dei trattamenti del Titolare riporta le seguenti informazioni (art. 30.1 GDPR):

a) il nome e i dati di contatto del Titolare e, ove applicabile, del Contitolare del trattamento, del suo rappresentante e del DPO;

b) le finalità del trattamento;

c) una descrizione delle categorie di interessati e delle categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49.2 GDPR, la documentazione delle garanzie adeguate;

f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32.1 GDPR.

Il Registro dei trattamenti del Responsabile riporta le seguenti informazioni (art. 30.2 GDPR):

a) il nome e i dati di contatto del Responsabile o dei Responsabili del trattamento, di ogni Titolare per conto del quale agiscono, del rappresentante del Titolare del trattamento o del Responsabile del trattamento e, ove applicabile, del DPO;

b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;

c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui all'art. 49.2 GDPR, la documentazione delle garanzie adeguate;

d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art. 32.1 GDPR.

Il Registro ha forma elettronica.

Il Registro è tenuto presso l'Azienda ULSS 7 Pedemontana sotto il coordinamento dell'Ufficio Privacy

aziendale e dell'UOC Sistemi Informativi per gli aspetti IT di competenza, ed è aggiornato con l'intervento e la supervisione dei Delegati ovvero dei Sub-Delegati se designati, per i trattamenti di pertinenza dell'Unità di competenza, attraverso il coordinamento dei rispettivi Punti di Contatto.

Gli Autorizzati di competenza dell'Unità prestano il loro ausilio nell'ambito e nei limiti dei compiti loro assegnati; parimenti operano, con funzioni di coordinamento, i Punti di Contatto.

10. Valutazione di Impatto (DPIA)

L'Azienda ULSS 7 Pedemontana, laddove operi quale Titolare, si impegna ad adottare una Valutazione di Impatto (o "DPIA": *Data Protection Impact Assessment*) nei casi previsti dall'art. 35 GDPR, ossia quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ovvero negli altri casi previsti dalla Disciplina Privacy.

La DPIA è svolta dall'Azienda ULSS 7 Pedemontana prima di procedere al trattamento.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

La DPIA mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare e/o valutare l'idoneità delle misure atte ad affrontarli e valutare altresì l'eventuale consultazione preventiva del Garante prevista dall'art. 36 GDPR laddove il trattamento possa presentare un rischio elevato in assenza di misure adottate per attenuare il rischio.

La DPIA è obbligatoria in tutti i casi in cui un trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'art. 35 GDPR esemplifica tali casi:

a) valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su tali persone fisiche;

b) trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9.1 GDPR o di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR;

c) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Altri casi in cui la DPIA sia richiesta sono individuati dal Garante, in particolare con l'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979], pubblicato in Gazzetta Ufficiale n. 269 del 19 novembre 2018, e successive modificazioni ed integrazioni, cui l'Ente rinvia a valere quale parte integrante del presente Regolamento. Tra detti casi, si annoverano:

- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);

- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, *device IoT*, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

La DPIA costituisce un documento scritto, anche elettronico, che contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati;

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Nei casi in cui l'Azienda ULSS 7 Pedemontana operi come Responsabile del trattamento, esso si impegna ad assistere il Titolare nello svolgimento della DPIA di spettanza di tale Titolare.

Salvo che sia diversamente disposto dall'Organigramma Privacy ovvero dai singoli atti di designazione, la DPIA è svolta, sotto il coordinamento del Referente Privacy o dell'Ufficio Privacy se nominato, nonché del Referente IT per gli aspetti connessi al sistema informativo, nonché primariamente dei rispettivi Punti di Contatto se previsti per l'Unità di competenza, a cura del Delegato, ovvero dei Sub-Delegati se designati, di competenza dell'Unità entro cui il trattamento dei dati personali oggetto di valutazione si inserisce. Nel caso di trattamenti strutturali o trasversali a più Aree, i singoli Delegati competenti si coordinano tra di loro.

Resta sempre salva la possibilità di avvalersi di Responsabili del trattamento a supporto dello svolgimento della DPIA.

Gli Autorizzati di competenza dell'Unità prestano il loro ausilio nell'ambito e nei limiti dei compiti loro assegnati; parimenti operano, con funzioni di coordinamento, i Punti di Contatto.

L'Azienda ULSS 7 Pedemontana può chiedere un parere sulla DPIA al proprio RPD/DPO.

11. Basi Giuridiche ed Altre Condizioni di Liceità

l'Azienda ULSS 7 Pedemontana fonda il trattamento dei dati personali su almeno una o più delle Basi Giuridiche appropriate che l'art. 6 GDPR individua come tali:

a) consenso dell'Interessato per una o più specifiche finalità;

b) necessità del trattamento per l'esecuzione di un contratto di cui l'Interessato è parte o per l'esecuzione di misure precontrattuali adottate su richiesta dello stesso;

c) necessità del trattamento per adempiere un obbligo legale cui è soggetto il Titolare;

d) necessità del trattamento per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;

e) necessità del trattamento per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

f) necessità del trattamento per il perseguimento del legittimo interesse del Titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato, in particolare se è un minore; salva la previsione per cui tale Base Giuridica non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Nel caso in cui la Base Giuridica che legittima il trattamento sia l'obbligo legale o l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare, detta Base deve essere stabilita:

a) dal diritto dell'Unione Europea; o

b) dal diritto dello Stato membro cui è soggetto il Titolare del trattamento.

Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'Interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, par. 1 GDPR (tra cui la sicurezza nazionale; la difesa, la sicurezza pubblica; la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica; altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro; la salvaguardia dell'indipendenza della magistratura e dei procedimenti giudiziari; le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate; una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente, all'esercizio di pubblici poteri nei casi previsti; la tutela dell'Interessato o dei diritti e delle libertà altrui; l'esecuzione delle azioni civili) al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il Titolare del trattamento tiene conto, tra l'altro:

a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;

b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'Interessato e il Titolare del trattamento;

c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9 GDPR, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10 GDPR;

d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati;

e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione.

Nel caso di trattamento di categorie particolari di dati, considerato il generale divieto di trattamento di tali dati di cui all'art. 9 par.1 GDPR, l'Azienda ULSS 7 Pedemontana si impegna a trattare detti dati unicamente in presenza di una o più delle Altre Condizioni di Liceità, ulteriori rispetto a quelle previste dall'art. 6 GDPR, che l'art. 9 par. 2 GDPR individua come tali:

a) consenso esplicito dell'Interessato per una o più finalità specifiche;

b) necessità del trattamento per assolvere gli obblighi ed esercitare i diritti specifici del Titolare o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'Interessato;

c) necessità del trattamento per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) trattamenti eseguiti da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'Interessato;

e) dati personali resi manifestamente pubblici dall'Interessato;

f) necessità del trattamento per accertare, esercitare o difendere un diritto in sede giudiziaria;

g) necessità del trattamento per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;

h) necessità del trattamento per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità; in questo caso i dati personali devono essere trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale o da altra persona soggetta all'obbligo di segretezza;

i) necessità del trattamento per motivi di interesse pubblico nel settore della sanità pubblica;

j) necessità del trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'art. 89.1 GDPR.

L'Azienda ULSS 7 Pedemontana si impegna a rispettare le eventuali ulteriori condizioni di liceità o legittimità, prescrizioni, misure, linee guida e simili, previste da Regole Deontologiche, Linee Guida, Prescrizioni, Codici di Condotta ed altre misure previste dalla vigente Disciplina Privacy, anche in considerazione di spazi di disciplina nazionali che il GDPR riconosce agli Stati membri ad esempio per i trattamenti di dati nell'ambito di rapporti di lavoro, dati genetici, biometrici e relativi alla salute,

ricerca, minori.

Nel caso in cui l'Azienda ULSS 7 Pedemontana individui il consenso quale Base Giuridica e/o altra Condizione di Liceità del trattamento, si impegna a raccoglierlo in modo libero, specifico, informato ed inequivocabile.

Nel caso di minori, la prestazione del consenso sarà uniformata alle regole specifiche dell'art. 8 GDPR nei casi ivi previsti, in particolare per i servizi della società dell'informazione.

Per talune tipologie di basi giuridiche (in particolare, per l'obbligo legale e per l'interesse pubblico), nonché per talune tipologie di dati (dati genetici, biometrici e relativi alla salute), così come per la ricerca scientifica, l'ordinamento italiano detta una disciplina di dettaglio. In particolare, il Codice Privacy, come riformato, detta una disciplina di dettaglio agli artt. 2-ter, 2-quater e 2-sexies, come segue:

- l'art. 2-ter Codice Privacy detta una disciplina specifica in relazione all'individuazione della base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, nel caso in cui sia invocata la base giuridica dell'obbligo legale (art. 6 par. 3 GDPR) ovvero l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri; nel caso dell'obbligo legale la base giuridica deve essere costituita da una norma di legge o di regolamento o da atti amministrativi generali;

- l'art. 2-quater Codice Privacy introduce la promozione delle regole deontologiche per i trattamenti previsti dalle disposizioni di cui agli artt. 6, par. 1, lettere c) (obbligo legale) ed e) (interesse pubblico) GDPR e 9 par. 4 (dati genetici, dati biometrici e dati sulla salute) GDPR;

- l'art. 2-sexies Codice Privacy introduce una disciplina specifica per il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante (art. 9 par. 2 lett. g GDPR): in tale caso la base giuridica deve essere costituita da una norma di legge o di regolamento o da atti amministrativi generali; la disposizione detta poi un elenco di materie che sono considerate di rilevante interesse pubblico.

12. Informazioni agli Interessati ("Informative")

L'Azienda ULSS 7 Pedemontana si impegna ad informare gli Interessati secondo la disciplina prevista dagli articoli 13 e/o 14 del GDPR, a seconda che il trattamento riguardi dati personali raccolti presso l'Interessato stesso (art. 13 GDPR) o non (art. 14 GDPR).

Nel primo caso (art. 13 GDPR), l'informativa rende le seguenti informazioni:

a) identità e dati di contatto del Titolare e, ove applicabile, del suo rappresentante;

b) dati di contatto del RPD/DPO, se nominato;

c) finalità del trattamento e basi giuridiche;

d) se il trattamento si fondi sul legittimo interesse ed in caso su quale;

e) eventuali destinatari o categorie di destinatari dei dati personali;

f) ove applicabile, trasferimenti verso Paesi extra UE o organizzazioni internazionali e relative

garanzie di adeguatezza;

g) periodo di conservazione oppure, se non è possibile, i criteri per la sua determinazione;

h) diritti dell'Interessato di accesso ai dati personali, rettifica o cancellazione degli stessi, limitazione del trattamento, opposizione, portabilità dei dati;

i) diritto di revoca del il consenso se il trattamento si fondi su di esso;

j) diritto di proporre reclamo ad un'autorità di controllo;

k) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;

l) eventuali processi decisionali automatizzati, compresa la profilazione, relativa importanza e conseguenze.

In questo caso l'informativa è contestuale alla raccolta.

Nel secondo caso (art. 14 GDPR), l'Informativa rende, oltre alle informazioni previste dall'art. 13 GDPR, anche le seguenti ulteriori informazioni:

a) categoria di dati trattati;

b) fonti di origine ed eventuali fonti accessibili al pubblico.

In questo caso l'informativa può essere posteriore al trattamento, ma deve essere fornita entro un termine ragionevole ed al più tardi entro un mese. Nel caso in cui i dati personali siano destinati alla comunicazione con l'Interessato, l'informativa è resa al più tardi al momento della prima comunicazione all'Interessato; oppure nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali.

L'Azienda ULSS 7 Pedemontana si riserva di valutare i casi di esenzione dall'informativa previsti dagli articoli 13 e/o 14 GDPR, ad esempio quando l'Interessato disponga già delle informazioni.

L'informazione dell'Interessato costituisce un importante presidio che permette all'Interessato il controllo sui propri dati personali anche tramite l'esercizio dei diritti previsti dagli artt. da 15 a 22 GDPR.

Salvo che sia diversamente disposto dall'Organigramma Privacy ovvero dai singoli atti di designazione, l'Informativa è predisposta, sotto il coordinamento del Referente Privacy o dell'Ufficio Privacy se nominato, nonché del Referente IT per gli aspetti connessi al sistema informativo, nonché primariamente dei rispettivi Punti di Contatto se previsti per l'Unità di competenza, a cura del Delegato, ovvero dei Sub-Delegati se designati, di competenza dell'Unità entro cui il trattamento dei dati personali oggetto dell'Informativa si inserisce.

Nel caso di informative che hanno ad oggetto trattamenti strutturali o trasversali a più Aree, i singoli Delegati competenti si coordinano tra di loro e chiedono, se del caso, linee di indirizzo al Vertice Gerarchico, anche attraverso i rispettivi Punti di Contatto. In tale contesto, l'individuazione delle Basi Giuridiche e delle Altre Condizioni di Liceità eventualmente applicabili è svolta analogamente a quanto sopra.

Gli Autorizzati di competenza dell'Unità prestano il loro ausilio nell'ambito e nei limiti dei compiti loro assegnati; parimenti operano, con funzioni di coordinamento, i Punti di Contatto.

13. Diritti dell'Interessato

L'Interessato è la persona fisica identificata o identificabile cui si riferiscono i dati personali.

Il GDPR impernia il sistema di protezione sul primario diritto di controllo che spetta all'Interessato sui propri dati personali (art. 12 GDPR).

Tale controllo si esplica attraverso tutte le misure e garanzie previste dalla disciplina ed in particolare attraverso l'esercizio dei diritti previsti dagli artt. da 15 a 22 GDPR, come tali:

- il diritto di accesso nei casi, modi e limiti previsti dall'art. 15 GDPR;
- il diritto di integrazione e rettifica nei casi, modi e limiti previsti dall'art. 16 GDPR;
- il diritto di cancellazione ("oblio") nei casi, modi e limiti previsti dall'art. 17 GDPR;
- il diritto di limitazione nei casi, modi e limiti previsti dall'art. 18 GDPR;
- il diritto alla portabilità dei dati, nei casi, modi e limiti previsti dall'art. 20 GDPR;
- il diritto di opposizione, nei casi, modi e limiti previsti dall'art. 21 GDPR;
- il diritto a non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. Anche a tale proposito, l'Azienda ULSS 7 Pedemontana si impegna ad adottare una propria politica di rigorosa applicazione dei divieti e delle norme regolatorie sull'uso di sistemi di intelligenza artificiale come previsto dal Regolamento (UE) 2024/1689 ("*AI Act*") e dalla correlata disciplina.

Costituiscono diritti dell'Interessato anche quello di revoca del consenso prestato ai sensi degli articoli 6, 7, 8 e 9 GDPR e quello di proporre reclamo all'autorità di controllo ai sensi dell'art. 77 GDPR, per l'Italia il Garante.

Sono in ogni caso fatte salve le eventuali discipline normative vigenti dell'Unione Europea o della Repubblica Italiana che limitino, mediante misure legislative, la portata degli obblighi e dei diritti di cui sopra, nonché dei principi di cui all'art. 5 GDPR, nella misura in cui le disposizioni ivi contenute corrispondano ai diritti e agli obblighi di cui sopra, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare le esigenze di cui all'art. 23 GDPR, tra cui e senza esclusione di ogni altra ivi prevista:

- la sicurezza nazionale;
- la sicurezza pubblica;
- la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica;
- altri importanti obiettivi di interesse pubblico generale, ad esempio di sanità pubblica e sicurezza sociale;
- le attività volte a prevenire, indagare, accertare e perseguire violazioni della deontologia delle professioni regolamentate;
- una funzione di controllo, d'ispezione o di regolamentazione connessa, anche occasionalmente,

all’esercizio di pubblici poteri;
- la tutela dell’Interessato o dei diritti e delle libertà altrui;
- l’esecuzione delle azioni civili.

Per quanto riguarda le persone decedute, è applicata la disposizione dell’art. 2-terdecies Codice Privacy secondo cui:

- i diritti di cui agli articoli da 15 a 22 GDPR riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'Interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione;
- l'esercizio di tali diritti non è ammesso nei casi previsti dalla legge o quando, limitatamente all'offerta diretta di servizi della società dell'informazione, l'Interessato lo ha espressamente vietato con dichiarazione scritta presentata al Titolare del trattamento o a quest'ultimo comunicata;
- la volontà dell'Interessato di vietare l'esercizio dei diritti di cui sopra deve risultare in modo non equivoco e deve essere specifica, libera e informata;
- il divieto può riguardare l'esercizio soltanto di alcuni dei diritti di cui sopra;
- l'Interessato ha in ogni momento il diritto di revocare o modificare il divieto di cui sopra;
- in ogni caso, il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'Interessato nonché del diritto di difendere in giudizio i propri interessi.

Gli Interessati possono svolgere la propria richiesta senza formalità particolari oppure utilizzando anche la modulistica presente sul sito web del Garante all’indirizzo https://www.garanteprivacy.it/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali.

L’Azienda ULSS 7 Pedemontana si impegna a riscontrare le richieste di esercizio dei diritti pervenute mediante risposta adeguata conformemente all’art. 12 GDPR, come segue.

Fatti salvi i casi in cui il trattamento non richiede o non richiede più l’identificazione, l’Interessato deve essere identificato e, qualora l’Azienda ULSS 7 Pedemontana nutra ragionevoli dubbi circa l’identità della persona fisica che presenta la richiesta di esercizio dei diritti, può richiedere ulteriori informazioni necessarie per confermare l’identità dell’Interessato.

Il Titolare del trattamento fornisce all’Interessato le informazioni relative all’azione intrapresa riguardo a una richiesta di esercizio dei diritti senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Titolare del trattamento informa l’Interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l’Interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell’Interessato.

Se non ottempera alla richiesta dell’Interessato, il Titolare del trattamento informa l’Interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell’inottemperanza e della possibilità di proporre reclamo all'autorità di controllo e di proporre ricorso giurisdizionale.

Le informazioni fornite ai sensi degli articoli 13 e 14 GDPR (informative) ed eventuali comunicazioni e azioni intraprese ai sensi degli articoli da 15 a 22 GDPR (esercizio dei diritti) e dell’articolo 34 GDPR (comunicazione in caso di violazione dei dati personali) sono gratuite. Se le richieste dell’Interessato sono manifestamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il Titolare del

trattamento può:

a) addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per fornire le informazioni o la comunicazione o intraprendere l'azione richiesta; oppure

b) rifiutare di soddisfare la richiesta.

Salvo che sia diversamente disposto dall'Organigramma Privacy ovvero dai singoli atti di designazione, il riscontro all'esercizio dei diritti dell'Interessato, così come di ogni altra segnalazione che pervenga all'Ente, è gestito, sotto il coordinamento del Referente Privacy o dell'Ufficio Privacy se nominato, nonché del Referente IT per gli aspetti connessi al sistema informativo, nonché primariamente dei rispettivi Punti di Contatto se previsti per l'Unità di competenza, a cura del Delegato, ovvero dei Sub-Delegati se designati, di competenza dell'Unità cui l'istanza o la segnalazione ineriscono.

Nel caso di istanze o segnalazioni che abbiano ad oggetto diritti o questioni che coinvolgono più Unità Operative o l'intera struttura l'Azienda ULSS 7 Pedemontana, i singoli Delegati competenti si coordinano tra di loro e chiedono, se del caso, linee di indirizzo al Vertice Gerarchico, anche attraverso i rispettivi Punti di Contatto.

Gli Autorizzati di competenza dell'Unità prestano il loro ausilio nell'ambito e nei limiti dei compiti loro assegnati; parimenti operano, con funzioni di coordinamento, i Punti di Contatto.

14. Misure di sicurezza

L'Azienda ULSS 7 Pedemontana predispone e mantiene costantemente aggiornate idonee misure di sicurezza fisiche, organizzative e tecniche, tra le quali (art. 32 GDPR):

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

In ogni caso le misure sono approntate tenendo conto dello stato dell'arte e dei costi di attuazione, 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, quale quello derivante dalla distruzione, perdita, modifica, divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

l'Azienda ULSS 7 Pedemontana si riserva l'adesione a codici di condotta o a meccanismi di certificazione quale elemento di dimostrazione della conformità, nonché l'esecuzione di protocolli di sicurezza standardizzati, quali quelli proposti per la sicurezza informatica dall'agenzia europea ENISA, ovvero di altri che si fondino sul trinomio R.I.D.: Riservatezza, Integrità, Disponibilità.

Ai fini di cui sopra, anche in base ai principi di *accountability*, privacy *by design* e privacy *by default*, l'Azienda ULSS 7 Pedemontana si riserva di eseguire una aggiornata mappatura dei processi e dei flussi di trattamento dei dati e, di conseguenza, di individuare le linee per una corretta ed aggiornata adozione

delle misure di sicurezza fisiche, organizzative e tecniche necessarie ed idonee a tutelare i dati personali dai rischi di trattamento, nonché gli ulteriori adempimenti necessari, predisponendo un elenco delle misure di sicurezza fisiche, organizzative e tecniche che applica alla propria struttura, come tali:

- misure di sicurezza fisiche: misure di sicurezza di carattere fisico finalizzate alla protezione reale di persone, cose e ambienti, a garanzia della sicurezza d'aria (al fine di evitare danni o accessi non autorizzati al perimetro fisico dell'Unità dell'Azienda ULSS 7 Pedemontana) e della protezione reale delle apparecchiature ove i dati sono custoditi (al fine di evitare che le stesse siano oggetto di danni ad esempio da incendio o allagamento, manomissioni o furti, nonché di assicurare una loro corretta e continua manutenzione);

- misure di sicurezza tecniche: misure di sicurezza di carattere tecnologico finalizzate alla protezione dei dati, tra cui meccanismi di sicurezza preordinati alla protezione di tutte le banche dati posseduti dall'Azienda ULSS 7 Pedemontana (come, ad esempio, quelli relativi all'autenticazione e al controllo degli accessi) e meccanismi di sicurezza preordinati alla creazione di una corretta pratica nella gestione della strumentazione informatica (cifratura, criptazione etc.);

- misure di sicurezza organizzative: misure di sicurezza di carattere procedurale e/o comportamentale finalizzate a disciplinare gli aspetti organizzativi e di condotta (come, ad esempio, procedure di comportamento riguardanti il personale, procedure di sensibilizzazione e formazione e simili).

Per tutte tali misure, l'Azienda ULSS 7 Pedemontana rinvia anche al contenuto specifico di separati disciplinari, regolamenti, procedure ed analoghi (tra cui regolamenti informatici, politiche di sicurezza, linee guida per la gestione delle operazioni di *disaster recovery e business continuity*) ed in genere al Sistema Privacy come meglio definito.

L'adozione delle Misure di Sicurezza è organizzata, sotto il coordinamento dell'Ufficio Privacy, nonché dall'UOC Sistemi Informativi per gli aspetti connessi al sistema informativo, nonché primariamente dei rispettivi Punti di Contatto se previsti per l'Unità di competenza, a cura del Delegato, ovvero dei Sub-Delegati se designati, di competenza dell'Unità cui la Misura di Sicurezza si applica.

Nel caso di Misure di Sicurezza strutturali o trasversali a più Aree, i singoli Delegati competenti si coordinano tra di loro e chiedono, se del caso, linee di indirizzo al Vertice Gerarchico, anche attraverso i rispettivi Punti di Contatto.

Gli Autorizzati di competenza dell'Unità prestano il loro ausilio nell'ambito e nei limiti dei compiti loro assegnati; parimenti operano, con funzioni di coordinamento, i Punti di Contatto

Resta sempre salva la possibilità di avvalersi di Responsabili del trattamento a supporto di tale adozione.

15. Gestione delle violazioni dei dati personali

In caso di violazione dei dati personali per cui possano risultare compromesse la Riservatezza e/o l'Integrità e/o la Disponibilità (criterio "RID") dei dati personali oggetto di trattamento ("*data breach*"), l'Azienda ULSS 7 Pedemontana reagisce prontamente all'evento e si riserva di valutare la notifica della violazione al Garante senza ritardo e comunque entro 72 ore dalla conoscenza dell'evento (motivando, nel caso, il ritardo), a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 33 GDPR.

Nel caso di notifica, l'Azienda ULSS 7 Pedemontana adotta la procedura di comunicazione elettronica prevista dal Garante.

Laddove la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, l'Azienda ULSS 7 Pedemontana si riserva di valutare anche la comunicazione agli Interessati coinvolti, sempre senza ingiustificato ritardo, ai sensi dell'art. 34 GDPR.

In ogni caso l'Azienda ULSS 7 Pedemontana documenta qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze ed i provvedimenti adottati per porvi rimedio e ciò anche nel caso dei c.d. "*near miss*", ossia delle "quasi-violazioni", ovvero degli incidenti di sicurezza che non costituiscono *data breach*. A tale fine utilizza un apposito registro ai sensi dell'art. 33 par. 5 GDPR.

Nel caso in cui l'Azienda ULSS 7 Pedemontana operi come Contitolare del trattamento, rimette le proprie valutazioni in tema di *data breach* a quanto convenuto in sede di accordo ai sensi dell'art. 26 GDPR.

Nel caso in cui l'Azienda ULSS 7 Pedemontana operi come Responsabile del trattamento, informa il Titolare non appena sia a conoscenza di una possibile violazione di dati.

Nel caso in cui l'evento coinvolga Responsabili del trattamento nominati dall'Azienda ULSS 7 Pedemontana, costoro sono debitamente coinvolti nel processo di istruzione e valutazione del caso.

L'Azienda ULSS 7 Pedemontana riserva ad apposita separata procedura la gestione di tutte le ipotesi di cui sopra a cui si rimanda interamente.

Salvo che sia diversamente disposto da tale procedura, la gestione del *data breach* è svolta, sotto il coordinamento dell'Ufficio Privacy, nonché dell'UOC Sistemi Informativi per gli aspetti connessi al sistema informativo, nonché primariamente dei rispettivi Punti di Contatto se previsti per l'Unità di competenza, a cura del Delegato, ovvero dei Sub-Delegati se designati, di competenza dell'Unità coinvolto dal *data breach*. Nel caso di *data breach* strutturali o trasversali a più aree, i singoli Delegati competenti si coordinano tra di loro.

Resta sempre salva la possibilità di avvalersi dei Responsabili del trattamento coinvolti dal *data breach* a supporto della sua gestione.

Gli Autorizzati di competenza dell'Unità prestano il loro ausilio nell'ambito e nei limiti dei compiti loro assegnati; parimenti operano, con funzioni di coordinamento, i Punti di Contatto.

L'Azienda ULSS 7 Pedemontana deve tenere costantemente aggiornato e relazionarsi con il RPD/DPO.

16. Formazione

L'Azienda ULSS 7 Pedemontana si riserva un piano periodico di formazione del personale specificamente dedicato alla protezione dei dati personali, nell'ambito delle funzioni previste dall'Organigramma Privacy.

17. Ordine gerarchico delle fonti e rinvio

Il presente Regolamento si conforma alla Disciplina Privacy, la quale in ogni caso si applica con prevalenza e con disapplicazione delle eventuali disposizioni del presente Regolamento che fossero, in ipotesi, in contrasto.

Il presente Regolamento si intende sovraordinato rispetto ad altri regolamenti aziendali o nomine o designazioni e simili, costituendo detti ulteriori regolamenti o nomine o designazioni un'appendice operativa del presente Regolamento, per cui in caso di eventuale contrasto di disposizioni, prevalgono le disposizioni del presente Regolamento con disapplicazione di quelle dei secondi per le parti interessate dall'eventuale contrasto.

Il presente Regolamento si applica in coordinamento con ogni altra regolamentazione predisposta dal Sistema Privacy dell'Azienda ULSS 7 Pedemontana in materia.

Resta salva la facoltà di prevedere disposizioni integrative del presente Regolamento, a condizioni che esse siano compatibili con i principi dettati dal presente Regolamento e siano comunque in conformità alla Disciplina Privacy.

Nel caso di eventuale contrasto, si dovranno dunque considerare vincolanti nell'ordine, con preferenza:

1) la Disciplina Privacy
2) il Regolamento "Sistema Privacy"
3) la nomina o designazione specifica prevista dal Sistema Privacy
4) il Regolamento di accesso alle funzioni
5) ogni altro regolamento o simile.

18. Revisioni

L'Azienda ULSS 7 Pedemontana si riserva di modificare, integrare, aggiornare, dettagliare o altrimenti revisionare il presente Regolamento ed ogni altro elemento del Sistema Privacy su base periodica, anche mediante ulteriori documenti di indirizzo, disciplinari, ulteriori regolamenti, istruzioni e simili, pubblicando tali modifiche, integrazioni, aggiornamenti, dettagli ed in genere revisioni con le stesse forme di pubblicità della originaria adozione o con forme analoghe.

19. Adozione, efficacia e pubblicità

Il presente Regolamento viene adottato l'Azienda ULSS 7 Pedemontana in persona del Direttore Generale ed è efficace e vincolante per tutto il proprio Organigramma Privacy.

Anche a tale fine, il Regolamento è debitamente reso noto a tutti i soggetti coinvolti secondo le migliori forme di pubblicità e circolarizzazione.

All. 2

REGIONE DEL VENETO

ULSS7 PEDEMONTANA

REGOLAMENTO DI COORDINAMENTO

E DI ACCESSO ALLE FUNZIONI

DELL'UFFICIO PRIVACY AZIENDALE

E DEL RESPONSABILE DELLA PROTEZIONE DEI DATI

ENTE:

Azienda ULSS n. 7 Pedemontana

Via dei Lotti, 40

36061 Bassano del Grappa (VI)

Tel. 0424 888111

CF e P. I.V.A. n. 00913430245

PEC protocollo.aulss7@pecveneto.it

in persona del Direttore Generale pro tempore

REGIONE DEL VENETO
ULSS7 PEDEMONTANA

INDICE DEL DOCUMENTO

0. **Definizioni**

Ai fini del presente Regolamento valgono le seguenti Definizioni, nonché ogni altra prevista dalla disciplina applicabile alla materia della protezione dei dati personali:

"GDPR": il Regolamento (UE) 2016/679 del Parlamento 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 (RGPD) o meglio conosciuto come *General Data Protection Regulation* (GDPR);

"Codice Privacy": il decreto legislativo 30 giugno 2003 n. 196, Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679, come riformato dal decreto legislativo 10 agosto 2018 n. 101 e ss.mm.ii;

"Garante": Autorità Garante per la Protezione dei Dati Personali, con sede in Roma, che rappresenta l'Autorità di controllo prevista dal GDPR per l'Italia;

"EDPB": *European Data Protection Board*, ossia il Comitato Europeo per la Protezione dei Dati, che svolge le funzioni già assegnate al Gruppo Art. 29 (Working Party 29);

"Disciplina Privacy": l'intero quadro che disciplina la materia della protezione dei dati personali ("privacy") come composto dal GDPR, dal Codice Privacy, dai provvedimenti del Garante, dalle linee guida dell'EDPB, nonché da ogni altro atto normativo, di indirizzo, giurisprudenziale o simile in materia;

"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 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;

"Categorie particolari di dati personali": i particolari dati personali, già definiti come "dati sensibili", che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, disciplinati all'art. 9 GDPR;

"Dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

"Dati biometrici": i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

"Dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

“Dati penali”: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, disciplinati all’art. 10 GDPR;

"Trattamento di dati personali": 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;

“Interessato”: la persona fisica, identificata o identificabile, cui si riferiscono i dati personali trattati;

"Titolare del trattamento" o “Titolare”: 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;

"Responsabile del trattamento" o “Responsabile”: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

"Autorizzato al trattamento" o “Incaricato”: la persona fisica autorizzata ed incaricata a compiere operazioni di trattamento sotto l’autorità del Titolare o del Responsabile e che a tale fine riceve da loro istruzioni;

“Delegato del trattamento”: particolare Autorizzato al trattamento con funzioni specifiche di coordinamento, sub-designazione ed altre disciplinate con la designazione;

“Sub-Delegato del trattamento”: particolare Autorizzato al trattamento con funzioni specifiche di coordinamento, sub-designazione ed altre disciplinate con la sub-designazione da parte del Delegato del trattamento;

“Punto di Contatto”: il soggetto autorizzato, nominato presso ciascuna Unità Operativa dell’AULSS 7 Pedemontana, che funge, in collaborazione con l’Ufficio Privacy, da punto di coordinamento privacy specifico per una o più Unità Operativa;

“Unità”: ciascuna area organizzativa dell’Ente, quale un settore, un’unità, un dipartimento o simile che abbia una propria struttura organizzativa;

“Ufficio Privacy”: l’ufficio denominato Unità Supporto Privacy, Ufficio Privacy o in altro analogo modo, sia personale che collegiale, che è stato predisposto dall’Ente con funzioni di coordinamento degli incombenti privacy di pertinenza dell’Ente;

“Responsabile della protezione dei dati” o “RPD” o “DPO”: il soggetto dotato di competenze specialistiche in materia, che svolge funzioni consultive e formative, di sorveglianza, di parere sulle valutazioni di impatto, di punto di contatto con il Garante e le altre funzioni ivi previste, ai sensi degli artt. da 37 a 39 GDPR;

“Destinatario”: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che

riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

"Terzo": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'Interessato, il Titolare del trattamento, il Responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del Titolare o del Responsabile;

"Informativa": l'insieme delle informazioni che il Titolare rende all'Interessato ai sensi degli articoli 13 e/o 14 GDPR;

"Basi giuridiche": le condizioni di liceità del trattamento ai sensi dell'art. 6 GDPR;

"Consenso": la prima delle basi giuridiche di cui all'art. 6 GDPR, consistente in qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

"Altre Condizioni di Liceità": le ulteriori condizioni di liceità del trattamento, quali ad esempio quelle stabilite dall'art. 9 GDPR per il trattamento delle categorie particolari di dati personali; altre condizioni sono dettate dal Codice Privacy, ad esempio attraverso il rinvio a regole deontologiche o misure di garanzia, o direttamente dal Garante, ad esempio attraverso prescrizioni;

"Diritti dell'Interessato": i diritti dell'Interessato ai sensi degli articoli da 15 a 22 del GDPR;

"Sistema Privacy": la concreta adozione ed attuazione della disciplina presso l'Ente, costituita da un insieme di misure tecniche ed organizzative conformi alla Disciplina Privacy, tra cui il Regolamento Privacy Aziendale e tutte le altre policy, procedure, protocolli, misure ed ogni altro incombente adottato dall'Ente per il rispetto della propria accountability;

"Regolamento": il presente documento comprensivo degli allegati;

"Ente": il soggetto che adotta ed attua il Sistema Privacy presso la propria organizzazione, individuato come da intestazione, come tale **Azienda ULSS n. 7 Pedemontana**, Via dei Lotti, 40 - 36061 Bassano del Grappa (VI), Tel. 0424 888111, CF e P. I.V.A. n. 00913430245, PEC protocollo.aulss7@pecveneto.it, in persona del Direttore Generale pro tempore.

Per ogni ulteriore definizione si fa riferimento al GDPR, al Codice Privacy ed alla residua legislazione e relativi provvedimenti dell'Autorità (la **"Disciplina Privacy"**).

1. Introduzione

In ossequio al principio di responsabilizzazione (*accountability*), tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, includendovi anche l'attuazione di politiche adeguate in materia di protezione dei dati.

A tale proposito l'Azienda ULSS 7 Pedemontana ha organizzato un proprio Ufficio Privacy, assegnandovi correlati compiti e funzioni.

Il GDPR ha inoltre introdotto, tra le varie, la figura del Responsabile della Protezione dei Dati (RPD).

Il RPD è il soggetto che deve essere designato nei casi previsti dall'art. 37 GDPR, deve possedere i requisiti previsti dal medesimo art. 37 GDPR, ricoprire la posizione descritta dall'art. 38 GDPR e assolvere alle funzioni e ai compiti individuati dall'art. 39 GDPR.

A supporto e migliore definizione del ruolo, dei requisiti, delle competenze e delle funzioni del RPD, il già Gruppo Art. 29, ora sostituito dall'EDPB, ha emesso le Linee-guida sui Responsabili della Protezione dei Dati (RPD) "WP243" del 13 dicembre 2016 e successivi aggiornamenti, a cui il presente Regolamento si ispira e che si intendono qui allegate, formandone parte integrante.

Ufficio Privacy e RPD collaborano tra di loro e con l'intera organizzazione dell'Azienda ULSS 7 Pedemontana, ciascuno secondo le proprie rispettive competenze e funzioni.

2. Fonti

La materia oggetto del presente Regolamento è regolata dalla Disciplina Privacy, costituita da un complesso di fonti normative, giurisprudenza e provvedimenti di indirizzo che man mano orientano l'interpretazione e l'adeguamento del quadro normativo rispetto al mutevole contesto economico, sociale e tecnologico. Di seguito si elencano le principali fonti cui questo Regolamento si ispira e si adegua, salva ogni altra che dovesse intervenire in deroga, integrazione o modifica:

- GDPR, come sopra definito;
- Codice Privacy, come sopra definito;
- provvedimenti del Garante;
- provvedimenti dell'EDPB;
- standard internazionali e *best practices* di settore applicabili;
- ogni altro atto normativo che dispone sulla protezione dei dati personali, anche di livello regionale.

Per quanto riguarda specificamente l'Azienda ULSS 7 Pedemontana, la Disciplina Privacy è integrata dal Sistema Privacy adottato dall'Azienda ULSS 7 Pedemontana, come sopra definito, il quale costituisce l'autoregolamentazione adottata dall'Ente per rispettare ulteriormente il principio di *accountability*.

3. Designazione e compiti dell'Ufficio Privacy e del RPD

L'Azienda ULSS 7 Pedemontana designa un proprio RPD con Deliberazione del Direttore Generale.

L'Ufficio Privacy afferisce alla U.O.C. Affari Generali, svolge i compiti precisati al paragrafo 8 del "Regolamento per la protezione dei dati personali -Sistema Privacy-" e risponde al Direttore Generale.

I riferimenti dell'Ufficio Privacy sono resi noti dall'Azienda ULSS 7 Pedemontana.

I riferimenti del RPD sono resi noti dall'Azienda ULSS 7 Pedemontana mediante pubblicazione dei dati di contatto sul sito web aziendale ed in ogni Informativa.

I riferimenti e i dati di contatto del RPD sono comunicati al Garante mediante apposita notifica.

Salvo quanto precede, in sintesi il RPD provvede a:

a) informare e fornire consulenza all'Azienda ULSS 7 Pedemontana nonché ai relativi dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR;

d) cooperare con l'autorità di controllo; e

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Resta salvo ogni altro compito assegnato al RPD con la Deliberazione del Direttore Generale suddetta.

L'Azienda ULSS 7 Pedemontana permette al RPD di svolgere il proprio ruolo in forma indipendente nel pieno rispetto delle prerogative, dei compiti e delle funzioni che il GDPR assegna a tale figura, adottando ogni comportamento idoneo.

A tale proposito, il RPD è tempestivamente e adeguatamente avvisato dall'Azienda ULSS 7 Pedemontana con riferimento a tutte le questioni riguardanti la protezione dei dati personali ed è sostenuto nell'assolvimento delle proprie funzioni, mediante assicurazione delle risorse necessarie, anche di collaborazione da parte del personale interno.

Il RPD ha diritto di accedere ai dati personali e ai trattamenti eseguiti dall'Azienda ULSS 7 Pedemontana per approfondire la propria conoscenza specialistica della sua struttura e, in particolare, del flusso dei dati ivi svolto.

Il RPD agisce in autonomia decisionale nell'assolvimento dei propri compiti funzionali e non riceve istruzioni per la loro esecuzione.

Il RPD tiene un rapporto diretto con il Vertice Gerarchico dell'Azienda ULSS 7 Pedemontana, anche grazie all'Ufficio Privacy, con cui mantiene un rapporto di collaborazione fiduciaria e diretta.

Il RPD, in ogni caso, mantiene il massimo segreto e la massima riservatezza in merito all'adempimento dei propri compiti e, in genere, alle informazioni assunte nello svolgimento del ruolo. Ciò detto, l'assunzione del ruolo di RPD (se esterno all'Azienda ULSS 7 Pedemontana) non implica peraltro alcun vincolo di esclusiva né orizzontale, né verticale, per cui il RPD (laddove esterno) rimane assolutamente libero di svolgere la propria professione ed anche il ruolo di RPD per altri enti pubblici e privati, salvo solo il limite del conflitto di interessi.

Fermo restando quanto precede, nell'ambito delle proprie funzioni, il RPD non è in ogni caso responsabile per gli adempimenti imposti dal GDPR e/o dalla legislazione nazionale, che sono e restano a cura e carico esclusivi dell'Azienda ULSS 7 Pedemontana, anche ai sensi delle linee guida "WP-243" del 13 dicembre 2016 del Gruppo di Lavoro art. 29 ("WP29").

L'assolvimento delle funzioni di RPD non prevede compiti/funzioni/responsabilità in merito all'attuazione della normativa presso l'Azienda ULSS 7 Pedemontana ed in particolare non prevedono lo svolgimento di compiti/funzioni/responsabilità di tipo operativo, che restano invece a diretto carico delle strutture aziendali.

Il RPD può operare anche grazie al team di lavoro di riferimento, cui il "Regolamento per la protezione dei dati personali -Sistema Privacy parimenti si riferisce".

4. Scopo del Regolamento

Anche alla luce delle dimensioni e della complessità organizzativa dell'Azienda ULSS 7 Pedemontana ed al fine di agevolare l'efficacia dello svolgimento dei rispettivi compiti e funzioni, il presente Regolamento intende disciplinare le **regole di coordinamento e di accesso alle funzioni dell'Ufficio Privacy e del RPD** da parte dell'organizzazione dell'AULSS 7 Pedemontana e di chiunque altro soggetto vi si intenda rivolgere, con conseguente modello organizzativo per gli adempimenti privacy cui l'Azienda ULSS 7 Pedemontana è soggetta.

5. Assegnazione dei compiti e delle funzioni nell'organizzazione dell'Azienda ULSS 7 Pedemontana

L'Azienda ULSS 7 Pedemontana ha assegnato specifici compiti e funzioni al proprio personale apicale ("Delegati", con eventuali "Sub-Delegati") e subordinato ("Autorizzati") di ciascuna Unità operativa di riferimento, in forza del rispettivo rapporto di lavoro o del diverso rapporto organico, nell'ambito del Sistema Privacy adottato dall'Ente stesso e del Modello Organizzativo aziendale.

Sono altresì previsti uno o più Punti di Contatto presso l'organizzazione, quali persone o uffici di ulteriore coordinamento delle esigenze privacy dell'Ente.

L'Unità Operativa di riferimento è individuata in base al principio di prossimità con il trattamento o i trattamenti di dati personali in considerazione.

La designazione dell'Ufficio Privacy e del RPD lasciano fermi ed inalterati tali compiti e funzioni in capo alle Unità di riferimento e si intende preordinata al loro migliore supporto.

Per ogni attività per cui sia richiesta un'istruttoria o altra misura operativa in relazione a questioni che coinvolgono la protezione dei dati personali, la relativa competenza è assegnata all'Unità di riferimento individuata in base al suddetto principio di prossimità.

L'Unità Operativa di riferimento vi provvede per il tramite dei propri rispettivi Autorizzati e comunque secondo la propria struttura organizzativa, sotto la supervisione del Delegato di riferimento.

In base al suddetto principio di prossimità, restano in ogni caso a carico delle Unità di riferimento, sotto la supervisione dei rispettivi Delegati, tra le altre:

1) le competenze relative agli aggiornamenti del Registro dei trattamenti;
2) le competenze relative alle informazioni agli Interessati ai sensi degli artt. 13 e 14 GDPR ("Informative");
3) le competenze relative alle istanze di esercizio dei diritti inviate dagli Interessati ai sensi degli artt. da 12 a 15 GDPR ed alle segnalazioni inviate da Interessati ed altri soggetti;
4) le competenze relative alle Valutazioni di Impatto (*Data Protection Impact Assessmen*t - DPIA) per i trattamenti che le richiedono;
5) le competenze relative alla designazione dei Responsabili ai sensi dell'art. 28 GDPR;
6) le competenze relative alla designazione dei soggetti Autorizzati ai sensi dell'art. 29 GDPR e 2-quaterdecies Codice Privacy, nonché di eventuali Sub-Delegati o Punti di Contatto;
7) le competenze relative a situazioni di violazione di dati personali (*data breach*) ai sensi degli artt. 33 e 34 GDPR;
8) le competenze relative alle eventuali consultazioni preventive o richieste di autorizzazione da inoltrare al Garante, nonché alle richieste di informazioni pervenute dal Garante o da altre Autorità, nonché relative ad ogni altro procedimento amministrativo, civile o penale da avviare o in corso;
9) le competenze relative alle Misure di Sicurezza di cui all'art. 32 GDPR di pertinenza di ciascuna Unità;
10) le competenze relative ad ogni altra questione che attenga alla protezione dei dati personali;

salve in ogni caso le attività di coordinamento proprie dell'Ufficio Privacy ed ogni altra misura organizzativa per cui valga quanto segue.

6. Registro dei trattamenti

Il Registro dei trattamenti costituisce l'adempimento di individuazione e catalogazione dei trattamenti previsto dall'art. 30 GDPR.

Considerata la necessità di omogeneizzare l'organizzazione delle informazioni anche a fronte della complessità organizzativa dell'Azienda ULSS 7 Pedemontana e delle categorie di trattamento interessate dalle attività aziendali, la tenuta del Registro è coordinata dall'Ufficio Privacy.

Spetta peraltro a ciascuna singola Unità di riferimento in base al principio di prossimità, sotto la supervisione del rispettivo Delegato, istruire le eventuali nuove categorie di trattamento in relazione all'implementazione del Registro. Spetta in particolare a ciascuna singola Unità:

- l'individuazione delle finalità di ciascun nuovo trattamento;
- la descrizione delle categorie di interessati e delle categorie di dati personali coinvolti;
- l'individuazione delle categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- l'istruttoria circa l'eventuale trasferimento di dati verso Paesi terzi o organizzazioni internazionali;
- l'individuazione dei termini ultimi previsti per la cancellazione delle diverse categorie di dati (*data retention*);
- la descrizione generale delle specifiche misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 GDPR adottate per il trattamento in questione, salve quelle generali già adottate dall'Ente.

L'Unità Operativa di riferimento, svolte le attività che precedono, apporta gli opportuni aggiornamenti al Registro, coordinandosi, per gli aspetti operativi di inserimento, con l'Ufficio Privacy.

Parimenti, l'Unità di riferimento verifica e si coordina a tale proposito con l'Ufficio Privacy, per ogni successivo aggiornamento.

7. Informazioni agli interessati ("Informative Privacy")

L'Interessato ha il diritto di essere informato sui trattamenti che lo riguardano attraverso le Informazioni previste dagli articoli 13 GDPR, per i dati raccolti presso di lui, e 14 GDPR per i dati non raccolti presso di lui ("Informative").

Considerata la necessità di omogeneizzare l'organizzazione delle Informative anche a fronte della complessità organizzativa dell'Ente e delle categorie di trattamento interessate dalle attività aziendali, in ogni caso sotto il coordinamento dell'Ufficio Privacy la resa dell'informativa all'Interessato e la relativa documentabilità sono di competenza:

- della Direzione Generale, per l'informativa generale relativa al trattamento dei dati personali degli Utenti aziendali nel loro complesso;
- delle singole Direzioni, per informative generali relative al trattamento dei dati personali di particolari categorie di Interessati che usufruiscono di servizi propri delle rispettive UOC;
- del UOC Provveditorato Economato e Gestione della Logistica, in persona del rispettivo Delegato, per l'allegazione tra gli atti delle procedure affidate a tale Unità, in relazione ai dati degli Interessati che partecipano a tali procedure in proprio o quali legali rappresentanti dei partecipanti o ad altro titolo;
- del Responsabile dell'Unità dell'UOC Gestione delle Risorse Umane, in qualità di Delegato di tale Servizio, in relazione ai dati del personale;
- di ciascun Delegato di competenza del trattamento, per i dati degli Assistiti, degli Utenti e di ogni altra persona usufruisca dei servizi aziendali di tale area;
- resta salva la competenza del Direttore dell'UOC Sistemi Informativi, in qualità di Delegato in relazione ai dati degli utenti online.

Nel caso di accordi, convenzioni o contratti di responsabilità diretta di una o più Direzioni, ciascuna di esse è responsabile della resa dell'informativa anche mediante delega di tale incombente a specifici Delegati.

Le Direzioni, l'UOC Provveditorato Economato e gestione della Logistica ed i Delegati, nell'assolvimento delle proprie rispettive funzioni di cui sopra, possono chiedere il coordinamento dell'Ufficio Privacy o rivolgersi al Responsabile della Protezione dei Dati, nei casi di oggettiva novità, oggettiva urgenza o particolare complessità.

Dal punto di vista operativo, la pubblicazione delle Informative in loco (presso i reparti, presso le aree comuni di accesso o transito da parte del pubblico e simili) è coordinata dall'Unità Operativa di riferimento sotto la supervisione del rispettivo Delegato, mentre la pubblicazione delle Informative online (sul sito web aziendale ed in altri contesti online) è coordinata dall'Ufficio Privacy unitamente all'Ufficio comunicazione e stampa.

Spetta peraltro a ciascuna singola Direzione o Unità Operativa di riferimento, in base al principio di prossimità, sotto la supervisione del rispettivo Delegato, istruire i casi in cui sia richiesta un'Informativa ed i relativi contenuti, anche in base agli aggiornamenti derivanti dal Registro dei trattamenti. Spetta in particolare a ciascuna singola Direzione o Unità Operativa:

- l'individuazione del Titolare o dei titolari del trattamento, dei relativi dati di contatto e dei relativi responsabili della protezione dei dati;
- l'individuazione delle finalità e delle basi giuridiche di ciascun trattamento;
- l'individuazione degli eventuali destinatari o delle eventuali categorie di destinatari dei dati personali;
- l'eventuale intenzione di trasferire dati personali verso paesi terzi od organizzazioni internazionali;
- l'individuazione del periodo di conservazione dei dati personali oppure, se non è possibile, dei criteri utilizzati per determinare tale periodo (*data retention*);
- l'individuazione dei diritti degli interessati in relazione al trattamento in questione, ivi comprese eventuali limitazioni;
- valutare se la comunicazione di dati personali sia un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- l'individuazione dell'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato;
- per i dati raccolti non presso l'Interessato, le categorie di dati personali in questione;
- per i dati raccolti non presso l'Interessato, la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

A tali fini, considerati anche gli aspetti giuridici relativi, ad esempio, all'individuazione delle basi giuridiche, del periodo di conservazione, dei diritti dell'Interessato e delle eventuali limitazioni e di eventuali altre porzioni di informazione che sottendono questioni giuridiche, la Direzione o l'Unità Operativa di riferimento può coordinarsi con l'Ufficio Privacy anche per l'istruttoria di tali informazioni o porzioni di informazione.

La Direzione o l'Unità Operativa di riferimento, svolte le attività che precedono, propone all'Ufficio Privacy un testo di Informativa, coordinandosi, per gli aspetti operativi di pubblicazione, con l'Ufficio Privacy stesso.

8. Istanze e segnalazioni da parte degli Interessati

Gli Interessati possono esercitare i diritti di cui agli articoli da 15 a 22 GDPR ("istanze"), quali quelli di accesso, rettifica, cancellazione, limitazione del trattamento, portabilità dei dati, opposizione, non sottoposizione a processi decisionali automatizzati ivi compresa la profilazione.

Gli Interessati ed ogni altro soggetto possono pure presentare segnalazioni per tutte le altre questioni relative al trattamento dei dati personali e all'esercizio dei diritti derivanti dalla Disciplina Privacy, nonché in generale in merito all'applicazione della Disciplina Privacy da parte dell'AULSS 7 Pedemontana ("segnalazioni").

L'invio della risposta alle istanze ed alle segnalazioni è di diretta ed esclusiva competenza dell'Ufficio Privacy, che vi provvede in base all'istruttoria svolta dall'Unità Operativa di riferimento.

Poiché la risposta alle istanze da parte dell'Azienda ULSS 7 Pedemontana deve pervenire all'Interessato senza ingiustificato ritardo e comunque, al più tardi, entro un mese dal loro ricevimento, salva proroga di due mesi nei casi di richieste complesse o numerose, salvo il caso di diniego motivato con apposita comunicazione da inviare all'Interessato con le modalità ed i termini disposti dall'art. 12 del GDPR, qualunque soggetto riceva tale Istanza deve inoltrarla all'Ufficio Privacy senza indugio e comunque entro 72 ore affinché questi provveda a richiedere l'istruttoria all'Unità di riferimento.

Analogamente vi provvede il RPD, laddove sia egli a ricevere direttamente l'Istanza.

L'Ufficio Privacy, ricevuta l'Istanza, la inoltra all'Unità Operativa di riferimento affinché questa svolga l'opportuna istruttoria (se tale Unità non vi abbia già provveduto) e ne restituisca l'esito all'Ufficio Privacy, unitamente ad una proposta di testo per il riscontro, entro il termine di successivi 14 giorni.

Analoga modalità di comunicazione e di inoltro interno è adottata per le segnalazioni, ancorché per le stesse non ricorra un termine di legge per il riscontro.

Salvo quanto precede, qualora la questione oggetto dell'Istanza o dalla Segnalazione comporti la soluzione di criticità particolari o sia particolarmente nuova o urgente, essa può essere vagliata ed istruita direttamente dall'Ufficio Privacy o anche dal RPD medesimo, mettendone a conoscenza l'Unità Operativa di riferimento per opportunità di coordinamento, se del caso. In tale ipotesi il RPD e l'Ufficio Privacy si coordinano al fine di rendere la risposta all'Interessato o al diverso mittente e comunque al fine di osservare al meglio i termini e le condizioni di legge.

Laddove l'invio di una comunicazione da parte di un Interessato o di un terzo dia adito a possibili interpretazioni circa la sua natura di Istanza di esercizio dei diritti o di Segnalazione, ad esempio in relazione alla possibile diversa natura di istanza di accesso agli atti ai sensi della disciplina sull'accesso agli atti amministrativi (Legge 241/1990) o di istanza di accesso civico ai sensi della disciplina sulla trasparenza amministrativa (D.Lgs. 33/2013), la qualificazione di tale natura spetta primariamente all'Unità Operativa di riferimento in base al principio di prossimità e, solo in caso di particolare

complessità, tale Unità Operativa può contattare l'Ufficio Privacy per l'opportuno supporto giuridico. Laddove tale attività qualifichi la natura della comunicazione come diversa da un'Istanza di esercizio dei diritti o da una Segnalazione, il seguito di competenza viene regolato dal modello organizzativo dell'Azienda ULSS 7 Pedemontana applicabile alla diversa materia.

9. Valutazioni di Impatto (*Data Protection Impact Assessment* - DPIA)

La Valutazione di Impatto (*Data Protection Impact Assessment* - DPIA) costituisce l'adempimento di analisi di un trattamento che preveda rischi elevati per i diritti e le libertà delle persone fisiche, in particolare in relazione all'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento.

La DPIA è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari o di dati relativi a condanne penali e a reati;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Altri casi in cui la DPIA sia richiesta sono individuati dal Garante, in particolare con l'Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979], pubblicato in Gazzetta Ufficiale n. 269 del 19 novembre 2018, e successive modificazioni ed integrazioni, cui l'Azienda ULSS 7 Pedemontana rinvia a valere quale parte integrante del presente Regolamento. Tra detti casi, si annoverano (rinviando per l'elenco integrale a tale Allegato):

- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i *Big Data*);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, *device IoT*, ecc.);

- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Considerata la complessità delle categorie di trattamento interessate dalle attività aziendali, la valutazione della necessità di svolgere una DPIA è demandata a ciascuna singola Unità Operativa di riferimento in base al principio di prossimità del trattamento.

Spetta a tale Unità Operativa di riferimento, sotto la supervisione del rispettivo Delegato, istruire la DPIA ed in particolare provvedere a redigere:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal Titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli Interessati;

d) un elenco delle misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Considerata la necessità di coordinare le DPIA aziendali in un'ottica di omogeneizzazione degli strumenti utilizzati a tale fine, terminata l'attività istruttoria e predisposti i contenuti in bozza, l'Unità Operativa di riferimento si coordina con l'Ufficio Privacy al fine di formalizzare tale bozza in specifica DPIA da adottarsi secondo gli strumenti in uso presso l'AULSS 7 Pedemontana a tale fine.

10. Responsabili del trattamento

Il Responsabile del trattamento è il soggetto che tratta dati personali per conto del Titolare e che a tale fine deve sottoscrivere un contratto o altro atto equipollente vincolante secondo i contenuti minimi previsti dall'art. 28 GDPR.

Considerata la complessità delle categorie di trattamento interessate dalle attività aziendali, l'allegazione e verifica della relativa sottoscrizione sono di competenza:

- dell'UOC Provveditorato Economato e gestione della Logistica, in persona del rispettivo Delegato, per l'allegazione tra gli atti delle procedure affidate a tale Unità e del Direttore dell'Esecuzione del Contratto (DEC) per la sottoscrizione dell'atto;

- di ciascun Delegato di competenza del trattamento assegnato per conto al Responsabile, laddove la gestione del rapporto non sia affidata all'UOC Provveditorato Economato e gestione della Logistica, sia per l'allegazione che per la sottoscrizione.

Nel caso di accordi, convenzioni o contratti di responsabilità diretta di una o più Direzioni, ciascuna di esse è responsabile dell'allegazione e della relativa sottoscrizione, anche mediante delega di tale incombente a specifici Delegati.

L'UOC Provveditorato Economato e gestione della Logistica, i Delegati o le Direzioni, nell'assolvimento delle proprie rispettive funzioni inerenti la nomina del Responsabile del trattamento

di cui sopra, possono chiedere il coordinamento dell'Unità Supporto Privacy o rivolgersi al Responsabile della Protezione dei Dati, nei casi di oggettiva novità, oggettiva urgenza o particolare complessità.

La conservazione dei Contratti di Responsabile è curata dall'Unità Operativa che perfeziona il contratto, la convenzione o il rapporto con il soggetto esterno. Ogni Unità Operativa a tale fine si coordina con l'Ufficio Privacy per gli aspetti relativi alle nuove acquisizioni.

Spetta peraltro a ciascuna singola Direzione o Unità Operativa di riferimento in base al principio di prossimità, sotto la supervisione del rispettivo Delegato, tenere ed istruire i rapporti con i soggetti individuati o individuabili quali Responsabili del trattamento e sottoporre loro il modello di Contratto di Responsabile del trattamento secondo lo schema adottato dall'AULSS 7 Pedemontana, salve, anche in tale ipotesi, le competenze proprie dell'UOC Provveditorato Economato e gestione della Logistica.

Spetta in ogni caso all'Unità Operativa di riferimento istruire tutte le informazioni utili e necessarie affinché il modello di Contratto di Responsabile applicato sia conforme ai contenuti minimi di cui all'art. 28 GDPR.

L'Unità Operativa di riferimento, svolte le attività che precedono, propone il testo di Contratto all'Ufficio Privacy, coordinandovisi per gli aspetti operativi di sottoscrizione e conservazione.

Quanto sopra si applica, con le dovute analogie, anche al caso in cui il Titolare debba sottoscrivere un Accordo di Contitolarità con altri Titolari ai sensi dell'art. 26 GDPR.

11. Autorizzati del trattamento

L'Autorizzato al trattamento è il soggetto che agisce sotto l'autorità del Titolare o del Responsabile ed effettua operazioni di trattamento di dati personali.

Considerata la complessità delle categorie di trattamento interessate dalle attività aziendali, spetta a ciascuna singola Unità Operativa di riferimento in base al principio di prossimità, sotto la supervisione del rispettivo Delegato, individuare, designare ed istruire debitamente i propri rispettivi Autorizzati al trattamento, utilizzando l'apposito modello di designazione secondo lo schema adottato dall'Azienda ULSS 7 Pedemontana.

Spetta in ogni caso all'Unità Operativa di riferimento istruire tutte le informazioni utili e necessarie affinché il modello di lettera di designazione sia idonea a conferire all'Interessato tutte le informazioni di cui egli abbia bisogno per trattare i dati personali in modo conforme alla disciplina.

L'Unità Operativa di riferimento, svolte le attività che precedono, si coordina, per eventuali altri aspetti operativi, con l'Ufficio Privacy.

12. Violazioni di dati personali (*data breach*)

La violazione di dati personali ("*data breach*") costituisce un evento patologico del trattamento di dati personali che si verifica allorquando si realizzi una lesione della riservatezza, dell'integrità o della disponibilità dei dati personali, per fatto doloso o colposo.

La disciplina prevede l'obbligo di notificare l'evento al Garante, al più presto e comunque entro le 72 ore dal momento in cui il Titolare ne è venuto a conoscenza, a meno che non sia improbabile che la

violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

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 anche all'Interessato senza ingiustificato ritardo.

L'Ente ha adottato uno specifico Regolamento *Data Breach* vincolante per tutta la propria organizzazione, cui si fa rinvio.

In ogni caso, considerata la complessità delle categorie di trattamento interessate dalle attività aziendali, spetta a ciascuna singola Unità Operativa di riferimento in base al principio di prossimità, sotto la supervisione del rispettivo Delegato, individuare ed istruire debitamente le situazioni che potrebbero dare origine ad ipotesi di violazione di dati personali e comunicare l'eventuale ricorrenza di tali ipotesi, prontamente, all'Ufficio Privacy, anche al fine di agevolare l'attivazione della procedura prevista dal Regolamento *Data Breach*.

13. Procedimenti

Laddove l'Azienda ULSS 7 Pedemontana debba avviare procedimenti di Consultazione Preventiva al Garante nei casi di cui all'art. 36 GDPR o richieste di autorizzazione al Garante anche ai sensi dell'art. 110-bis Codice Privacy, considerata la complessità organizzativa dell'Azienda ULSS 7 Pedemontana, spetta a ciascuna singola Unità Operativa di riferimento in base al principio di prossimità, sotto la supervisione del rispettivo Delegato, individuare ed istruire debitamente il procedimento.

A tale fine, anche in considerazione degli aspetti giuridici sottesi, l'Unità Operativa di riferimento si coordina con l'Ufficio Privacy per i relativi contenuti ed aspetti procedurali.

In ogni caso, spetta esclusivamente all'Ufficio Privacy organizzare gli aspetti procedurali, ad esempio di invio della richiesta, coordinandosi per gli aspetti formali di sottoscrizione e protocollazione con gli uffici gerarchici dell'Ente.

Analogamente e per gli stessi motivi, nei casi di Richiesta di Informazioni o altre richieste o procedimenti pervenuti dal Garante, considerata la complessità organizzativa dell'Azienda ULSS 7 Pedemontana, spetta a ciascuna singola Unità Operativa di riferimento, in base al principio di prossimità, sotto la supervisione del rispettivo Delegato, individuare ed istruire debitamente la richiesta o il procedimento.

Anche a tale fine, in considerazione degli aspetti giuridici sottesi, l'Unità Operativa di riferimento si coordina in ogni caso con l'Ufficio Privacy per i relativi contenuti ed aspetti procedurali, ad esempio di invio e seguito. In ogni caso, l'invio delle risposte al Garante spetta esclusivamente all'Ufficio Privacy, il quale si coordina per gli aspetti formali di sottoscrizione e protocollazione con gli uffici gerarchici dell'Ente.

Analogamente valga con riferimento ad ogni altro procedimento amministrativo, civile o penale davanti ad ogni altra Autorità che inerisce la protezione dei dati personali.

14. Competenze concorrenti e strategiche o direzionali

Nel caso in cui uno o più degli adempimenti e misure di cui al presente Regolamento o la diversa

questione che sottende un tema di protezione dei dati personali sia di competenza concorrente tra più Unità di riferimento, queste si coordinano tra di loro e con l'Ufficio Privacy.

Nel caso in cui uno o più degli adempimenti e misure di cui al presente Regolamento o la diversa questione che sottende un tema di protezione dei dati personali sia di natura strategica o direzionale per l'Azienda ULSS 7 Pedemontana, interessando l'organizzazione nel suo complesso o un'area direzionale complessiva, la competenza spetta alla Direzione pertinente e l'Ufficio Privacy coordina direttamente le attività, contattando e coordinandosi con le Unità Operative di riferimento maggiormente interessate e coordinandosi in ogni caso con le Direzioni e/o con gli altri uffici gerarchici e direzionali dell'Ente pertinenti e con il Vertice Gerarchico dell'AULSS 7 Pedemontana.

Resta salvo che, in ogni caso, le Direzioni dettano le linee di indirizzo e di direzione per il trattamento dei dati personali in relazione agli archivi o banche dati di rispettiva afferenza.

15. Accesso alle funzioni dell'Ufficio Privacy

L'Ufficio Privacy svolge i compiti e le funzioni che gli sono attribuiti dalla rispettiva Delibera, dal Regolamento Privacy Aziendale ed in generale dal Sistema Privacy dell'Ente, in conformità al presente Regolamento.

Primariamente, ciascun Delegato o Sub-Delegato si riferisce alle competenze proprie del Punto di Contatto di competenza dell'Unità Operativa di afferenza, quale primo riferimento di coordinamento per tutti gli incombenti di natura privacy.

Salvo quanto precede, l'Ufficio Privacy può essere contattato dal personale delle Unità Operative di riferimento per fini di informazione e consulenza specifica nell'ambito della protezione dei dati personali, solo in regime di *second opinion* e solo in presenza di un'istruttoria già predisposta dall'Unità Operativa di riferimento medesima, anche attraverso il Punto di Contatto, per cui si rinvia ai paragrafi che precedono.

In particolare, l'accesso alle funzioni dell'Ufficio Privacy è giustificato, solo dopo aver documentato il previo coordinamento del Punto di Contatto:

1) nei casi in cui l'istruttoria necessiti di valutazioni di stretta natura giuridica;
2) nei casi in cui l'istruttoria coinvolga questioni caratterizzate da una complessità particolarmente elevata, da una novità particolare o da una particolare ed oggettiva urgenza determinata da fattori esterni all'organizzazione del lavoro;
3) nei casi in cui l'istruttoria coinvolga altri enti del Servizio Sanitario Regionale del Veneto o Nazionale o comunque sia di interesse per il modello organizzativo privacy sanitario regionale del Veneto o nazionale;
4) nel caso di richieste che pervengano direttamente dalle Direzioni dell'Azienda ULSS 7 Pedemontana

Laddove l'Ufficio Privacy riceva direttamente ai propri dati di contatto istanze di esercizio dei diritti degli Interessati, segnalazioni, richieste di informazione da parte del Garante, altre richieste da parte di altri enti e/o rispettivi RPD o da altre autorità, l'Ufficio stesso provvede, secondo le proprie funzioni, a coordinarsi con l'Unità Operativa di riferimento, anche attraverso il Punto di Contatto, ed in ogni caso valuta l'opportuno coordinamento con il RPD.

L'Ufficio Privacy è sempre informato nei casi in cui l'istruttoria coinvolga rapporti con altri enti istituzionali del Servizio Sanitario Regionale del Veneto o Nazionale o comunque sia di interesse strategico per il modello organizzativo regionale sanitario del Veneto o nazionale, anche per le correlate interazioni con i rispettivi Uffici Privacy degli altri enti.

16. Accesso alle funzioni del RPD

Il RPD svolge le funzioni minime che gli sono attribuite dall'art. 39 GPDR, come esposte in introduzione, e gli eventuali compiti e le funzioni ulteriori che sono predisposte dal modello organizzativo adottato dall'Ente.

In relazione alle funzioni attribuite dall'art. 39 GDPR, il RPD può essere contattato:

- dall'Ufficio Privacy in regime di ulteriore *second opinion*, a valle di un'istruttoria già avviata sia dall'Unità di riferimento che dall'Ufficio Privacy stesso;
- direttamente dal personale dell'Unità di riferimento in base al principio di prossimità del trattamento in questione, anche attraverso i Punti di Contatto, solamente nei casi di estrema complessità, di estrema novità o di estrema ed oggettiva urgenza determinata da fattori esterni all'organizzazione del lavoro, in ogni caso sempre in regime di *second opinion*, a valle di un'istruttoria già avviata da tale Unità. In tale caso il RPD coinvolge l'Ufficio Privacy per i necessari coordinamenti;
- direttamente dalle Direzioni dell'Azienda ULSS 7 Pedemontana.

Laddove il RPD riceva direttamente ai propri dati di contatto istanze di esercizio dei diritti degli Interessati, segnalazioni, richieste di informazione da parte del Garante, altre richieste da parte di altri enti e/o rispettivi RPD o da altre autorità, il RPD stesso provvede direttamente secondo le proprie funzioni nei casi in cui il compito coinvolga personalmente la sua funzione, oppure provvede a coordinarsi con l'Ufficio Privacy per il seguito di competenza.

Il RPD è sempre informato nei casi in cui l'istruttoria coinvolga rapporti con altri enti istituzionali del Servizio Sanitario Regionale del Veneto o Nazionale o sia comunque di interesse strategico per il modello organizzativo regionale sanitario del Veneto o nazionale, anche per le correlate interazioni con i rispettivi RPD degli altri enti.

Resta sempre salva la relazione diretta del RPD con il Vertice Gerarchico dell'Azienda ULSS 7 Pedemontana.

17. Modalità di accesso alle funzioni dell'Ufficio Privacy e del RPD

L'accesso alle funzioni dell'Ufficio Privacy e del RPD si svolge:

1) in via documentale ed epistolare, tramite l'organizzazione e lo svolgimento di un'istruttoria documentale e lo scambio di informazioni a mezzo posta elettronica o altro mezzo di comunicazione scritta;
2) laddove necessiti anche lo scambio di informazioni in riunione, vista anche la complessità della questione trattata o altri motivi di opportunità, a mezzo videoconferenza tramite gli appositi strumenti in uso presso l'Ente;
3) nei casi di particolare complessità o di stretta opportunità, anche a fronte di eventuali motivi

istituzionali, a mezzo riunioni in presenza presso la sede dell'Azienda ULSS 7 Pedemontana o presso altre sedi regionali.

In ogni caso, l'accesso alle funzioni di cui sopra si attiene a principi di sinteticità e razionalizzazione.

Di ciascun accesso viene tenuta traccia documentale, anche mediante verbalizzazione delle riunioni.

18. Accesso alle competenze delle Unità di riferimento

Nei casi in cui l'Ufficio Privacy o il RPD necessitino di accedere alle competenze proprie delle Unità di riferimento del trattamento, in base al principio di prossimità, si osservano regole di condotta analoghe e speculari a quelle sopra disciplinate, salvo in ogni caso il diritto sia dell'Ufficio Privacy, che del RPD, di accedere alle relative informazioni e richiedere le opportune istruttorie nell'ambito dei compiti e delle funzioni che sono loro attribuiti dal Sistema Privacy ed in genere dal modello organizzativo dell'Azienda ULSS 7 Pedemontana e, per quanto riguarda il RPD, direttamente anche dal GDPR ed in generale dalla Disciplina Privacy.

In particolare, le Unità Operative di riferimento devono agevolare lo svolgimento delle funzioni del RPD in relazione a:

1) attività informativa e consulenziale;
2) attività di sorveglianza;
3) attività pareristica in relazione a valutazioni di impatto;
4) attività correlata ad ipotesi di violazione di dati personali;
5) attività correlata a procedimenti da avviarsi o procedimenti in corso;
6) ogni altra attività contempli rapporti con il Garante o con altre autorità;
7) ogni altra attività contempli rapporti con altri enti del Servizio Sanitario Regionale o Nazionale.

19. Principio di competenza e responsabilizzazione

Le Unità Operative di riferimento restano, con riferimento al Sistema Privacy ed in genere al modello organizzativo predisposto dall'Azienda ULSS 7 Pedemontana, ciascuna per la quota di rispettiva competenza, gli unici soggetti a cura e carico dei quali incombe il diretto onere di corretta conformazione al GDPR, secondo il principio di competenza e di responsabilizzazione (c.d. *accountability*). Anche a tale fine si riferiscono primariamente e direttamente ai Punti di Contatto di competenza dell'Unità Operativa.

Le attività di coordinamento con l'Ufficio Privacy e con il RPD sono tese ad agevolare il rispetto di tali principi, ma non sostituiscono i compiti e le funzioni sopra attribuiti.

Ciò detto, l'Ufficio Privacy e il RPD rispondono nei limiti e secondo le proprie rispettive competenze ed i propri rispettivi ruoli istituzionali.

20. Principio di continua formazione

L'Azienda ULSS 7 Pedemontana impronta la propria politica di protezione dei dati personali ad un principio di continua formazione della propria organizzazione, che si realizza in primo luogo attraverso una predisposizione dell'intero personale alla migliore comprensione dei temi della protezione dei dati

personali ed alla correlata predisposizione ad avviare e preservare una propria autoformazione.

Salvo quanto precede, ciascuna Unità Operativa di riferimento espone all'Ufficio Privacy, anche attraverso i Punti di Contatto, affinché questo si coordini con l'Ufficio Formazione, il rispettivo fabbisogno formativo e si coordina per le conseguenti attività progettuali.

21. Rapporti esterni all'organizzazione

Il Regolamento è applicabile, in quanto compatibile, anche a chiunque, esterno all'organizzazione dell'Ente, debba accedere alle funzioni dell'Ufficio Privacy e del RPD.

A tale proposito, le disposizioni del presente Regolamento si applicano in modo analogico, sostituendo alle competenze dell'Unità Operativa di riferimento quelle del diverso soggetto debba accedere alle funzioni in oggetto.

22. Ordine gerarchico delle fonti e rinvio

Il presente Regolamento si conforma alla Disciplina Privacy, la quale in ogni caso si applica con prevalenza e con disapplicazione delle eventuali disposizioni del presente Regolamento che fossero, in ipotesi, in contrasto.

Il presente Regolamento si applica in coordinamento con ogni altra regolamentazione predisposta dal Sistema Privacy dall'Azienda ULSS 7 Pedemontana e comunque se ed in quanto non contrasti con il contenuto di nomine o designazioni specifiche assegnate a ciascuna persona nell'ambito delle competenze assegnate con il Sistema Privacy.

Nel caso di eventuale contrasto, si dovranno dunque considerare vincolanti nell'ordine, con preferenza rispetto al presente Regolamento di accesso:

1) la Disciplina Privacy;
2) la nomina o designazione specifica prevista dal Sistema Privacy.

Il presente Regolamento si intende subordinato rispetto al Regolamento Privacy aziendale, di cui costituisce appendice operativa, per cui in caso di eventuale contrasto di disposizioni, prevalgono le disposizioni del secondo con disapplicazione di quelle del primo per le parti interessate dall'eventuale contrasto.

Nel caso di eventuale contrasto tra il Regolamento Privacy generale dell'Ente ed il presente Regolamento di accesso, il primo avrà applicazione con preferenza sul secondo, quindi in tal caso saranno vincolanti nell'ordine:

3) il Regolamento Privacy dell'Ente;
4) il presente Regolamento di accesso alle funzioni dell'Ufficio Privacy e del DPO.

In caso di previsioni integrative, ma compatibili con il Regolamento generale sul "Sistema Privacy", previste dal presente Regolamento di accesso, avranno viceversa applicazione dette disposizioni integrative di natura operativa.

Parimenti, avrà applicazione integrativa ogni altra previsione disposta da nomine o designazioni o

simili, a condizione che non contrasti con il contenuto del Regolamento generale sul "Sistema Privacy", nel qual caso prevarrà quest'ultimo.23. Revisione e modifica del Regolamento

Il presente Regolamento mira ad agevolare lo svolgimento delle attività tramite procedure a carattere prettamente operativo, riesaminabili in qualunque momento, al fine di garantire la costante efficacia di questo strumento, apportandovi, se del caso, eventuali miglioramenti.

Salvo quanto precede, il Regolamento è soggetto a revisione periodica su base almeno annuale.

24. Adozione, efficacia e pubblicità

Il presente Regolamento viene adottato dall'Ente in persona del proprio legale rappresentante pro tempore ed è efficace e vincolante per tutta la propria organizzazione e, in quanto compatibile, per chiunque debba accedere alle funzioni dell'Ufficio Privacy e del RPD.

Il Regolamento entra in vigore dal giorno successivo alla sua pubblicazione e resta in vigore fino a nuova disposizione.

Ferma la pubblicazione che precede, il Regolamento è debitamente reso noto a tutto il personale coinvolto in operazioni di trattamento dei dati personali di cui l'Ente è Titolare, Contitolare o Responsabile, secondo le migliori forme di pubblicità e circolarizzazione.

All. 3

REGIONE DEL VENETO

ULSS7 PEDEMONTANA

Azienda ULSS n. 7 Pedemontana

Via dei Lotti, 40 – 36061 Bassano del Grappa (VI)

PROCEDURA DATA BREACH

Titolo	Procedura Data Breach		
Emesso da	Azienda ULSS n. 7 Pedemontana		
Approvato da	Azienda ULSS n. 7 Pedemontana		
Revisione	2		
Data revisione	09	luglio	2025

Definizioni

"Autorità di Controllo"	indica il Garante per la protezione dei Dati Personali.
"Autorizzato"	le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile e che agiscono sotto l'autorità del Titolare o del Responsabile ai sensi dell'art. 29 del GDPR.
"Categorie Particolari di Dati"	indica ogni dato personale idoneo a rivelare l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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 della persona.
"Dato/i Personale/i"	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.
"Dati Giudiziari"	indica ogni dato personale relativo a condanne penali e ai reati o a connesse misure di sicurezza ovvero relativo a provvedimenti giudiziari, sanzioni penali, o carichi pendenti, o la qualità dell'imputato o indagato ai sensi degli articoli 60 e 61 del Codice di Procedura Penale.
"Delegato"	indica la persona fisica che, in virtù e nei limiti dei poteri di organizzazione, gestione e controllo conferiti dal Titolare, è preposta all'esercizio delle funzioni di direzione, coordinamento e controllo delle attività di trattamento dei dati personali e dei correlati adempimenti previsti dal GDPR
"Delegato di Riferimento"	indica il Delegato che ha individuato uno o più Autorizzati all'interno della struttura di propria responsabilità: ciascun Autorizzato ha un solo Delegato di riferimento

“D.P.O.”	indica il *Data Protection Officer* (responsabile della protezione dei dati personali) nominato dal Titolare.
“GDPR”	indica il 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).
“Interessato”	la persona fisica identificata o identificabile a cui si riferiscono i dati personali.
“Responsabile”	indica la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.
“Subfornitore/Sub-Responsabile”	indica qualsiasi soggetto, persona fisica o giuridica, a cui il Responsabile ricorra per l’esecuzione di specifiche attività di Trattamento per conto del Titolare a cui sono imposti gli stessi obblighi del Responsabile.
“Terze Parti o Terzi”	indica la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che non sia l’Interessato, il Titolare, il Responsabile e gli Incaricati Autorizzati al trattamento dei datipersonali sotto l’autorità diretta del Titolare o del Responsabile.
“Titolare”	indica 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
“Trattamento”	indica 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"	indica 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.

Scopo

Scopo della presente procedura è descrivere le norme di comportamento che devono essere osservate in caso di violazione dei dati personali.

Destinatari

La presente procedura è vincolante per i dipendenti di ULSS7 senza distinzione di ruolo e/o livello, nonché per tutti i collaboratori in *stage*, i tirocinanti, gli specializzandi e per ogni eventuale ulteriore collaboratore al quale ULSS7 ritenga, al momento della stipula del contratto, di applicare la Procedura.

Conoscenza della procedura e formazione

La presente Procedura viene portata a conoscenza dei Destinatari con una o più tra le seguenti modalità:
- pubblicazione sul sito intranet aziendale;
- diffusione a mezzo Sistema di Gestione Documentale dell'Azienda ULSS 7 Pedemontana;
- pubblicazione sulla bacheca dell'angolo del dipendente;
- formazione specifica.

Responsabile per la procedura di *Data Breach*

Il Responsabile per la procedura di *Data Breach* è individuato nel Direttore UOC Affari Generali o suo delegato.

Registro delle Violazioni

ULSS7 mantiene aggiornato il Registro delle Violazioni contenente, fra le altre, le seguenti informazioni:
- la data scoperta dell'evento;
- la natura della violazione con indicazione, ove possibile, delle categorie e del numero approssimativo di interessati nonché delle categorie e del numero approssimativo di registrazioni dei dati personali in questione;
- 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 ("Azioni di miglioramento e/o correttive") e anche, se del caso, per attenuarne i possibili effetti negativi.

La tenuta e l'aggiornamento del Registro delle Violazioni è responsabilità del Titolare (in persona del legale rappresentante), il quale vi provvede con il supporto dei Delegati volta per volta coinvolti, del Responsabile IT (se necessario) e del D.P.O.
Quest'ultimo ha comunque accesso al Registro delle Violazioni.

Al presente documento si allega il modello aziendale della scheda di Registro delle Violazioni (**Sub-all. 2**)

Modalità operative

Chiunque verifichi il manifestarsi di una Violazione deve darne immediata comunicazione al Responsabile della Procedura di *Data Breach* di riferimento e/o a suo delegato, inviando un messaggio di posta elettronica all'indirizzo mail **privacy@aulss7.veneto.it**; qualora non fosse possibile adottare le modalità precedentemente indicate, il Responsabile di riferimento dovrà essere raggiunto con lo strumento ritenuto più idoneo.

Il segnalante, ed in generale chi accerta un evento che può risolversi in una violazione, NON deve compiere autonomamente alcuna azione correttiva, di ripristino o intervento sui sistemi informatici aziendali, ma limitarsi ad effettuare tempestivamente la segnalazione ed attendere l'intervento da parte delle funzioni aziendali competenti.

La segnalazione potrà essere inviata anche da un Responsabile del trattamento dei dati opportunamente nominato dal Titolare (cfr. art. 28 par. 3 lett. f GDPR)

Ricevuta la segnalazione, il Responsabile della Procedura di *Data Breach* di riferimento contatta tempestivamente il Titolare (in persona del legale rappresentante) e il D.P.O. per appurare l'entità e la natura della stessa Violazione, nonché provvedere alla redazione del Registro delle Violazioni, in conformità con le prescrizioni della presente procedura.

Qualora la Violazione riguardi dati trattati da ULSS7 in qualità di Responsabile, si procederà alla comunicazione della Violazione nei termini e con le modalità volta per volta concordati nella Nomina a Responsabile o altro atto giuridico stipulato con il Titolare.

Qualora la Violazione riguardi dati trattati da ULSS7 in qualità di Titolare, sarà necessario:

- procedere alla notificazione all'Autorità di controllo, competente senza ingiustificato ritardo tramite il modello di notifica al Garante qui di seguito allegato (**Sub-all. 1**) 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;
- comunicare la violazione all'interessato senza ingiustificato ritardo, sempre che la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Eseguite le operazioni di cui al paragrafo precedente, il Titolare (in persona del legale rappresentante) verifica - con il supporto del Delegato coinvolto, del Responsabile IT (se necessario) e del D.P.O. - l'applicazione delle misure di miglioramento e/o correttive, nonché il ripristino della situazione di normalità. Le decisioni in ordine alla notificazione all'Autorità di controllo ed alla comunicazione agli interessati sono assunte dal Titolare (in personale del legale rappresentante), sentiti il Delegato di riferimento, il Responsabile IT (se necessario) e il D.P.O.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Sub-all 1

V.2021-04

Notifica di una violazione dei dati personali

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

Questo servizio *online* per la notifica di una violazione dei dati personali deve essere utilizzato esclusivamente da soggetti (pubbliche amministrazioni, imprese, associazioni, partiti, professionisti, ecc.) che trattano dati personali in qualità di titolari del trattamento.

Per rivolgersi al Garante in qualità di interessato, per lamentare una violazione della disciplina in materia di protezione dei dati personali, occorre inviare una segnalazione (art. 144 del Codice in materia di protezione dei dati personali) che il Garante può valutare anche ai fini dell'emanazione di provvedimenti correttivi, oppure proporre un reclamo (art. 77 del Regolamento (UE) 2016/679 e artt. da 140-*bis* a 143 del Codice in materia di protezione dei dati personali).

Maggiori informazioni sono disponibili sul sito istituzionale del Garante (https://www.gpdp.it/web/guest/home/diritti/come-agire-per-tutelare-i-tuoi-dati-personali).

Facsimile a titolo dimostrativo non utilizzabile per l'invio della notifica al Garante.

Notifica di una violazione dei dati personali

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

A) Dati del soggetto che effettua la notifica

Il soggetto che effettua la notifica è la persona fisica che, per conto titolare del trattamento, tramite questa procedura *online* notifica una violazione dei dati personali al Garante, assumendosi la responsabilità circa la veridicità delle informazioni fornite. Pertanto, la notifica dovrà essere effettuata dal rappresentante legale del titolare del trattamento o da un altro soggetto che agisce su sua delega.

Il sottoscritto Cognome[1*] …….. Nome[1*] …….
E-mail[2*] ……
nella sua qualità[3] di

0 rappresentante legale

0 delegato del rappresentante legale

Cognome[4*] …….. Nome[4*] …….

notifica la seguente violazione di dati personali e ☐ dichiara di aver preso visione dell'informativa sul trattamento dei dati personali e di essere consapevole 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*) o dell'art. 44 del d.lgs. 51/2018 (*Falsità in atti e dichiarazioni al Garante*), salvo che il fatto non costituisca più grave reato.

———————————

[1] Indicare il **Cognome** e il **Nome** del soggetto che effettua la notifica (e che successivamente dovrà apporre la sua firma digitale, conformemente alle istruzioni che riceverà via e-mail).

[2] Indicare un indirizzo **E-mail** valido per la ricezione delle istruzioni per il completamento della procedura di notifica. Nel caso venga indicata una casella PEC, verificare che la stessa sia abilitata alla ricezione di messaggi di posta elettronica ordinaria. Si consiglia, inoltre, di verificare che il messaggio non sia stato spostato automaticamente o per errore nella cartella "spam" o "posta indesiderata.

[3] Indicare se il soggetto che effettua la notifica è il "rappresentante legale" del Titolare del trattamento dati – di cui alla successiva Sez. C - oppure se agisce in **qualità** di "delegato del rappresentante legale.

[4] Qualora la notifica venga effettuata su delega del rappresentante legale è necessario indicare il Cognome ed il Nome del soggetto delegante (il rappresentante legale).

B) Tipo di notifica

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione al Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore (**Prima notifica**). Qualora e nella misura in cui il titolare del trattamento non disponga di tutte le informazioni, può fornirle in fasi successive (**Notifica integrativa**) senza ulteriore ingiustificato ritardo (cfr. art. 33, par. 4, del Regolamento).

0 ***Prima notifica***

0 a) Completa

0 b) Preliminare[1]

La notifica viene effettuata

0 ai sensi dell'art. 33 del RGPD

0 ai sensi dell'art. 26 d.lgs. 51/2018

0 ***Notifica integrativa***[2]

0 c) fascicolo n. [3*] ..... PIN [3*] .....

———————————

[1] Il titolare del trattamento avvia il processo di notifica pur in assenza di un quadro completo della violazione impegnandosi ad effettuare una successiva notifica integrativa per completare il processo di notifica.

[2] Il titolare del trattamento, avvalendosi delle previsioni di cui all'art. 33 par. 4 del Regolamento, integra una precedente notifica.

[3] È necessario inserire il numero del fascicolo ed il relativo PIN. Il numero di **fascicolo** unitamente al PIN sono indicati nella e-mail, indirizzata al soggetto che ha effettuato la prima notifica, con la quale è stata comunicata la corretta conclusione della procedura.

B1) Motivo dell'integrazione

Se procedi con la notifica integrativa per i motivi a) o b) troverai le informazioni che hai già fornito con l'ultima notifica e che potrai modificare. Il suo contenuto, previa integrazione o modifica, annulla e sostituisce la precedente.

Se la notifica che intendi integrare è stata trasmessa con le precedenti modalità non troverai le informazioni che hai già fornito, e non sarà possibile compilare la sez. C e i punti 2 e 3 della sez. F. La notifica integrativa, ed il suo contenuto, integrerà e sostituirà la precedente notifica.

1. Si procede all'integrazione per:

- 0 a) Fornire ulteriori informazioni senza completare il processo di notifica
- 0 b) Fornire ulteriori informazioni e completare il processo di notifica
- 0 c) Completare il processo di notifica senza fornire ulteriori informazioni
- 0 d) Annullare una precedente notifica per le seguenti motivazioni:

C) Titolare del trattamento

1. *Il titolare del trattamento è:*

Indicare l'eventuale registro all'interno del quale è censito il Titolare/Responsabile del trattamento che effettua la comunicazione. A tal fine si rappresenta che (cfr. DL 19 ottobre 2012, n. 179) tutte le imprese costituite in forma societaria e tutte le imprese individuali iscritte al registro delle imprese o all'albo delle imprese artigiane, nonché tutti i professionisti iscritti ad Ordini o Collegi professionali sono censiti all'interno dell'Indice nazionale dei domicili digitali delle imprese e dei professionisti (INIPEC). Inoltre, tutte le pubbliche amministrazioni (es. scuole, comuni, ecc.) sono iscritte nell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

0 Censito nell'Indice nazionale dei domicili digitali delle imprese e dei professionisti
(INI-PEC www.inipec.gov.it - art. 6-bis Codice Amministrazione Digitale - D.Lgs n. 82/2005)

0 Censito nell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi - *(Tipologie Enti: Pubbliche Amministrazioni)*
(*IPA www.indicepa.gov.it - art. 6-ter Codice Amministrazione Digitale - D.Lgs n. 82/2005*)

0 Non censito in nessuno dei due precedenti indici

2. *Dati del titolare del trattamento*

Indicare le informazioni relative al Titolare del trattamento (nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

Denominazione* .....
Codice Fiscale [1]* ..... Soggetto privo di C.F./P.IVA italiana ☐
Stato* .....
Provincia* ..... Comune* ..... CAP* .....
Indirizzo* .....
Telefono* .....
E-mail[2]* .....
PEC[2]* .....

———————————

[1] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;
- Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

[2] Per i soggetti che risultano essere censiti in uno degli indici INI-PEC o IPA è **obbligatorio** fornire l'indirizzo PEC, mentre il conferimento dell'indirizzo e-mail è facoltativo. Per i soggetti che non risultano essere censiti in uno dei due citati indici, o che operano in un altro Stato, è obbligatorio fornire un valido indirizzo e-mail, mentre il conferimento della PEC è facoltativo.

Notifica di una violazione dei dati personali

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

C1) Rappresentante del titolare del trattamento non stabilito nello Spazio Economico Europeo

Il titolare del trattamento non stabilito nello Spazio Economico Europeo, qualora offra beni o servizi a interessati nello Spazio Economico Europeo, oppure effettui il monitoraggio del loro comportamento (cfr. art. 3, par. 2, del Regolamento), è tenuto, ai sensi dell'art. 27 del Regolamento, a designare per iscritto un rappresentante in uno dei Paesi dello Spazio Economico Europeo in cui si trovano i predetti interessati, fatti salvi i casi in cui il trattamento è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati o dati relativi a condanne penali e reati, ed è improbabile che presenti un rischio per i diritti e le libertà degli interessati, oppure il trattamento è effettuato da autorità o organismi pubblici.

1. Rappresentante del titolare del trattamento

0 a) Compila la sezione

0 b) Procedi con la notifica senza compilare questa sezione

2. Dati del rappresentante del titolare del trattamento

Denominazione[1*] .....

Codice Fiscale/P.IVA* ..... Soggetto privo di C.F./P.IVA italiana ☐

Stato* .....

Provincia* ..... Comune* ..... CAP* .....

Indirizzo* .....

Telefono* .....

E-mail[2*] .....

PEC[2*] .....

———————————

[1] Indicare le informazioni relative al Rappresentante del titolare del trattamento (nel caso di impresa indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale).

[2] È obbligatorio fornire almeno un recapito tra E-mail e PEC.

D) Dati di contatto per informazioni relative alla violazione

Il titolare del trattamento deve 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 (cfr. art. 33, par. 3, lett. b), del Regolamento).

o ***1) Responsabile della protezione dei dati***

- o i cui dati di contatto sono stati già comunicati con la comunicazione protocollo[1*] n.……..
- o i cui dati di contatto sono stati già comunicati al Garante, ma al momento non si dispone[2] del numero di protocollo della relativa comunicazione

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……

o ***2) Altro soggetto***

Cognome* …… Nome* ……..
E-mail* ……..
Recapito telefonico per eventuali comunicazioni* ……
Funzione rivestita* ……

———————————

[1] Indicare il numero di protocollo assegnato alla comunicazione dei dati di contatto del RPD.

[2] Selezionare questa opzione se al momento della compilazione non è possibile reperire il numero di protocollo assegnato alla comunicazione dei dati di contatto che sarà comunicato con una successiva notifica integrativa.

E) Ulteriori soggetti coinvolti nel trattamento

Indicare i riferimenti di ulteriori soggetti coinvolti ed il ruolo svolto (contitolare, responsabile[1])

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

Denominazione[2*] ……

Codice Fiscale[3*] ……Soggetto privo di C.F./P.IVA ☐

Ruolo O Contitolare O Responsabile

———————————

[1] In tale tipologia rientra anche l'altro responsabile (c.d. sub-responsabile) di cui all'art. 28, par. 2, del RGPD o all'art. 18, comma 2, del d.lgs. 51/2018.

[2] Nel caso di impresa o di soggetto pubblico indicare i dati della persona giuridica e non della persona fisica corrispondente al rappresentante legale.

[3] In relazione all'indicazione del Codice Fiscale si rappresenta che:

- I soggetti censiti nell'indice IPA appartenenti alla categoria "Pubbliche Amministrazioni" **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora ne siano in possesso);
- Le imprese censite nell'indice INI-PEC **devono** indicare il Codice Fiscale così come indicato nello stesso indice (e non la Partita IVA qualora non coincidente con il Codice Fiscale);
- I professionisti censiti nell'indice INI-PEC **devono** indicare il numero di Partita IVA utilizzato per lo svolgimento dell'attività professionale;

  Solo i soggetti stranieri o le organizzazioni prive di Codice Fiscale e P.IVA devono selezionare la casella "Soggetto Privo di CF/P.IVA".

Notifica di una violazione dei dati personali

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

F) Informazioni sulla violazione

1. *Momento in cui è avvenuta la violazione*

- o a) Il ___ /___ /_____
- o b) Dal ___/___ /_____ (la violazione è ancora in corso)
- o c) Dal ___/___ /_____ al ___ /___ /_____
- o d) In un tempo non ancora determinato

Ulteriori informazioni circa le date in cui è avvenuta la violazione

2. *Modalità con la quale il titolare è venuto a conoscenza della violazione*

- o a) Rilevazione da parte del titolare[1]
- o b) Comunicazione da parte del responsabile del trattamento
- o c) Segnalazione da parte di un interessato
- o d) Segnalazione da parte di un soggetto esterno
- o e) Notizie stampa
- o f) Altro

3. *Momento in cui il titolare è venuto a conoscenza della violazione*

Data …… **Ora** ……..

4. *Motivi del ritardo (in caso di notifica oltre le 72 ore)*

5. *Natura della violazione*

[ ] a) Perdita di riservatezza[2]
[ ] b) Perdita di integrità[3]
[ ] c) Perdita di disponibilità[4]

6. *Causa della violazione*

[ ] a) Azione intenzionale interna
[ ] b) Azione accidentale interna
[ ] c) Azione intenzionale esterna
[ ] d) Azione accidentale esterna
[ ] e) Sconosciuta

[ ] **f)** Non ancora determinata

7. *Descrizione della violazione*[5]

8. *Descrizione dei sistemi, software, servizi e infrastrutture IT coinvolti nella violazione, con indicazione della loro ubicazione*

9. *Misure tecniche e organizzative, in essere al momento della violazione, adottate per garantire la sicurezza dei dati personali coinvolti*

10. Categorie di interessati coinvolti nella violazione

[ ] a) Dipendenti/Consulenti
[ ] b) Utenti/Contraenti/Abbonati/Clienti (attuali o potenziali)
[ ] c) Associati, soci, aderenti, simpatizzanti, sostenitori
[ ] d) Soggetti che ricoprono cariche sociali
[ ] e) Beneficiari o assistiti
[ ] f) Pazienti
[ ] g) Minori
[ ] h) Persone vulnerabili (es. vittime di violenze o abusi, rifugiati, richiedenti asilo)
[ ] i) Altro

[ ] l) Categorie ancora non determinate

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

o a) N. …….. interessati
o b) Circa n. …….. interessati
o c) Non determinabile
o d) Non ancora determinato

12. Categorie di dati personali oggetto di violazione

[ ] a) Dati anagrafici (nome, cognome, sesso, data di nascita, luogo di nascita, codice fiscale)
[ ] b) Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile)
[ ] c) Dati di accesso e di identificazione (username, password, customer ID, altro…)
[ ] d) Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro…)
[ ] e) Dati relativi alla fornitura di un servizio di comunicazione elettronica (dati di traffico, dati relativi alla navigazione internet, altro…)
[ ] f) Dati relativi a condanne penali e ai reati o a connesse misure di sicurezza
[ ] g) Dati di profilazione
[ ] h) Dati relativi a documenti di identificazione/riconoscimento (carta di identità, passaporto, patente, CNS, altro…)
[ ] i) Dati relativi all'ubicazione
[ ] l) Dati che rivelano l'origine razziale o etnica
[ ] m) Dati che rivelano le opinioni politiche
[ ] n) Dati che rivelano le convinzioni religiose o filosofiche
[ ] o) Dati che rivelano l'appartenenza sindacale
[ ] p) Dati relativi alla vita sessuale o all'orientamento sessuale
[ ] q) Dati relativi alla salute
[ ] r) Dati genetici

[ ] s) Dati biometrici
[ ] t) Altro

[ ] u) Categorie ancora non determinate

13. *Numero (anche approssimativo) di registrazioni[6] dei dati personali oggetto di violazione*

o a) N. ……..
o b) Circa n. ……..
o c) Non determinabile
o d) Non ancora determinato

14. *Descrizione di dettaglio delle categorie di dati personali oggetto della violazione per ciascuna categoria di interessati*

15. *Allegati*

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Es. verifiche interne, monitoraggi, ecc
2. Diffusione/ accesso non autorizzato o accidentale
3. Modifica non autorizzata o accidentale
4. Impossibilità di accesso o distruzione non autorizzata o accidentale
5. Indicare le circostanze in cui si è verificata la violazione e le cause, tecniche o organizzative, che l'hanno determinata
6. Ad esempio numero di fatture, ordini, referti, immagini, record di un database o numero di transazioni.

G) Probabili conseguenze della violazione

1. Probabili conseguenze della violazione per gli interessati

1.1. In caso di perdita di riservatezza:

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

[ ] e) In corso di valutazione[4]

1.2. In caso di perdita di integrità:

[ ] a) I dati sono stati modificati e resi inconsistenti
[ ] b) I dati sono stati modificati mantenendo la consistenza
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.3. In caso di perdita di disponibilità:

[ ] a) Mancato accesso a servizi
[ ] b) Malfunzionamento e difficoltà nell'utilizzo di servizi
[ ] c) Altro

[ ] d) In corso di valutazione[4]

1.4. Ulteriori considerazioni sulle probabili conseguenze

2. Potenziale impatto per gli interessati

[ ] a) Perdita del controllo dei dati personali
[ ] b) Limitazione dei diritti
[ ] c) Discriminazione
[ ] d) Furto o usurpazione d'identità
[ ] e) Frodi
[ ] f) Perdite finanziarie
[ ] g) Decifratura non autorizzata della pseudonimizzazione
[ ] h) Pregiudizio alla reputazione
[ ] i) Perdita di riservatezza dei dati personali protetti da segreto professionale
[ ] l) Conoscenza da parte di terzi non autorizzati
[ ] m) Qualsiasi altro danno economico o sociale significativo

[ ] n) Non ancora definito

3. Gravità del potenziale impatto per gli interessati

o a) Trascurabile
o b) Bassa
o c) Media
o d) Alta
o e) Non ancora definita

Motivazioni

4. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

H) Misure adottate a seguito della violazione

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

2. Misure tecniche e organizzative adottate (o di cui si propone l'adozione[1]) per prevenire simili violazioni future

3. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

———————————

1. Nella descrizione distinguere le misure adottate da quelle in corso di adozione

I) Valutazione del rischio per gli interessati

Non sono state fornite alcune delle informazioni (es. categorie e numero di interessati, categorie e numero di registrazioni di dati personali, probabili conseguenze della violazione, ecc.) di cui il titolare del trattamento dovrebbe tenere conto nella valutazione del rischio per i diritti e le libertà degli interessati derivante dalla violazione dei dati personali. Pertanto si invita il titolare del trattamento a prestare particolare attenzione nella compilazione della presente sezione, fornendo le motivazioni che lo hanno portato a ritenere che la violazione dei dati personali sia suscettibile, o meno, di presentare un rischio elevato per gli interessati.

Il Regolamento (spec. cons. nn. 75 e 76) suggerisce che, di norma, nella valutazione del rischio si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbero essere determinati in base a una valutazione oggettiva.
Le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018, individuano i seguenti fattori da considerare – a fronte di una violazione dei dati personali – nella valutazione del rischio per i diritti e le libertà degli interessati: il tipo di violazione; la natura, il carattere sensibile e il volume dei dati personali; la facilità di identificazione degli interessati; la gravità delle conseguenze per gli interessati; le caratteristiche particolari dell'interessato; le caratteristiche particolari del titolare del trattamento dei dati; nonché il numero di interessati coinvolti.

1. Il titolare del trattamento ritiene[1] che:

- o a) la violazione sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o b) la violazione non sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche
- o c) siano necessari ulteriori elementi per effettuare la valutazione del rischio per i diritti e le libertà delle persone fisiche

Motivazioni

2. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

L) Comunicazione della violazione agli interessati

Si evidenzia che, 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 è tenuto, ai sensi dell'art. 34 del Regolamento, a comunicare la violazione agli interessati coinvolti senza ingiustificato ritardo, a meno che sia soddisfatta una delle condizioni previste dal par. 3 del citato articolo.

1. La violazione è stata comunicata direttamente agli interessati?

- o a) Sì, è stata comunicata il ___/___/_____
- o b) No, sarà comunicata entro il ___/___/_____
- o c) No, sono tuttora in corso le dovute valutazioni
- o d) No, perché la violazione non è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- o e) No e non sarà comunicata perché:

[ ] e1) il titolare 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 (es. cifratura);

Descrivere le misure applicate

[ ] e2) il titolare 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

[ ] e3) detta comunicazione richiederebbe sforzi sproporzionati. Il titolare ha proceduto o procederà con una comunicazione pubblica o una misura simile, tramite la quale gli interessati sono o saranno informati con analoga efficacia.

Descrivere la modalità tramite la quale gli interessati sono stati informati

Notifica di una violazione dei dati personali

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

2. Numero di interessati a cui è stata comunicata la violazione

N. …….. interessati

3. Canale utilizzato per la comunicazione agli interessati

[ ] a) SMS
[ ] b) Posta cartacea
[ ] c) Posta elettronica
[ ] d) Altro

4. Contenuto della comunicazione agli interessati

5. Allegati

[ ] Intendo allegare un documento contenente ulteriori informazioni

M) Altre informazioni

1. La violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative[1]?

O Sì O No

Indicare a quale organismo e in virtù di quale norma

2. È stata effettuata la segnalazione all'autorità giudiziaria o di polizia?

O Sì O No

Note

———————————

1. Ad esempio: Regolamento (UE) 910/2014 (eIDAS), d.lgs. 65/2018 attuativo della Direttiva (UE) 2016/1148 (NIS)

N) Informazioni relative a violazioni transfrontaliere

Un trattamento transfrontaliero (cfr. art. 4, punto 23), del Regolamento) è un trattamento che ha luogo nell'ambito di stabilimenti in più di un Paese dello Spazio Economico Europeo (di cui fanno parte gli Stati membri dell'Unione Europea, nonché l'Islanda, il Liechtenstein e la Norvegia), oppure che ha luogo nell'ambito di un unico stabilimento in un Paese dello Spazio Economico Europeo, ma che può avere impatti significativi sui diritti e sulle libertà di interessati in più di un Paese dello Spazio Economico Europeo.

1. ***La violazione riguarda un trattamento transfrontaliero effettuato da un titolare stabilito all'interno dello Spazio Economico Europeo?***

   - o a) Sì
   - o b) No
   - o c) Sono tuttora in corso le dovute valutazioni

2. ***Indicare l'autorità di controllo capofila[1]***

   - o a) Garante per la protezione dei dati personali
   - o b) Altra autorità di controllo: [Selezionare]
   - o c) Non si dispone di elementi per individuare l'autorità di controllo capofila

3. ***Indicare i Paesi dello Spazio Economico Europeo in cui si trovano stabilimenti del titolare, specificando quelli coinvolti nella violazione, o in cui si trovano gli interessati coinvolti nella violazione***

	Stabilimenti del titolare	Stabilimenti coinvolti nella violazione	Interessati coinvolti nella violazione
Italia	[ ]	[ ]	[ ]
Austria	[ ]	[ ]	[ ]
Belgio	[ ]	[ ]	[ ]
Bulgaria	[ ]	[ ]	[ ]
Cipro	[ ]	[ ]	[ ]
Croazia	[ ]	[ ]	[ ]
Danimarca	[ ]	[ ]	[ ]
Estonia	[ ]	[ ]	[ ]
Finlandia	[ ]	[ ]	[ ]
Francia	[ ]	[ ]	[ ]
Germania	[ ]	[ ]	[ ]
Grecia	[ ]	[ ]	[ ]
Irlanda	[ ]	[ ]	[ ]
Islanda	[ ]	[ ]	[ ]
Lettonia	[ ]	[ ]	[ ]
Liechtenstein	[ ]	[ ]	[ ]
Lituania	[ ]	[ ]	[ ]

Lussemburgo	[ ]	[ ]	[ ]
Malta	[ ]	[ ]	[ ]
Norvegia	[ ]	[ ]	[ ]
Paesi Bassi	[ ]	[ ]	[ ]
Polonia	[ ]	[ ]	[ ]
Portogallo	[ ]	[ ]	[ ]
Rep. Ceca	[ ]	[ ]	[ ]
Romania	[ ]	[ ]	[ ]
Slovacchia	[ ]	[ ]	[ ]
Slovenia	[ ]	[ ]	[ ]
Spagna	[ ]	[ ]	[ ]
Svezia	[ ]	[ ]	[ ]
Ungheria	[ ]	[ ]	[ ]

4. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)

[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner
[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

———————————

1. L'autorità di controllo dello stabilimento principale in cui ha luogo il trattamento o dello stabilimento unico del titolare del trattamento

O) Informazioni relative a violazioni che riguardano trattamento effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo

Il Regolamento si applica anche al trattamento di dati personali di interessati che si trovano nello Spazio Economico Europeo, effettuato da un titolare del trattamento che non è stabilito nello Spazio Economico Europeo, laddove tale trattamento riguardi: a) l'offerta di beni o la fornitura di servizi a interessati nello Spazio Economico Europeo, oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dello Spazio Economico Europeo (cfr. art. 3, par. 2, del Regolamento)

1. ***La violazione riguarda un trattamento, a cui si applica il Regolamento, effettuato da un titolare stabilito al di fuori dello Spazio Economico Europeo?***

   o a) Sì
   o b) No

2. ***Indicare gli altri Paesi dello Spazio Economico Europeo in cui si trovano gli interessati coinvolti nella violazione***

   [ ] Austria
   [ ] Belgio
   [ ] Bulgaria
   [ ] Cipro
   [ ] Croazia
   [ ] Danimarca
   [ ] Estonia
   [ ] Finlandia
   [ ] Francia
   [ ] Germania
   [ ] Grecia
   [ ] Irlanda
   [ ] Islanda
   [ ] Lettonia
   [ ] Liechtenstein
   [ ] Lituania
   [ ] Lussemburgo
   [ ] Malta
   [ ] Norvegia
   [ ] Paesi Bassi
   [ ] Polonia
   [ ] Portogallo
   [ ] Rep. Ceca
   [ ] Romania
   [ ] Slovacchia
   [ ] Slovenia
   [ ] Spagna

[ ] Svezia
[ ] Ungheria

3. *Indicare le altre autorità di controllo a cui è stata eventualmente notificata la violazione*

[ ] Austria - Data Protection Authority
[ ] Belgio - Data Protection Authority
[ ] Bulgaria - Commission for Personal Data Protection
[ ] Cipro - Office of the Commissioner for Personal Data Protection
[ ] Croazia - Personal Data Protection Agency - AZOP
[ ] Danimarca - Data Protection Agency
[ ] Estonia - Data Protection Inspectorate
[ ] Finlandia - Office of the Data Protection Ombudsman
[ ] Francia - CNIL - National Commission for Informatics and Liberties
[ ] Germania - Federal Commissioner for Data Protection and Freedom of Information (BfDI)
[ ] Germania (Baden-Wurttemberg) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Bavaria - Private Sector) - Bavarian Lander Office for Data Protection Supervision (BayLDA)
[ ] Germania (Bavaria - Public sector) - Lander Commissioner for Data Protection (BayLfD)
[ ] Germania (Berlin) - Berlin Commissioner for Data Protection and Freedom of Information
[ ] Germania (Brandenburg) - Lander Commissioner for Data Protection and the Right for Access to Information
[ ] Germania (Bremen) - Lander Commissioner for Data Protection and Freedom of Information - Free Hanseatic city of Bremen
[ ] Germania (Hamburg) - Hamburg Commissioner for Data Protection and Freedom of Information
[ ] Germania (Hesse) - Hessian Commissioner for Data Protection and Freedom of Information
[ ] Germania (Lower Saxony) - Lander Commissioner for Data Protection (LfD)
[ ] Germania (Mecklenburg-Western Pomerania) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (North Rhine-Westphalia) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Rhineland-Palatinate) - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saarland) - Independent Data Protection Center Saarland - Lander Commissioner for Data Protection and Freedom of Information
[ ] Germania (Saxony) - Saxon Data Protection Commissioner
[ ] Germania (Saxony-Anhalt) - Lander Commissioner for Data Protection
[ ] Germania (Thuringia) - Thuringian Lander Commissioner for Data Protection and Freedom of Information (TLfDI)
[ ] Grecia - Hellenic Data Protection Authority
[ ] Irlanda - Data Protection Commission (DPC)
[ ] Islanda - Data Protection Authority
[ ] Lettonia - Data State Inspectorate
[ ] Liechtenstein - Data Protection Authority
[ ] Lituania - State Data Protection Inspectorate
[ ] Lituania - The Office of Inspector of Journalist Ethics
[ ] Lussemburgo - National Commission for Data Protection (CNPD)
[ ] Malta - Office of the Information and Data Protection Commissioner
[ ] Norvegia - Norwegian Data Protection Authority
[ ] Paesi Bassi - Authority for Personal Data
[ ] Polonia - Office for the Protection of Personal Data
[ ] Portogallo - National Commission for Data Protection (CNPD)
[ ] Rep. Ceca - Office for Personal Data Protection
[ ] Romania - National Supervisory Authority For Personal Data Processing
[ ] Slovacchia - Office for Personal Data Protection
[ ] Slovenia - Information Commissioner

[ ] Spagna - Spanish Agency for Data Protection
[ ] Svezia - Data Protection Authority
[ ] Ungheria - National Authority for Data Protection and Freedom of Information

[ ] Intendo allegare copia (in lingua inglese) della notifica effettuata

REGIONE DEL VENETO
ULSS7 PEDEMONTANA

Sub-all. 2

REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI EX ART. 33, PAR. V, GDPR

INFORMAZIONI SULL'EVENTO		
NUMERO		
DATA E ORA DI RILEVAZIONE DEL DATA BREACH		
DATA E ORA DELL'EVENTO		
UNITÀ IN CUI SI E' VERIFICATO		
TIPO DI VIOLAZIONE	VIOLAZIONE DELLA RISERVATEZZA (in caso di divulgazione dei dati personali o accesso agli stessi autorizzati o accidentali)	
	VIOLAZIONE DELL'INTEGRITA' (in caso di modifica non autorizzata o accidentale dei dati personali)	
	VIOLAZIONE DELLA DISPONIBILITA' (in caso di perdita accesso o distruzione accidentali o non autorizzati di dati personali)	
CATEGORIE DI DATI OGGETTO DI VIOLAZIONE		
NUMERO DEGLI INTERESSATI COINVOLTI NELLA VIOLAZIONE		

REGIONE DEL VENETO

ULSS7 PEDEMONTANA

TIPOLOGIE DI INTERESSATI COINVOLTI NELLA VIOLAZIONE		
DESCRIZIONE DETTAGLIATA (compresi sistemi interessati)		
ANALISI DELLE CAUSE	DISATTENZIONE	
	EVENTO FORTUITO	
	AZIONE IMPROPRIA	
	MANCATO RISPETTO DELLE PROCEDURE	
	MANCANZA DI INFORMAZIONE E FORMAZIONE	
POSSIBILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI		
MISURE	• Misure Tecniche	

PREVENTIVE INDIVIDUATE PER EVITARE IL RIPETERSI DELL'EVENTO	• Misure organizzative	
	• Misure procedurali	
	• Misure formative	
MISURE CORRETTIVE ADOTTATE	• Misure Tecniche	
	• Misure organizzative	
	• Misure procedurali	
	• Misure formative / informative	
NOTIFICAZIONE ALL'AUTORITÀ DI CONTROLLO	Sì perché / no perché	
COMUNICAZIONE AGLI INTERESSATI	Sì perché / no perché	

All. 4

REGIONE DEL VENETO

ULSS7 PEDEMONTANA

AZIENDA ULSS 7 PEDEMONTANA

Regolamento sull'utilizzo degli strumenti

"Google Workspace"

INDICE DEI CONTENUTI:

Azienda ULSS n. 7 Pedemontana - Via dei Lotti n. 40 – 36061 Bassano del Grappa (VI) – C.F. e P. IVA 00913430245
Centralino Bassano del Grappa: 0424/888111 – Centralino Santorso: 0445/571111 – Fax: 0424/885223
PEC: protocollo.aulss7@pecveneto.it - sito web: www.aulss7.veneto.it

DEFINIZIONI

Per una corretta interpretazione del presente regolamento, si definiscono, di seguito, i seguenti termini:

- **Google Workspace**: una suite di applicazioni e strumenti *cloud-based* forniti da Google, utilizzati per migliorare la produttività, la collaborazione e la gestione delle informazioni aziendali. Include Gmail, Google Drive, Google Docs, Google Sheets, Google Calendar, Google Meet, e altri strumenti.
- **Dati Sensibili**: qualsiasi informazione che possa identificare direttamente o indirettamente una persona fisica, come previsto dalle normative vigenti, incluse ma non limitate a informazioni riguardanti la salute, l'origine etnica, l'orientamento sessuale, o altri dati protetti dalla legge (GDPR, d.lgs. 196/2003 e ss.mm.ii.).
- **Dati anonimi**: dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.
- **Informazioni Sanitarie**: dati relativi allo stato di salute fisico o mentale di un paziente, comprese diagnosi, trattamenti, terapie, e altre informazioni di carattere clinico.
- **Autorizzato al trattamento**: è il soggetto che operando sotto la responsabilità del titolare del trattamento o del responsabile ha accesso ai dati personali.
- **Account Google Workspace**: L'account individuale fornito dall'Azienda ULSS 7 Pedemontana per l'accesso agli strumenti Google Workspace. Esso è protetto da credenziali (nome utente e password) ed è strettamente personale.
- **Autenticazione a Due Fattori**: (2FA): Una misura di sicurezza aggiuntiva che richiede all'utente di fornire due forme di identificazione per accedere a un sistema (ad esempio, una password e un codice inviato al telefono).
- **UOC Sistemi Informativi**: l'Unità Operativa aziendale responsabile della gestione, manutenzione e sicurezza dei sistemi informatici.
- **Violazione di Sicurezza**: qualsiasi accesso non autorizzato, divulgazione, modifica o distruzione di dati aziendali o personali, o qualsiasi comportamento che possa compromettere la sicurezza delle informazioni aziendali.
- **GDPR**: Il Regolamento Generale sulla Protezione dei Dati (*General Data Protection Regulation*), normativa europea che disciplina la protezione e la privacy dei dati personali dei cittadini nell'Unione Europea.

Azienda ULSS n. 7 Pedemontana - Via dei Lotti n. 40 – 36061 Bassano del Grappa (VI) – C.F. e P. IVA 00913430245
Centralino Bassano del Grappa: 0424/888111 – Centralino Santorso: 0445/571111 – Fax: 0424/885223
PEC: protocollo.aulss7@pecveneto.it - sito web: www.aulss7.veneto.it

1. INTRODUZIONE

Google Workspace è una suite di strumenti e servizi di produttività *cloud-based* forniti da Google attiva su tutte ULSS della ragione Veneto.

Nell'azienda ULSS 7 Pedemontana, Google Workspace è utilizzato per ottimizzare la collaborazione, la comunicazione e la gestione delle informazioni. È essenziale garantire che questi strumenti siano utilizzati in modo sicuro, etico e conforme alle normative sulla protezione dei dati (come il GDPR), con particolare riferimento ai dati sanitari.
Questo regolamento fornisce una base per garantire un uso corretto e sicuro degli strumenti Google Workspace nel contesto aziendale, assicurando la protezione dei dati sensibili e il rispetto delle normative vigenti.

2. OBIETTIVI

Il presente regolamento ha lo scopo di definire le modalità di utilizzo degli strumenti Google Workspace da parte dei dipendenti dell'azienda ULSS 7 Pedemontana, nel rispetto delle normative vigenti e per assicurare l'efficace gestione delle informazioni aziendali.

3. STRUMENTI INCLUSI

Gli strumenti principali di Google Workspace soggetti a questo regolamento includono, ma non sono limitati a:

- **Gmail**: per la gestione della posta elettronica aziendale.
- **Google Chat**: per comunicazioni rapide in tempo reale.
- **Google Drive**: per l'archiviazione e la condivisione di documenti e file.
- **Google Documenti, Fogli, Presentazioni**: per la creazione e modifica di documenti, fogli di calcolo e presentazioni.
- **Google Calendario**: per la gestione degli appuntamenti e delle riunioni.
- **Google Meet**: per le videoconferenze.
- **Google Moduli**: per la raccolta di dati attraverso moduli.
- **Google Contatti:** per la gestione rubrica aziendale.

4. RESPONSABILITÀ DELL'UTENTE

- **Account Google Workspace**: ogni dipendente è responsabile della protezione del proprio account Google Workspace. Le credenziali di accesso (username e password) sono personali e non devono essere condivise con altri.
- **Protezione dei Dati**: l'uso degli strumenti di Google Workspace deve essere conforme alle normative sulla privacy, come il GDPR, al "Regolamento per l'utilizzo degli strumenti telematici" e al Modello Aziendale di gestione della privacy disponibile nel Portale Intranet. È vietato condividere informazioni sensibili o sanitarie dei pazienti senza le necessarie autorizzazioni.
- **Sicurezza e Accesso**: è obbligatorio utilizzare password sicure e modificarle periodicamente. L'accesso a Google Workspace è protetto con password e l'autenticazione a due fattori (2FA). I dispositivi fissi o mobili da cui si accede a Google Workspace devono essere protetti da password, PIN o misure di sicurezza equivalenti.
- **Utilizzo Etico**: gli strumenti di Google Workspace devono essere utilizzati esclusivamente per scopi lavorativi e in conformità con il "Codice di comportamento dei dipendenti dell'Azienda U.L.S.S. 7 Pedemontana" ed il "Regolamento per l'utilizzo degli strumenti telematici" pubblicati nella Intranet Aziendale. L'uso per finalità personali o non autorizzate è vietato.

Azienda ULSS n. 7 Pedemontana - Via dei Lotti n. 40 – 36061 Bassano del Grappa (VI) – C.F. e P. IVA 00913430245
Centralino Bassano del Grappa: 0424/888111 – Centralino Santorso: 0445/571111 – Fax: 0424/885223
PEC: protocollo.aulss7@pecveneto.it - sito web: www.aulss7.veneto.it

5. GESTIONE DEI DATI

Si rammenta l'uso consapevole dell'utilizzo degli strumenti Google Workspace per lo scambio di dati sensibili e/o sanitari pertanto gli stessi potranno essere condivisi previo opportune misure di sicurezza (es. anonimizzazione, criptazione etc)

- **Google meet:** Le videoconferenze su Google Meet devono essere protette limitando opportunamente le autorizzazioni per gli invitati. Le riunioni non devono essere registrate, a meno che ciò non sia stato approvato da tutti i partecipanti.

- **Google Drive**: È necessario mantenere un'organizzazione coerente e chiara dei documenti per facilitare l'accesso e la gestione delle informazioni. I file e le cartelle contenenti dati sensibili devono essere protetti con accesso limitato solo ai soggetti autorizzati allo specifico trattamento dati.

- **Google Documenti, Fogli, Presentazioni**: la collaborazione su documenti di Google Workspace deve essere limitata ai soli soggetti autorizzati. Gli utenti che abilitano altri a visualizzare o modificare un documento devono verificare che le impostazioni di condivisione siano correttamente impostate e riferite ai soli autorizzati.

6. MISURE DI SICUREZZA E MONITORAGGIO

- **Autenticazione a Due Fattori (2FA):** tutti gli utenti sono obbligati all'autenticazione a due fattori per proteggere l'accesso ai propri account Google Workspace.
- **Controllo degli Accessi**: l'Azienda ULSS 7 Pedemontana si riserva il diritto di monitorare e limitare l'accesso agli strumenti di Google Workspace per garantire la sicurezza delle informazioni aziendali. Eventuali accessi sospetti o violazioni devono essere immediatamente segnalati all'UOC Sistemi Informativi.

7. VIOLAZIONI E SANZIONI

- **Violazione delle Norme**: ogni violazione delle norme contenute nel presente regolamento sarà soggetta a indagini interne all'esito delle quali potrà comportare, se del caso, le sanzioni disciplinari previste dal "Codice di comportamento dei dipendenti dell'Azienda U.L.S.S. 7 Pedemontana".
- **Segnalazione delle Violazioni**: eventuali sospette violazioni di sicurezza o dell'utilizzo degli strumenti Google Workspace devono essere segnalate senza ingiustificato ritardo all'UOC Sistemi Informativi.

8. FORMAZIONE

Per chi utilizza questi strumenti è a disposizione la piattaforma di Azienda Zero contenente dei video tutorial e degli approfondimenti raggiungibili tramite i seguenti link:

https://goolearning.azero.veneto.it/video-didattici

https://goolearning.azero.veneto.it

Azienda ULSS n. 7 Pedemontana - Via dei Lotti n. 40 – 36061 Bassano del Grappa (VI) – C.F. e P. IVA 00913430245
Centralino Bassano del Grappa: 0424/888111 – Centralino Santorso: 0445/571111 – Fax: 0424/885223
PEC: protocollo.aulss7@pecveneto.it - sito web: www.aulss7.veneto.it

11. AGGIORNAMENTI DEL REGOLAMENTO

Questo Regolamento sarà soggetto a revisioni periodiche per garantire la sua conformità con le normative vigenti e con le nuove tecnologie. Qualsiasi modifica verrà comunicata al personale in modo tempestivo.

9. DATA DI ENTRATA IN VIGORE

10 giorni a partire dalla data di pubblicazione della Deliberazione del Direttore Generale di riferimento.

10. RESPONSABILE DELLA REVISIONE

Gruppo di lavoro Sicurezza Informatica.

Azienda ULSS n. 7 Pedemontana - Via dei Lotti n. 40 – 36061 Bassano del Grappa (VI) – C.F. e P. IVA 00913430245
Centralino Bassano del Grappa: 0424/888111 – Centralino Santorso: 0445/571111 – Fax: 0424/885223
PEC: protocollo.aulss7@pecveneto.it - sito web: www.aulss7.veneto.it