REGOLAMENTO AZIENDALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

INDICE

PREMESSA

A - DISCIPLINA QUADRO

Il Regolamento Europeo 2016/679 "Regolamento Generale sulla Protezione dei dati 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" - d'ora innanzi denominato "GDPR" - rivisita completamente la prospettiva della disciplina sulla privacy, istituendo un quadro normativo incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (principio di "accountability"). La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti e al contempo di essere in grado di comprovarlo; ciò adottando una serie di strumenti che lo stesso GDPR indica, partendo da un'attenta valutazione di rischi e impatti e con una pianificazione di attività tali da poter incidere significativamente sotto il profilo culturale, organizzativo e tecnologico.
Con il Decreto Legislativo n. 101 del 10 agosto 2018, il Legislatore ha modificato la normativa nazionale rappresentata dal Decreto Legislativo n. 196/2003 (Codice in materia di protezione dei dati) adeguando le parti incompatibili o contrastanti con il GDPR.
In particolare, l'art. 2 *quaterdecies* del D. Lgs. 196/2003, introdotto dal D.Lgs. 101/2018, conferisce ai titolari e responsabili del trattamento la possibilità di prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità; da ciò discendendo la necessità – soprattutto per sistemi complessi quali le Aziende Sanitarie ed Ospedaliere – di strutturare un'articolata architettura in grado di definire i rispettivi ruoli di professionisti e operatori.
All'interno di tale contesto, quindi, il presente Regolamento costituisce lo strumento attraverso il quale l'Azienda Ospedaliera Ospedali Riuniti Marche Nord – d'ora innanzi denominata "Azienda Ospedaliera" - rappresenta il proprio modello organizzativo e gestionale per il trattamento dei dati personali in linea ed in costante adeguamento rispetto al quadro normativo sopra richiamato.

B - PRINCIPALE NORMATIVA E ATTI DI RIFERIMENTO:

- Legge n. 241/1990 e ss.mm.ii. "*Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi*" e ss.mm.ii;
- D.Lgs. n. 196/2003 "*Codice in materia di protezione dei dati personali*", integrato con le modifiche introdotte dal D.Lgs. n. 101/2018 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*";
- D.Lgs. 82/2005 e ss.mm.ii. "*Codice dell'Amministrazione Digitale*";
- Deliberazione del Garante per la protezione dei dati personali n. 243 del 14/06/2007 "*Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*";

- Provvedimento del Garante per la protezione dei dati personali del 27/11/2008, modificato con Provvedimento del 25/06/2009 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*";
- Deliberazione del Garante per la protezione dei dati personali n. 36 del 19/11/2009 "*Linee guida in tema di referti on-line – 19 novembre 2009*";
- D.L. n. 179/2012, art. 12, comma 5 "*Ulteriori misure urgenti per la crescita del paese*";
- D.Lgs. n. 33/2013 e ss.mm.ii. "*Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*";
- DPCM dell'08/08/2013 "*Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali*";
- Deliberazione del Garante per la protezione dei dati personali n. 243 del 15/05/2014 "*Linee guida del Garante per la Protezione dei Dati Personali 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 del Garante per la protezione dei dati personali n. 331 del 04/06/2015 "*Linee Guida in materia di Dossier Sanitario*";
- Provvedimento del Garante per la protezione dei dati personali n. 393 del 02/07/2015 "*Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche*";
- DPCM n. 178 del 29/09/2015 "*Regolamento in materia di fascicolo sanitario elettronico*";
- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46 CE (regolamento generale sulla protezione dei dati);
- Provvedimento del Garante per la protezione dei dati personali n. 512 del 19/12/2018 "*Regole deontologiche relative al trattamento di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101*";
- Provvedimento del Garante per la protezione dei dati personali n. 55 del 07/03/2019 "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*";
- Provvedimento del Garante per la protezione dei dati personali n. 146 del 05/06/2019 "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, del d.lgs. 10 agosto 2018 n. 101*";
- D.L. n. 34/2020 "*Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19*";
- Decreto del Dirigente del Servizio Sanità della Regione Marche n. 6 del 22/03/2021 "*Art. 11 D.L. 19.05.2020 n. 34 – Misure urgenti in materia di Fascicolo Sanitario Elettronico – Aggiornamento modulistica*";
- Provvedimento del Garante per la protezione dei dati personali n. 186 del 29/04/2021 "*Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico*";
- Determina DG AORMN n. 483 del 27/06/2017 "*Regolamento in materia di accesso a documenti, dati e informazioni. Adozione*";

- Determina DG AORMN n. 547 del 20/07/2017 "*Accesso alla documentazione sanitaria. Definizione tariffe e modulistica*";
- Determina DG AORMN n. 449 del 31/07/2018 "*Regolamento UE 2016/679 (RGPD). Designazione Responsabile della protezione dei dati (RPD);*
- Determina DG AORMN n. 135 del 20/03/2019 "*Definizione degli aspetti organizzativi e funzionali per la gestione della Privacy ai fini dell'adeguamento dell'organizzazione aziendale al Regolamento Europeo 20167679. Adozione*";
- Determina DG AORMN n. 354 del 20/06/2019 "*Misure organizzative ex Regolamento UE 2016/679 (GDPR). Nomina Responsabili del trattamento e designazione Incaricati*";
- Determina DG AORMN n. 389 del 31/07/2020 "*Modifica composizione Gruppo multidisciplinare di supporto al Responsabile della protezione dei dati di cui alla determina DG n. 449 del 31/07/2018*";
- Determina DG AORMN n. 128 del 19/03/2021 "*Misure organizzative ex Regolamento UE 2016/679 (GDPR). Aggiornamento criteri di designazione dei Responsabili interni del trattamento di cui alla determina DG 354/2019*".

C - DEFINIZIONI:

Si richiamano, di seguito, alcune delle definizioni contenute nell'art. 4 del GDPR:

- **«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;

- **«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;

- **«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;

- **«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;

- **«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;
- **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
- **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
- **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
- **«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;
- **«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;
- **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
- **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
- **«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR.

TITOLO I – IL TRATTAMENTO DEI DATI PERSONALI

Art. 1 - Oggetto ed ambito di applicazione

1. Il presente Regolamento disciplina il sistema di gestione dei dati personali all'interno dell'Azienda Ospedaliera, nel rispetto di quanto previsto dal GDPR e dal quadro normativo nazionale di riferimento in tema di protezione dei dati personali.

2. La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale riconosciuto dalla Unione Europea e a tal fine l'Azienda Ospedaliera mette in atto 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 degli interessati.
3. Il trattamento dei dati personali - nell'ambito di ogni articolazione organizzativa dell'Azienda Ospedaliera - viene effettuato garantendo a chiunque il rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati stessi.

Art. 2 - Principi applicabili al trattamento dei dati personali

1. Al trattamento dei dati personali si applicano i principi di cui all'art. 5 del GDPR.
Ai sensi di quanto previsto dal citato art. 5 del GDPR, i dati personali sono:
a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) 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 («esattezza»);
e) 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, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) 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 («integrità e riservatezza»).
2. Il Titolare del trattamento – attraverso la complessiva struttura organizzativa aziendale - è competente in ordine al rispetto e all'applicazione dei citati principi ed in grado di comprovarlo verso l'esterno («responsabilizzazione»).

Art. 3 – Base giuridica del trattamento

1. Le condizioni di liceità - in presenza delle quali si effettuano operazioni di trattamento di dati personali – sono quelle indicate all'art. 6 del GDPR, come di seguito riportate:
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. Tale condizione non si applica al trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Art. 4 – Categorie di dati personali

1. Ai sensi di quanto previsto all'art. 4 del GDPR, l'Azienda Ospedaliera effettua il trattamento dei soli dati necessari rispetto alle finalità per le quali vengono raccolti o trattati, tra cui:

- dati personali comuni, quali nome, cognome, residenza, cittadinanza, recapito telefonico, codice fiscale;
- categorie particolari di dati personali (art. 9 del GDPR);
- dati economici, quali retribuzione, compensi, benefici, agevolazioni;
- dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR).

2. I dati personali trattati dall'Azienda Ospedaliera, nelle forme e nei limiti di quanto previsto dalla vigente normativa, sono raccolti:

- prioritariamente presso l'Interessato o anche presso persone diverse nei casi in cui questi sia minorenne o incapace o non sia in grado di fornirli;
- presso enti del SSN, presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti le professioni sanitarie.

Art. 5 – Categorie di soggetti interessati

1. Per soggetto interessato è da intendersi la persona fisica cui i dati trattati si riferiscono.
2. L'Azienda Ospedaliera tratta i dati personali relativi, principalmente, a:

- utenti, assistiti, pazienti e loro familiari e/o accompagnatori;
- personale sanitario, amministrativo, tecnico e professionale, con rapporto di dipendenza, consulenza o collaborazione;
- soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture aziendali, quali specializzandi, studenti, tirocinanti, volontari;
- soggetti che intrattengono rapporti contrattuali con l'Azienda Ospedaliera stessa ai fini della fornitura di beni e servizi, attività di assistenza o consulenza, esecuzione di opere edilizie, interventi di manutenzione su software o dispositivi medici o altre prestazioni;
- soggetti e imprese partecipanti a bandi di gara o di pubblico concorso.

Art. 6 – Categorie di trattamenti

1. In conformità all'art. 4, n. 2) del GDPR, per trattamento si intende qualunque operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali o insiemi di dati personali, quali:

- la raccolta dei dati;

- la registrazione dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
- l'organizzazione dei dati, cioè il processo di lavorazione finalizzato a favorirne la fruibilità attraverso l'aggregazione, la disaggregazione, l'accorpamento, la catalogazione;
- la conservazione dei dati;
- l'adattamento o la modifica in relazione a variazioni o a nuove acquisizioni;
- l'estrazione;
- la consultazione;
- l'uso;
- la comunicazione dei dati mediante trasmissione ad uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; la comunicazione dei dati avviene solo nei casi previsti da norme di legge o regolamento;
- la comunicazione dei dati mediante diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati;
- la limitazione, cioè il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
- la cancellazione;
- la distruzione.

2. Le operazioni di trattamento possono essere effettuate solo dal Titolare, dai Responsabili del trattamento, dai professionisti designati in qualità di Responsabili "interni" e dal personale autorizzato. Non è consentito il trattamento di dati personali da parte di persone non autorizzate.

Art. 7 – Finalità del trattamento

1. Il trattamento di dati personali effettuato dall'Azienda Ospedaliera è finalizzato principalmente:

- allo svolgimento dei compiti del Servizio Sanitario Nazionale di rilevante interesse pubblico e all'espletamento delle funzioni istituzionali previste dalla normativa vigente;
- all'erogazione di prestazioni sanitarie specialistiche (comprensive di tutte le necessarie attività di supporto) volte alla tutela della salute e dell'incolumità fisica degli utenti, di terzi e della collettività;
- allo svolgimento di attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
- allo svolgimento di attività amministrative connesse e correlate all'erogazione di prestazioni sanitarie;
- all'esecuzione di adempimenti amministrativi, gestionali e contabili connessi e correlati alle proprie funzioni istituzionali delle Aziende e/o ad obblighi di legge;
- alla tutela della sicurezza e della salute dei lavoratori e sorveglianza igienico sanitaria delle proprie strutture;
- alla gestione delle proprie risorse umane, tecnologiche, strumentali e patrimoniali.

Art. 8 - Categorie particolari di dati personali

1. L'attività dell'Azienda Ospedaliera nell'ambito dell'assistenza sanitaria comporta il trattamento di dati personali appartenenti alle categorie particolari di cui all'articolo 9 del GDPR, tra cui dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati che rivelino l'origine razziale o etnica, le convinzioni religiose o l'appartenenza sindacale, dati genetici. Il trattamento di tali categorie di dati è

consentito qualora si verifichi uno dei casi indicati al paragrafo 2 del citato art. 9 del GDPR, qui di seguito richiamati:

a) l'Interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche […..];

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 […..];

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 […..];

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, se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale;

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, 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.

2. In conformità a quanto previsto dall'art. 2-*sexies*, comma 1, del D. Lgs. 196/2003 e ss.mm.ii., i trattamenti delle categorie particolari di dati personali, necessari per motivi di interesse pubblico rilevante ai sensi dell'art. 9, paragrafo 2, lettera g) del GDPR, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato. Il citato articolo individua, altresì, i motivi di interesse pubblico rilevante che consentono il trattamento di categorie particolari di dati personali.

3. I dati rientranti nelle categorie particolari sono trattati dall'Azienda Ospedaliera qualora essenziali e necessari allo svolgimento delle attività istituzionali ad essa assegnate e nel caso in cui tali attività non possano essere eseguite mediante il trattamento di dati anonimi o di dati personali di diversa natura.

Art. 9 - Il trattamento dei dati dei lavoratori

1. L'Azienda Ospedaliera tratta i dati personali, anche di natura sensibile o giudiziaria, dei propri lavoratori per finalità considerate di rilevante interesse pubblico, quali instaurazione, gestione ed estinzione dei rapporti di lavoro di qualunque tipo (subordinato o autonomo), gestione della materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

2. Il trattamento dei dati personali rientranti nelle categorie particolari è effettuato solo se necessario:

a) per adempiere a specifici obblighi previsti da leggi, regolamenti o contratti collettivi ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché ai fini del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza, di igiene e sicurezza del lavoro, nonché in materia fiscale e sindacale;

b) anche fuori dei casi di cui alla lettera a) - in conformità alla legge e per scopi determinati e legittimi - ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti o benefici accessori;

c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo;

d) per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione, nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

e) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;

f) per garantire le pari opportunità nel lavoro;

g) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro.

L'Azienda Ospedaliera adotta adeguate misure nel trattamento dei dati personali dei dipendenti idonei a rivelare lo stato di salute, le abitudini sessuali, l'origine razziale ed etnica, le convinzioni politiche o d'altro genere.

3. I dati che rivelano le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico sono trattati esclusivamente in caso di fruizione di permessi in occasione di festività religiose o, nei casi previsti dalla legge, per l'esercizio dell'obiezione di coscienza.

4. I dati che rivelano le opinioni politiche o l'appartenenza sindacale, o l'esercizio di funzioni pubbliche e incarichi politici, di attività o di incarichi sindacali sono trattati esclusivamente ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o dai contratti collettivi anche aziendali, nonché per consentire l'esercizio dei diritti sindacali compreso il trattamento dei dati inerenti alle trattenute per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali.

5. Il trattamento di dati genetici non viene in alcun caso effettuato al fine di stabilire l'idoneità professionale di un candidato all'impiego o di un lavoratore, neppure con il consenso dell'interessato.
6. Tutte le comunicazioni all'interessato contenenti categorie particolari di dati – sia in modalità elettronica che cartacea – avvengono mediante forme di trasmissione individualizzate nei confronti dell'interessato stesso o di un suo delegato e solo per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo viene trasmesso - di regola - in plico chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto.
7. I documenti che contengono categorie particolari di dati personali, qualora debbano essere trasmessi ad altre Unità Operative in ragione delle rispettive competenze, contengono esclusivamente le informazioni necessarie allo svolgimento della specifica funzione istituzionale senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo. A tal fine vengono osservate modalità di trasmissione della documentazione che ne garantiscano la ricezione e il relativo trattamento dei dati unicamente da parte delle competenti Unità Operative e del personale autorizzato ivi afferente.
8. La documentazione inerente i turni di servizio - qualora occorra mettere a disposizione di soggetti diversi dall'Interessato (ad es. altri colleghi) i dati relativi alle presenze e assenze – non può contenere in alcun caso, nemmeno attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilità di particolari categorie di dati personali (es. permessi sindacali o dati sanitari).
9. La pubblicazione delle graduatorie per la selezione di personale o per la concessione di benefici economici, agevolazioni o contributi, viene effettuata dopo avere verificato che le informazioni ivi contenute non comportino la divulgazione di dati personali non necessari, né di dati idonei a rivelare lo stato di salute. Non sono ostensibili, se non nei casi previsti dalla legge, le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché ogni altra condizione idonea a rivelare informazioni di natura sensibile.
10. Le disposizioni di cui al presente articolo si applicano anche al trattamento dei dati personali di soggetti non inquadrati nell'ambito del rapporto di lavoro dipendente, quali liberi professionisti, consulenti collaboratori, frequentatori, titolari di corse di studio, docenti.

Art. 10 - Periodo di conservazione dei dati personali

1. I dati personali sono conservati solo per il tempo necessario al conseguimento delle finalità per le quali sono stati trattati, nel rispetto del principio di minimizzazione di cui all'articolo 5, comma 1, lettera c) del GDPR nonché degli obblighi di legge cui è tenuto il Titolare. In riferimento alla documentazione sanitaria ed amministrativa, l'Azienda Ospedaliera si attiene al rispetto dei tempi di conservazione previsti dal vigente ordinamento giuridico.
2. L'Azienda Ospedaliera assicura l'adozione di adeguate misure e procedure attraverso le quali:

- procedere alla distruzione dei dati personali, secondo le modalità previste dalla legge, una volta compiuto il termine di conservazione dei documenti analogici e digitali e dei dati personali ivi contenuti;
- 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 Ospedaliera stessa;
- procedere al riutilizzo degli apparati di memoria o *hardware* con modalità tali da garantire che non sia possibile accedere ad alcun dato personale.

Art. 11 - Categorie di destinatari

1. I dati personali oggetto di trattamento da parte dell'Azienda Ospedaliera vengono comunicati o trasmessi esclusivamente ai soggetti autorizzati ed ai responsabili del trattamento designati dal Titolare del trattamento.
2. I dati personali, inclusi quelli rientranti nelle categorie particolari e i dati giudiziari (artt. 9 e 10 del GDPR), potranno essere comunicati ad altro soggetto pubblico o a terzi quando ciò sia previsto da una norma di legge o di regolamento o nel caso risulti necessario per lo svolgimento delle funzioni istituzionali assegnate all'Azienda Ospedaliera o per le specifiche finalità per le quali i dati sono stati raccolti e trattati.
3. Al di fuori dei casi previsti da una norma di legge o di regolamento, i dati personali potranno essere comunicati solo previo consenso esplicito dell'Interessato.

Art. 12 - Comunicazione dei dati all'interessato

1. I dati personali rientranti nelle categorie particolari (art. 9 GDPR) possono essere resi noti al soggetto interessato - oltrechè mediante comunicazione diretta allo stesso - anche attraverso modalità telematiche con modalità previste dalla specifica normativa e su consenso dell'Interessato.
2. La documentazione sanitaria viene consegnata in busta chiusa e può essere ritirata dall'interessato o da suo delegato, salvo il caso di documentazione contenente dati di natura sensibile disciplinata da norme speciali che prevedono il ritiro esclusivamente da parte della persona cui tali documenti sono riferiti (es. referti HIV).

Art. 13 - Accesso a documenti, dati e informazioni. Accesso documentale, accesso civico semplice e accesso civico generalizzato

1. L'Azienda Ospedaliera applica le disposizioni ed i principi di cui all'art. 59 del D. Lgs. 196/2003 e ss.mm.ii. in materia di accesso a documenti amministrativi contenenti dati personali - disciplinato dalla L. 241/90 e ss.mm.ii. - e di accesso civico (semplice e generalizzato) - disciplinato dal D. Lgs. 33/2013 e ss.mm.ii..
2. In osservanza delle richiamate disposizioni l'Azienda Ospedaliera valuta caso per caso, anche con riguardo ad altre regolamentazioni specifiche, la possibilità da parte di terzi di accedere a documenti contenenti dati di cui agli artt. 9 e 10 del GDPR.
3. Ai sensi dell'art. 60 del D. Lgs. 196/2003 e ss.mm.ii., qualora il trattamento concerna dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento 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.
4. Si fa espresso rinvio – per gli ulteriori profili – al vigente Regolamento aziendale in materia di accesso a documenti, dati e informazioni, pubblicato sul sito *web* istituzionale, alla Sezione "Amministrazione Trasparente", sottosezioni "Disposizioni generali" – "Atti amministrativi generali" – "Regolamenti aziendali".

Art. 14 - Accesso alle cartelle cliniche

1. Ai sensi dell'art. 92, comma 2, del D. Lgs. 196/2003 e ss.mm.ii., eventuali richieste di presa visione o di rilascio di copia della cartella clinica e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'Interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a) di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'articolo 9, paragrafo 2, lettera f), del GDPR, di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale;
b) di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale.

Art. 15 - Certificato di assistenza al parto

1. Ai fini della dichiarazione di nascita, il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita.
2. In caso di madre che abbia dichiarato di non voler essere nominata si applicano le disposizioni di cui all'art. 93, commi 2 e 3, del D. Lgs. 196/2003 e ss.mm.ii.., ovvero:

- il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendano identificabile la madre che abbia dichiarato di non voler essere nominata, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento;
- durante il periodo di cui al precedente punto, la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati della madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Art. 16 – Fascicolo Sanitario Elettronico Regionale (FSE)

1. Il Fascicolo Sanitario Elettronico (FSE) è lo strumento digitale messo a disposizione dalla Regione Marche per la raccolta di documenti, dati sanitari e socio-sanitari generati da eventi clinici ed episodi assistenziali avvenuti per ciascun assistito, al fine di documentarne l'intera storia clinica e di salute e ottimizzarne le procedure di cura.
2. L'Azienda Ospedaliera - per la specifica finalità di cura - è Titolare del trattamento relativamente ai dati e documenti sanitari redatti presso l'Azienda stessa che alimentano il Fascicolo Sanitario Elettronico.
Ai sensi e per gli effetti del D.L. 34/2020 (convertito con modificazioni dalla L. 77/2020) – che ha comportato l'introduzione di una serie di misure volte ad agevolarne la diffusione e l'utilizzo - il Fascicolo Sanitario Elettronico è alimentato in modo continuo e automatico da parte dei soggetti che prendono in cura l'assistito nell'ambito del Servizio Sanitario Nazionale, anche al di fuori della regione di residenza dello stesso.
3. E', invece, richiesto il consenso dell'assistito per permettere la consultazione dei dati e documenti presenti nel Fascicolo Sanitario Elettronico da parte degli operatori sanitari, tenuti al segreto professionale o comunque all'obbligo di segretezza.
4. Il FSE consente a ciascun assistito di disporre sempre delle informazioni sanitarie e socio sanitarie che lo riguardano accedendo a documenti quali, referti, prescrizioni farmaceutiche e altri documenti.
5. L'accesso ai dati e documenti socio-sanitari ivi contenuti è consentito ai professionisti ed operatori sanitari che abbiano necessità di consultarli per finalità di cura previo, quindi, consenso libero e informato dell'assistito. A tale fine l'Azienda Ospedaliera si attiene alle disposizioni e istruzioni in merito impartite dalla Regione Marche, assicurandone l'applicazione per il tramite delle competenti strutture organizzative appositamente individuate.

Art. 17 – Dossier Sanitario

1. Il Dossier Sanitario è lo strumento informatico di raccolta e gestione dei dati e documenti sanitari del paziente, relativi ad eventi clinici presenti e trascorsi originati all'interno dell'Azienda Ospedaliera, quali prestazioni di laboratorio, visite ambulatoriali, accessi al Pronto Soccorso, ricoveri.
2. Il Dossier Sanitario persegue la finalità di rendere più efficienti i processi di diagnosi e cura del paziente erogati dall'Azienda stessa, consentendo ai diversi professionisti che vi operano di accedere a tutte le informazioni cliniche relative ai precedenti eventi clinici.
3. Il Dossier Sanitario può essere attivato unicamente previa acquisizione del consenso del paziente.
Il mancato consenso al trattamento mediante Dossier Sanitario in ogni caso non incide sulla possibilità di accedere alle prestazioni di cura richieste.
4. Al Dossier Sanitario può accedere, in forma protetta e riservata, solamente personale sanitario, autorizzato al trattamento, che svolga la propria attività presso le strutture dell'Azienda Ospedaliera e sia a vario titolo direttamente coinvolto nel percorso di cura del paziente.
5. Il Dossier Sanitario consente ai professionisti che prendono in cura il paziente di disporre di un quadro di informazioni e dati sanitari al fine di fornire un livello di assistenza il più completo e adeguato possibile.

Art. 18 – Videosorveglianza

1. L'installazione di sistemi di videosorveglianza è autorizzata dall'Azienda Ospedaliera nel rispetto delle disposizioni vigenti in materia, solo quando ciò sia strettamente indispensabile per garantire la sicurezza di dipendenti, pazienti e la tutela del patrimonio aziendale e per assicurare il monitoraggio di determinate categorie di pazienti che necessitano di continuo controllo delle condizioni di salute.
2. Il trattamento dei dati personali effettuato tramite sistemi di videosorveglianza avviene nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori (art. 4, L. 300/1970 e ss.mm.ii.) e dei Provvedimenti adottati in materia dall'Autorità Garante per la protezione dei dati personali.
3. Per quanto concerne la disciplina dei diversi aspetti inerenti la videosorveglianza, si fa espresso rinvio agli atti adottati dall'Azienda Ospedaliera (Informativa e accordo sindacale), pubblicati sul sito *web* istituzionale, alla Sezione "Privacy".

TITOLO II – I SOGGETTI DEL TRATTAMENT0

Art. 19 - Il Titolare del trattamento

1. Il Titolare del trattamento, nella persona del Legale rappresentante *pro - tempore* dell'Azienda Ospedaliera, è definito all'art. 4 del GDPR come "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", e, "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".
2. Al Titolare competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
3. Il Titolare è il soggetto su cui grava la responsabilità generale del trattamento, adempie alle prescrizioni contenute nelle varie disposizioni del GDPR e dimostra che il trattamento dei dati personali è effettuato

conformemente al GDPR stesso secondo il principio di responsabilità, oltrechè l'efficacia delle misure adottate ("accountability").

4. Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione e la cifratura dei dati personali, la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati.

5. Gli artt. 24 e 25 del GDPR individuano gli obblighi generali in capo al Titolare del trattamento, mentre obblighi specifici sono contenuti in varie altre disposizioni del GDPR stesso. In particolare, il Titolare:

- designa il Responsabile della protezione dei dati di cui all'art. 37 del GDPR;
- nomina con proprio atto i responsabili del trattamento dei dati personali di cui all'art. 28 del GDPR impartendo agli stessi - 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, all'esercizio dei diritti dell'interessato di cui al Capo III del GDPR;
- attribuisce, nell'ambito dell'assetto organizzativo aziendale, specifici compiti e funzioni connessi al trattamento dei dati ai soggetti designati secondo quanto previsto dall'art. 2-*quaterdecies*, comma 1, del D. Lgs. 196/2003 e ss.mm.ii.;
- individua le modalità più opportune per autorizzare al trattamento dei dati le persone che operano sotto la propria diretta autorità, ai sensi dell'art. 2-*quaterdecies*, comma 2, del D. Lgs. 196/2003 e ss.mm.ii.;
- tiene il registro delle attività di trattamento svolte sotto la propria responsabilità secondo quanto previsto dall'art. 30 del GDPR;
- in caso di violazione dei dati personali provvede alla notifica al Garante per la protezione dei dati personali senza ingiustificato ritardo secondo le modalità e i contenuti di cui all'art. 33 del GDPR;
- svolge, nei casi previsti dall'art. 35 del GDPR, una valutazione d'impatto sulla protezione dei dati consultandosi con il Responsabile della protezione dei dati e procede, qualora necessario, alla consultazione preventiva di cui all'art. 36 del GDPR.

6. Il Titolare può dimostrare il rispetto degli obblighi a suo carico anche attraverso l'adesione a codici di condotta o a meccanismi di certificazione di cui agli artt. 40 e 42 del GDPR.

7. Il Titolare del trattamento adotta misure tecniche ed organizzative adeguate onde perseguire le seguenti finalità:

- garantire, ed essere al contempo in grado di dimostrare, che il trattamento è effettuato in conformità al GDPR; ciò comportando l'attuazione di adeguate politiche in materia di protezione dei dati;
- proteggere i dati fin dalla fase di ideazione e progettazione del trattamento o di un sistema e nel corso del trattamento stesso (c.d. "Privacy by design"), ad esempio mediante tecniche di pseudonimizzazione (art. 25 del GDPR);
- assicurare che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni singola finalità del trattamento (c.d. "Privacy by default") rendendo inaccessibili i dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica, e ciò con riferimento alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione ed all'accessibilità (art. 25 del GDPR).

8. Nell'individuazione delle misure tecniche ed organizzative adeguate, il Titolare del trattamento tiene conto dei seguenti elementi:

- lo stato dell'arte ed i costi di attuazione limitatamente all'approccio di Privacy by Design;
- la natura del trattamento;
- l'ambito di applicazione;
- il contesto;
- le finalità del trattamento;
- i rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Art. 20 - Contitolari del trattamento

1. Ai sensi dell'art. 26 del GDPR, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono Contitolari del trattamento.
2. I Contitolari stabiliscono in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR stesso - con particolare riguardo all'esercizio dei diritti dell'interessato – e le rispettive funzioni di comunicazione delle informazioni.
3. 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. Il contenuto essenziale dell'accordo è messo a disposizione dell'Interessato.
4. In ogni caso, l'accordo interno tra Contitolari non pregiudica i diritti dell'Interessato il quale, indipendentemente dalle disposizioni di tale accordo, può esercitare i propri diritti nei confronti di ciascun Titolare del trattamento.

Art. 21 - Interessato e soggetti terzi

1. L'Interessato del trattamento è la persona fisica cui si riferiscono i dati personali.
2. Ai sensi dell'art. 4, n. 10), del GDPR i soggetti terzi sono la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non siano l'Interessato, il Titolare del trattamento, il Responsabile e le persone autorizzate al trattamento.
3. Il quadro normativo di cui al GDPR attribuisce al soggetto interessato l'esercizio di una serie di diritti in tema di protezione dei dati personali, oggetto di trattazione al Titolo III del presente Regolamento.
4. Le modalità per l'esercizio dei diritti dell'Interessato sono riportate nell'informativa generale e nelle diverse Informative specifiche sul trattamento dei dati messa a disposizione degli interessati e pubblicate sul sito *web* istituzionale dell'Azienda Ospedaliera, alla Sezione "Privacy".
5. L'Azienda Ospedaliera ha reso, altresì, disponibile all'Interessato apposita modulistica da utilizzare per l'esercizio dei propri diritti in materia di protezione dei dati personali, parimenti pubblicata nell'ambito della citata Sezione del sito *web*.

Art. 22 – Il Responsabile del trattamento *ex* art. 28 del GDPR

1. Ai sensi dell'art. 28 del GDPR il Responsabile del trattamento è la persona fisica o giuridica – esterna all'Azienda Ospedaliera – che, in virtù di rapporti contrattuali (generalmente finalizzati all'acquisizione di servizi), tratta i dati personali per conto del Titolare, previa designazione.
2. L'Azienda Ospedaliera designa responsabili del trattamento tutti i soggetti esterni cui è affidato lo svolgimento di attività/servizi di competenza aziendale, ivi comprese le attività manutentive, che comunque comportano necessariamente il trattamento di dati personali.

3. L'Azienda Ospedaliera designa quali responsabili del trattamento dei dati personali esclusivamente soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche ed organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'Interessato.
4. L'atto di designazione viene predisposto secondo schema tipo redatto in conformità alle disposizioni di cui all'art. 28 del GDPR come pubblicato sul sito *web* istituzionale dell'Azienda Ospedaliera in "Bandi e Gare – Bandi di gara e contratti – Modulistica specifica per appalti".
5. Tale atto di designazione/contratto – stipulato in formato elettronico – vincola il Responsabile al Titolare del trattamento in particolar modo per quanto riguarda la durata, la natura, la finalità del trattamento, il tipo di dati trattati, le categorie di interessati, gli obblighi ed i diritti del Titolare del trattamento.
6. Nel caso in cui il Responsabile del trattamento ricorra, previa specifica autorizzazione, ad un Sub – Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto dell'Azienda Ospedaliera, a tale Sub – Responsabile sono imposti, mediante un contratto, gli stessi obblighi a cui è stato sottoposto il Responsabile. Qualora il Sub - Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti dell'Azienda Ospedaliera l'intera responsabilità dell'adempimento degli obblighi del Sub – Responsabile.
7. Nel rispetto delle istruzioni operative impartire dal Titolare, spetta al Direttore/Dirigente Responsabile del procedimento di acquisizione di determinato servizio curare l'istruttoria finalizzata alla formalizzazione dell'atto di designazione del soggetto esterno in qualità di Responsabile del trattamento; ciò avvalendosi anche del supporto consulenziale del Responsabile della protezione dei dati.
8. Il Titolare del trattamento può delegare il Direttore/Dirigente Responsabile del procedimento alla nomina del Responsabile del trattamento *ex* art. 28 del GDPR.

Art. 23 - Soggetti designati in qualità di Responsabili "interni" del trattamento

1. L'art. 2-*quaterdecies*, comma 1, del D. Lgs. 196/2003 e ss.mm.ii. conferisce al Titolare del trattamento la possibilità di prevedere che – nell'ambito del proprio assetto organizzativo - specifici compiti e funzioni connesse al trattamento dei dati personali siano attribuiti a persone fisiche espressamente designate operanti sotto la sua autorità.
2. Ai sensi del richiamato art 2-*quaterdecies*, comma 1, del D. Lgs. 196/2003 e ss.mm.ii., l'Azienda Ospedaliera, in considerazione della complessità e dell'eterogeneità delle proprie attività e compiti istituzionali e della necessità di assicurare nei diversi livelli la più efficace applicabilità delle disposizioni in materia di protezione dei dati personali, tenuto conto altresì delle disposizioni di natura organizzativa e gestionale contenute nell'Atto aziendale e nei relativi provvedimenti attuativi, designa quali Responsabili "interni" del trattamento i titolari dei seguenti incarichi:

- Direttori di Struttura Complessa (ovvero sostituti ex art. 22 del CCNL Area Sanità 2016 – 2018 del 19.12.2019)
- Responsabili di Struttura Semplice Dipartimentale
- Responsabile dell'Ufficio Relazioni con il Pubblico
- Responsabile del Servizio di Prevenzione e Protezione Aziendale;

ciascuno in riferimento ai trattamenti rientranti nell'espletamento delle funzioni/attività istituzionali e gestionali assegnate in ragione delle specifiche competenze, professionalità e responsabilità.
3. I soggetti designati in qualità di Responsabili "interni" del trattamento, in ragione dell'incarico ricoperto all'interno dell'Azienda Ospedaliera, svolgono compiti e funzioni di vigilanza sul rispetto e attuazione delle

istruzioni privacy da parte del personale autorizzato al trattamento di dati personali in servizio presso le strutture rispettivamente dirette.
4. I soggetti designati in qualità di Responsabili "interni" del trattamento sono nominati con determina del Direttore Generale dell'Azienda Ospedaliera – oggetto di periodico aggiornamento - e nell'effettuare i compiti di cui al comma 3 del presente articolo si attengono – a loro volta – alle specifiche istruzioni loro fornite dal Titolare del trattamento. In caso di vacanza della titolarità degli incarichi di cui al precedente comma 2 e nelle more del relativo conferimento, le correlate responsabilità gestionali in tema di applicazione delle misure *privacy* sono in capo al Direttore Sanitario e al Direttore Amministrativo in funzione dello specifico ambito organizzativo.
5. La UOC Gestione ed Amministrazione delle Risorse Umane - in sede di conferimento di nuovi incarichi di direzione/responsabilità di struttura complessa ovvero di struttura semplice dipartimentale – provvede all'inserimento di specifica clausola contrattuale contenente la designazione del titolare di incarico in qualità di Responsabile "interno" del trattamento e fornendo al medesimo le relative istruzioni.

Art. 24 – Gli Autorizzati al trattamento

1. Ai sensi dell'art. 2-*quaterdecies*, comma 2, del D. Lgs. 196/2003 e ss.mm.ii. e dell'art. 29 del GDPR, tutto il Personale in servizio a diverso titolo all'interno delle Unità Operative aziendali è autorizzato – sulla base di determina del Direttore Generale dell'Azienda Ospedaliera – al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza.
2. Gli Autorizzati si attengono con scrupolo e diligenza alle istruzioni impartite dal Titolare e loro fornite dal designato in qualità di Responsabile "interno" del trattamento della struttura di appartenenza, il quale deve garantirne il rispetto e l'attuazione attraverso attività di vigilanza.
3. La UOC Gestione ed Amministrazione delle Risorse Umane - in sede di assunzione in servizio di nuove unità di Personale – provvede all'inserimento di specifica clausola contrattuale contenente l'autorizzazione del neo assunto ad effettuare il trattamento di dati personali nell'ambito dello svolgimento delle proprie attività istituzionali e fornendo contestualmente le relative istruzioni sulla cui osservanza e rispetto è tenuto, appunto, a vigilare il designato in qualità di Responsabile "interno" del trattamento della rispettiva struttura.
4. Sono, altresì, Autorizzati al trattamento soggetti quali volontari, tirocinanti, studenti, specializzandi che prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'Azienda Ospedaliera in attività comportanti il trattamento di dati personali dell'Azienda stessa.
5. Sempre in analogia alle modalità previste al comma 3 del presente articolo, la UOC Direzione Medica dei Presidi e la UOC Direzione Amministrativa di Presidio - in sede di autorizzazione alla frequenza delle strutture aziendali da parte di volontari, tirocinanti, studenti e specializzandi – provvedono all'inserimento di specifica clausola contenente l'autorizzazione delle predette figure ad effettuare il trattamento di dati personali nell'ambito della frequenza delle strutture aziendali e fornendo, parimenti, le relative istruzioni sulla cui osservanza e rispetto è tenuto a vigilare il designato in qualità di Responsabile "interno" del trattamento della rispettiva struttura.

Art. 25 - Il Responsabile della protezione dei dati (RPD)

1. Il GDPR, ai sensi dell'art. 37, comma 1, lett. a), prevede l'obbligo per il Titolare del trattamento di designare il Responsabile della protezione dei dati "quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali".

2. Al fine di dare attuazione alle disposizioni di cui al GDPR onde assicurare lo svolgimento delle funzioni e dei compiti stabiliti dagli artt. 38 e 39, l'Azienda Ospedaliera – con apposito atto pubblicato sul sito *web* istituzionale - ha designato quale Responsabile della protezione dei dati un professionista interno; ciò nella logica di promuovere forme di valorizzazione e crescita del personale, intese come incremento delle conoscenze, delle capacità e dello sviluppo professionale.
3. Il Responsabile della protezione dei dati costituisce il punto di contatto tra il Titolare che lo ha designato e l'Autorità Garante Privacy, con la quale deve cooperare per tutte le questioni connesse al trattamento dei dati personali, consultandola anche preventivamente quando necessario.
4. Il Responsabile della protezione dei dati, comunque tenuto al rispetto delle norme in materia di segreto o riservatezza, deve in ogni modo facilitare l'accesso, da parte dell'Autorità Garante, ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti istituzionali, compresi quelli finalizzati all'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi.
5. Il Responsabile della protezione dei dati è preposto allo svolgimento – in ambito aziendale – delle seguenti funzioni e compiti stabiliti dall'art. 39 del GDPR:
a) informare e fornire consulenza al Titolare del trattamento, nonché al personale aziendale che esegue attività di trattamento dati, in merito agli obblighi derivanti dal GDPR e dalla relativa normativa di attuazione;
b) sorvegliare l'osservanza della normativa privacy e delle politiche aziendali sempre in materia di protezione dei dati, 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, parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del GDPR;
d) cooperare con l'Autorità di controllo;
e) fungere da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
6. In riferimento ai compiti di cui al punto b), rientrano - in particolare - la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità e l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e dei soggetti preposti al trattamento dei dati personali nel contesto aziendale; ciò anche mediante la realizzazione di audit interni sotto il coordinamento del RPD stesso, onde assicurare la *compliance* dell'organizzazione ai principi ed alle disposizioni vigenti in materia.
7. Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
8. Il Responsabile della protezione dei dati provvede, altresì:

- a supportare il Titolare nella tenuta del Registro delle attività di trattamento di cui all'art. 30 del GDPR;
- alla formalizzazione della documentazione privacy quali istruzioni, informative, modulistica, procedure, oltreché di ogni opportuna e adeguata misura organizzativa;
- al coordinamento del Gruppo multidisciplinare di supporto al RPD stesso;
- a supportare le Unità Operative aziendali per gli ambiti e le materie di cui al GDPR;

- a gestire i contatti con gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

9. Il Responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del Titolare del trattamento ed è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti.
10. Per poter svolgere i compiti assegnatigli dal GDPR, il Responsabile della protezione dei dati può legittimamente accedere a tutte le informazioni necessarie ad individuare i trattamenti svolti per conto del Titolare al fine di effettuare una analisi e verifica dei trattamenti in termini di loro conformità ed eventuale necessità di rettifica.
11. Il Titolare del trattamento fornisce al Responsabile della protezione dei dati le risorse umane, tecnologiche, strumentali ed economiche necessarie per assolvere i compiti assegnati - comprese quelle necessarie ad aggiornare e mantenere la propria conoscenza specialistica - oltre al supporto attivo da parte delle diverse articolazioni aziendali e un tempo sufficiente per l'espletamento dei compiti sopra descritti.
12. Il Responsabile della protezione dei dati è designato dall'Azienda Ospedaliera in funzione delle qualità professionali - in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati - e della capacità di assolvere i compiti di cui all'articolo 39 del GDPR, in coerenza con gli indirizzi forniti dall'Autorità Garante in ordine a "designazione, posizione e compiti del Responsabile della protezione dei dati" di cui al Provvedimento del 29 aprile 2021 citato in premessa.
13. L'Azienda Ospedaliera pubblica i dati di contatto del Responsabile della protezione dei dati e li comunica all'Autorità Garante della Protezione dei dati personali in conformità alle indicazioni fornite dall'Autorità stessa e si assicura che sia tempestivamente e adeguatamente coinvolto su tutte le questioni riguardanti la protezione dei dati personali.
14. Il Responsabile della protezione dei dati, nello svolgimento dei propri compiti, può avvalersi di Referenti Privacy individuati nell'ambito delle diverse Unità Operative dell'Azienda Ospedaliera e gli viene assicurata la necessaria collaborazione da parte della UOC Servizio Informatico, UOC Ingegneria Clinica ed *Information and Communication Technology* e UOC Servizio Tecnico e Manutenzioni in merito all'applicazione interna delle misure di sicurezza e di protezione dei dati personali per i trattamenti automatizzati adottati.

Art. 26 – Ruolo del Responsabile per la transizione al digitale (RTD)

1. In relazione ai compiti e funzioni propri del Responsabile per la transizione al digitale (RTD) di cui all'art. 17 del D.Lgs. 82/2005 e ss.mm.ii. (Codice dell'Amministrazione Digitale) e relative disposizioni di attuazione, aventi rilevanza per gli aspetti inerenti la protezione dei dati personali, lo stesso RTD – nominato con apposita determina del Direttore Generale - opera nel rispetto dei principi di *privacy by design e privacy by default* previsti dal GDPR.
2. Il Responsabile per la transizione al digitale si avvale dei più opportuni strumenti di raccordo e consultazione con le altre figure coinvolte nel processo di digitalizzazione dell'Azienda e, tra gli altri, il Responsabile della protezione dei dati.

Art. 27 – Ruolo della UOC Servizio Informatico e della UOC Ingegneria Clinica ed *Information and Communication Technology*

1. Nell'ambito del sistema di *Data Protection Governance* Aziendale, per quanto attiene gli specifici aspetti della sicurezza informatica, la UOC Servizio Informatico e la UOC Ingegneria Clinica ed *Information and Communication Technology* – in ragione degli ambiti di rispettiva competenza – provvedono a:

- assicurare i sistemi di autenticazione/autorizzazione ai sistemi informativi di settore;

- curare la protezione della rete telematica aziendale;
- individuare l'elenco degli amministratori di sistema dei quali definisce i compiti e le misure per la registrazione e la conservazione delle attività svolte, ad eccezione dei trattamenti affidati ad un Responsabile del trattamento per i quali provvede quest'ultimo;
- elaborare e rendere disponibili misure di sicurezza a protezione della riservatezza, disponibilità e integrità delle banche dati aziendali, tra le quali: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative adottate;
- fornire, per gli ambiti di rispettiva competenza, il necessario supporto e collaborazione al Titolare, ai soggetti designati in qualità di Responsabili "interni" del trattamento e al Responsabile della protezione dei dati.

Art. 28 - Gli Amministratori di Sistema

1. L'Azienda Ospedaliera applica quanto previsto dal Provvedimento del Garante per la Protezione dei Dati personali del 27 novembre 2008, modificato con provvedimento del 25 giugno 2009 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".
2. Come previsto dal richiamato Provvedimento del Garante per la Protezione dei Dati vengono definiti Amministratori di Sistema "le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (…) vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. Gli amministratori di sistema così ampiamente individuati (…) nelle loro consuete attività sono, in molti casi, concretamente responsabili di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati".
3. Il Direttore della UOC Servizio Informatico ed il Direttore della UOC Ingegneria Clinica ed *Information and Communication Tecnhology*, sulla base di apposito atto, rivestono in Azienda anche il ruolo di "Amministratore di Sistema", cui competono conseguentemente – ognuno per gli ambiti di rispettiva competenza – la designazione del personale dipendente operante sempre in qualità di Amministratore di Sistema all'interno delle strutture da essi dirette, secondo le specifiche indicazioni di cui al richiamato Provvedimento.
4. Gli Amministratori di Sistema vengono nominati previa valutazione dell'esperienza, capacità e affidabilità dei soggetti designati.
5. La designazione è individuale mediante apposito atto e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato, ivi compreso il profilo relativo alla sicurezza.
6. L'operato degli Amministratori di sistema è oggetto, con cadenza almeno annuale, di una attività di verifica da parte dei Responsabili delle suddette Unità Operative, in modo da accertarne la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti di dati personali previste dalle norme vigenti.

Art. 29 – Gruppo multidisciplinare di supporto al Responsabile della protezione dei dati

1. A supporto delle attività proprie del Responsabile della protezione dei dati, con apposito atto, è costituito un Gruppo multidisciplinare con competenze medico/sanitarie, tecnico/informatiche e giuridico/legali.
2. La composizione del Gruppo multidisciplinare è formata da membri permanenti che rivestono ruoli chiave all'interno dell'organizzazione aziendale e possiedono competenze tali da garantire presidio normativo, tecnico e sanitario (sia di ambito medico che infermieristico) per ogni profilo attinente la protezione dei dati personali.
3. Nell'ottica della massima applicazione del principio di *accountability* previsto dal GDPR, il Gruppo multidisciplinare fornisce supporto e consulenza al Responsabile della protezione dei dati nello svolgimento di attività di elaborazione proposte/soluzioni alla Direzione Generale, rilascio pareri, formalizzazione documenti/informative e attività di sorveglianza.
4. Le attività dei componenti del Gruppo - coordinate dal Responsabile della protezione dei dati - possono essere assolte sia attraverso la partecipazione a sedute tematiche a seguito di apposita convocazione, sia tramite contatti e confronti diretti del Responsabile della protezione dei dati con singoli componenti in ragione della specificità della questione oggetto di trattazione.
5. Le sedute del Gruppo multidisciplinare sono tenute e calendarizzate a cura del Responsabile della protezione dei dati il quale ha facoltà di convocare ulteriori professionalità aziendali sulla base delle tematiche e problematiche da esaminare e decisioni da assumere.

Art. 30 – Il Referente Privacy di struttura

1. In ragione della complessità delle funzioni istituzionali svolte e della quantità e natura dei dati trattati, oltreché della necessità di garantire l'adozione di misure organizzative armoniche presso ciascuna Struttura/Servizio/Ufficio, il modello di *Data Protection Governance* aziendale contempla l'individuazione di un Referente Privacy di struttura onde assicurare un presidio coordinato delle operazioni di trattamento sulla base di una corretta circolazione di flussi informativi in materia di protezione dei dati personali tra tutti i soggetti coinvolti (Titolare, Responsabile della protezione dei dati, designati in qualità di Responsabili "interni" del trattamento, UOC Servizio Informatico, UOC Ingegneria Clinica ed *Information and Communication Tecnhology*, ecc.).
2. Il Referente Privacy – già Autorizzato al trattamento sulla base di quanto previsto all'art. 24 del presente Regolamento – opera sotto la vigilanza del soggetto designato in qualità di Responsabile "interno" del trattamento e, in particolare, per quanto concerne la tematica della protezione dei dati personali, è tenuto a:

- curare che nell'ambito dell'articolazione organizzativa presso la quale presta servizio tutte le comunicazioni/informazioni da parte del Titolare o del Responsabile della protezione dei dati vengano capillarmente e adeguatamente trasmesse all'interno dell'articolazione organizzativa stessa;
- fornire supporto al designato in qualità di Responsabile "interno" del trattamento nell'applicazione e attuazione delle istruzioni e misure impartite dal Titolare o dal Responsabile della protezione dei dati;
- gestire i contatti con il Responsabile della protezione dei dati in ordine alla soluzione di specifiche problematiche formulando anche proposte;

3. Lo stesso Referente Privacy di struttura viene, altresì, coinvolto dal Responsabile della protezione dei dati nell'esecuzione dei diversi adempimenti quali gestione *data breach*, aggiornamento Registro delle attività di trattamento, valutazioni di impatto.
4. Il Referente Privacy di struttura viene individuato dal designato in qualità di Responsabile "interno" del trattamento mediante comunicazione scritta al Responsabile della protezione dei dati.
5. Il Responsabile della protezione dei dati provvede - periodicamente - a richiedere ai designati in qualità di Responsabili "interni" l'aggiornamento dei nominativi dei Referenti Privacy. In caso di mancata individuazione, il ruolo si intende assunto dallo stesso designato in qualità di Responsabile "interno" del trattamento.

TITOLO III – I DIRITTI DELL'INTERESSATO

Art. 31 - Informazioni sul trattamento dei dati personali

1. L'Azienda Ospedaliera - quale Titolare del trattamento - è dotata di un sistema documentale relativamente alle informazioni sul trattamento da fornire al soggetto interessato. Tali informazioni, in linea con i principi contenuti nel GDPR, sono rese all'utente in forma coincisa, trasparente, intelligibile e con un linguaggio semplice e chiaro.
2. L'Azienda Ospedaliera – in relazione ai diversi ambiti di attività istituzionale – ha adottato specifiche Informative sul trattamento dei dati personali che riportano le seguenti informazioni stabilite dall'art. 13 del GDPR:

- l'identità e i dati di contatto del Titolare del trattamento e del Responsabile della protezione dei dati;
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- i legittimi interessi perseguiti dal Titolare del trattamento o da terzi (nel caso di trattamenti basati sull'art. 6, par. 1, lettera f) del GDPR);
- gli eventuali destinatari, o categorie di destinatari, cui possono essere comunicati i dati;
- ove applicabile, l'intenzione del Titolare di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione UE, nei termini previsti da GDPR;
- il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- l'esistenza del diritto dell'Interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
- qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio del consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali;
- 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'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.

3. In linea con le indicazioni formulate dall'Autorità Garante per la protezione dei dati personali, l'Azienda Ospedaliera – per il tramite dei propri professionisti/operatori – rende disponibile le diverse Informative sul trattamento dei dati personali in formato cartaceo nei luoghi di maggiore e frequente contatto con l'utenza e provvede alla pubblicazione delle stesse alla Sezione "Privacy" del proprio sito *web* istituzionale.
4. Il personale autorizzato al trattamento – sulla base delle istruzioni all'uopo impartite dal Titolare – invita l'utenza a prendere visione dell'Informativa privacy o direttamente mediante lettura della stampa cartacea disponibile nei diversi punti d'accesso alle strutture o mediante lettura della stessa sul sito *web*.
5. Qualora l'Azienda Ospedaliera intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'Interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

Art. 32 - Il consenso al trattamento dei dati

1. In conformità ai contenuti del Provvedimento n. 55/2019 dell'Autorità Garante per la protezione dei dati personali "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – 7 marzo 2019", l'Azienda Ospedaliera assicura la piena applicazione del principio in base al quale, nel caso di trattamenti di dati personali per "finalità di cura" effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza, non viene richiesto il consenso del paziente; ciò in quanto trattasi di attività di trattamento di dati personali necessari alla prestazione sanitaria richiesta dall'interessato.
2. Sono da intendersi necessari alla prestazione sanitaria richiesta dall'interessato anche i trattamenti di dati personali connessi alle attività amministrativo/contabili che l'Azienda Ospedaliera, ai sensi di disposizioni di legge o di regolamento, è tenuta ad effettuare in qualità di soggetto pubblico operante nell'ambito del Servizio Sanitario Regionale e che, appunto, in quanto tali, non richiedono - parimenti a quelli di cui al precedente comma - l'acquisizione del consenso dell'interessato.
3. Diversamente, i trattamenti di dati personali attinenti solo in senso lato alla cura – ma non strettamente necessari anche se effettuati da professionisti sanitari – richiedono una distinta base giuridica da individuarsi nel consenso o in altro presupposto di liceità.
4. Per quanto concerne l'individuazione dei trattamenti di dati personali in ambito sanitario che richiedono il consenso esplicito dell'interessato, l'Azienda Ospedaliera ha recepito le indicazioni fornite dall'Autorità Garante con il richiamato Provvedimento n. 55/2019 dandone evidenza nell'ambito dell'Informativa sul trattamento dei dati personali per l'erogazione di prestazioni sanitarie, anch'essa pubblicata alla Sezione "Privacy" del proprio sito *web* istituzionale.
5. Qualora sia richiesto il consenso dell'interessato, lo stesso deve essere reso mediante sottoscrizione di apposita modulistica in uso presso le Unità Operative, previa visione e presa d'atto dell'Informativa.
6. L'eventuale rifiuto a prestare il consenso al trattamento dei dati per finalità diverse da quelle di cura, comporta l'impossibilità di effettuare il relativo trattamento dei dati.
7. Se il consenso dell'Interessato è prestato nel contesto di una dichiarazione scritta che riguarda altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro.

8. L’interessato ha il diritto di revocare il proprio consenso al trattamento dei dati personali in qualsiasi momento e ciò non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'Interessato è informato di ciò.
9. La manifestazione del consenso sarà valida ed efficace fino alla revoca dello stesso.
10. Il consenso è revocato con la stessa facilità con cui è accordato.
11. Qualora il trattamento dei dati personali sia fondato sul rilascio del preventivo consenso da parte dell’Interessato, è compito dell’Azienda Ospedaliera dimostrare che questi abbia prestato il proprio consenso libero e informato al trattamento dei dati personali.
12. Il Titolare assicura attraverso idonee modalità l’archiviazione dei consensi espressi dagli interessati in modo da rendere fruibili e rintracciabili le autorizzazioni da questi rilasciate.
13. Il consenso al trattamento dei dati è comunque distinto dal consenso informato alla prestazione sanitaria.

Art. 33 - Diritto di accesso

1. Ai sensi dell’art. 15 del GDPR l'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di 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 o organizzazioni internazionali;
d) quando possibile, 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 dell'Interessato 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 della protezione dei dati;
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 per l'interessato.
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento.
3. L’Azienda Ospedaliera fornisce una copia dei dati personali oggetto di trattamento.
4. Nell’addebitare i costi sostenuti per il rilascio di copie all’interessato, l’Azienda Ospedaliera applica quanto previsto sul punto dalla vigente regolamentazione in materia di accesso a documenti, dati e informazioni richiamata in premessa e a cui si fa espresso rinvio. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
5. Il diritto di ottenere una copia dei dati personali non deve ledere i diritti e le libertà altrui.

Art. 34 - Diritto di rettifica

1. Ai sensi dell'art. 16 del GDPR l'Interessato ha il diritto di ottenere dal Titolare del trattamento la 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.

Art. 35 - Diritto alla cancellazione

1. Ai sensi dell'art. 17 del GDPR l'Interessato, fatti salvi i casi di esclusione previsti dalla legge, ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il Titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:
a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
b) l'Interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
c) l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento.
2. L'esercizio di tale diritto in ambito sanitario va rapportato agli obblighi di conservazione documentale previsti dalla legge ed ai motivi di esclusione richiamati all'art. 17, paragrafo 3, del GDPR.

Art. 36 - Diritto di limitazione di trattamento

1. L'art. 18 del GDPR stabilisce il diritto dell'Interessato a che i suoi dati siano utilizzati limitatamente a quanto necessario ai fini della conservazione.
2. L'art. 4, n. 3) del GDPR definisce la limitazione di trattamento come il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.
3. L'Interessato ha il diritto di ottenere dal Titolare del trattamento la limitazione del trattamento quando ricorre una delle seguenti ipotesi previste, sempre, all'art. 18, paragrafo 1, del GDPR:
a) l'Interessato contesta l'esattezza dei dati personali;
b) il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
c) benché il Titolare non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
d) l'Interessato si è opposto al trattamento e si è in attesa delle verifiche necessarie per determinare se i motivi legittimi del Titolare del trattamento siano prevalenti rispetto a quelli dell'Interessato.
4. Le modalità per limitare il trattamento dei dati personali possono consistere nel trasferire temporaneamente i dati selezionati verso un altro sistema di trattamento, nel rendere i dati personali selezionati inaccessibili agli utenti o nel rimuovere temporaneamente i dati pubblicati dal sito *web*.
5. Se il trattamento è limitato, i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.

6. L'Interessato che ha ottenuto la limitazione del trattamento è informato dal Titolare del trattamento prima che detta limitazione sia revocata.

Art. 37 - Diritto alla portabilità dei dati

1. Ai sensi dell'art. 20 del GDPR, l'Interessato - nei casi di trattamento effettuato con mezzi automatizzati - ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e ha il diritto di trasmettere tali dati ad altro Titolare senza impedimenti da parte del Titolare cui li ha forniti.
2. Il diritto alla portabilità è esercitabile qualora il trattamento sia basato sul consenso o su un contratto stipulato con l'Interessato.
3. Nell'esercitare il proprio diritto, l'Interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile.
4. L'esercizio del diritto alla portabilità dei dati non è applicabile laddove il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare.

Art. 38 - Diritto di opposizione

1. Ai sensi dell'art. 21 del GDPR, l'Interessato – per motivi specifici che lo riguardano - ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali effettuato dal Titolare per l'esecuzione di compiti di interesse pubblico o fondato sul perseguimento di un legittimo interesse.
2. In tali casi il Titolare si astiene dal trattare ulteriormente i dati personali salvo che dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'Interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
3. 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. 39 - Reclamo all'Autorità Garante per la protezione dei dati personali

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'Interessato che ritenga che il trattamento che lo riguarda violi il GDPR ha il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali ai sensi dell'articolo 77 del GDPR.

Art. 40 - Diritti riguardanti le persone decedute

1. Ai sensi di quanto previsto dall'art. 2-*terdecies* del D.Lgs. 196/2003 e ss.mm.ii., i diritti di cui agli articoli da 15 a 22 del GDPR, riferiti a dati personali concernenti persone decedute, possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

Art. 41 – Modalità per l'esercizio dei diritti dell'Interessato

1. L'insieme dei diritti contemplato dal GDPR consente al soggetto interessato – previa presentazione di specifica richiesta al Titolare – di verificare e assicurarsi che i propri dati personali non vengano utilizzati in maniera non corretta o comunque per finalità diverse dallo scopo legittimo per cui sono stati inizialmente conferiti all'Azienda.

2. L'Azienda Ospedaliera - in coerenza con quanto previsto all'art. 12 del GDPR - fornisce le dovute comunicazioni all'Interessato che esercita uno dei diritti di cui agli artt. 15 – 22 del GDPR stesso in forma coincisa, trasparente e facilmente accessibile, con un linguaggio semplice e chiaro, soprattutto se le informazioni sono destinate a soggetto minore.
3. Le informazioni richieste sono rese al più tardi entro un mese dal ricevimento della richiesta stessa.
Il termine di cui al precedente comma può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il Titolare informa l'Interessato di tale proroga e dei motivi del ritardo entro un mese dal ricevimento della richiesta.
4. Se non ottempera alla richiesta dell'Interessato, il Titolare – sempre entro un mese dal ricevimento della richiesta – informa l'Interessato stesso circa i motivi dell'inottemperanza e della possibilità di proporre reclamo all'Autorità Garante per la protezione dei dati personali e di proporre ricorso giurisdizionale.
5. Se l'Interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'Interessato.
6. Le comunicazioni rese all'Interessato a seguito dell'esercizio dei propri diritti in materia di protezione dei dati personali sono gratuite. Qualora le richieste dell'Interessato fossero manifestamente infondate o eccessive – in particolare per il loro carattere ripetitivo – il Titolare si riserva la facoltà di addebitare un contributo spese nella misura determinata dalla vigente regolamentazione aziendale in tema di accesso a documenti, dati e informazioni oppure di rifiutare il soddisfacimento della richiesta.
7. E' posto in capo al Titolare l'onere di dimostrare il carattere manifestamente infondato o eccessivo della richiesta.
8. Al fine di agevolare l'Interessato nell'esercizio dei propri diritti in materia di protezione dei dati personali, l'Azienda Ospedaliera ha provveduto a formalizzare e rendere disponibile apposita modulistica pubblicata sul sito web istituzionale, alla Sezione "Privacy".

TITOLO IV – MISURE TECNICHE ED ORGANIZZATIVE

Art. 42 - Misure di sicurezza di carattere generale

1. L'Azienda Ospedaliera, nell'effettuare attività di trattamento dei dati personali, garantisce l'applicazione di idonee e preventive misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita - anche accidentale - dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
2. Nell'ambito dell'Azienda Ospedaliera il sistema gestionale privacy rappresenta un requisito indispensabile di qualità, per assicurare il quale, l'Azienda stessa adotta tutte le misure tecniche ed organizzative necessarie a far sì che la protezione dei dati personali e la loro tenuta in sicurezza siano non solo il rispetto di un obbligo normativo ma anche l'occasione di una crescita organizzativa e culturale.
3. In conformità ai principi contenuti agli artt. 24, 25 e 32 del GDPR, il Titolare del trattamento – attraverso i designati in qualità di Responsabili "interni" del trattamento, il personale autorizzato ed in particolare mediante il supporto del Responsabile della protezione dei dati, della UOC Servizio Informatico e della UOC Ingegneria Clinica ed *Information and Communication Technology* – mette in atto misure e tecniche organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono:

- la pseudominizzazione e la cifratura dei dati personali trattati;

- procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4. Il Titolare e i soggetti designati in qualità di Responsabili "interni" del trattamento fanno sì che chiunque agisca sotto la loro autorità e ha accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare e dai Responsabili medesimi.

5. L'accesso ad ogni sistema informatizzato è consentito solo se necessario e coerente rispetto al trattamento dei dati per il quale si è stati formalmente autorizzati ed è consentito soltanto utilizzando apposite credenziali di autorizzazione fornite dall'Azienda, strettamente personali e della cui riservatezza risponde personalmente il singolo soggetto autorizzato al trattamento dei dati personali.

6. I relativi processi di assegnazione di credenziali di accesso ai predetti sistemi sono gestiti – a seconda dei rispettivi ambiti di competenza – dalla UOC Servizio Informatico e dalla UOC Ingegneria Clinica ed *Information and Communication Technology* che provvedono ad elaborare specifiche *policy* finalizzate ad assicurare la sicurezza dei trattamenti, con il coinvolgimento del Responsabile della protezione di dati.

7. Tutti i soggetti autorizzati al trattamento sono tenuti a trattare i soli dati essenziali per svolgere l'attività istituzionale, riducendo al minimo l'utilizzo di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante l'utilizzo di dati anonimi o mediante modalità che consentano di identificare l'Interessato unicamente in caso di necessità.

8. I dati su supporto cartaceo devono essere conservati in luoghi e contenitori atti ad evitare perdite, sottrazioni, danneggiamenti, distruzioni e l'accesso a soggetti diversi dal personale autorizzato al relativo trattamento, nel rispetto, peraltro, del principio della tutela della riservatezza di terzi.

9. Gli atti e i documenti devono essere conservati in archivi ad accesso protetto ed i soggetti autorizzati al trattamento sono tenuti a conservarli e restituirli al termine delle operazioni effettuate.

10. Nel caso di trattamenti di categorie particolari di dati personali, di cui agli artt. 9 e 10 del GDPR, oltre a quanto previsto, debbono essere osservate le seguenti ulteriori misure:

- gli atti e i documenti sono conservati in locali o contenitori muniti di serratura, fino alla loro eventuale distruzione nel rispetto dei limiti temporali previsti dalla normativa in tema di scarto degli atti d'archivio;
- l'accesso agli archivi è oggetto di controllo nel rispetto delle procedure aziendali vigenti.

11. Il trattamento dei dati – anche appartenenti alle categorie particolari – effettuato mediante strumenti elettronici è assoggettato all'osservanza delle seguenti misure di carattere generale predisposte e messe in atto dalla UOC Servizio Informatico e/o dalla UOC Ingegneria Clinica ed *Information and Communication Technology*, in funzione degli ambiti di rispettiva competenza:

- autenticazione informatica, secondo le specifiche procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito al personale autorizzato ed agli addetti alla gestione o manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati e ad accessi non consentiti;

- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati rientranti nelle categorie particolari di cui all'art. 9 del GDPR.

12. In caso di trattamenti di dati personali affidati a soggetti esterni all'Azienda Ospedaliera in forza di rapporti contrattuali per la fornitura di beni e servizi, tali soggetti - nominati in qualità di Responsabili del trattamento *ex* art. 28 del GDPR - sono tenuti ad assicurare al Titolare di aver adottato, prima di effettuare le previste attività di trattamento dei dati, ogni misura minima di sicurezza prevista dalla normativa vigente in materia di protezione dei dati e di amministrazione digitale.

Art. 43 - La tenuta in sicurezza di documenti ed archivi

1. Gli archivi che custodiscono i dati di cui è Titolare del trattamento l'Azienda, cartacei o digitali, devono essere collocati in locali idonei in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo aziendale.
2. La documentazione archiviata, anche digitalmente, contenente i dati personali è conservata secondo le modalità e i tempi previsti dalla legge ed è poi sottoposta a scarto di archivio o a distruzione come da vigente normativa.
3. I designati in qualità di Responsabili "interni" del trattamento e gli Autorizzati, attenendosi alle istruzioni ricevute, attivano 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.
4. I supporti contenenti dati personali diversi dal cartaceo (supporti informatici, magnetici, videoregistrazioni effettuate nell'ambito dell'attività clinica, immagini iconografiche, ecc.), sono conservati e custoditi secondo le modalità e i termini previsti dalla normativa vigente.
5. Gli archivi cartacei e digitali sono oggetto di trattamento da parte di personale autorizzato e adeguatamente formato in materia di protezione dei dati, che deve assicurarne la riservatezza, protezione ed integrità per tutto il tempo in cui ne mantiene la disponibilità.
6. L'Azienda Ospedaliera assicura l'adozione di misure e procedure attraverso le quali:
   - si proceda alla distruzione di documenti in formato cartaceo e digitale, una volta terminato il limite di conservazione degli stessi e dei dati ivi riportati,
   - siano smaltiti apparati *hardware* o supporti rimovibili di memoria con modalità che impediscano di accedere ad alcun dato personale; ciò anche in caso di riutilizzo degli stessi.
7. Relativamente agli archivi informatizzati contenenti dati personali l'Azienda Ospedaliera adotta idonee procedure di sicurezza, quali:
   - salvataggio periodico dei dati;
   - misure di contenimento dei virus/*malware* informatici e di protezione perimetrale da *cyber* attacchi alle infrastrutture ICT aziendali;
   - *disaster recovery* e continuità operativa;
   - conservazione sostitutiva come da vigente normativa.

Art. 44 – Altre misure per il rispetto e la tutela della riservatezza dell'Interessato

1. L'Azienda Ospedaliera adotta - nell'organizzazione delle prestazioni e dei servizi - misure volte a garantire il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto da disposizioni normative in materia di protezione dei dati personali e sensibili. Tali misure comprendono:

- soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
- l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere e della situazione logistica;
- soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
- cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
- il rispetto della dignità dell'Interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati. In particolare, la dignità deve essere rispettata anche in relazione alle modalità di visita e di intervento sanitario effettuati alla presenza di personale autorizzato quali tirocinanti, volontari, studenti e specializzandi;
- la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;
- la formale previsione di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;
- la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
- la sottoposizione dei soggetti autorizzati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

Art. 45 - Sensibilizzazione e formazione

1. L'Azienda Ospedaliera promuove al suo interno ogni iniziativa di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

2. In tale ambito, una delle iniziative di sensibilizzazione è costituita dall'attività formativa ed informativa rivolta al personale in tema di *privacy*; ciò allo scopo di garantire un aggiornamento formativo costante sulla normativa tecnica in continua evoluzione involgente problematiche connesse alla relativa applicazione e attuazione nel contesto operativo e gestionale, onde assicurare il corretto funzionamento del sistema privacy e favorire una crescita culturale sull'importanza della protezione dei dati personali.

3. In riferimento alle anzidette finalità e nell'ottica della valorizzazione e mantenimento delle professionalità interne, specie in una fase di così complessa e delicata transizione verso sistemi e modelli gestionali del tutto innovativi e di rilevanza strategica, il Responsabile della protezione dei dati promuove – nell'ambito della pianificazione annuale delle attività formative aziendali – la realizzazione di eventi formativi su tematiche inerenti la privacy.

4. L'Azienda Ospedaliera – allo scopo di diffondere la conoscenza del sistema di *governance* della privacy in ambito istituzionale - alimenta l'apposita Sezione "Privacy" del sito *web* con policy, Informative redatte *ex* art. 13 del GDPR, procedure, modulistiche e atti organizzativi.

Art. 46 - Il Registro delle attività di trattamento

1. Il Titolare del trattamento tiene un Registro delle attività di trattamento svolte sotto la propria responsabilità contenente le informazioni di cui all'art. 30, paragrafo 1, del GDPR:

a) il nome e i dati di contatto 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;
e) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) una descrizione generale delle misure di sicurezza tecniche e organizzative.

2. Il Titolare, nell'ottica della piena applicazione del principio di *accountability* – su proposta del Responsabile della protezione dei dati - si riserva la facoltà di integrare i campi informativi del Registro con ulteriori informazioni rispetto a quelle obbligatorie riportate nell'elenco di cui al precedente comma.
Il Registro delle attività di trattamento dell'Azienda Ospedaliera - quale parte integrante del complessivo sistema di gestione dei dati personali – si fonda sulla mappatura dei dati trattati nonché sulla ricognizione di tutti gli elementi rilevanti di un trattamento di dati personali.
3. Il Registro delle attività di trattamento dell'Azienda Ospedaliera è strutturato attraverso un percorso metodologico che riconduce alla responsabilità organizzativa dei soggetti designati in qualità di Responsabili "interni" del trattamento – di cui all'art. 23 del presente Regolamento - i corrispondenti trattamenti di dati personali effettuati presso la Struttura/Servizio/Ufficio diretti; ciò secondo una logica che prende a riferimento le macro attività istituzionali proprie della *mission* aziendale e l'articolata trasversalità e interconnessione dei diversi processi mediante i quali vengono erogate sia prestazioni sanitarie che di carattere amministrativo e tecnico.
4. Il Titolare, avvalendosi del supporto e della consulenza del Responsabile della protezione dei dati, assicura la gestione, l'aggiornamento e la conservazione del Registro su formato elettronico.
5. Il Registro delle attività di trattamento - stante la sua natura fortemente dinamica ed evolutiva – viene, altresì, adeguato in funzione dei futuri sviluppi, anche applicativi, del complessivo quadro normativo di riferimento oltreché dei possibili mutamenti degli assetti organizzativi aziendali.
6. Dietro richiesta, il Responsabile della protezione dei dati provvede a mettere il Registro delle attività di trattamento a disposizione dell'Autorità Garante per la protezione dei dati personali.

Art. 47 - La valutazione di impatto sulla protezione dei dati e la consultazione preventiva

1. Ai sensi dell'art. 35 del GDPR, quando un trattamento di dati personali comporta rischi elevati per i diritti e le libertà dei soggetti interessati – anche in relazione all'uso di nuove tecnologie, alla natura, all'oggetto al contesto ed alle finalità dei trattamenti stessi – deve essere sottoposto a valutazione d'impatto.
2. La valutazione di impatto è richiesta, in particolare, nei seguenti casi:

a) in caso di valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato - compresa la profilazione – e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) in caso di trattamento – su larga scala – di categorie particolari di dati personali di cui all'art. 9, paragrafo 1, del GDPR, o di dati relativi a condanne penali e a reati di cui all'art. 10 del GDPR;
c) in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
3. La valutazione di impatto è, altresì, obbligatoria allorché vengano effettuati trattamenti di dati personali rientranti nelle tipologie di cui all'elenco allegato al Provvedimento dell'Autorità Garante n. 467 dell'11.10.2018.
4. Sempre ai sensi dell'art. 35 del GDPR, la valutazione di impatto contiene almeno:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dall'Azienda;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
5. Il processo inerente l'effettuazione della valutazione è affidato dal Titolare al Responsabile della protezione dei dati.
6. La valutazione di impatto è gestita dal Responsabile della protezione dei dati mediante procedura informatizzata strutturata secondo i contenuti di cui al precedente comma, avvalendosi del necessario supporto dei designati in qualità di Responsabili "interni" del trattamento – in funzione degli specifici ambiti del trattamento – oltrechè del Direttore della UOC Servizio Informatico, del Direttore della UOC Ingegneria Clinica ed *Information and Communication Technology* e del Gruppo multidisciplinare di supporto al Responsabile della Protezione dei Dati.
7. La valutazione di impatto – se necessario – è sottoposta a riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione stessa almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.
8. 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 Ospedaliera, prima di procedere al trattamento, consulta l'Autorità Garante per la protezione dei dati personali secondo le modalità previste dall'art. 36 del GDPR.

Art. 48 - La violazione dei dati personali

1. I dati personali trattati possono essere soggetti al rischio di perdita, distruzione o diffusione indebita (ad esempio a seguito di attacchi informatici), accessi abusivi, incidenti o eventi avversi, determinandosi, in tali casi, una possibile violazione di dati personali (*data breach*).
2. Ai sensi dell'art. 32, paragrafo 1, del GDPR, il Titolare, in caso di violazione dei dati personali, è obbligato a notificare la violazione all'Autorità Garante per la protezione dei dati personali 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 dei soggetti interessati.
3. Qualora la notifica non sia effettuata entro 72 ore, questa deve essere corredata dei motivi del ritardo.
Ai sensi dell'art. 32, paragrafo 3, del GDPR, 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 della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
c) descrivere le probabili conseguenze della violazione dei dati personali;
d) descrivere le misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Ai sensi dell'art. 33, paragrafo 4, del GDPR, sussiste un obbligo a carico del Titolare di documentare la violazione di dati personali, comprese le circostanze ad essa relative, le sue conseguenze ed i provvedimenti adottati per porvi rimedio.
6. Ai sensi dell'art. 34 del GDPR, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati, il Titolare è tenuto a comunicare la violazione al soggetto interessato senza ingiustificato ritardo, salvo i casi di esclusione previsti dal richiamato art. 34 del GDPR.
7. Ogni operatore dell'Azienda Ospedaliera autorizzato a trattare dati personali - qualora venga a conoscenza di un potenziale caso di *data breach* - avvisa tempestivamente il designato in qualità di Responsabile "interno" del trattamento a cui il medesimo afferisce.
8. Il designato in qualità di Responsabile "interno" del trattamento - valutato l'evento - se ritiene confermata la segnalazione di potenziale *data breach*, ne fornisce comunicazione al Responsabile della protezione dei dati.
9. Il Responsabile della protezione dei dati effettua, a sua volta, una valutazione dell'evento avvalendosi del supporto e della collaborazione di professionalità interne all'Azienda Ospedaliera, necessarie per la corretta analisi di contesto, quali:

- RTD
- Servizio Informatico
- Ingegneria Clinica ed *Information and Communication Technology*
- Unità Operativa Complessa Servizio informatico
- Gruppo di supporto al RPD
- Direzione Medica dei Presidi
- Direttori/Responsabili di struttura coinvolti nell'evento.

10. A seguito delle determinazioni sul punto raggiunte e solo qualora si debba ritenere che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche interessate, il Responsabile della protezione dei dati supporta il Titolare del trattamento nella predisposizione della notificazione all'Autorità Garante in ottemperanza alle prescrizioni di cui al richiamato art. 33 del GDPR.
11. Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, queste ultime devono essere informate senza ingiustificato ritardo al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali pregiudizi derivanti dalla violazione.
12. Il Responsabile della protezione dei dati supporta il Titolare del trattamento nella predisposizione della comunicazione all'interessato/agli interessati, da inviarsi nei tempi e con le modalità che il Titolare stesso - sempre attraverso la funzione consulenziale del Responsabile della protezione dei dati - individuerà come

più opportune, anche tenendo conto di eventuali indicazioni all'uopo fornite dall'Autorità Garante. La comunicazione descriverà con linguaggio semplice e chiaro la natura della violazione dei dati personali, le probabili conseguenze derivanti dalla stessa, oltreché le relative misure individuate per porvi rimedio.

13. Il Responsabile della protezione dei dati cura la tenuta di apposito elenco delle violazioni nell'ambito del quale vengono documentati tutti gli eventi di *data breach* occorsi presso l'Azienda Ospedaliera dall'entrata in vigore del GDPR e il cui aggiornamento avviene tramite il Responsabile della protezione dei dati per conto del Titolare.

14. L'Azienda Ospedaliera ha provveduto a formalizzare e rendere disponibile specifica Istruzione Operativa disciplinante la modalità di gestione di una violazione di dati personali pubblicata sul sito web istituzionale, alla Sezione "Privacy", oltrechè nell'ambito del Sistema Qualità (Intranet aziendale–modulistica qualità/qualità/macroarea organizzativa/documenti trasversali).

TITOLO V – NORME FINALI

Art. 49 – Disposizioni finali

1. Per tutto quanto non previsto dal presente Regolamento, si fa espresso rinvio alle disposizioni normative di livello comunitario e nazionale vigenti in materia di protezione di dati personali, nonché agli specifici provvedimenti dell'Autorità Garante.

2. Dalla data di approvazione del presente Regolamento cessa di avere efficacia ogni disposizione regolamentare ed organizzativa in contrasto con quanto dallo stesso disciplinato.

3. Il presente Regolamento è pubblicato sul sito *web i*stituzionale alla Sezione "Amministrazione Trasparente" – sottosezione "Disposizioni Generali" e alla Sezione "Privacy".

4. I diversi atti, quali, modulistica, procedure, Informative, adottati dall'Azienda Ospedaliera relativamente alla tematica della protezione dei dati sono consultabili nell'ambito della citata Sezione "Privacy", il cui aggiornamento è curato dal Responsabile della protezione dei dati.