REGOLAMENTO AZIENDALE DISCIPLINANTE LA PROTEZIONE DEI DATI PERSONALI

INDICE del Regolamento aziendale

PARTE PRIMA: INTRODUZIONE

Art. 1 – Premessa di carattere generale

PARTE SECONDA: DISPOSIZIONI GENERALI

Art. 2 – Oggetto e ambito di applicazione

Art. 3 – Finalità

Art. 4 – Glossario

Art. 5 – Principi applicabili al trattamento dei dati personali

Art. 6 – Informazioni all'interessato

Art. 7– Diritto all'anonimato

Art. 8 – Rispetto dei codici deontologici

Art. 9– Valutazione preventiva dell'impatto privacy

Art.10 – Accesso ai data base e profili di autorizzazione

Art. 11 – Comunicazione di dati a terzi

PARTE TERZA: SOGGETTI

Art. 12 – Titolare del trattamento dei dati

Art. 13 – Contitolare del Trattamento

Art. 14 – Responsabile della protezione dei dati

Art. 15 – Ufficio Privacy

Art. 16 – Responsabile del trattamento dei dati

Art. 17 – Referente del trattamento dei dati

Art. 18 – Autorizzato al trattamento dei dati

PARTE QUARTA: DIRITTI DELL'INTERESSATO

Art. 19 – Informativa

Art. 20 – Diritti dell'interessato

Art. 21 – Diritti di Rettifica Cancellazione e Limitazione

Art. 22 – Diritto di opposizione

Art. 23 – Diritto alla portabilità dei dati

Art. 24 – Processo automatizzato (profilazione)

Art. 25 – Diritto di Accesso

Art. 26 – Comunicazione di dati all'interessato

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI

Art. 27 – Registro delle attività di trattamento dei dati personali

Art. 28 – Sicurezza del trattamento

Art. 29 – Tenuta in sicurezza dei documenti e degli archivi

Art. 30 – Violazione dei dati personali

Art. 31– Limiti alla conservazione dei dati personali

PARTE SESTA: MODALITÀ DI TRATTAMENTO DEI DATI

Art. 32 – Trattamento di categorie particolari di dati personali

Art. 33 – Trattamento di dati giudiziari

Art. 34 – Trasferimento di dati personali all'estero

PARTE SETTIMA: DISPOSIZIONI RELATIVE A PARTICOLARI SITUAZIONI DI TRATTAMENTO

Art. 35 – Videosorveglianza

Art. 36 – Fascicolo e Dossier Sanitario Elettronico

Art. 37 – Accesso alle liste di attesa

PARTE OTTAVA: DISPOSIZIONI FINALI

Art. 38 – Formazione

Art. 39 – Entrata in vigore

Art. 40 – Normativa

PARTE PRIMA: INTRODUZIONE

Art. 1 – Premessa di carattere generale

Il presente Regolamento in materia di protezione dei dati personali (così detta “privacy”) è uno strumento di applicazione del D.lgs. 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy” come novellato dal recente D.lgs. 10 agosto 2018 n. 101) e, in particolare, del Regolamento Europeo n. 2016/679, anche conosciuto come “GDPR”), che ha trovato diretta ed immediata applicazione sul territorio nazionale e a far data dal 25 maggio 2018.

Con l’entrata in vigore del GDPR e del successivo D.lgs. 101 del 10 agosto 2018 di adeguamento al GDPR , buona parte delle disposizioni legislative di cui al previgente Codice della privacy sono state abrogate . Fermi restando i principi cardine posti alla base del diritto alla protezione dei dati personali, l’elemento più importante ed impattante sulle organizzazioni, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della “responsabilizzazione” (accountability nell’accezione inglese) che pone in carico al Titolare del trattamento dei dati l’obbligo di attuare politiche adeguate in materia di protezione dei dati, con l’adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della “conformità” o *compliance* nell’accezione inglese); vi è quindi l’obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l’applicazione del Regolamento UE.

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino-utente che si rivolge alla struttura sanitaria, di una completa riservatezza sotto il profilo sostanziale attraverso il pieno rispetto dei diritti e della dignità del singolo individuo.

PARTE SECONDA: DISPOSIZIONI GENERALI

Art. 2 – Oggetto e ambito di applicazione

Il presente Regolamento disciplina la tutela delle persone in ordine al trattamento dei dati personali da parte dell'Azienda USL Toscana Nord – Ovest (per brevità di seguito chiamata "Azienda"), 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), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Art. 3 – Finalità

L'Azienda garantisce che il trattamento dei dati personali 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.

Art. 4 – Definizioni - Glossario

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

a) «**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;
b) «**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;
c) «**limitazione di trattamento**»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
d) «**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;
e) «**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;
f) «**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;

g) «**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;
h) **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;
i) «**delegato del trattamento**» la persona fisica che tratta dati personali per conto del titolare del trattamento alla quale è affidato il coordinamento e la vigilanza delle operazioni di trattamento dei dati personali effettuate dagli incaricat
j) «**autorizzato del trattamento**»: la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento;
k) «**interessato**»: la persona fisica cui si riferiscono i dati personali;
l) «**destinatario**»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
m) «**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;
n) «**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;
o) «**violazione dei dati personali**»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
p) «**dati genetici**»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
q) «**dati biometrici**»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
r) «**dati relativi alla salute**»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
s) «**dati anonimi**»: i dati che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;
t) «**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;
u) «**diffusione**»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
v) «**autorità di controllo**»: l'autorità pubblica indipendente individuata nel Garante per la protezione dei dati personali.

Art. 5 – Principi applicabili al trattamento dei dati personali

Il trattamento dei dati personali è effettuato nel rispetto dei seguenti principi:

a) «**liceità, correttezza e trasparenza**»: i dati sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) «**limitazione della finalità**»; i dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, del Regolamento UE, considerato incompatibile con le finalità iniziali;

c) «**minimizzazione dei dati**»: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) «**esattezza**»: i dati devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
e) «**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;
f) «**integrità e riservatezza**»: i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
g) «**responsabilizzazione**»: il titolare del trattamento è competente per il rispetto dei principi indicati nelle precedenti lettere e deve essere in grado di comprovarlo.

Art. 6 –Informazioni all'interessato

L'Azienda per ogni trattamento è tenuta a fornire le informazioni previste dall'art. 13 del Regolamento UE.

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'idonea base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 e coincidono, in linea di massima, con quelli previsti attualmente dal vigente Codice della privacy (consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati).

Per quanto concerne la specifica disciplina del "consenso" in ambito sanitario e nel contesto del Servizio Sanitario Pubblico Nazionale, si fa espresso rinvio al contenuto dell'articolo 2- septies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018) rubricato "Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute"

Art. 7 – Diritto all'anonimato

L'Azienda garantisce, nell'ambito dei dati previsti dall'art. 9 del Regolamento UE, 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 o di altre forme di pseudonimizzazione.

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.

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.

Per garantire la conoscenza capillare delle disposizioni introdotte dal Regolamento UE, e di conseguenza dal presente Regolamento, al momento dell'ingresso in servizio è fornita, a cura della U.O.C. Gestione Risorse Umane, ad ogni dipendente (oltre che ad ogni collaboratore, consulente o titolare di borsa di studio) una specifica comunicazione in materia di privacy mediante apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti),con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "autorizzati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679, e nel contempo vengono loro fornite le opportune "istruzioni operative".

Detta comunicazione conterrà anche i riferimenti per reperire il Regolamento aziendale sul sito internet nonché sullo spazio intranet aziendale, cosicché l'interessato, nel sottoscrivere il contratto di lavoro (o la lettera di incarico), sia reso edotto dell'esistenza del Regolamento e delle modalità di consultazione del medesimo.

Art. 9 – Valutazione preventiva dell'impatto privacy

L'Azienda effettua, 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 (art. 35 GDPR) derivante sulla privacy degli interessati fin dalla progettazione del relativo processo aziendale.

Prima dell'avvio di un nuovo trattamento l'Azienda effettua un'analisi dei rischi in maniera tale da orientare le decisioni che verranno successivamente assunte verso soluzioni che siano effettivamente capaci di tutelare il dato già in sede di prima raccolta, con conseguente anticipazione di responsabilità alla fase di progettazione del trattamento stesso.

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.

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.

L'Azienda attiva tutte le azioni necessarie al rispetto delle misure e prescrizioni specifiche individuate dal Garante per la privacy per il corretto trattamento dei dati, in modo

particolare per quanto riguarda i trattamenti resi possibili dai processi di innovazione digitale e dai diversi modelli di sistemi informativi sanitari integrati.

Art. 10– Accesso ai data base 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 autorizzato e nel rispetto degli ambiti di trattamento consentiti.

L'assegnazione dei predetti profili ai singoli operatori incaricati del trattamento dei dati è effettuata a cura dei rispettivi responsabili del trattamento.

Per ciascuna banca dati (applicativo informatico) deve essere definito l'elenco dei profili di accesso e le loro specificità 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, nel rispetto de principio di minimizzazione, 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.

Periodicamente i referenti del trattamento aggiornano i profili di autorizzazione del personale assegnato.

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 contenenti dati particolari devono essere tracciati.

Art. 11 – 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 comunque 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.

PARTE TERZA: SOGGETTI

Art. 12 – Titolare del trattamento dei dati

Il Titolare del trattamento dei dati personali ai sensi e per gli effetti di legge è l'Azienda Usl Toscana Nord-Ovest in persona del suo legale rappresentante.

Al Titolare competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Al Titolare in particolare spetta :

a) richiedere al Garante per la privacy l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;

b) nominare i referentii e i responsabili del trattamento dei dati personali, 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;

c) nominare il Responsabile per la protezione dei dati;

d) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

e) 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. 13 – Contitolare del trattamento dei dati

L'art. 26 del Regolamento Europeo n. 2016/679 disciplina la fattispecie in cui due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento.

Essi determinano in modo trasparente, mediante un accordo di contitolarità, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati ed il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

Art. 14 – Responsabile della protezione dei dati

Il Regolamento Europeo ai sensi ex artt. 37, 38 e 39 impone obbligatoriamente al Titolare la nomina del Data Protection Officer - DPO (in italiano: Responsabile della protezione dei dati - 'RPD')

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 (RPD esterno);
- 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, ai delegati nonché ai dipendenti 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 (art. 35 del Regolamento UE);

d) cooperare con il Garante per la privacy;

e) fungere da punto di contatto per il Garante per la privacy per questioni connesse al trattamento, tra cui la consultazione preventiva (art.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 privacy.

Art. 15 – Ufficio Privacy

L'Ufficio Privacy Aziendale, ha il ruolo strategico di supporto al Responsabile della Protezione dei Dati ed è inserito all'interno del Dipartimento Affari Legali con le seguenti funzioni:

1. supporta la Direzione Aziendale impostando le procedure per la corretta applicazione della normativa di settore e ne cura gli adempimenti;
2. svolge attività di consulenza e formazione, sia per la Direzione Aziendale, sia nei confronti delle varie articolazioni organizzative, fornendo risposte a quesiti e richieste provenienti dai dipendenti e dagli utenti;
3. collabora col Responsabile della Protezione dei Dati nella gestione delle segnalazioni di casi di violazione dei dati personali (c.d. data breach) e delle istanze avanzate dagli interessati al Titolare del trattamento;
4. aggiorna e conserva il Registro delle attività di trattamento e il Registro delle violazioni previsti rispettivamente dagli artt. 30 e 33 del Regolamento U. E.
5. gestisce le istanze ex artt.15-22 del Regolamento U. E.

Art. 16 – Responsabile del trattamento dei dati

La nomina a Responsabile del trattamento (ex art. 28 GDPR) è effettuata dal Titolare attribuendo, a soggetti esterni all'Azienda a seguito di sottoscrizione di specifico contratto, attività di competenza aziendale o che svolgono attività connesse, strumentali e di supporto, ivi incluse le attività manutentive, che comportano l'uso di dati personali, comuni e/o sensibili.

La funzione di Responsabile del trattamento dei dati è attribuita personalmente e non è suscettibile di delega.

Il responsabile del trattamento può ricorrere ad un altro responsabile del trattamento (comma 2 art. 28 GDPR) previa autorizzazione scritta, specifica o generale del titolare del trattamento.

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 / incaricati del 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.

Art. 17 – Referente del trattamento dei dati

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 individua quali Referenti del trattamento, in relazione alle funzioni di specifica competenza derivanti dal rapporto giuridico esistente con la stessa Azienda, i seguenti soggetti:

- Direttore Amministrativo;
- Direttore Sanitario;
- Direttore dei Servizi Socio-Sanitari;
- Direttori di presidio Ospedaliero;

- Direttori di distretto;
- Direttore di dipartimento di prevenzione;
- Direttori di unità operativa complessa;
- Direttori di unità operativa semplice;

Il Titolare può, inoltre, individuare quali Referenti del trattamento altri soggetti (dirigenti / funzionari / titolari di incarichi) in virtù delle particolarità organizzative e funzionali delle attività di competenza.

In particolare il Referente del trattamento deve:

a) trattare i dati personali osservando le disposizioni di legge e regolamentari, nonché le specifiche istruzioni impartite dal Titolare;

b) 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;

c) assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

d) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti dalla normativa vigente compreso il costante aggiornamento del registro dei trattamenti;

e) 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 degli autorizzati al trattamento dei dati rispondano ai principi di necessità, pertinenza e non eccedenza;

f) verificare che all'interessato o al soggetto presso il quale sono raccolti i dati sia data l'informativa e quando previsto, il consenso al trattamento dei dati;

I Referenti del trattamento rispondono al Titolare 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 Referente del trattamento non è a sua volta delegabile ed in caso di assenza o impedimento le relative attribuzioni sono esercitate da chi lo sostituisce per le attività di istituto.

I referenti al trattamento devono sottoscrivere l'atto di delega conferita assumendo tutte le responsabilità dei compiti e delle funzioni attribuite e oggetto di delega, mentre in capo al Titolare permangono il potere di controllo e il potere di avocazione/sostituzione in caso di inerzia del delegato.

I responsabili provvedano inoltre ad individuare con atto scritto il personale afferente alla struttura da essi diretta quali autorizzati del trattamento dei dati personali fornendo loro adeguate istruzioni.

Art. 18 – Autorizzato (esterno ed interno) al trattamento dei dati

Il Titolare e il Referente del trattamento 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 con il presente Regolamento individua quale autorizzato del trattamento 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, in relazione alle funzioni di specifica competenza derivanti dai predetti rapporti giuridici e comportanti il trattamento di dati personali.

Gli autorizzati al trattamento a seconda del rapporto giuridico nei confronti dell'Azienda si dividono in autorizzati interni o esterni:

a) Autorizzati interni del trattamento dei dati: al momento dell'ingresso in servizio è fornita, a cura della U.O.C. Gestione Risorse Umane, ad ogni dipendente (oltre che ad ogni collaboratore, consulente o titolare di borsa di studio) una specifica comunicazione in materia di privacy mediante apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti), con la quale detti soggetti (dipendenti e non dipendenti) vengono nominati quali "autorizzati al trattamento dei dati" ai sensi del D.lgs. 196/2003 e del Regolamento UE 2016/679, impartendo loro anche le opportune "istruzioni operative" .

b) Autorizzati esterni del trattamento dei dati: tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa Azienda, pur non essendo dipendenti e neppure titolari di incarichi di collaborazione, studio o consulenza conferiti dalla medesima, debbono essere designati da parte del Responsabile.

PARTE QUARTA: DIRITTI DELL'INTERESSATO

Art. 19 – Informativa

Il principio di trasparenza previsto dall'art. 5, par. 1, lett. a) del GDPR impone ai titolari di informare gli interessati sui principali elementi del trattamento, al fine di renderli consapevoli sulle principali caratteristiche dello stesso.

L'Azienda predispone un'informativa di carattere generale da fornire alla generalità dei pazienti/utenti le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie

L'Azienda predispone altresì informative specifiche sul trattamento dei dati personali relativi a particolari attività di trattamento ai soli pazienti/utenti effettivamente interessati.

In ogni caso le informazioni devono essere chiare e comprensibili, in forma concisa, trasparente, intelligibile e facilmente accessibile.

L'informativa sul trattamento dei dati personali riporta le informazioni previste dalla normativa vigente relativamente a:

b) l'identità e i dati di contatto del Titolare del trattamento e del Responsabile per la protezione dei dati;

c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;

d) le modalità di trattamento dei dati personali;

e) l'obbligatorietà o meno del conferimento dei dati;

f) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

g) coloro ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;

h) come possono essere esercitati i diritti di accesso in base alle disposizioni vigenti;

i) 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;

j) 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;

k) il diritto di proporre reclamo al Garante per la privacy;

l) 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;

m) 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;

n) 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.

Le informazioni sono fornite per iscritto o con mezzi elettronici e se richiesto dall’interessato anche oralmente, purché sia comprovata con altri mezzi l’identità dell’interessato.

Art. 20 – Diritti dell’interessato

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.

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 senza ingiustificato ritardo e l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

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

Nel caso in cui l'interessato promuova istanza ai sensi del presente articolo, i delegati al trattamento sono tenuti a fornire al Rpd la massima collaborazione in modo tale da fornire riscontro all'interessato.

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.

Art. 21– Diritti di Rettifica Cancellazione e Limitazione

Ai sensi degli artt. 16, 17 e 18 del Regolamento Europeo, l'Interessato può inoltre esercitare i seguenti diritti :

1. La richiesta di rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.
2. La richiesta da cancellazione dei dati personali qualora i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati, siano spirati i termieni di conservazione; l'interessato revochi il consenso su cui si basa il trattamento, e se non sussiste altro fondamento giuridico per il trattamento.

   Il diritto di cancellazione non è applicabile nella misura in cui il trattamento sia necessario:

   a) per l'adempimento di un obbligo legale che richiede il trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;

   b) per motivi di interesse pubblico nel settore della sanità pubblica in conformità all'art.9, paragrafo 2, lettera h) e i) e dell'art. 9, paragrafo 3.

3. La limitazione è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati o si oppone al loro trattamento.

Per esercitare i diritti sopra citati, l'interessato può inviare richiesta al Titolare o al Responsabile della Protezione dei Dati personali.

Art. 22 – Diritto di opposizione

L'interessato ha il diritto di opporsi ai sensi dell'art. 21 del Regolamento Europeo in qualsiasi momento 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.

Art. 23 – Diritto alla portabilità dei dati

Si tratta di uno dei nuovi diritti previsti dall'art 20 del regolamento, il quale non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato.

L'esercizio di tale diritto non deve ledere i diritti e le libertà altrui, ed inoltre il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro Titolare indicato dall'interessato, se tecnicamente possibile.

Art. 24 – Processo automatizzato (profilazione)

Come stabilito dall'articolo n. 22 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

(a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;

(b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;

(c) si basi sul consenso esplicito dell'interessato.

Art. 25 – Diritto di accesso

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. 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, individuato espressamente dall'interessato o colui che abbia prescritto la prestazione, che, a sua volta, li renderà noti all'interessato;

b) una spiegazione orale o un giudizio scritto da parte di un medico dell'Azienda

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, su esplicita richiesta dell'interessato.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI

Art. 27 – Registro delle attività di trattamento dei dati personali

L'Azienda tiene un registro informatizzato delle attività di trattamento svolte sotto la propria responsabilità, periodicamente aggiornato a cura dei referenti del trattamento con il supporto dell'Ufficio Privacy 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.

Tale registro viene tenuto anche dai Referenti e Responsabili ed eventuali Sub-Responsabili del trattamento.

L'Azienda predispone l'aggiornamento del registro, di norma con cadenza semestrale od ogni qualvolta se ne ravvisi la necessità.

Art. 28 – Sicurezza del trattamento

Il Titolare, i Referenti e gli Autorizzati del trattamento dei dati sono tenuti ad adottare, così come previsto dalle disposizioni vigenti in materia di protezione dei dati ogni misura di sicurezza necessaria per assicurare un livello adeguato di sicurezza dei dati personali trattati.

Tali soggetti, 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, mettono 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:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

In caso di violazione dei dai personali tale soggetti sono tenuti ad attivare il supporto tecnico informatico al fine di ripristinare tempestivamente disponibilità e accesso dei dati personali e di comunicarlo al Rpd per le ulteriori azioni da porre in essere .

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 pertinente con il trattamento di dati per il quale il soggetto è stato precedentemente autorizzato al trattamento ed è consentito soltanto utilizzando apposite credenziali che devono essere strettamente personali e non divulgate a terzi.

Art. 29 – Tenuta in sicurezza dei documenti e degli archivi

Gli archivi che custodiscono i dati di cui l’Azienda è Titolare del trattamento, sia cartacei che 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.

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.

Gli archivi cartacei e digitali sono oggetto di trattamento da parte del Referente o Responsabile del trattamento dei dati di competenza, che deve 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.

Art. 30 – Violazione dei dati personali

Ogni Referente, Responsabile ed Autorizzato del trattamento dei dati personali o amministratore di sistema è tenuto ad informare senza ingiustificato ritardo il Titolare in caso di una violazione dei dati personali (data breach, Pro Az. 139 del 16/01/2020)

L'Azienda provvede a notificare, avvalendosi della collaborazione del Responsabile per la protezione dei dati e dell'Ufficio Privacy, la violazione al Garante per la privacy 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:

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.

Il Referente e/o l'Autorizzato sono tenuti in caso di violazione dei dati personali a fornire al Rpd la massima collaborazione per la redazione della notifica al fine del rispetto dei tempi previsti,

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 nel registro delle violazioni 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 privacy di verificare il rispetto delle disposizioni di legge.

Art. 31 – Limiti alla conservazione dei dati personali

L'Azienda assicura l'adozione di procedure attraverso le quali:

- si proceda alla distruzione dei documenti analogici e digitali, una volta terminato il limite minimo di conservazione dei documenti e dei dati in questi riportati;
- lo smaltimento di apparati hardware o supporti rimovibili di memoria non renda possibile accedere ad alcun dato personale di cui è titolare l'Azienda Sanitaria;
- il riutilizzo di apparati di memoria o hardware non renda possibile accedere ad alcun dato personale di cui è titolare l'Azienda Sanitaria.

PARTE SESTA : MODALITA' DI TRATTAMENTO DEI DATI

Art. 32 – Trattamento di categorie particolari di dati personali

Come stabilito dall'articolo n. 9 del Regolamento UE n. 2016/679, 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.

Si fa presente, inoltre, che il Regolamento UE consente di "mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute" (articolo n. 9, paragrafo n. 4).

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 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;

c) 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;

d) 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;

e) 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;

f) 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;

g) 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.

Art. 33 – Trattamento di dati giudiziari

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. 34 – 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.

PARTE SETTIMA : DISPOSIZIONI RELATIVE A PARTICOLARI SITUAZIONI DI TRATTAMENTO

Art. 35 – Videosorveglianza

L’installazione di apparecchiature di videosorveglianza è autorizzata dal Titolare, (Pro Az. 137 del 07/08/2020) previo accordo con le organizzazioni sindacali, solo quando ciò sia strettamente indispensabile per la sicurezza degli utenti del personale 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 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 fornisce al Delegato o Responsabile del trattamento le istruzioni necessarie sulle modalità di trattamento dei dati raccolti con le apparecchiature di videosorveglianza, sulle misure di sicurezza da osservare, nonché sull’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.

Possono accedere alle immagini rilevate per le predette finalità solo i soggetti specificatamente autorizzati (personale medico e infermieristico, altro).

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 cittadino / paziente può, inoltre, decidere, attraverso rilascio di specifico consenso orale, se inserire o non inserire nel Dossier e Fascicolo Sanitario Elettronico le informazioni relative ad eventi sanitari pregressi all'istituzione degli stessi.

Per quanto concerne le informazioni sanitarie ricomprese tra quelle "a maggior tutela dell'anonimato", come per esempio: Test HIV, Interruzioni Volontarie di Gravidanza, utilizzo di sostanze stupefacenti, parto anonimo, atti di violenza sessuale o di pedofilia, è necessario che il paziente fornisca esplicito consenso all'inserimento di dette informazioni nel Dossier Sanitario e Fascicolo Elettronico rispetto al quale, altrimenti, saranno escluse.

L'Azienda assicura, a tutela della riservatezza del paziente, che una volta manifestata la volontà del medesimo in merito al trattamento dei dati personali mediante costituzione sia del Dossier che del Fascicolo Sanitario Elettronico, lo stesso interessato possa decidere di oscurare taluni dati o documenti sanitari consultabili tramite tale strumento.

L' "Oscuramento" dell'evento clinico (revocabile nel tempo) avverrà con modalità tali da garantire che i soggetti abilitati all'accesso non possano venire a conoscenza del fatto che l'interessato ha effettuato tale scelta (cd. "Oscuramento dell'oscuramento").

I dati personali utilizzati per la costituzione del Dossier Sanitario Elettronico vengono trattati rispettando i principi di correttezza, liceità, necessità e finalità stabiliti dal Decreto Legislativo 196/2003 e osservando le misure di sicurezza previste dall'Allegato "B" - Disciplinare Tecnico del medesimo Decreto Legislativo.

Il paziente, in sede di nota informativa, è anche informato del fatto che in qualsiasi momento, rivolgendosi al Titolare del Trattamento dei dati, è in grado di (così come previsto dall'articolo 7 del Decreto Legislativo 196/2003):

- revocare il consenso ad alimentare il Dossier con l'inserimento di esami o referti

(“istanza di revoca”);

- esercitare la facoltà di oscurare eventi clinici che lo riguardano (“istanza di oscuramento”);
- esercitare il diritto di accesso ai dati personali contenuti nel Dossier Sanitario Elettronico (“istanza di esercizio dei diritti”);
- visionare gli accessi che sono stati effettuati sul proprio Dossier Sanitario Elettronico da parte dei soggetti abilitati alla consultazione (“istanza di accesso”);

Art. 37 – Accesso alle liste di attesa

Per le finalità di cui all’articolo 3, comma 8, della legge 23 dicembre 1994, n. 724 l’interessato ha diritto di a conoscere il numero di posizione che occupa nelle liste delle prestazioni specialistiche ambulatoriali, di diagnostica strumentale e di laboratorio, dei ricoveri ospedalieri e nelle altre liste di attesa, ma non può essere messo a conoscenza dei nominativi delle persone che lo precedono o che lo seguono nell’elenco.

Fuori dei casi previsti dal comma 1, le informazioni sulle prenotazioni e sui relativi tempi di attesa sono fornite ai soggetti che vi abbiano interesse, a norma della legge n. 241/1990 e con la salvaguardia del diritto alla riservatezza delle persone.

PARTE OTTAVA :DISPOSIZIONI FINALI

Art. 38 – Formazione

L'Azienda organizza, tramite il supporto della U.O.S. Privacy, 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. 39– Entrata in vigore

Il presente Regolamento entra in vigore dalla data di pubblicazione della delibera di approvazione.

E' redatto allo stato della vigente legislazione ed è soggetto a variazioni o integrazioni a seguito di eventuali successivi interventi normativi o provvedimenti della Autorità Garante per la protezione dei dati personali che dovessero incidere sul suo contenuto.

Per tutto quanto non previsto si applica la suddetta normativa di settore.

L'Ufficio Privacy Aziendale provvede a dare pubblicità al Regolamento tramite la sua pubblicazione nella sezione Privacy dei siti internet e intranet aziendali e invio a tutti i delegati del trattamento per la relativa diffusione a tutti gli operatori.

Art. 40– Nomativa

La normativa di riferimento, a cui si rinvia per tutti gli aspetti non espressamente disciplinati dal presente regolamento, è la seguente:

a) Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 “Regolamento Generale sulla Protezione dei Dati”, conosciuto anche come RGPD;

b) Decreto legislativo 30 Giugno 2003, n. 196 “Codice in materia di protezione dei dati personali”, come modificato dal decreto Legislativo 10 Agosto 2018, n. 101;

c) Provvedimento del Garante della Privacy n. 55 del marzo 2019 recante: "Chiarimenti sull’applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario”;

d) Decreto del Presidente della Giunta regionale 26 ottobre 2021, n. 13 “Regolamento in attuazione dell’articolo 1, comma 1, della legge regionale 3 aprile 2006 n. 13 (Trattamento delle categorie particolari di dati personali e di quelli relativi a condanne penali e ai reati da parte della Regione Toscana, aziende sanitarie, enti, aziende e agenzie regionali e soggetti pubblici nei confronti dei quali la Regione esercita poteri di indirizzo e controllo).

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: FOLENA MANUELA
DATA FIRMA: 22/12/2022 14:17:01
IMPRONTA: 376231356435313963376237336239643537306539306533623234663664393033363333316463 62