Azienda ULSS n. 2 Marca trevigiana

Sede Legale via Sant'Ambrogio di Fiera, 37 31100 Treviso

DELIBERAZIONE DEL DIRETTORE GENERALE

n. 203 del 03/02/2023

Il Direttore generale dell'Azienda ULSS n. 2 Marca trevigiana dott. Francesco Benazzi, nominato con D.P.G.R. n. 21 del 26 febbraio 2021, coadiuvato da:

Direttore amministrativo	- Mangione Patrizia
Direttore sanitario	- Formentini Stefano
Direttore dei servizi socio-sanitari	- Rigoli Roberto

ha adottato la presente deliberazione:

OGGETTO

REGOLAMENTO CONCERNENTE LA PROTEZIONE DEI DATI PERSONALI - AGGIORNAMENTO.

OGGETTO

REGOLAMENTO CONCERNENTE LA PROTEZIONE DEI DATI PERSONALI - AGGIORNAMENTO.

Il Direttore incaricato dell'U.O.C. Affari Generali e Legali, responsabile del procedimento, verificata la compatibilità con le norme nazionali, regionali e regolamenti vigenti in materia, relaziona al Direttore Generale quanto di seguito riportato:

PREMESSO che con precedente deliberazione:
- n. 1820 del 25.10.2018 è stato approvato il "Regolamento concernente la protezione dei dati personali";
- n. 1867 del 29.10.2020 è stato adottato in via definitiva il nuovo Atto Aziendale dell'Azienda ULSS n. 2 Marca trevigiana, a seguito della presa atto del decreto n. 103 del 28 settembre 2020 del Direttore Generale Area Sanità e Sociale, da ultimo aggiornato con deliberazione n. 2280 del 2.12.2022;

CONSIDERATO che a seguito del predetto Atto Aziendale si rende necessario provvedere all'aggiornamento del sistema aziendale di gestione della privacy ed, in particolare, del modello organizzativo al fine di meglio definire l'organigramma privacy, nonché compiti, funzioni e responsabilità dei diversi soggetti coinvolti;

VISTI i seguenti provvedimenti normativi per la materia in oggetto:

- Decreto Legislativo 30.6.2003, n. 196 "Codice in materia di protezione dei dati personali", come modificato dal Decreto Legislativo 10.8.2018, n. 101;
- Regolamento (UE) 27.4.2016, n. 2016/679 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);
- Decreto Legislativo 7.3.2005, n. 82 "Codice dell'Amministrazione digitale";
- Legge 7.8.1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- Decreto Legislativo 14.3.2013, n. 33 "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni";
- Decreto Legge n. 18.10.2012, n. 179 – art. 12 "Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario";
- Deliberazione n. 25 del 16.7.2009 del Garante per la protezione dei dati personali ad oggetto "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e Dossier sanitario";
- Deliberazione n. 88 del 2.3.2011 del Garante per la protezione dei dati personali ad oggetto "Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web";

- Deliberazione n. 31 del 25.1.2012 del Garante per la protezione dei dati personali ad oggetto "Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute";
- Deliberazione n. 243 del 15.5.2014 del Garante per la protezione dei dati personali ad oggetto "Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati";
- Deliberazione n. 331 del 4.6.2015 del Garante per la protezione dei dati personali ad oggetto "Linee guida in materia di Dossier sanitario";

DATO ATTO che, nell'ambito delle misure adottate in materia, con precedente deliberazione n. 1743 del 15.10.2020, il dott. Carlo Frattin è stato nominato quale Responsabile per la protezione dei dati personali;

SI PROPONE sulla base dei presupposti di fatto e delle ragioni giuridiche risultanti dalla relativa istruttoria di:
- aggiornare il "Regolamento concernente la protezione dei dati personali", nel testo allegato al presente provvedimento per farne parte integrante e sostanziale;
- adottare le istruzioni operative per la gestione di eventi potenzialmente qualificabili come violazione dei dati personali (c.d. *data breach*), delegando fin d'ora l'UOC Affari Generali e Legali alla loro integrazione e/o modificazione;
- confermare il Responsabile per la protezione dei dati personali già nominato;
- confermare il Referente informatico per la protezione dei dati nella persona del Responsabile dell'UOSD Sistemi Informativi;
- nominare la dott.ssa Marzia Volpato quale Referente aziendale per la protezione dei dati personali;

VISTE le Leggi Regionali n. 55 e n. 56 del 14 settembre 1994;

VISTO l'art. 3, comma 6, del D.Lgs. n. 502/1992 e successive modificazioni ed integrazioni;

IL DIRETTORE GENERALE

VISTA la suesposta relazione;

CONDIVISE le motivazioni in essa indicate e fatta propria la proposta del succitato Dirigente proponente;

ACQUISITO il parere favorevole del Direttore Amministrativo, del Direttore Sanitario e del Direttore dei Servizi Socio-Sanitari, per le parti di rispettiva competenza;

DELIBERA

1) di aggiornare il "Regolamento concernente la protezione dei dati personali", nel testo allegato al presente provvedimento per farne parte integrante e sostanziale;

2) di adottare le istruzioni operative per la gestione di eventi potenzialmente qualificabili come

violazione dei dati personali (c.d. *data breach*), delegando fin d'ora l'UOC Affari Generali e Legali alla loro integrazione e/o modificazione;

3) di confermare quale Responsabile per la protezione dei dati personali il dott. Carlo Frattin;

4) di confermare quale Referente informatico per la protezione dei dati personali il Responsabile dell'UOSD Sistemi Informativi;

5) di nominata quale Referente aziendale per la protezione dei dati personali la dott.ssa Marzia Volpato;

6) di dare atto che nessun onere deriva dall'assunzione del presente provvedimento;

7) di dichiarare il presente provvedimento esecutivo dalla data di adozione.

*****

Documento firmato digitalmente e conservato secondo la normativa vigente.

Per il parere favorevole di competenza:

Il Direttore amministrativo	Mangione Patrizia
Il Direttore sanitario	Formentini Stefano
Il Direttore dei servizi socio-sanitario	Rigoli Roberto

Il Direttore generale
Benazzi Francesco

REGIONE DEL VENETO

ULSS2 MARCA TREVIGIANA

REGOLAMENTO

CONCERNENTE LA PROTEZIONE DEI DATI PERSONALI

approvato con deliberazione n. … del …

in vigore dal …

CAPO I – DISPOSIZIONI GENERALI

CAPO II – MODELLO ORGANIZZATIVO PER LA GESTIONE DELLA PRIVACY

CAPO III – DIRITTI DELL'INTERESSATO

CAPO IV – MODALITÀ E MISURE DI TRATTAMENTO DEI DATI PERSONALI

CAPO V – DISPOSIZIONI RELATIVE A PARTICOLARI SITUAZIONI DI TRATTAMENTO

CAPO VI – DISPOSIZIONI FINALI

CAPO I – DISPOSIZIONI GENERALI

Art. 1 – Oggetto e ambito di applicazione

Il presente Regolamento disciplina la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Decreto Legislativo 30.6.2003 n. 196 “Codice in materia di protezione dei dati personali”, da ultimo modificato dal D.Lgs. 10.8.2018, n. 101, ed in conformità al Regolamento UE 27.4.2016, n. 2016/679 (di seguito anche Regolamento UE o GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Art. 2 – Finalità

L'Azienda ULSS n. 2 Marca trevigiana (di seguito Azienda) garantisce che il trattamento dei dati a tutela delle persone fisiche 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 personali, a prescindere dalla nazionalità o dalla residenza dell’interessato.
L’Azienda, in base alle specifiche attività svolte di volta in volta e alle circostanze dei rapporti giuridici di riferimento, assume il ruolo di titolare o contitolare ovvero di responsabile o sub-responsabile del trattamento dei dati; il presente regolamento si applica a prescindere dal ruolo ricoperto dalla stessa Azienda.

Art. 3 – Definizioni

Ai fini del presente Regolamento e, comunque, in sede di trattamento di dati personali da parte dell’Azienda, s’intende per:

TERMINE	DEFINIZIONE
archivio	qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
autorità di controllo	l’autorità pubblica indipendente individuata nel Garante per la protezione dei dati personali;
autorizzato al trattamento	la persona fisica autorizzata (detta anche “incaricato”) a compiere operazioni di trattamento;
comunicazione	il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall’interessato, dal rappresentante del titolare o del responsabile non stabiliti nel territorio dell’Unione europea, dalle persone autorizzate al trattamento dei dati personali sotto l’autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;
consenso dell'interessato	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;
dati anonimi	i dati che in origine, o a seguito di trattamento, non possono essere associati ad un interessato identificato o identificabile;
dati giudiziari	Ogni dato personale relativo a condanne penali o 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;

dati particolari (detti anche sensibili)	dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale dati genetici categoria particolare di 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 categoria particolare di 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 categoria particolare di 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 relativi alla vita sessuale o all'orientamento sessuale della persona
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;
diffusione	il dare conoscenza dei dati personali ad numero indeterminato di soggetti, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
interessato	la persona fisica identificata o identificabile a cui si riferiscono i dati personali;
limitazione di trattamento	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
profilazione	qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
pseudonimizzazione	il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;
punto di contatto privacy	soggetto individuato dal coordinatore / referente / delegato privacy per la gestione degli adempimenti relativi privacy nella rispettiva articolazione aziendale di riferimento;
referente aziendale	il coordinatore dell'ufficio privacy;

per la protezione dei dati personali	
referente informatico per la protezione dei dati	il soggetto che sovrintende alla gestione informatica del trattamento dei dati personali;
responsabile del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo, esterni all'organizzazione dell'Azienda, che tratta dati personali per conto del titolare 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;
titolare del trattamento	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
trattamento	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
ufficio privacy	l'articolazione aziendale competente in materia di protezione dei dati personali;
violazione dei dati personali	la violazione di sicurezza (detta anche "data breach") 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;

Art. 4 – Sistema aziendale di gestione della privacy

L'Azienda adotta, secondo il principio della responsabilizzazione (*accountability*), le misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente alla normativa vigente, tenuto conto della relativa natura, ambito di applicazione, contesto e finalità di trattamento e possibile rischio di lesione dei diritti e delle libertà delle persone fisiche.

Le misure adottate sono aggiornate periodicamente e negli ulteriori casi in cui si rendesse necessario e nel loro insieme costituiscono il sistema aziendale di gestione della privacy, che comprende:

a) modello organizzativo, secondo l'Allegato n. 1 del presente Regolamento:
   - direttore generale;
   - responsabile della protezione dei dati;
   - ufficio privacy e referente aziendale per la protezione dei dati personali;
   - servizio sistemi informativi e referente informatico per la protezione dei dati;
   - coordinatori privacy;
   - referenti privacy;
   - delegati privacy;

- punti di contatto privacy;
- autorizzati al trattamento;

b) altre misure, tra le quali:
- registro delle attività di trattamento dei dati;
- analisi dei rischi;
- valutazione preventiva dell'impatto privacy;
- misure tecniche e organizzative;
- sistema di attribuzione delle responsabilità del trattamento dei dati personali;
- rilascio delle specifiche autorizzazioni al trattamento dei dati mediante gli appositi gestionali informatici in uso nell'Azienda;
- formazione dei delegati, dei punti di contatto, dei responsabili e degli incaricati del trattamento dei dati;
- informative da fornire agli interessati;
- responsabili del trattamento.

Art. 5 – Principi applicabili al trattamento dei dati personali

Il trattamento dei dati personali è effettuato secondo i seguenti principi:

liceità correttezza trasparenza	i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
minimizzazione dei dati	i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
limitazione della conservazione	i dati devono essere 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'articolo 89, paragrafo 1, del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate a tutela dei diritti e delle libertà dell'interessato;
responsabilizzazione	il titolare del trattamento è competente per il rispetto dei principi indicati nelle precedenti lettere e deve essere in grado di comprovarlo.

Ai sensi dell'art. 6, comma 1, del GDPR il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario 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) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Inoltre i dati sono trattati in modo lecito se il trattamento rispetta:
- i presupposti e limiti stabiliti dalla normativa vigente e dalle disposizioni del Garante;
- le eventuali disposizioni contenute nei codici di deontologia e di buona condotta;

- le misure minime di sicurezza;
- le normative di settore (a titolo esemplificativo: osservanza del segreto professionale, rispetto della riservatezza in materia di interruzione della gravidanza o di tossicodipendenza o di soggetti HIV).

Ai sensi dell'art. 9, comma 1, del GDPR è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.

Ai sensi dell'art. 9, comma 2, del GDPR il divieto non si applica se si verifica uno dei seguenti casi:

a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al precedente comma;
b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento 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) il trattamento è necessario 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) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, 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) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) il trattamento è necessario 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, fatte salve le condizioni e le garanzie di cui al comma successivo;
i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, del Regolamento UE sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

I dati personali di cui all'art. 9, comma 1, del GDPR possono essere trattati per le finalità di cui al comma 2, lettera h) del medesimo articolo, se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti.

Ai sensi dell'art. 10 del GDPR il trattamento di dati giudiziari è ammesso se indispensabile per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa.

Il trattamento dei dati giudiziari, compresa la loro comunicazione, è consentito solo se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

Art. 6 – Diritto all'autodeterminazione dell'interessato al trattamento dei dati personali

L'Azienda garantisce il diritto dei cittadini-utenti all'autodeterminazione, fornendo all'interessato le informazioni previste dagli artt. 13 e 14 del Regolamento UE ed acquisendo preventivamente il consenso nei casi previsti dalla legge.

Art. 7 – Diritto all'anonimato

L'Azienda garantisce, nell'ambito dei dati di cui all'elenco del seguente comma 2, l'adempimento dell'obbligo di un trattamento dei dati non immediatamente identificativi del cittadino-utente, che si realizza, di norma, attraverso l'utilizzo di codici alfanumerici, che comunque il titolare, il delegato, il responsabile, ovvero gli incaricati a ciò specificamente autorizzati hanno la possibilità di ricondurre ad un determinato soggetto.

Il trattamento dei dati relativi alle seguenti informazioni è sottoposto ad un regime normativo di particolare tutela:
- sieropositività;
- interruzione volontaria di gravidanza;
- vittime di violenza sessuale o di pedofilia;
- uso di sostanze stupefacenti, di sostanze psicotrope e di alcool;
- parto in anonimato.

L'Azienda è impegnata a favorire fra gli operatori l'adozione di comportamenti corretti improntati alla massima attenzione e cautela nel trattamento dei sopracitati dati ipersensibili.

Art. 8 – Rispetto dei codici deontologici

L'Azienda promuove il rispetto, da parte dei propri professionisti iscritti in albi professionali, delle disposizioni contenute nei rispettivi codici deontologici.

Qualunque trattamento di dati personali deve essere effettuato in ottemperanza a quanto in essi stabilito, pena la non liceità del trattamento stesso.

Art. 9 – Mappatura dei trattamenti, analisi dei rischi e definizione delle misure di sicurezza tecniche e organizzative adeguate

In riferimento ai trattamenti svolti l'Azienda:
- mantiene aggiornati i registri di cui all'art. 30 del GDPR;
- effettuata, ove necessario, l'analisi dei rischi;
- definisce le misure tecniche e organizzative adeguate ai sensi dell'art. 32 del GDPR in base alle risultanze dell'analisi dei rischi.

Art. 10 – Valutazione d'impatto sulla protezione dei dati e consultazione preventiva del Garante

Ai sensi dell'art. 25 del GDPR l'Azienda assicura, nei casi in cui il trattamento, per la sua natura, il suo oggetto o le sue finalità, presenti rischi specifici per i diritti e le libertà degli interessati, una valutazione preventiva dell'impatto derivante sulla privacy degli interessati fin dalla progettazione del relativo processo aziendale (*data protection by default and by design*).

Nei casi previsti dall'art. 35 del GDPR la valutazione d'impatto sulla protezione dei dati verte, in particolare, sulle misure di sicurezza, sulle garanzie e sui meccanismi previsti per assicurare la protezione dei dati personali e per comprovare il rispetto della normativa vigente in materia.

Nei casi previsti dall'art. 36 del GDPR l'Azienda, prima di procedere al trattamento, consulta il Garante per la privacy qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

Art. 11 – Politiche di accesso alle banche dati e profili di autorizzazione

Nel rispetto del principio di necessità e pertinenza del trattamento dei dati personali, i profili di accesso ai gestionali informatici aziendali sono configurati sulla base delle attività affidate a ciascun soggetto autorizzato e nel rispetto degli ambiti di trattamento consentiti.

Per ciascuna banca dati (applicativo informatico) deve essere definito l'elenco dei profili di accesso e le loro specificità.

Le finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria (a titolo esemplificativo: prenotazione e pagamento di una prestazione) devono essere realizzate garantendo il principio della necessità del trattamento, e quindi precludendo, per quanto possibile, l'accesso al personale amministrativo alle informazioni sanitarie, mediante la previsione di profili diversi di abilitazione in funzione della diversa tipologia di operazioni consentite.

In ogni caso gli accessi ai dati personali contenuti nei data base aziendali devono essere ridotti allo stretto necessario per consentire l'espletamento delle ordinarie attività lavorative. Il trattamento dei dati deve, pertanto, essere evitato ogni volta in cui lo stesso non sia indispensabile per il perseguimento degli scopi prefissati.

I profili di autorizzazione del personale autorizzato al trattamento vengono periodicamente aggiornati dai soggetti che li hanno originariamente attribuiti.

Al fine di garantire che il trattamento dei dati inerenti allo stato di salute degli interessati sia effettuato con un idoneo livello di sicurezza, gli accessi ai software clinici devono essere tracciati.

Art. 12 – Comunicazione di dati a terzi

L'Azienda effettua la comunicazione di dati personali a terzi, pubblici e privati, solo in conformità a quanto previsto dalle vigenti disposizioni legislative e regolamentari in materia.

Nell'ipotesi in cui la comunicazione sia espressamente consentita da specifica disposizione di legge o di regolamento, l'Azienda evita il trattamento dei dati personali quando le finalità da perseguire nei singoli casi possono essere realizzate mediante l'utilizzo di dati anonimi o ricorrendo ad opportune tecniche di crittografia.

CAPO II – MODELLO ORGANIZZATIVO PER LA GESTIONE DELLA PRIVACY

Art. 13 – Direttore generale

Il Titolare del trattamento dei dati personali ai sensi e per gli effetti di legge è l'Azienda ULSS n. 2 Marca trevigiana.

Il Direttore generale, quale legale rappresentante dell'Azienda, avvalendosi se del caso del Responsabile della protezione dei dati, dell'Ufficio privacy e del Referente informatico per la protezione dei dati, provvede a:

a) approvare il Regolamento concernente la protezione dei dati personali;
b) approvare il modello organizzativo di cui all'art. 4;
c) nominare il Responsabile per la protezione dei dati, come stabilito dall'art. 37 del GDPR;
d) nominare il Referente aziendale per la protezione dei dati personali;
e) nominare il Referente informatico per la protezione dei dati;
f) nominare i Coordinatori privacy, i Referenti privacy e i Delegati privacy, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il

trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;

g) nominare i responsabili del trattamento ai sensi dell'art. 28 del Regolamento UE;
h) sottoscrivere gli accordi di contitolarità ai sensi dell'art. 26 del Regolamento UE;
i) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
j) mettere in atto le misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente ai principi del Regolamento UE.

Art. 14 – Responsabile della protezione dei dati

L'Azienda provvede alla nomina del Responsabile della protezione dei dati (RPD) in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa, delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti stabiliti per legge.

Il Responsabile della protezione dei dati deve:
- adempiere le proprie funzioni in piena indipendenza e in assenza di conflitti di interesse (in linea di principio, non può trattarsi di soggetto che ricopra ruoli gestionali e che decida sulle finalità o sugli strumenti del trattamento di dati personali);
- operare alle dipendenze del Titolare oppure sulla base di un contratto di servizio;
- disporre di risorse umane e finanziarie, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Responsabile della protezione dei dati provvede in particolare a:
a) informare e fornire consulenza al Titolare del trattamento e ai soggetti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE nonché da altre disposizioni relative alla protezione dei dati;
b) sorvegliare l'osservanza del Regolamento UE, di altre disposizioni relative alla protezione dei dati nonché delle politiche del Titolare 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 del Regolamento UE;
d) cooperare con il Garante per la protezione dei dati;
e) fungere da punto di contatto per il Garante per la privacy per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento UE, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il Responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.

Il Titolare del trattamento pubblica i dati di contatto del Responsabile della protezione dei dati e li comunica al Garante per la protezione dei dati.

Gli interessati possono contattare il Responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti.

Art. 15 – Ufficio privacy e Referente aziendale per la protezione dei dati personali

L'Azienda provvede, se del caso, alla nomina del Referente aziendale per la protezione dei dati personali in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa, delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti stabiliti per legge.

Il Referente aziendale per la protezione dei dati personali, che coordina l'Ufficio privacy, si avvale della collaborazione del Referente informatico per la protezione dei dati per l'esecuzione degli adempimenti in materia di privacy in relazione alla specifica competenza.

Il Referente aziendale per la protezione dei dati personali svolge in particolare i seguenti compiti:

a) informa e fornisce consulenza al Titolare, ai Coordinatori privacy, ai Referenti privacy e ai Delegati privacy nonché ai dipendenti che eseguono il trattamento per quanto riguarda gli adempimenti derivanti dalla normativa in materia di riservatezza e protezione dei dati personali;
b) aggiorna il registro dei trattamenti sulla base delle informazioni fornite dai Coordinatori privacy, Referenti privacy e Delegati privacy;
c) tiene i rapporti con il Responsabile della protezione dei dati ed eventualmente con il Garante per la protezione dei dati personali;
d) effettua, di concerto con il Servizio Sistemi Informativi aziendale, per la parte di competenza, l'analisi dei rischi e predispone la valutazione d'impatto sulla protezione dei dati, nei casi ritenuti necessari;
e) predispone i modelli documentali, le informative, le istruzioni operative e le procedure necessarie per l'osservanza della disciplina in materia di protezione dei dati personali;
f) vigila sull'osservanza del Regolamento UE, nonché delle politiche del Titolare in materia di protezione dei dati personali, comprese l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa al trattamento ed alle connesse attività di controllo;
g) cura la costituzione e l'aggiornamento degli archivi sotto specificati, sulla base dei dati forniti dai Coordinatori privacy, Referenti privacy e Delegati privacy, nonché dalla struttura deputata alla gestione delle risorse umane, i quali hanno la piena e completa responsabilità in merito a informazioni di dati deficitari o totalmente mancanti:
   - censimento dei trattamenti dei dati personali;
   - elenco dei responsabili dei trattamenti, anche esterni, con i relativi recapiti;
   - elenco degli archivi cartacei con indicazione delle rispettive sedi e caratteristiche;
   - elenco delle banche dati personali informatiche custodite dall'Azienda, con indicazione delle rispettive sedi e caratteristiche fornite dal Referente informatico per la protezione dei dati;
h) effettua i necessari approfondimenti per l'applicazione della normativa in materia di protezione dei dati personali, anche mediante la costituzione di appositi gruppi di lavoro.
i) predispone e propone al direttore della struttura complessa di riferimento le procedure, le istruzioni operative ed ogni altro atto per la successiva approvazione mediante apposita determinazione.

Art. 16 – Servizio Sistemi Informativi e Referente informatico per la protezione dei dati personali

L'Azienda provvede, se del caso, alla nomina del Referente informatico per la protezione dei dati in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa, delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti stabiliti per legge.

Il Referente informatico per la protezione dei dati svolge in particolare i seguenti compiti:
a) collabora con il Referente aziendale per la protezione dei dati personali, nonché con i Coordinatori privacy, i Referenti privacy e i Delegati privacy nell'assolvimento delle funzioni per gli aspetti di propria competenza;
b) predispone e cura l'attuazione di quanto necessario in merito agli aspetti della sicurezza informatica dei trattamenti con strumenti elettronici;
c) effettua, di concerto con l'Ufficio Privacy aziendale, per la parte di competenza, l'analisi dei rischi e predispone la valutazione d'impatto sulla protezione dei dati, nei casi ritenuti necessari;
d) cura i rapporti con i soggetti ai quali l'Azienda ha affidato la gestione delle reti informative e delle tecnologie informatiche, al fine di garantire che le procedure informatiche siano conformi alla normativa in materia di protezione dei dati personali;
e) cura la tenuta dell'elenco delle banche dati informatiche custodite dall'Azienda, con indicazione delle rispettive sedi e caratteristiche;
f) cura la tenuta dell'elenco dei soggetti abilitati a ciascun applicativo secondo i profili di autorizzazione istituiti.

Art. 17 – Coordinatori privacy, Referenti privacy e Delegati privacy

In considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di garantire a tutti i livelli l'osservanza della vigente normativa in materia di privacy, il Direttore generale, in base all'organizzazione stabilita dal vigente Atto Aziendale, con il presente Regolamento individua quali Coordinatori privacy, Referenti privacy e Delegati privacy, in relazione alle funzioni di specifica competenza derivanti dal rapporto giuridico esistente con la stessa Azienda, i seguenti soggetti:
a) Coordinatori privacy:
   - Direttore amministrativo;

- Direttore sanitario;
- Direttore dei servizi socio-sanitari;

b) Referenti privacy:
- Direttori medici di ospedale;
- Direttori di distretto;
- Direttore del dipartimento di prevenzione;

c) Delegati privacy:
- Direttori medici di ospedale;
- Direttori di distretto;
- Direttori di unità operativa complessa;
- Responsabili di unità operativa a valenza dipartimentale;
- Responsabili di unità operativa in staff alla Direzione aziendale;
- Dirigenti che svolgono attività libero professionale intramuraria;
- Sperimentatori principali o responsabili di studi clinici o osservazionali.

I Coordinatori privacy provvedono a:
a) svolgere i compiti attribuiti dal Titolare;
b) nominare il punto di contatto privacy;
c) svolgere i compiti dei delegati privacy negli ambiti di propria diretta afferenza;
d) vigilare sull'operato dei Referenti privacy della rispettiva area funzionale;
e) svolgere le funzioni dei Referenti privacy per gli ambiti che ne siano sprovvisti.

I Referenti privacy provvedono a:
a) svolgere i compiti attribuiti dal Titolare;
b) svolgere i compiti dei delegati privacy negli ambiti di propria diretta afferenza;
c) vigilare l'operato dei Delegati privacy della rispettiva struttura tecnico funzionale (ospedali, distretti, dipartimento di prevenzione);
d) svolgere le funzioni dei Delegati privacy per gli ambiti che ne siano sprovvisti.

I Delegati privacy provvedono a:
a) svolgere i compiti attribuiti dal Titolare o dal soggetto che li ha nominati;
b) nominare il punto di contatto privacy;
c) definire l'ambito di operatività e le istruzioni operative necessarie degli autorizzati al trattamento dei dati personali secondo la procedura aziendale in uso;
d) vigilare sull'operato del personale autorizzato della rispettiva articolazione funzionale;
e) trattare i dati personali osservando le disposizioni di legge e regolamentari, nonché le specifiche istruzioni impartite dal Titolare;
f) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
g) garantire che, presso la propria struttura, le persone autorizzate al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;
h) tenendo conto della natura del trattamento, assistere il Titolare del trattamento nelle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto dalla normativa vigente;
i) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente;
j) contribuire alle attività di verifica del rispetto degli obblighi in materia, comprese le ispezioni, realizzate dal Titolare del trattamento o da altro soggetto da questi incaricato;
k) verificare che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, nonché i profili di autorizzazione dei soggetti autorizzati al trattamento dei dati rispondano ai principi di necessità, pertinenza e non eccedenza;
l) verificare che all'interessato o al soggetto presso il quale sono raccolti i dati sia data l'informativa;
m) verificare che l'interessato o altro soggetto legittimato presti, quando previsto, il consenso al trattamento dei dati;
n) disporre, se del caso, che il personale presente nella propria struttura sia individuato quale soggetto

autorizzato del trattamento, fornendo al riguardo le istruzioni necessarie;
o) fornire al Responsabile per la protezione dei dati e al Referente aziendale per la protezione dei dati personali ogni informazione e notizia rilevante ai fini degli obblighi in materia;
p) ottemperare ad ogni altro adempimento stabilito dal Titolare in relazione al trattamento dei dati personali;
q) collaborare con il Referente aziendale per la protezione dei dati personali e con il Referente informatico per la protezione dei dati nell'espletamento dei rispettivi compiti al fine di:
   - predisporre e aggiornare il registro delle attività di trattamento del titolare / contitolare e del responsabile / sub responsabile;
   - predisporre le misure di sicurezza tecniche e organizzative adeguate per la protezione dei dati, vigilando sulla loro applicazione;
   - segnalare i casi in cui a seguito di attacchi informatici, accessi abusivi, incidenti o eventi avversi come incendi o altre calamità, si dovessero verificare la perdita, la distruzione o la diffusione indebita di dati personali trattati nel rispetto dei provvedimenti del Garante (*data-breach*);
r) sottoscrivere le nomine a responsabile del trattamento ex art. 28 GDPR in relazione ai contratti che ha il potere di sottoscrivere;
s) sottoscrivere gli accordi di contitolarità ex art. 26 GDPR in relazione ai contratti che ha il potere di sottoscrivere;
t) verificare periodicamente che la documentazione adottata in materia di protezione dei dati personali rispecchi i trattamenti effettivamente svolti;
u) segnalare al Servizio Formazione e all'Ufficio Privacy le necessità formative in materia di protezione dei dati personali, collaborando nella relativa organizzazione.

I Delegati privacy rispondono al Direttore Generale di ogni violazione o mancata attivazione di quanto previsto dalla vigente normativa in materia di privacy e dalle istruzioni ricevute, ivi comprese quelle riguardanti l'adozione delle misure di sicurezza.

La funzione di Delegato privacy non è a sua volta delegabile. In caso di assenza o impedimento del Delegato privacy le relative attribuzioni sono esercitate da chi lo sostituisce per le attività di istituto.

Ai fini dell'individuazione da parte del Direttore generale dei Coordinatori privacy, Referenti privacy e Delegati privacy, la struttura competente alla gestione del personale del presente articolo provvede a:
d) predisporre il contratto di lavoro o di incarico, l'atto di autorizzazione all'esercizio della libera professione intramuraria o l'atto di autorizzazione allo svolgimento dello studio clinico o osservazionale mediante l'inserimento di un'apposita clausola che specifichi l'individuazione del soggetto quale Coordinatore privacy, Referente privacy e Delegato privacy in relazione alle funzioni di competenza derivanti dal rapporto giuridico esistente con l'Azienda o dall'atto di autorizzazione;
e) comunicare al Servizio Sistemi Informativi ogni spostamento interno, cessazione o altra variazione del predetto rapporto giuridico o dell'atto di autorizzazione, che incida sulla figura di Coordinatore privacy, Referente privacy e Delegato privacy, per il blocco delle specifiche autorizzazioni precedentemente rilasciate per il trattamento dei dati.

Per coloro che – alla data di entrata in vigore del presente Regolamento – ricoprono già una delle funzioni indicate dal comma 1 del presente articolo, l'individuazione quali Coordinatori privacy, Referenti privacy e Delegati privacy s'intende formalizzata e regolarizzata ad ogni conseguente effetto di legge con apposita comunicazione mediante l'utilizzo del gestionale informatico per il personale dipendente e convenzionato – funzionalità "Angolo del dipendente" o altra modalità equivalente.

Art. 18 – Punti di contatto privacy

I Coordinatori privacy, i Referenti privacy e i Delegati privacy individuano uno o più Punti di contatto privacy tra il personale afferente alle proprie strutture di direzione.

Il Punto di contatto per il trattamento dei dati provvede a:
a) collaborare per la predisposizione e l'aggiornamento del registro delle attività di trattamento del titolare / contitolare e del responsabile / sub responsabile;
b) supportare il soggetto che lo ha nominato nelle funzioni di vigilanza;
c) segnalare al Referente aziendale per la protezione dei dati personali la necessità di predisporre una nuova modulistica o di aggiornare quella esistente, collaborando con lo stesso a tale scopo;

d) segnalare al Referente aziendale per la protezione dei dati personali la necessità di predisporre una valutazione d'impatto sulla protezione dei dati personali e/o collaborare nella predisposizione della stessa e nell'espletamento degli obblighi correlati;
e) collaborare con il Referente aziendale per la protezione dei dati personali e con il Servizio Sistemi Informativi nell'effettuazione dell'analisi dei rischi;
f) conservare e mettere a disposizione del personale afferente al proprio ambito la documentazione predisposta dal Referente aziendale per la protezione dei dati personali;
g) fungere da punto di riferimento del personale afferente al proprio ambito per l'applicazione della documentazione fornita dal Referente aziendale per la protezione dei dati personali.

Art. 19 – Personale autorizzato al trattamento dei dati

Il Titolare, i Coordinatori privacy, i Referenti privacy e i Delegati privacy possono autorizzare persone fisiche al trattamento dei dati personali sotto la propria responsabilità.

In considerazione della complessità e della molteplicità delle proprie funzioni istituzionali e della necessità di garantire a tutti i livelli l'osservanza della vigente normativa in materia di privacy, l'Azienda quale Titolare con il presente Regolamento individua quale personale autorizzato al trattamento dei dati tutto il personale che abbia con la stessa un rapporto giuridico di lavoro, di collaborazione, di consulenza, di prestazione d'opera professionale o di altra tipologia per lo svolgimento di attività istituzionali, in relazione alle funzioni di specifica competenza derivanti dai predetti rapporti giuridici, fornendo al riguardo le istruzioni necessarie.

I Coordinatori privacy, i Referenti privacy e i Delegati privacy dispongono, se del caso, che l'ulteriore personale presente nella propria struttura sia individuato quale personale autorizzato, fornendo al riguardo le istruzioni necessarie.

L'ambito di operatività del trattamento dei dati da parte del personale autorizzato è individuato dai Coordinatori privacy, dai Referenti privacy e dai Delegati privacy mediante l'utilizzo dei gestionali in uso nell'Azienda.

Il personale autorizzato ha accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti istituzionali di propria competenza.

Il personale autorizzato al trattamento dei dati, che svolge attività di supporto all'esercizio dell'attività libero professionale intramuraria del personale dirigenziale, potrà procedere al trattamento dei dati secondo le specifiche autorizzazioni già in possesso per lo svolgimento delle attività istituzionali.

Durante il trattamento od in caso di allontanamento dal posto di lavoro, il personale autorizzato deve adottare le misure previste e a propria disposizione, secondo le istruzioni ricevute dal Titolare, per evitare l'accesso non autorizzato da parte di terzi, anche se dipendenti, ai dati personali trattati o in trattamento.

Anche il personale autorizzato che non è tenuto per legge al segreto professionale, è sottoposto al rispetto di regole di condotta analoghe al segreto professionale e all'assunzione di comportamenti metodologicamente corretti in materia di riservatezza e di protezione dei dati.

Ai fini dell'individuazione del personale autorizzato al trattamento dei dati la struttura competente alla gestione del personale del presente articolo provvede a:
a) predisporre il contratto di lavoro o di incarico mediante l'inserimento di un'apposita clausola che specifichi l'individuazione del soggetto quale persona autorizzata al trattamento dei dati in relazione alle funzioni di competenza derivanti dal rapporto giuridico esistente con l'Azienda;
b) comunicare al Servizio Sistemi Informativi ogni spostamento interno, cessazione o altra variazione del predetto rapporto giuridico, che incida sulla figura del personale autorizzato, per il blocco delle specifiche autorizzazioni precedentemente rilasciate per il trattamento dei dati.

Per coloro che – alla data di entrata in vigore del presente Regolamento – risultano avere già in atto un rapporto giuridico con l'Azienda, l'individuazione quale personale autorizzato al trattamento dei dati s'intende formalizzata e regolarizzata ad ogni conseguente effetto di legge con apposita comunicazione mediante l'utilizzo del gestionale informatico per il personale dipendente e convenzionato – funzionalità

"Angolo del dipendente" o altra modalità equivalente.

Art. 20 – Obblighi delle persone che operano all'interno dell'Azienda

Tutte le persone che funzionalmente svolgono operazioni di trattamento di dati all'interno dell'Azienda a qualsiasi titolo, con o senza retribuzione, compresi a titolo esemplificativo 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 individuati dai competenti Coordinatori privacy, Referenti privacy e Delegati privacy quali soggetti autorizzati al trattamento dei dati, fornendo al riguardo le istruzioni necessarie.

CAPO III – DIRITTI DELL'INTERESSATO

Art. 21 – Informativa

Le informative sul trattamento dei dati personali devono essere predisposte in modo chiaro e comprensibile per fornire all'interessato tutte le informazioni necessarie relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile.

L'informativa sul trattamento dei dati personali riporta le informazioni previste dagli articoli 13 e 14 del regolamento UE relativamente a:

a) l'identità e i dati di contatto del Titolare del trattamento e del Responsabile per la protezione dei dati;
b) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
c) le modalità di trattamento dei dati personali;
d) l'obbligatorietà o meno del conferimento dei dati;
e) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
f) coloro ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
g) come possono essere esercitati i diritti di accesso in base alle disposizioni vigenti;
h) l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento l'accesso ai dati personali e la rettifica del trattamento che lo riguarda o di opporsi al loro trattamento;
i) qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio di consenso al trattamento, il diritto di revocarlo in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
j) il diritto di proporre reclamo al Garante per la privacy;
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) l'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;
m) nel caso in cui i dati personali non siano stati ottenuti 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.

L'informativa all'interessato viene resa anche per estratto tramite l'affissione di appositi manifesti o la somministrazione di appositi documenti nei locali di accesso all'utenza.

L'informativa sul trattamento dei dati personali non viene fornita all'interessato da parte dell'Azienda nel caso in cui lo stesso interessato disponga già delle suindicate informazioni o nel caso in cui comunicarle risulti impossibile o implicherebbe uno sforzo sproporzionato, in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, purché in tali casi siano state adottate preventivamente misure tecniche e organizzative adeguate per la protezione dei dati specie al fine di garantire il rispetto del principio della minimizzazione dei dati, e ulteriori misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato.

Le informazioni sono fornite per iscritto o con altri mezzi, anche – se del caso – con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con

altri mezzi l'identità dell'interessato.

Art. 22 – Diritti dell'interessato

L'interessato ha il diritto di ottenere dall'Azienda la conferma che sia o meno in corso un trattamento di dati personali che lo riguarda e, in tal caso, ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi od organizzazioni internazionali;
d) il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo al Garante per la privacy;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'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.

L'interessato ha il diritto di ottenere dall'Azienda la rettifica dei dati personali inesatti che lo riguardano, l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa, nonché il loro aggiornamento.

L'interessato, nell'esercizio dei diritti sopra riportati può conferire per iscritto, delega o procura a persone fisiche o ad associazioni.

I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chiunque abbia legittimo interesse, documentato nelle forme di legge, anche mediante delega o procura a persone fisiche o ad associazioni, conferita per iscritto e nelle forme di legge.

Gli interessati possono contattare il Responsabile per la protezione dei dati per tutte le questioni relative al trattamento dei propri dati personali e all'esercizio dei propri diritti.

Art. 23 – Diritto di opposizione

L'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano e l'Azienda si astiene dal trattarli ulteriormente salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, diritti e libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici l'interessato ha il diritto di opporsi al trattamento di dati personali che lo riguarda, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico

Art. 24 – Diritto di accesso alla documentazione e diritto alla riservatezza

L'Azienda, in osservanza delle disposizioni vigenti in tema di riservatezza e di trasparenza, valuta anche con riguardo ad altre regolamentazioni specifiche, caso per caso, la possibilità degli interessati di accedere ai documenti.

Quando il trattamento concerne dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, l'accesso ai relativi dati è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Art. 25 – Diritto di accesso generalizzato

Nel caso in cui nel corso della procedura di accesso civico ai sensi del D.Lgs. n. 33/2013 venissero in evidenza problematiche connesse alla tutela della privacy di soggetti terzi, l'accesso civico generalizzato deve essere rifiutato laddove possa arrecare un pregiudizio concreto alla protezione dei dati personali in conformità con la disciplina legislativa in materia.

Il Coordinatore privacy, il Referente privacy e il Delegato privacy interessato dall'accesso civico generalizzato, sentito – se del caso – il Responsabile per la trasparenza, dovrà operare la valutazione caso per caso al fine di verificare la sussistenza o meno del pregiudizio nel rispetto della normativa di settore, in particolare delle Linee Guida adottate dall'Autorità Nazionale Anticorruzione d'intesa con il Garante di cui alla delibera n. 1309 del 28/12/2016.

Art. 26 – Comunicazione di dati all'interessato

I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato solo attraverso:
a) la consegna dei dati al medico di fiducia che, a sua volta, li renderà noti all'interessato;
b) una spiegazione orale o un giudizio scritto da parte di un medico del servizio dell'Azienda o, su delega, da parte di operatore sanitario dello stesso servizio;
c) modalità telematiche nei casi e nei modi previsti dalla specifica normativa.

La documentazione sanitaria che viene consegnata in busta chiusa può essere ritirata dall'interessato o da altra persona diversa da questo delegata, salvo il caso di documenti relativi a dati regolati da normative speciali che prevedono il ritiro diretto dell'interessato.

CAPO IV – MODALITÀ E MISURE DI TRATTAMENTO DEI DATI PERSONALI

Art. 27 – Responsabile del trattamento dei dati

I soggetti che, per esigenze organizzative dell'Azienda e in funzione del perseguimento dei suoi fini istituzionali e in base a uno specifico rapporto giuridico, effettuano con utilizzazione della propria organizzazione o di quella dell'Azienda stessa trattamenti di dati per conto di quest'ultima, sono nominati responsabili del trattamento, in conformità a quanto previsto dall'art. 28 del Regolamento UE.

La nomina a Responsabile del trattamento è effettuata dal Titolare. A tal fine le strutture aziendali secondo le rispettive competenze predispongono l'atto di nomina a Responsabile del trattamento, allegandolo se del caso alla deliberazione con la quale si approva lo schema contrattuale o di convenzione. L'atto di nomina sarà perfezionato contestualmente alla sottoscrizione del contratto o della convenzione.

La sottoscrizione dell'atto di nomina e l'impegno a rispettare le disposizioni della normativa di settore è condizione essenziale per l'inizio dello specifico rapporto giuridico tra le parti.

Le strutture aziendali competenti per la gestione del contratto o della convenzione devono provvedere all'applicazione di quanto disciplinato nel presente Regolamento, adeguando, se necessario, anche mediante apposito atto aggiuntivo, i contratti o le convenzioni in essere ai sensi del presente Regolamento e della normativa vigente.

Nei contratti di affidamento di attività o di servizi all'esterno dell'Azienda è inserita un'apposita clausola di garanzia con cui il soggetto affidatario, individuato Responsabile del trattamento dei dati, si impegna, nel trattamento dei dati personali effettuati in forza del rapporto contrattuale, all'osservanza delle norme vigenti in materia di privacy e di quanto disposto dall'Azienda.

Inoltre, qualora tra le attività oggetto del contratto o della convenzione rientrino le funzioni proprie dei cd. amministratori di sistema, di cui al provvedimento del Garante del 27/11/2008, la suddetta clausola deve essere opportunamente integrata con l'impegno ad osservare le disposizioni del Garante in materia di Amministratori di Sistema conservando direttamente e specificatamente gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema fornendo il relativo elenco al Titolare.

Rientra nella figura di amministratore di sistema il soggetto professionale dedicato alla gestione e alla manutenzione di impianti di elaborazione con i quali vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza nella misura in cui consentano di intervenire sui dati personali.

Il Responsabile del trattamento, in particolare, si impegna a:

a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa in materia di privacy;
b) trattare i dati personali, anche di natura sensibile e giudiziaria, dei pazienti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con l'Azienda e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
c) rispettare i principi in materia di sicurezza dettati dalla normativa vigente in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
d) adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del Regolamento UE;
e) nominare, al proprio interno, i soggetti autorizzati al trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
f) attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a), del Regolamento UE;
g) specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati;
h) assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento UE (sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
i) su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
j) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento UE e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Il Responsabile del trattamento risponde dell'attività di trattamento in termini di corretto adempimento delle prestazioni ai sensi degli artt. 1218 e 1223 del Codice Civile.

Art. 28 – Registro delle attività di trattamento dei dati personali

L'Azienda tiene un registro delle attività di trattamento svolte sotto la propria responsabilità, periodicamente aggiornato, che evidenzia i diversi livelli di responsabilità attribuiti in relazione al trattamento dei dati e contiene almeno le seguenti informazioni:

a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del Responsabile della protezione dei dati;
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 al secondo comma dell'articolo 49 del Regolamento UE, 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.

Il registro è tenuto in formato elettronico e, su richiesta, viene messo a disposizione del Garante per la protezione dei dati personali.

Ogni Responsabile del trattamento tiene un registro di tutte le categorie di attività relative ai trattameni svolti per conto di un Titolare del trattamento.

Art. 29 – Sicurezza del trattamento

L'Azienda, quale titolare del trattamento, è tenuta ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati e amministrazione digitale, ogni misura di sicurezza necessaria per assicurare un livello adeguato di sicurezza dei dati personali trattati.

A tal fine, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, l'Azienda mette in atto misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio.

Le misure comprendono, tra le altre, se del caso:
a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente disponibilità e accesso dei dati personali in caso di incidente.

Nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

L'accesso ad ogni procedura informatica è consentito solo se congruente con il trattamento di dati per il quale il soggetto è stato precedentemente autorizzato al trattamento ed è consentito soltanto utilizzando apposite credenziali di autorizzazione composte da un user-id, attribuito dal competente amministratore di sistema aziendale, e da una password.

La password è strettamente personale e a nessun titolo può essere comunicata a terzi; della sua riservatezza risponde personalmente il singolo incaricato del trattamento dei dati personali.

Art. 30 – Misure di sicurezza per i trattamenti di dati affidati a soggetti esterni

I Responsabili e gli eventuali Sub-Responsabili del trattamento, previamente autorizzati per iscritto dal Titolare, sono tenuti ad assicurare a quest'ultimo di aver adottato, prima di effettuare attività di trattamento di dati, ogni misura di sicurezza prevista dalla normativa vigente in tema di protezione di dati e amministrazione digitale.

Tali soggetti sono comunque tenuti a:
a) assicurare il rispetto delle specifiche istruzioni operative impartite dall'Azienda per la tenuta in sicurezza dei dati oggetto di affidamento e di aver ulteriormente attivato ogni altra misura idonea alla protezione dei dati loro affidati;
b) comunicare all'Azienda le procedure adottate per la sicurezza dei dati con riferimento, tra l'altro, a:
   - l'attività svolta e le misure di sicurezza adottate;
   - l'elenco degli incaricati del trattamento e l'indicazione della sede presso la quale le relative autorizzazioni sono custodite;
   - l'elenco delle risorse hardware e software;
   - le procedure di continuità operativa ed emergenza adottate;
   - le misure di eventuale recupero da disastro adottate;
   - le misure adottate di back-up degli specifici sistemi informativi aziendali utilizzati per i trattamenti autorizzati, di contenimento dei virus / malware informatici, e altre misure, comprese quelle di

eventuale conservazione sostitutiva;
- le eventuali criticità che potrebbero costituire occasione di accesso non consentito o perdita / manomissione del patrimonio informativo gestito per conto dell'Azienda;
- le misure adottate per la cifratura o la separazione dei dati relativi alla salute;
- le misure adottate per la gestione delle disposizioni in tema di amministratori di sistema;
- le verifiche periodiche sul mantenimento in sicurezza che sono state adottate, con la relativa documentazione.

Il mancato rispetto da parte del Responsabile del trattamento dell'adozione delle misure di sicurezza adeguate a prevenire o contenere i rischi che possono riguardare i dati oggetto dell'affidamento può costituire titolo per la risoluzione per giusta causa del rapporto sottostante e per chiedere il risarcimento dei danni subiti.

Art. 31 – Tenuta in sicurezza dei documenti e degli archivi

Gli archivi che custodiscono i dati di cui l'Azienda è Titolare del trattamento, cartacei e digitali, devono essere collocati in locali non esposti a rischi ambientali in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo aziendale in tema di continuità operativa, conservazione sostitutiva e *disaster recovery*.

La documentazione archiviata, anche digitalmente, che riporta dati personali è conservata soltanto per il tempo previsto dalla legge e poi sottoposta a scarto di archivio o cancellata definitivamente.

Il Coordinatore privacy, il Referente privacy, il Delegato privacy e il Responsabile del trattamento attivano, attenendosi alle disposizioni e alle procedure aziendali vigenti, i meccanismi necessari a garantire l'accesso selezionato ai dati e l'accesso controllato ai locali dove questi sono collocati mediante registrazione degli accessi ed esclusione degli stessi fuori dell'orario di servizio dell'archivio medesimo.

I supporti, diversi dal materiale cartaceo, contenenti dati personali (supporti informatici, magnetici, videoregistrazioni effettuate nell'ambito dell'attività clinica, bobine di microfilm, immagini iconografiche, altro) debbono essere conservati e custoditi con le modalità indicate per gli archivi cartacei, se non diversamente stabilito, nei modi e termini previsti dalla normativa vigente.

Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Coordinatore privacy, Referente privacy, Delegato privacy e del Responsabile del trattamento dei dati di competenza, che devono assicurarne la riservatezza, protezione ed integrità per tutto il tempo in cui ne mantiene la disponibilità.

Per quanto riguarda la documentazione cartacea facente parte dell'archivio aziendale storico e/o di deposito, l'Azienda predispone periodicamente un piano di scarto d'archivio.

Relativamente agli archivi informatizzati di dati l'Azienda adotta, facendo seguito alle disposizioni vigenti in tema di protezione dei dati e amministrazione digitale, idonee procedure di:
- salvataggio periodico degli archivi di dati personali;
- misure di contenimento dei virus / maleware informatici e di protezione perimetrale da cyber attacchi alle infrastrutture ICT aziendali;
- disaster recovery e continuità operativa;
- conservazione sostitutiva.

Art. 32 – Limiti alla conservazione dei dati personali

L'Azienda provvede all'adozione di apposite misure e procedure attraverso le quali:
- procedere alla distruzione dei dati personali, una volta terminato il limite minimo di conservazione dei documenti analogici e digitali e dei dati personali in questi riportati;
- smaltire gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare l'Azienda;
- assicurare che il riutilizzo degli apparati di memoria o hardware sia effettuato con modalità da garantire che non sia possibile accedere ad alcun dato personale di cui è titolare l'Azienda.

Art. 33 – Trasferimento di dati personali all'estero

Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il Titolare del trattamento e il Responsabile del trattamento rispettano le condizioni stabilite dal Regolamento UE, al fine di assicurare che il livello di protezione delle persone fisiche garantito dal medesimo Regolamento UE non sia pregiudicato.

Art. 34 – Violazione dei dati personali

Il Titolare adotta le istruzioni operative per la gestione di eventi potenzialmente qualificabili come violazione dei dati personali (*data breach*).

Tutti i soggetti che operano all'interno dell'Azienda o per conto della stessa sono tenuti all'osservanza delle predette istruzioni operative, informando tempestivamente i soggetti di riferimento senza ingiustificato ritardo in caso di una violazione dei dati personali.

L'Azienda provvede a notificare, avvalendosi della collaborazione del Responsabile per la protezione dei dati e del Referente aziendale privacy, la violazione al Garante per la protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà degli interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.

Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente.

La notifica della violazione dei dati personali deve almeno:
a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del Responsabile per la protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire contestualmente le informazioni, queste possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio; tale documentazione consente al Garante per la protezione dei dati personali di verificare il rispetto delle disposizioni di legge.

CAPO V – DISPOSIZIONI RELATIVE A PARTICOLARI SITUAZIONI DI TRATTAMENTO

Art. 35 – Uso di strumenti di videosorveglianza e videocontrollo

L'installazione di apparecchiature di videosorveglianza è autorizzata dal Titolare, previo accordo con le organizzazioni sindacali, solo quando ciò sia strettamente indispensabile per la sicurezza delle persone e delle attrezzature (controllo di corridoi, di sale di attesa, di spazi esterni, di porte di accesso agli edifici, altro) e non siano attuabili o sufficienti altre misure di sorveglianza.

Il trattamento dei dati personali con le apparecchiature di cui al comma 1 è effettuato nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori e delle prescrizioni del Garante per la privacy.

Il Titolare adotta specifico regolamento sulle modalità di trattamento dei dati raccolti con le apparecchiature di videosorveglianza, sulle misure di sicurezza da osservare, e predispone la relativa informativa da fornire agli utenti, agli operatori e alle altre persone che a qualsiasi titolo accedono agli spazi sorvegliati, in relazione alle finalità e alla tipologia del sistema di sorveglianza.

L'attività di videocontrollo (visione *in live*), che si distingue rispetto alle attività di videosorveglianza propriamente dette, ha particolari finalità, come a titolo esemplificativo quella relativa alla sorveglianza remota di pazienti ricoverati, per esclusive finalità di cura e tutela della salute. Possono accedere alle immagini rilevate per le predette finalità solo i soggetti autorizzati.

Tale attività non prevede ordinariamente la registrazione di immagini. L'attività di videocontrollo sarà indicata nell'informativa prestata al paziente nonché nell'informativa breve affissa nei locali interessati.

Le modalità di accesso alle riprese video da parte di terzi legittimati (familiari, parenti, conoscenti) di ricoverati in reparti dove non sia consentito agli stessi di recarsi personalmente devono in ogni caso consentire mediante adeguati accorgimenti tecnici la sola visione dell'immagine del proprio congiunto o conoscente.

Le immagini idonee a rilevare lo stato di salute non devono essere diffuse.

Art. 36 – Fascicolo sanitario elettronico e dossier sanitario elettronico

Il fascicolo sanitario elettronico (FSE) e il dossier sanitario elettronico (DSE) sono trattamenti di dati effettuati tramite strumenti informatici di insiemi di dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito ai fini di:
a) prevenzione, diagnosi, cura e riabilitazione;
b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;
c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.

Il suddetto insieme di dati sanitari risulta diversamente denominato in funzione del suo ambito di operatività. Si ha un:
- *dossier sanitario* qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (a titolo esemplificativo, ospedale o clinica privata) al cui interno operino più professionisti;
- *fascicolo sanitario elettronico* qualora tale strumento sia formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale.

Il trattamento di dati sanitari di cui al precedente comma 1, costituisce trattamento ulteriore rispetto al trattamento effettuato dal sanitario con le informazioni acquisite in occasione della cura del singolo evento clinico per il quale l'interessato si rivolge ad esso.

Nell'eventualità di porre in atto trattamenti riferiti al FSE ed al DSE deve essere garantito il principio di autodeterminazione dell'interessato mediante la predisposizione di idonea ed adeguata informativa e con l'acquisizione di un consenso espresso e specifico, anche per gli eventi clinici pregressi, garantendo i relativi diritti di revoca e oscuramento dei dati, nonché il rispetto degli adempimenti previsti dalle disposizioni vigenti in materia di protezione dei dati.

Art. 37 – Accesso alle liste di attesa

Ai sensi dell'articolo 3, comma 8, della legge 23 dicembre 1994, n. 724 e ai fini del diritto di accesso garantito dalla legge 7 agosto 1990, n. 241, le unità sanitarie locali, i presidi ospedalieri e le aziende ospedaliere devono tenere, sotto la personale responsabilità del direttore sanitario, il registro delle prestazioni specialistiche ambulatoriali, di diagnostica strumentale e di laboratorio e dei ricoveri ospedalieri ordinari. Tale registro sarà soggetto a verifiche ed ispezioni da parte dei soggetti abilitati ai sensi delle vigenti disposizioni. Tutti i cittadini che vi abbiano interesse possono richiedere alle direzioni sanitarie notizie sulle prenotazioni e sui relativi tempi di attesa, con la salvaguardia della riservatezza delle persone.

Ai sensi dell'art. 41, comma 6, del D.Lgs. n. 33/2013, gli enti, le aziende e le strutture pubbliche e private che erogano prestazioni per conto del servizio sanitario sono tenuti ad indicare nel proprio sito, in una apposita sezione denominata «Liste di attesa», i criteri di formazione delle liste di attesa, i tempi di attesa previsti e i tempi medi effettivi di attesa per ciascuna tipologia di prestazione erogata. Sono altresì tenuti a pubblicare nel proprio sito internet istituzionale i bilanci certificati e i dati sugli aspetti qualitativi e quantitativi dei servizi erogati e sull'attività medica svolta.

Art. 38 – Procedure organizzative a tutela della riservatezza in ambito sanitario

Presso tutti i presidi ospedalieri e tutte le sedi distrettuali dell'Azienda, a cura del dirigente responsabile del presidio o della sede medesimi, d'intesa ove necessario con il dirigente amministrativo di riferimento, sono adottate le procedure, quali l'adozione di opportuna segnaletica per delimitare le distanze di cortesia, atte a garantire la riservatezza degli utenti in occasione di richiesta o fruizione di prestazioni sanitarie (prenotazioni, esami diagnostici, visite mediche, certificazioni, altro) o amministrative (rimborsi, indennità, altro).

I suddetti dirigenti nonché i Delegati dei trattamenti sono tenuti ad adottare idonee misure atte a garantire che le informazioni sanitarie personali rese agli utenti verbalmente (chiamata dei pazienti, indagine anamnestica, elaborazione diagnostica, colloqui con familiari, altro) o tramite supporto cartaceo (documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati.

Le strutture ospedaliere possono fornire informazioni sui degenti, anche tramite il centralino telefonico, limitatamente alla loro presenza in ospedale e sulla loro collocazione all'interno della struttura solo con il consenso dell'interessato.

Non possono essere esposti al pubblico, nei reparti o in altri locali, i nominativi dei pazienti ricoverati.

Il trattamento dei dati idonei a rivelare le convinzioni religiose non può avvenire in maniera sistematica e preventiva ma solo su richiesta dell'interessato o, qualora lo stesso sia impossibilitato, di un terzo legittimato quale ad esempio un familiare, un parente o un convivente.

Può essere data notizia, anche per via telefonica, circa una prestazione di pronto soccorso ovvero darne conferma. La notizia o la conferma devono essere fornite ai soli terzi legittimati quali possono essere familiari, parenti, conviventi ed altri, valutate le diverse circostanze del caso, nella consapevolezza che si tratta di verifica dagli esiti incerti. Le informazioni saranno comunque limitate al solo fatto che è in atto o si è svolta una prestazione di pronto soccorso e non devono contenere dati personali più dettagliati sullo stato di salute dell'interessato.

Art. 39 – Redazione degli atti e pubblicità

I responsabili delle strutture organizzative che propongono una deliberazione o che adottano un provvedimento dirigenziale verificano, alla luce dei principi di pertinenza e non eccedenza sanciti dalla normativa, che l'inclusione nel testo e nell'oggetto di dati personali sia realmente necessaria per perseguire le finalità dell'atto stesso.

Devono essere privilegiate modalità di redazione degli atti che prevedono l'utilizzo di dati anonimi o non direttamente identificativi, quali codici o altri riferimenti se lo scopo cui l'atto è preordinato è ugualmente raggiungibile.

L'Azienda garantisce la riservatezza dei dati sensibili in sede di pubblicazione all'Albo on-line delle deliberazioni o di altri atti, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati.

Art. 40 – Obblighi di trasparenza

L'Azienda assolve agli obblighi di legge in materia di trasparenza, quale livello essenziale delle prestazioni concernenti diritti civili e sociali ai sensi dell'art.117, lettera m) della Costituzione, con la pubblicazione sul

proprio sito internet istituzionale dei dati di cui al D.Lgs. n. 33/2013, nel rispetto delle linee guida impartite dal Garante per la protezione dei dati personali.

CAPO VI – DISPOSIZIONI FINALI

Art. 41 – Formazione

L'Azienda organizza, di norma nell'ambito del piano annuale di formazione del personale, interventi di formazione e aggiornamento in materia di tutela della riservatezza e protezione dei dati personali, finalizzati alla conoscenza delle norme, all'adozione di idonei modelli di comportamento e procedure di trattamento, alla conoscenza delle misure di sicurezza per il trattamento e la conservazione dei dati, dei rischi individuati e dei modi per prevenire danni ai dati stessi.

Art. 42 – Semplificazione amministrativa

L'Azienda, considerando la semplificazione quale fattore principale su cui far leva per il perseguimento dei fondamentali principi di buon andamento, efficienza, efficacia ed economicità dell'attività amministrativa, promuove azioni e progetti volti alla semplificazione dei processi e delle procedure interne rivolti all'esecuzione di adempimenti normativi e regolamentari anche in materia di protezione dei dati personali.

Art. 43 – Norma di rinvio

Per tutto quanto non previsto dal presente Regolamento si rinvia alla normativa comunitaria, statale e regionale in materia, nonché ai provvedimenti emanati dal Garante per la protezione dei dati personali.

Gli eventuali interventi del legislatore nazionale e regionale successivi all'entrata in vigore del presente Regolamento, di modifica del quadro normativo sulla riservatezza e protezione dei dati personali, producono un automatico adeguamento del presente Regolamento con successivo e necessario aggiornamento del medesimo.

Art. 44 – Abrogazione di norme

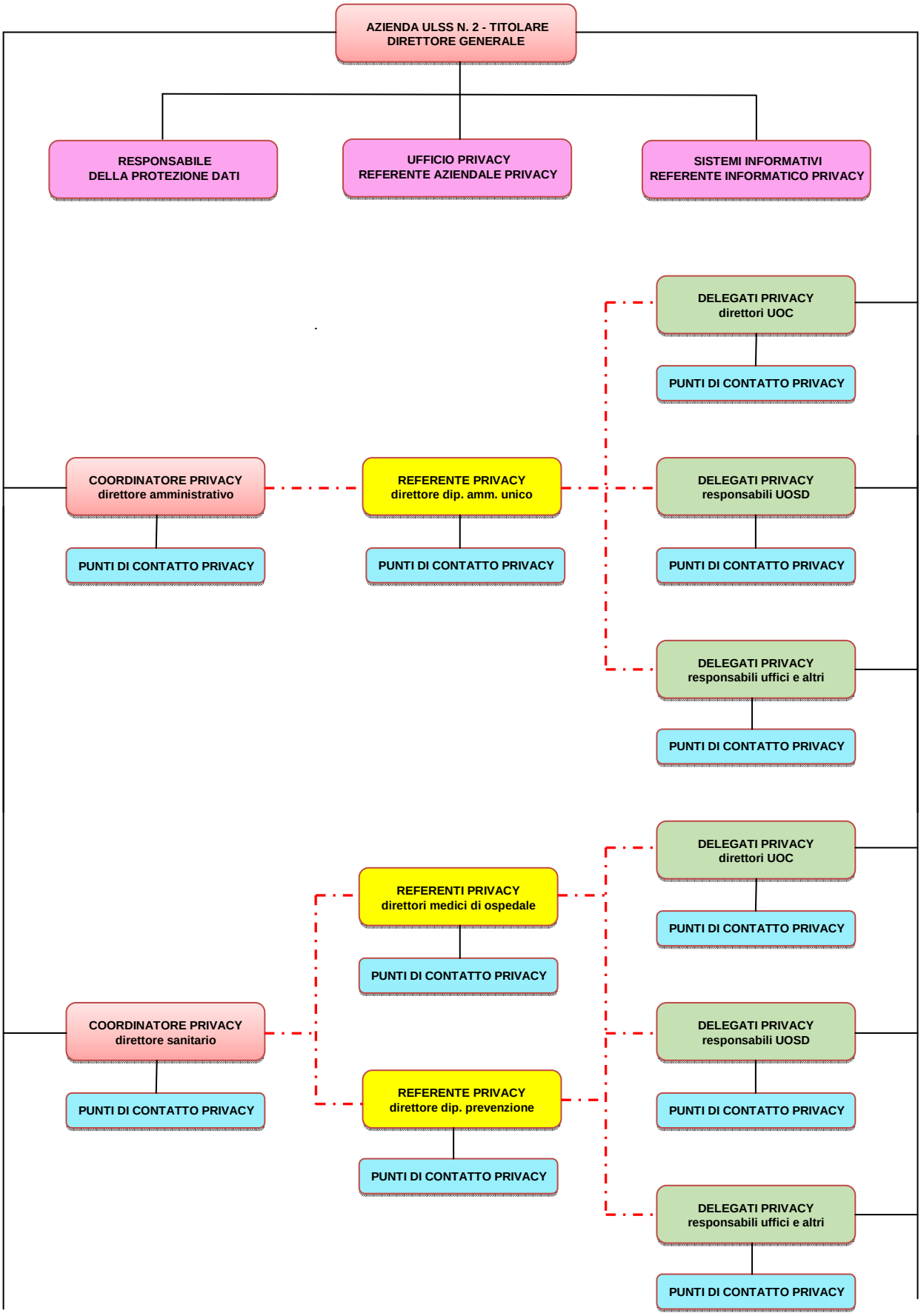
Dalla data di entrata in vigore del presente Regolamento sono abrogate tutte le precedenti disposizioni emanate in materia e con esso incompatibili.

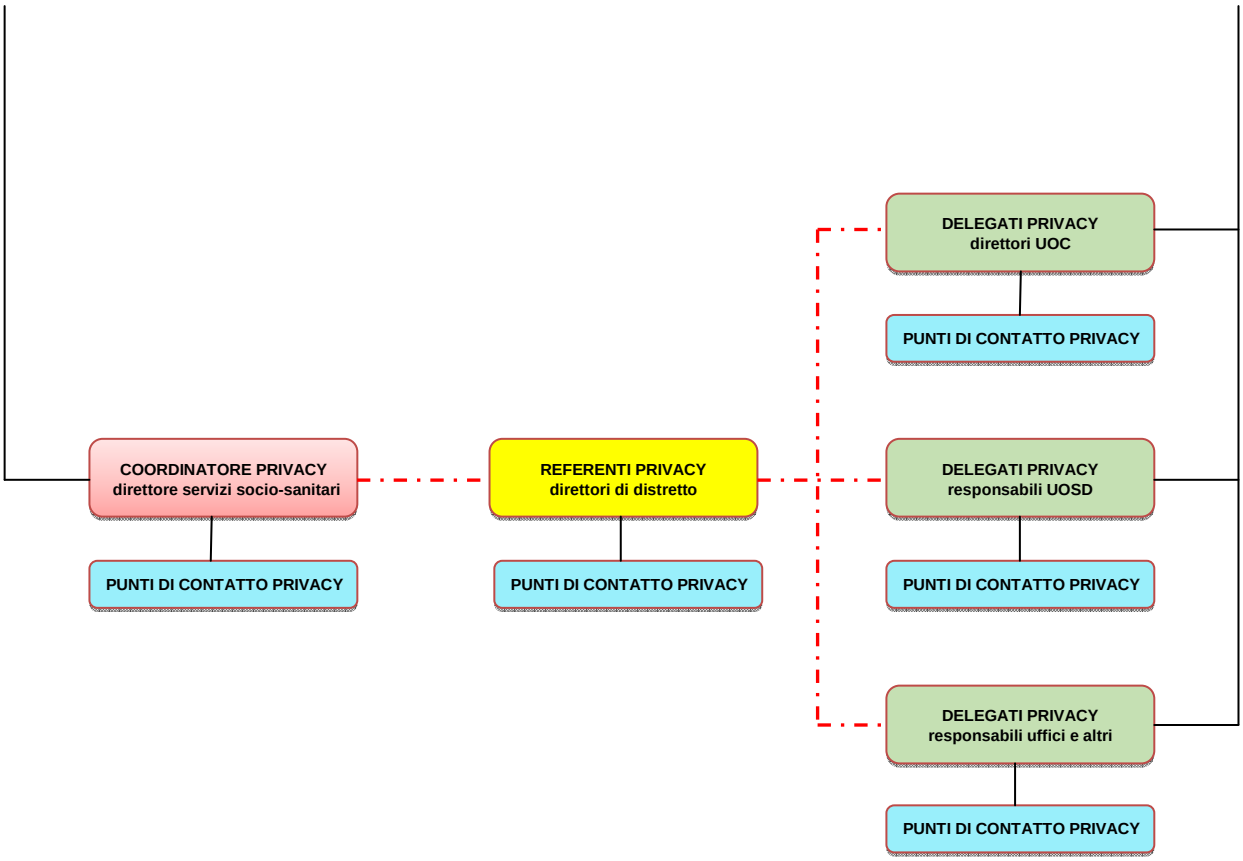
Art. 45 – Entrata in vigore

Il presente Regolamento entra in vigore nel quindicesimo giorno successivo a quello della pubblicazione della relativa deliberazione di approvazione nell'Albo on-line istituzionale.

ALLEGATO N. 1

MODELLO ORGANIZZATIVO (art. 4)





ISTRUZIONI OPERATIVE
PER LA GESTIONE DI EVENTI POTENZIALMENTE QUALIFICABILI COME VIOLAZIONE DI DATI PERSONALI (C.D. "DATA BREACH")
(art. 34 regolamento aziendale e art. 33 Regolamento UE 2016/679)

Art. 1 – Scopo

Scopo delle presenti istruzioni operative è descrivere le norme di comportamento che devono essere osservate in caso di violazione dei dati personali (c.d. *data breach*).

Art. 2 – Destinatari

Le istruzioni operative sono vincolanti per tutti i soggetti che svolgono operazioni di trattamento di dati all'interno e/o per conto dell'Azienda ULSS n. 2 Marca trevigiana.

Art. 3 – Conoscenza delle istruzioni operative e formazione

Le istruzioni operative sono portate a conoscenza dei Destinatari con una o più delle seguenti modalità:
- distribuzione tramite portale denominato "Angolo del Dipendente";
- comunicazione circolare, anche avvalendosi dei responsabili di ciascuna area organizzative, per dare atto di eventuali aggiornamenti;
- pubblicazione della versione in vigore negli ambienti comuni ritenuti idonei (a titolo esemplificativo intranet, bacheca on line del personale, ecc.);
- partecipazione ad incontri di formazione.

Art. 4 – Registro delle Violazioni

L'Azienda ULSS 2 Marca Trevigiana mantiene aggiornato il registro delle violazioni compilando il modello allegato *sub* A, contenente le seguenti informazioni:
- data di scoperta dell'evento;
- 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;
- descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla Violazione ("Azioni di miglioramento e/o correttive") e anche, se del caso, per attenuarne i possibili effetti negativi.

L'Ufficio Privacy è responsabile della tenuta e dell'aggiornamento del registro delle violazioni, a cui provvede con il supporto degli ulteriori soggetti, che ritenga opportuno coinvolgere caso per caso, e del Responsabile della protezione dei dati; quest'ultimo ha in ogni caso accesso al registro delle violazioni.

Art. 5 – Modalità operative

Chi rileva un evento che può costituire una violazione:
a) non deve compiere autonomamente alcuna azione correttiva, di ripristino o intervento sui sistemi informatici, ma limitarsi ad effettuare tempestivamente la segnalazione ed attendere l'intervento da parte delle funzioni competenti, secondo le istruzioni che seguono;
b) deve darne immediata comunicazione al Coordinatore/Referente/Delegato privacy di riferimento, raggiungendolo di persona, telefonicamente oppure, se impossibilitato, con lo strumento ritenuto più idoneo: il Coordinatore/Referente/Delegato privacy.

Il Coordinatore/Referente/Delegato privacy di riferimento provvede a:
a) contattare tempestivamente il Servizio Sistemi Informativi e/o gli altri soggetti che ritenga opportuno coinvolgere caso per caso al fine di appurare l'entità e la natura dell'evento;
b) contattare l'Ufficio privacy al fine di appurare se l'evento costituisca una violazione ai sensi di legge; in tal caso sarà redatto il verbale di ricevuta segnalazione, compilando il modello allegato *sub* B.

L'Ufficio privacy provvede a:
a) informare il Direttore Generale e il Responsabile della protezione dei dati;
b) compilare il registro delle violazioni;
c) qualora la violazione riguardi dati trattati dall'Azienda in qualità di Titolare del trattamento:
    1. notificare all'Autorità di Controllo competente senza ingiustificato ritardo e, ove possibile, entro 72

ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche; qualora la notifica all'Autorità di Controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo; la notificazione deve essere effettuata mediante l'apposita procedura telematica al seguente link: https://servizi.gpdp.it/databreach/s/scelta-auth;

2. 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;
3. verifica e coordina l'applicazione delle misure di miglioramento e/o correttive, nonché il ripristino della situazione di normalità con il supporto dei Sistemi Informativi, del Responsabile della protezione dei dati e degli ulteriori soggetti che ritenga opportuno coinvolgere caso per caso;

d) qualora la violazione riguardi dati trattati dall'Azienda in qualità di Responsabile del trattamento, dopo le operazioni indicate nei commi 1 e 2 del presente articolo, informare il Titolare del trattamento nei termini e con le modalità concordati nel contratto o altro atto giuridico stipulato con quest'ultimo.

Le decisioni in ordine alla notificazione all'Autorità di Controllo ed alla comunicazione agli interessati sono assunte dal Direttore Generale.

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

REGISTRO DELLE VIOLAZIONI DEI DATI PERSONALI
EX ART. 33 DEL REGOLAMENTO UE 2016/679

§§§

INFORMAZIONI SULL'EVENTO		
NUMERO/ANNO		
DATA E ORA DI RILEVAZIONE DEL DATA BREACH		
MODALITA' DI RILEVAZIONE DEL DATA BREACH		
DATA E ORA DELL'EVENTO		
EVENTUALI MOTIVI DI RITARDO NELLA RILEVAZIONE		
AREA / REPARTO IN CUI SI È 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)	
CAUSE DELLA VIOLAZIONE	AZIONE INTENZIONALE INTERNA	
	AZIONE ACCIDENTALE INTERNA	
	AZIONE INTENZIONALE ESTERNA	

	AZIONE ACCIDENTALE ESTERNA	
	SCONOSCIUTA	
	ALTRO (SPECIFICARE)	
CATEGORIE DI DATI OGGETTO DI VIOLAZIONE		
NUMERO DEGLI INTERESSATI E VOLUME DI DATI COINVOLTI NELLA VIOLAZIONE		
TIPOLOGIE DI INTERESSATI COINVOLTI NELLA VIOLAZIONE		
DESCRIZIONE DETTAGLIATA (compresi sistemi interessati)		
POSSIBILI CONSEGUENZE DELLA VIOLAZIONE DEI DATI		

POTENZIALI EFFETTI NEGATIVI PER LE PERSONE FISICHE		
MISURE PREVENTIVE INDIVIDUATE PER EVITARE IL RIPETERSI DELL'EVENTO	Misure Tecniche	
	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	

REGIONE DEL VENETO
ULSS2 MARCA TREVIGIANA

VERBALE DI RICEVUTA SEGNALAZIONE
DI EVENTO QUALIFICABILE COME VIOLAZIONE DEI DATI PERSONALI

Numero	
Data e ora di rilevazione dell'evento	
Data e ora dell'evento	
Area / reparto in cui si è verificato l'evento	
Descrizione dettagliata dell'eventi (compresi sistemi interessato)	

Data _____

Nome e firma del soggetto di riferimento privacy

_____

Ufficio privacy

_____