REGIONE CAMPANIA
AZIENDA SANITARIA NAPOLI 3 SUD
Via Marconi n. 66
80059 - Torre del Greco (Na)
C.F. e Partita I.V.A. 06322711216

DELIBERAZIONE N. 754 DEL 16/05/2024

OGGETTO:	**REVOCA, AI SENSI DELL'ART. 21 QUINQUIES COMMA 1, DELLA LEGGE N. 241/1990, DELLA DELIBERAZIONE DEL DIRETTORE GENERALE N.1102 DEL 30.11.2022 E ADOZIONE DEL NUOVO REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.**

STRUTTURA PROPONENTE:	**U.O.C. AFFARI ISTITUZIONALI E SEGRETERIE**

PROVVEDIMENTO:	**Immediatamente Esecutivo**

IL DIRETTORE GENERALE

dr. Giuseppe Russo, nominato con Delibera della Giunta Regionale della Campania n. 321 del 21 Giugno 2022 e con D.P.G.R.C. n. 111 del 4 Agosto 2022, con l'assistenza del Segretario verbalizzante, previa acquisizione del parere del Direttore Amministrativo Aziendale e del Direttore Sanitario Aziendale, ha adottato la deliberazione in oggetto di cui al testo che segue:

Azienda Sanitaria Locale Napoli 3 Sud
Sede Legale Via Marconi n. 66 – 80059 Torre del Greco
U.O.C. AFFARI ISTITUZIONALI E SEGRETERIE
C.F. e Partita I.V.A. 06322711216

OGGETTO: REVOCA, AI SENSI DELL'ART. 21 QUINQUIES COMMA 1, DELLA LEGGE N. 241/1990, DELLA DELIBERAZIONE DEL DIRETTORE GENERALE N.1102 DEL 30.11.2022 E ADOZIONE DEL NUOVO REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI.

Il Direttore UOC Affari Istituzionali

Alla stregua dell'istruttoria compiuta dal Direttore UOC Affari Istituzionali e dalla Responsabile della UOS Privacy e delle risultanze degli atti tutti richiamati nelle premesse che seguono, costituenti istruttoria a tutti gli effetti di legge, nonché dell'espressa dichiarazione di regolarità tecnica e amministrativa della stessa, resa dallo stesso Dirigente responsabile proponente a mezzo della sottoscrizione della presente;

Dichiarata:

altresì, espressamente con la sottoscrizione, nella qualità di delegato del Titolare del trattamento anche nella fase di pubblicazione, la conformità del presente atto al Regolamento europeo n. 679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;

allo stato ed in relazione al procedimento di cui al presente atto, l'insussistenza del conflitto di interessi ai sensi dell'art. 6 bis della Legge n. 241/1990, delle disposizioni di cui al vigente Codice di Comportamento Aziendale e delle misure previste dal vigente Piano Triennale della Prevenzione della corruzione e della Trasparenza;

infine, la conformità del presente atto ai princìpi di cui alla legge 6 novembre 2012, n. 190.

Premesso:
- che il 24 maggio 2016 entrava in vigore il Regolamento Generale per la Protezione dei Dati personali n. 2016/679 (General Data Protection Regulation o GDPR);
- che, al fine di dare attuazione alle nuove disposizioni normative in materia di protezione dei dati personali, questa Azienda, con Deliberazione n. 52 del 17.01.2018, adottava il proprio Regolamento in materia;
- che, successivamente, in data 10 agosto 2018 è stato emanato il D.Lgs. 101/2018 avente ad oggetto "Disposizioni per l'adeguamento della normativa nazionale al Regolamento UE 2016/679", con la finalità di adeguare la normativa nazionale ex D.Lgs. 196/2003 (Codice della Privacy) alla nuova normativa comunitaria;
- che, pertanto, alla luce delle intervenute modifiche normative, questa Azienda, con Deliberazione del Direttore Generale n.1102 del 30.11.2022 ha proceduto alla revoca parziale della Deliberazione n. 52 del 17.01.2018 e al contestuale aggiornamento del Regolamento interno in materia di protezione dei dati personali.

Preso atto:
- che con Deliberazione del Direttore Generale n. 854 del 20.07.2023 è stato adottato il nuovo Atto Aziendale, approvato con D.G.R.C. n. 470 del 01.08.2023 e attuato con Deliberazioni del Direttore Generale dell'ASL Napoli 3 Sud n. 457 del 22.03.2024 e n. 471 del 25.03.2024;

- che lo stesso ha modificato l'organizzazione aziendale istituendo, all'interno della UOC Affari Istituzionali, la UOS Privacy cui sono stati demandati tutti gli adempimenti in materia di privacy in applicazione del Regolamento UE 2016/679;
- che alla stessa UOS sono state affidate tutte le attività tese a garantire adeguata compliance aziendale nella materia *de qua*;

Considerato:
- che negli anni successivi all'entrata in vigore del Regolamento UE 2016/679, l'Autorità Garante per la Protezione dei Dati Personali ha emanato numerosi provvedimenti e linee guida in ordine alla corretta applicazione della normativa;
- che, al fine di garantire all'Azienda una regolamentazione interna costantemente aggiornata e aderente alla continua evoluzione normativa, nonché al mutato assetto aziendale, si è reso necessario revisionare il testo del Regolamento, trasmettendone copia con nota prot. n.56644 del 8.03.2024 al DPO Aziendale, Avv. Stefano Rotondo e al Compliance Officer, Dott. Giuseppe Napolitano, per l'acquisizione di un preliminare parere in merito;
- che con note prot. n. 73579 e n. 73990 del 2.04.2024, il DPO Aziendale ed il Compliance Officer Aziendale hanno rispettivamente fornito parere favorevole all'adozione del nuovo Regolamento per la Protezione dei Dati Personali;

Rilevato:
- che la normativa europea fa carico alle Pubbliche Amministrazioni di non limitarsi alla semplice osservanza formale degli adempimenti in materia di privacy e sicurezza dei dati personali, ma attua un mutamento culturale e concettuale che richiede un assetto organizzativo diretto all'adeguamento delle norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie (cloud computing, digitalizzazione, social media, cooperazione applicativa, interconnessione di banche dati, pubblicazione automatizzata di dati on line) nelle Amministrazioni Pubbliche;

Preso atto del parere favorevole espresso dal DPO Aziendale e dal Compliance Officer ai fini dell'adozione del nuovo regolamento in materia di protezione dei dati personali;

Ritenuto, pertanto, necessario, alla luce di quanto sopra evidenziato, procedere alla revoca della Deliberazione n.1102 del 30.11.2022 e, per l'effetto, adottare il nuovo Regolamento Aziendale in materia di Protezione dei Dati Personali;

PROPONE AL DIRETTORE GENERALE

- Di revocare, ai sensi dell'art 21 quinquies, comma 1 della Legge n. 241/1990, la Deliberazione del Direttore Generale n.1102 del 30.11.2022 avente ad oggetto "Revoca parziale della deliberazione del Direttore Generale n.52 del 17.01.2018 - Presa d'atto ed adozione del nuovo Regolamento in materia di protezione dei dati personali";

- Di adottare il nuovo Regolamento Aziendale in materia di protezione dei dati personali che si allega al presente atto, quale parte integrante e sostanziale;

- Di dare mandato alla UOC Relazioni con il Pubblico, affinché provveda alla pubblicazione del presente atto nella sezione "Privacy".

L'estensore
Il Dirigente Amministrativo
Dott.ssa Alessia Cifaldi

Il Coll. Amministrativo
Dott.ssa Francesca Esempio

Il Direttore UOC Affari Istituzionali
Dott. Marco Tullo
(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate
– Sostituisce la firma autografa)

Il Direttore Generale

In forza della Delibera della Giunta Regionale della Campania n. 321 del 21 Giugno 2022 e con D.P.G.R.C. n. 111 del 4 Agosto 2022

Preso atto della dichiarazione resa dal dirigente proponente con la sottoscrizione, in ordine alla regolarità tecnica ed amministrativa del presente atto, nonché relativa alla conformità dello stesso atto alle disposizioni vigenti in materia di tutela della privacy;

Sentito il parere favorevole espresso dal Direttore Amministrativo e dal Direttore Sanitario

Il Direttore Amministrativo
dr. Michelangelo Chiacchio

Il Direttore Sanitario
dr. Ferdinando Primiano

(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate – Sostituisce la firma autografa)

DELIBERA

- Di revocare, ai sensi dell'art 21 quinquies, comma 1 della Legge 241/1990**,** la Deliberazione n.1102 del 30.11.2022 avente ad oggetto "Revoca parziale della deliberazione del direttore generale n.52 del 17.01.2018 - Presa d'atto ed adozione del nuovo Regolamento in materia di protezione dei dati personali";

- Di adottare il nuovo Regolamento Aziendale in materia di protezione dei dati personali che si allega al presente atto, quale parte integrante e sostanziale;

- Di dare mandato alla UOC Relazioni con il Pubblico, affinché provveda alla pubblicazione del presente atto nella sezione "Privacy".

Il Direttore della UOC Affari Istituzionali e la Responsabile della UOS Privacy saranno responsabili, in via esclusiva, dell'esecuzione della presente deliberazione, che viene resa immediatamente esecutiva, data l'urgenza, curandone tutti i consequenziali adempimenti, nonché quelli di pubblicità e di trasparenza previsti dal D.L.gs 14 marzo 2013 n° 33 e s.m.i.

Il Direttore Generale
dott. Giuseppe Russo
(Firmato digitalmente ai sensi del D. Lgs. 7.3.2005 n. 82 s.m.i. e norme collegate – Sostituisce la firma autografa)

REGOLAMENTO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

adottato dall'A.S.L. Napoli 3 Sud ai sensi del Regolamento UE 2016/679 del Parlamento UE e del Consiglio del 27 aprile 2016 (GDPR), che stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati, e del D.lgs. 30 giugno 2003, n. 196, così come modificato dal D.lgs. 10agosto 2018, n. 101, recante il "Codice in materia di protezione dei dati personali".

(Revisione 02/2024)

Sommario

PREMESSA

Il presente Regolamento è uno strumento di applicazione del Decreto Legislativo 30 giugno 2003, n. 196 (il cosiddetto "Codice sulla privacy"), così come riformato dal Decreto Legislativo 10 agosto 2018, n. 101, e del Regolamento UE 2016/679, nell'ambito dell'organizzazione aziendale.

Esso si è reso necessario per recepire in un unico testo parte della normativa in tema di trattamento dei dati personali, a cui si fa riferimento per quanto non espressamente regolato (il Regolamento UE 2016/679 del Parlamento UE 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; il D. Lgs. n. 196 del 30 giugno 2003, così come novellato dal d. lgs. n. 101 del 10 agosto 2018; le linee guida e i pareri dell'Autorità Garante; le linee guida del Gruppo di Lavoro Articolo 29; le linee guida del Comitato UE per la Protezione dei Dati Personali; le deliberazioni adottate dall'Azienda Sanitaria Napoli 3 sud).

Il presente Regolamento è sottoposto ad aggiornamento periodico a cura della UOS Privacy, con il supporto del personale interno ed eventuali consulenti esterni, in linea con le novità normative e giurisprudenziali, nonché alla luce delle pronunce delle predette autorità.

Dall'esame della materia emerge come sia, oramai, imprescindibile un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come garanzia, per il cittadino che si rivolge alle strutture sanitarie, di una riservatezza totale dal punto di vista reale e sostanziale (cosiddetta funzione proattiva).

Il diritto alla privacy è un vero e proprio diritto inviolabile della persona che non si limita alla tutela della riservatezza o alla protezione dei dati, ma implica il pieno rispetto dei diritti e delle libertà fondamentali e della dignità.

Per questi motivi la cultura della privacy necessita di crescere e rafforzarsi, principalmente fra gli operatori della sanità, perché solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di legge, nel trattamento di dati di competenza, con la consapevolezza di non affrontare un inutile gravame, bensì di contribuire concretamente al miglioramento della qualità del rapporto con l'Utenza.

Art. 1 OGGETTO

Il presente Regolamento disciplina, all'interno dell'Azienda Sanitaria Locale Napoli 3 Sud, la tutela delle persone fisiche in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dalla normativa vigente.
Il presente regolamento aziendale viene redatto in conformità a quanto previsto dal Regolamento UE 2016/679 del Parlamento UE e del Consiglio del 27 aprile 2016 (GDPR), che stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati, e dal D.lgs. 30 giugno 2003, n. 196, così come modificato dal D.lgs. 10 agosto 2018, n. 101, recante il "Codice in materia di protezione dei dati personali".

Art. 2 FINALITÀ

L'Azienda garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o della loro residenza.
La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale e, come sancito nell'art. 8, paragrafo 1, della Carta dei Diritti Fondamentali, *"Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano".*

Art. 3 SENSIBILIZZAZIONE
(art. 29 Regolamento UE 2016/679)

L'Azienda sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.
A tal riguardo, uno degli strumenti essenziali di sensibilizzazione è l'attività formativa del personale aziendale e l'attività informativa diretta a tutti coloro che hanno rapporti con l'Azienda. Per garantire la conoscenza capillare delle disposizioni del presente Regolamento, al momento dell'ingresso in servizio è data ad ogni dipendente una specifica comunicazione (con apposita clausola inserita nel contratto di lavoro) con i riferimenti del presente Regolamento, il quale è oggetto di pubblicazione sul sito aziendale e riporta i principi fondamentali della materia, esposti in modo semplice, chiaro e puntuale.
Ogni dipendente si impegna, pertanto, a scaricarne una copia, prenderne visione ed attenersi alle sue prescrizioni.

Art. 4 DEFINIZIONI
(art. 4 Regolamento UE 2016/679)

Il dato personale è 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.

Il trattamento è 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 messaa disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

Il Titolare del trattamento è 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.

Il Responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Il destinatario è 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.

Il consenso dell'interessato è 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.

La violazione dei dati personali è costituita dalla 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.

Art. 5 TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

(artt. 24 e 25 Regolamento UE 2016/679)

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti della normativa vigente, è l'ASL Napoli 3 Sud, rappresentata dal Direttore Generale, in qualità di legale rappresentante, con sede in Via Guglielmo Marconi, n. 66, Torre del Greco (Na).

Il Titolare determina le finalità e le modalità del trattamento dei dati personali, ovvero avvalendosi della collaborazione della UOS Privacy, con il supporto del personale interno ed eventuali consulenti esterni, provvede:

a) a individuare e nominare, con proprio atto e ai sensi dell'art. 6 del presente Regolamento, i soggetti Designati con specifici compiti e funzioni connessi al trattamento dei dati personali, impartendo ad essi per la corretta gestione e tutela dei dati personali, a titolo esemplificativo, i compiti e le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato, all'adozione delle misure di sicurezza per la conservazione, protezione e riservatezza dei dati, all'eventuale uso di apparecchiature di videosorveglianza;
b) a nominare gli Amministratori di sistema e il Responsabile della protezione dei dati personali (DPO);
c) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
d) a mettere in atto misure tecniche e organizzative adeguate a garantire che il trattamento sia effettuato conformemente al presente Regolamento;
e) a documentare le violazioni dei dati personali e notificarle al Garante, ovvero agli interessati, nei casi di cui agli artt. 33 e 34 del Regolamento UE 2016/679.

Art. 6 SOGGETTI DESIGNATI A SPECIFICI COMPITI E FUNZIONI CONNESSI AL TRATTAMENTO

(art. 29 Regolamento UE 2016/679 e 2 *quaterdecies* Codice Privacy)

In considerazione della complessità e della molteplicità delle funzioni istituzionali dell'Azienda, ai sensi dell'art. 29 del Regolamento UE 2016/679 e 2 *quaterdecies* del D.lgs. 196/2003 (così come modificato dal D.lgs. 101/2018), il Titolare del trattamento prevede, per il tramite del Direttore Generale dell'ASL, di attribuire specifici compiti e funzioni connessi al trattamento dei dati personali a persone fisiche espressamente designate nell'ambito del proprio assetto organizzativo.

Sono individuati quali soggetti designati a svolgere specifici compiti e funzioni connessi al trattamento dei dati personali:

a) i Dirigenti responsabili di Distretto, Dipartimento, Presidio ospedaliero, Struttura complessa e Struttura dipartimentale, per le banche dati cartolari e per le banche dati elettroniche delle singole strutture;

b) Il Dirigente responsabile dell'U.O.C. Sistemi Informatici ITC per le banche dati elettroniche gestite centralmente.

Il Titolare del trattamento informa ciascun soggetto designato delle responsabilità che gli sono affidate mediante la comunicazione di apposito atto di individuazione.

I soggetti designati a svolgere specifici compiti e funzioni connessi al trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto prescritto nel suddetto atto di individuazione.

Art. 7 SOGGETTI AUTORIZZATI AL TRATTAMENTO

(art. 29 Regolamento UE 2016/679 e 2 *quaterdecies* Codice Privacy)

Le persone fisiche, dipendenti e assimilati, che svolgono attività di trattamento dei dati personali all'interno dell'organizzazione e sotto l'autorità del Titolare del trattamento, vengono a tale fine debitamente individuati, autorizzati e istruiti, in ossequio a quanto previsto dall'art. 29 del Regolamento UE 2016/679e 2 *quaterdecies* del D.lgs. 196/2003 (così come novellato dal D.lgs. 101/2018).

L'Autorizzato collabora con il Titolare e il Designato, contribuendo a favorire all'interno dell'organizzazione il rispetto di quanto previsto dall'art. 13 del presente Regolamento, segnalando eventuali situazioni di rischio nel trattamento dei dati e fornendo ogni informazione necessaria per l'espletamento delle funzioni di controllo.

L'Autorizzato è tenuto alla completa riservatezza sui dati di cui sia venuto a conoscenza in occasione dell'espletamento della sua attività, impegnandosi a comunicarli esclusivamente ai soggetti indicati dal Titolare e dal Designato, nei soli casi previsti dalla legge e/o nello svolgimento dell'attività istituzionale dell'Azienda.

Tutti coloro che svolgono un'attività di trattamento dei dati all'interno dell'organizzazione aziendale, pur non essendo dipendenti dell'Azienda, ma che operano temporaneamente presso la medesima (ad es. tirocinanti, volontari, borsisti), devono essere autorizzati e istruiti secondo le modalità descritte nel presente articolo.

Art. 8 RESPONSABILI DEL TRATTAMENTO

(art. 28 Regolamento UE 2016/679)

Tutti i soggetti esterni che effettuano operazioni di trattamento sui dati personali di cui l'Azienda è Titolare e per suo conto sono nominati "Responsabili del trattamento" qualora sussistano le condizioni di cui all'art. 28 del Regolamento UE 2016/679.

Al fine di mantenere il rispetto della normativa vigente in materia, il Titolare del trattamento elabora e diffonde apposita procedura per la gestione degli atti di nomina a Responsabile del trattamento, che chiunque operi all'interno dell'organizzazione aziendale è tenuto a conoscere e rispettare, in relazione al ruolo ricoperto.

I Responsabili hanno l'obbligo di:

a) trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della normativa vigente in materia di privacy;
b) adottare tutte le misure idonee a prevenire e/o evitare la comunicazione o diffusione dei dati, il rischio di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;
c) individuare al loro interno i soggetti autorizzati al trattamento e garantire che i dati trattati siano portati a conoscenza soltanto del personale così autorizzato;
d) trattare i dati personali dei pazienti esclusivamente per le finalità previste dal contratto o dalla convenzione e per il tempo strettamente necessario al raggiungimento delle finalità definite dal Titolare secondo il contratto;
e) attenersi alle disposizioni impartite dal Titolare del trattamento;
f) specificare i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti;
g) comunicare le misure di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.

La designazione del Responsabile viene effettuata mediante "atto di nomina" da parte del Titolare del trattamento, da allegare agli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti dei dati personali esternamente all'Azienda.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le parti.

Art. 9 UNITA' OPERATIVA SEMPLICE PRIVACY

La **U.O.S. Privacy** svolge le seguenti attività, riferendone in via diretta al Titolare del trattamento dei dati (ASL Napoli 3 Sud) in persona del legale rappresentante p.t.:

- supporto alle articolazioni aziendali nella predisposizione della specifica documentazione privacy relativamente ai processi interni e\o esterni che richiedono adeguata regolamentazione in materia;
- predisposizione ed aggiornamento delle informative privacy per i soggetti interessati (utenza, dipendenti, fornitori etc.);
- predisposizione atti di nomina ex art. 28 GDPR (necessaria per il censimento nonché la responsabilizzazione di tutti i soggetti esterni che a vario titolo esercitano attività a loro demandate dal Titolare del Trattamento);
- predisposizione atti di nomina ex art.29 GDPR (riferita ai Direttori/responsabili delle articolazioni aziendali e a tutto il personale autorizzato al trattamento dei dati);
- supporto al Titolare del Trattamento nella predisposizione ed aggiornamento del Registro delle attività di trattamento ex art.30 GDPR;

- supporto al Titolare del trattamento nella predisposizione ed aggiornamento della Valutazione d'impatto sulla protezione dei dati (DPIA: Data Protection Impact Assessment) prevista dall'art. 35 GDPR;
- predisposizione ed aggiornamento di regolamenti, procedure, indirizzi, codici comportamentali e linee guida tese a disciplinare i processi aziendali al fine di assicurare una corretta e puntuale attuazione della specifica normativa in materia di tutela della privacy;
- monitoraggio dell'effettiva attuazione delle policy adottate dall'Azienda in materia di protezione dei dati personali;
- supporto al Data Protection Officer aziendale nelle attività a lui demandate dalla vigente normativa, nonché nelle attività di audit presso le articolazioni aziendali e nei contatti con l'Autorità Garante per la Protezione dei Dati Personali;
- predisposizione ed esecuzione di un piano di audit interno rivolto a tutte le articolazioni aziendali e finalizzato alla verifica dello stato di compliance privacy aziendale;
- predisposizione ed aggiornamento di regolamenti e procedure per la gestione dei Data Breach (violazione dei dati personali);
- aggiornamento costante dell'apposita sezione "Privacy" del sito web aziendale in via diretta ovvero mediante l'ausilio della UOC Relazioni con il Pubblico;
- promozione e predisposizione di iniziative di formazione permanente per la diffusione della cultura della privacy rivolte al personale dipendente, di concerto con la UOSD Formazione e Aggiornamento Professionale;
- supporto alla UOC Affari Legali per la composizione delle controversie in materia di Protezione di Dati Personali.

Art. 10 AMMINISTRATORI DI SISTEMA

L'Amministratore di sistema e/o gli Amministratori di sistema sono nominati con atto formale del Direttore Generale per sovraintendere alla gestione, alla manutenzione delle banche dati e, nel suo complesso, al sistema informatico dell'Azienda.

Gli Amministratori di sistema svolgono attività, quali: il salvataggio dei dati, l'organizzazione dei flussi di rete,la gestione dei supporti di memorizzazione e la manutenzione hardware e propongono al Titolare del trattamentoun documento di valutazione del rischio informatico.

Nel rispetto della normativa in materia di protezione dei dati e della sicurezza, gli Amministratori di sistema devono adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni (access log) devono essere complete, inalterabili, verificabile la loro integrità e adeguate al raggiungimento dello scopo di verifica per cui sono richieste. Le registrazioni devono comprendere il riferimento temporale e la descrizione dell'evento che le ha generate e devono essere conservate per un periodo congruo, non inferiore ai sei mesi.

Secondo la normativa vigente, l'operato degli Amministratori di sistema deve essere verificato, con cadenza annuale, da parte del Titolare del trattamento, in modo da controllare la sua rispondenza alle misure tecnico-organizzative e di sicurezza attivate rispetto all'attività di trattamento dei dati personali.

L'Azienda applica quanto previsto dal Provvedimento del Garante della Privacy in materia di "*misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" del 27 novembre 2008, così come modificato in base al provvedimento del 25 giugno 2009.

Art. 11 DATA PROTECTION OFFICER (D.P.O.)

(artt. 37-39 Regolamento UE 2016/679)

Il Titolare del trattamento designa il Responsabile della protezione dei dati o Data Protection Officer (D.P.O.), mediante individuazione di un soggetto che presenti un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali.

Egli opera alle dipendenze del Titolare del trattamento oppure sulla base di un contratto di servizio e:

- adempie alle sue funzioni in totale indipendenza e in assenza di conflitti di interesse;
- dispone, a cura del Titolare del trattamento, delle risorse necessarie per adempiere ai suoi compiti e accedere ai dati personali e ai trattamenti;
- tiene il segreto o la riservatezza in merito all'adempimento dei propri compiti.

Il D.P.O. svolge i seguenti compiti:

a) informa e fornisce consulenze al Titolare del trattamento, nonché ai dipendenti che eseguono il trattamento dei dati in merito agli obblighi vigenti relativi alla protezione dei dati;
b) verifica l'attuazione e l'applicazione della normativa vigente in materia, nonché delle politiche del Titolare o del Responsabile del trattamento relative alla protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, mediante periodici audit di verifica;
c) fornisce, qualora venga richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei datie sorveglia i relativi adempimenti;
d) funge da punto di contatto per gli interessati in merito al trattamento dei loro dati personali e all'esercizio dei diritti;
e) funge da punto di contatto con il Garante per la protezione dei dati personali per questioni connesse al trattamento dei dati, tra cui la consultazione preventiva, di cui all'art. 19 del presente Regolamento.

L'incarico viene conferito come Incarico professionale di alta specialità.

Art. 12 I DATI TRATTATI

(art. 4 Regolamento UE 2016/679)

Nell'esercizio delle sue funzioni istituzionali, l'Azienda tratta, in modo anche automatizzato (totalmente o parzialmente), le seguenti categorie di dati relativi a utenti, pazienti, congiunti o esercenti la tutela/curatela dei pazienti, dipendenti e fornitori:

a) dati personali;
b) categorie particolari di dati;
c) dati relativi a condanne penali o reati.

1) **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.

2) **Categorie particolare di dati**: sono considerate categorie particolari di dati quelle che si riferiscono all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, o all'appartenenza sindacale, nonché relative a dati genetici, dati biometrici, dati intesi a identificare in modo univoco una persona fisica, nonché relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

2a) **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, eche risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

2b) **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.

2c) **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 disalute.

3) **Dati personali relativi a condanne penali e reati**: è il dato personale idoneo a rivelare iprovvedimenti giudiziari penali, ai reati o a connesse misure di sicurezza.

Art. 13 I PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI PERSONALI

(artt. 5, 6 e 9 Regolamento UE 2016/679)

Sin dalla progettazione del trattamento e per l'intera durata dello stesso, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principio di "liceità, correttezza e trasparenza");
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non siano incompatibili con tali finalità (principio di "limitazione della finalità");
c) adeguati, pertinenti e non eccedenti, cioè limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "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 (principio di "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 stati 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; in ogni caso, i tempi di conservazione devono essere determinati o determinabili, tramite l'indicazione di criteri di cui, e resi conoscibili all'Interessato, mediante consegna dell'informativa (principio di "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 (principio di *"integrità e riservatezza*").

I dati si intendono trattati lecitamente solo se, e nella misura in cui, ricorrano almeno una delle seguenti condizioni:

a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un

minore.

Sarà vietato, inoltre, trattare i dati rientranti nelle particolari categorie, così come definiti dall'art. 12 del presente Regolamento, salvo l'applicabilità di almeno una tra le seguenti basi giuridiche:

a) l'interessato ha esplicitamente prestato il proprio consenso, in ordine ad 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, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismoa motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato;
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unioneo 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 membrio conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanziedi cui al paragrafo 3;
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;
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storicao a fini statistici in conformità dell'articolo 89, paragrafo 1, del Regolamento UE 2016/679, e in proporzione 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.

Relativamente ai dati personali di cui alla lettera h) del presente articolo, gli stessi possono essere trattati da o sotto la responsabilità di un professionista a ciò specificamente preposto e soggetto al segreto professionale.

I dati particolare il cui trattamento è necessario per motivi di interesse pubblico rilevante ai sensi della lettera g), vengono trattati nel rispetto di quanto previsto dall'art. 2 *septies* del D.lgs. 196/2003.

Art. 14 L'ATTIVITA' DI TRATTAMENTO

Con l'espressione "trattamento", ai sensi dell'art. 4 del Regolamento UE 2016/679, deve intendersi qualunque operazione o complesso di operazioni, compiute con o senza l'ausilio di processi automatizzatie applicate a dati personali o insieme di dati personali, concernenti:

a) la raccolta dei dati;
b) la registrazione dei dati, cioè il loro inserimento su supporti, automatizzati o manuali, al fine di

rendere i dati disponibili per successivi trattamenti;

c) l'organizzazione dei dati in senso stretto, cioè il processo di lavorazione che ne favorisca la fruibilità attraverso l'aggregazione o la disaggregazione, l'accorpamento, la catalogazione, ecc.;
d) la conservazione dei dati alla quale la legge dedica particolari attenzioni sotto il profilo della sicurezza;
e) la consultazione;
f) l'elaborazione, ovvero le operazioni che attribuiscono significato ai dati in relazione allo scopo peri quali essi sono stati raccolti;
g) la modificazione dei dati registrati in relazione a variazioni o a nuove acquisizioni;
h) la selezione, l'estrazione, e il raffronto, ipotesi specifiche che rientrano nell'ipotesi più generale dell'elaborazione;
i) l'utilizzo;
j) l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte tra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;
k) il blocco, ovvero la conservazione dei dati con sospensione temporanea dei trattamenti;
l) la comunicazione, ovvero la trasmissione dei dati ad uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; non è comunicazione la trasmissione dei dati allo stesso interessato, al Responsabile del trattamento, ai Designati e agli Autorizzati al trattamento;
m) la diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati (es.: pubblicazione all'albo, giornale, ecc.);
n) la cancellazione;
o) la distruzione.

Il trattamento dei dati personali è esercitabile solo da parte del Titolare del trattamento, dei Designati e degli Autorizzati. Non è consentito il trattamento da parte di persone non autorizzate.

Il trattamento dei dati personali raccolti direttamente dall'Azienda o pervenuti in via indiretta da altri soggetti è effettuato sia con strumenti elettronici, sia senza l'ausilio degli strumenti stessi.

Il trattamento di dati personali comunicati dall'interessato direttamente o eventualmente raccolti presso gli uffici dell'Asl Napoli 3 Sud (es. Presidi Ospedalieri, C.U.P., Distretti, Dipartimento di Prevenzione, ecc..)è effettuato secondo quanto stabilito dall'art. 13 del presente Regolamento.

Il trattamento si considera lecito nelle specifiche ipotesi disciplinate dagli artt. 6 e 9 del Regolamento UE 2016/679.

Il trattamento dei dati personali è effettuato dall'Azienda in quanto soggetto pubblico che svolge proprie funzioni istituzionali ed è finalizzato, pertanto, all'erogazione delle prestazioni sanitarie, allo svolgimento degli adempimenti amministrativi-contabili e alle attività di organizzazione e di controllo a supporto dell'erogazione delle prestazioni sanitarie, con particolare riguardo alle attività di:

a) prevenzione collettiva e di sanità pubblica svolte dal Dipartimento di Prevenzione, anche a supporto delle autorità sanitarie;
b) diagnostica strumentale e di laboratorio;
c) ricovero ordinario e in day hospital;
d) ricovero in regime residenziale e semiresidenziale;
e) prestazioni sanitarie a rilevanza sociale;
f) attività o servizi socio-assistenziali su delega dei singoli enti locali;
g) medicina legale;
h) ricerca e sperimentazione, nonché elaborazione statistica, epidemiologica e sociologica;
i) sorveglianza sanitaria dei lavoratori che operano all'interno dell'Azienda.

L'azienda effettua, altresì, i trattamenti di dati personali previsti da norme legislative e regolamentari riguardanti:

a) la gestione del personale dipendente, ivi comprese le procedure di assunzione;
b) la gestione dei soggetti che intrattengono rapporti giuridici con l'Azienda, diversi dal rapporto di lavoro dipendente e che operano a qualsiasi titolo all'interno dell'Azienda stessa, ivi compresi gli specializzandi, gli allievi e i docenti di corsi, i tirocinanti, i volontari;
c) la gestione dei rapporti con i consulenti, i fornitori per l'approvvigionamento di beni e di servizi, nonché con le imprese per l'esecuzione di opere edilizie e di interventi di manutenzione;
d) la gestione dei rapporti con i soggetti accreditati o convenzionati;
e) la gestione dei rapporti con la Procura della Repubblica e gli altri soggetti pubblici competenti, per le attività ispettive di vigilanza, di controllo e di accertamento delle infrazioni alle leggi e regolamenti.

La UOS Privacy provvede al monitoraggio di tutti i trattamenti di dati effettuati, direttamente o con l'ausilio dei soggetti Designati, in base alle scelte discrezionali di volta in volta effettuate dalla Direzione Strategica.

È compito del Designato al trattamento dei dati effettuare la valutazione periodica della non eccedenza dei dati trattati nell'ambito dell'unità organizzativa che opera sotto la sua responsabilità.

La comunicazione dei dati personali trattati dall'Azienda a soggetti esterni, pubblici o privati, può avvenire solo sulla scorta delle regole stabilite dal presente regolamento.

Art. 15 IL TRATTAMENTO DI DATI RELATIVI A CONDANNE PENALI E REATI

(art. 10 Regolamento UE 2016/679 e 2 *octies* Codice Privacy)

Così come sancito dagli artt. 10 del Regolamento UE 2016/679 e 2 *octies* del D.lgs. 196/2003, l'Azienda può trattare i dati personali relativi a condanne penali, reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, del Regolamento UE 2016/679, solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, e a fronte di appropriate garanzie per i diritti e le libertà degli interessati.

In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui sopra, nonchéle garanzie di cui al comma precedente, sono individuati con decreto del Ministro della Giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante.

Fermo quanto sopra disposto, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito per:

a) l'adempimento di obblighi e l'esercizio di diritti da parte del titolare o dell'interessato in materia di diritto del lavoro o comunque nell'ambito dei rapporti di lavoro, nei limiti stabiliti da leggi, regolamenti e contratti collettivi;
b) l'adempimento degli obblighi previsti da disposizioni di legge o di regolamento in materia di mediazione finalizzata alla conciliazione delle controversie civili e commerciali;
c) la verifica o l'accertamento dei requisiti di onorabilità, requisiti soggettivi e presupposti interdittivi nei casi previsti dalle leggi o dai regolamenti;
d) l'accertamento di responsabilità in relazione a sinistri o eventi attinenti alla vita umana, nonché la prevenzione, l'accertamento e il contrasto di frodi o situazioni di concreto rischio per il corretto esercizio dell'attività assicurativa, nei limiti di quanto previsto dalle leggi o dai regolamenti in materia;
e) l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
f) l'esercizio del diritto di accesso ai dati e ai documenti amministrativi, nei limiti di quanto previsto

dalle leggi o dai regolamenti in materia;

g) l'esecuzione di investigazioni o le ricerche o la raccolta di informazioni per conto di terzi ai sensi dell'articolo 134 del testo unico delle leggi di pubblica sicurezza;
h) l'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia o in materia di prevenzione della delinquenza di tipo mafioso e di altre gravi forme di pericolosità sociale, nei casi previsti da leggi o da regolamenti, o per la produzione della documentazione prescritta dalla legge per partecipare a gare d'appalto;
i) l'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto, in adempimento di quanto previsto dalle vigenti normative in materia di appalti;
j) l'attuazione della disciplina in materia di attribuzione del rating di legalità delle imprese ai sensi dell'articolo 5-ter del decreto-legge 24 gennaio 2012, n. 1, convertito, con modificazioni, dalla legge 24 marzo 2012, n. 27;
k) l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo.

Nei casi in cui ai paragrafi precedenti, qualora non siano individuate le garanzie appropriate per i diritti e le libertà degli interessati, tali garanzie sono previste con il decreto di cui al paragrafo 3 del presente articolo.

Art. 16 Il TRATTAMENTO DEI DATI DEL PERSONALE DIPENDENTE DELL'AZIENDA E CONVENZIONATO

L'Azienda può trattare i dati dei propri dipendenti al fine di istaurare, gestire o estinguere il rapporto di lavoro.

Per le categorie particolari di dati, il trattamento è ammesso esclusivamente per le seguenti finalità:

a) per adempiere o per esigere l'adempimento di specifici obblighi o per eseguire specifici compiti previsti dalla normativa dell'Unione europea, da leggi, da regolamenti o da contratti collettivi anche aziendali, ai sensi del diritto interno, in particolare ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro (art. 88 del Regolamento UE 2016/679), nonché del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza ed assistenza anche integrativa, o in materia 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, liberalità 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; il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsia contenziosi in atto o a situazioni precontenziose;
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.

È vietato, in ogni caso, il trattamento:

- di dati che rivelino le opinioni politiche in caso di partecipazione di dipendenti ad operazioni elettorali in qualità di rappresentanti di lista, in applicazione del principio di necessità, nell'ambito della documentazione da presentare al fine del riconoscimento dei benefici di legge;
- dati genetici al fine di stabilire l'idoneità professionale di un dipendente, neppure con il consenso dell'interessato.

Per quanto attiene alle modalità di trattamento, devono osservarsi le seguenti prescrizioni:

a) i dati devono essere raccolti, di regola, presso l'interessato;
b) in tutte le comunicazioni all'interessato che contengono categorie particolari di dati devono essere utilizzate forme di comunicazione anche elettroniche individualizzate nei confronti di quest'ultimo o di un suo delegato, anche per il tramite di personale autorizzato. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo dovrà essere trasmesso, di regola, in plico chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto;
c) i documenti che contengono categorie particolari di dati, ove debbano essere trasmesse ad altri ufficio funzioni in ragione delle rispettive competenze, devono contenere esclusivamente le informazioni necessarie allo svolgimento della funzione senza allegare, ove non strettamente indispensabile, documentazione integrale o riportare stralci all'interno del testo;
d) quando per ragioni di organizzazione del lavoro, e nell'ambito della predisposizione di turni di servizio, si proceda a mettere a disposizione a soggetti diversi dall'interessato (altri colleghi) dati relativi a presenze ed assenze dal servizio, il datore di lavoro non deve esplicitare, 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).

Per i trattamenti dei dati connessi alla gestione del rapporto di lavoro con il personale dipendente dell'Azienda è predisposta apposita informativa.

Secondo la normativa vigente, l'Azienda adotta le massime cautele nel trattamento dei dati personali del proprio dipendente; in particolare per quanto attiene alle categorie particolari di dati, nonché quelle relativea condanne penali e reati.

Il trattamento dei dati personali deve avvenire nel rispetto dei principi di cui all'art. 13 del presente Regolamento.

L'Azienda assolve agli obblighi di legge in materia di trasparenza della Pubblica Amministrazione con la pubblicazione sul sito istituzionale dei dati relativi al personale.

La pubblicazione delle graduatorie di selezione del personale o relative alla concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, deve essere effettuata dopo un'attenta verifica che le indicazioni contenute non comportino la divulgazione di dati idonei a rivelare lo stato di salute, utilizzando, piuttosto, diciture generiche o codici numerici. Non sono infatti ostensibili le notizie concernenti la natura delle infermità e degli impedimenti personali o familiari che causino l'astensione del lavoro, nonché le componenti della valutazione o le notizie concernenti il rapporto di lavoro tra il personale dipendente e l'amministrazione, idonee a rivelare taluna delle informazioni di natura sensibile.

L'Azienda applica quanto previsto dalle Linee Guida in materia di trattamento dei dati personali dei lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico, delib. n. 23 del 14 giugno 2007, doc. web n. 1417809.

Art. 17 REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

(art. 30 Regolamento UE 2016/679)

Il Titolare del trattamento istituisce un registro in forma scritta delle attività di trattamento svolte sotto la propria responsabilità, che deve essere continuamente aggiornato e messo a disposizione delle autorità di controllo. Tale registro può essere tenuto sia in forma cartacea che elettronica, a patto che rispetti la forma scritta e ne sia verificabile la data di prima istituzione.

Il registro del Titolare del trattamento contiene almeno le informazioni indicate nell'art. 30, par. 1, del Regolamento UE 2016/679, ma può essere riportata nel registro qualsiasi altra informazione che il Titolare ritenga utile; invero, il Registro dei Trattamenti rappresenta uno dei principali strumenti di accountability, utile a rendere un quadro chiaro e aggiornato dei trattamenti in essere all'interno dell'azienda e a dare evidenza del rispetto dei principi normativi vigenti in caso di eventuale supervisione dell'Autorità Garante.

Art. 18 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

(art. 35 Regolamento UE 2016/679)

La valutazione d'impatto sulla protezione dei dati personali (DPIA) deve essere realizzata dal Titolare del trattamento prima di procedere a un tipo di trattamento che, considerata la natura, l'oggetto, il contesto, le finalità, nonché tenuto conto dell'uso di nuove tecnologie, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Al fine di mantenere il rispetto della normativa vigente in materia, il Titolare del trattamento elabora e diffonde apposita procedura per la gestione della DPIA, che chiunque operi all'interno dell'organizzazione aziendale è tenuto a conoscere e rispettare, in relazione al ruolo ricoperto.

Prioritariamente deve essere definito dal titolare del trattamento l'elenco delle tipologie di trattamenti soggette al requisito della valutazione d'impatto sulla protezione dei dati. La valutazione d'impatto sulla protezione dei dati personali può riguardare una singola operazione di trattamento dei dati, un insieme di trattamenti simili che presentano rischi analoghi o un prodotto tecnologico. Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il Titolare del trattamento, se necessario, procede a un riesame della valutazione d'impatto sulla protezione dei dati.

Il titolare del trattamento, nello svolgere l'attività di valutazione, si consulta con il responsabile della protezione dei dati.

La valutazione deve contenere almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione sulla necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Art. 19 CONSULTAZIONE PREVENTIVA

(art. 36 Regolamento UE 2016/679)

Il Titolare consulta il Garante per la Protezione dei Dati Personali, prima di procedere al trattamento dei dati e per il tramite del *Data Protection Officer*, qualora la valutazione d'impatto sulla protezione dei datiabbia evidenziato che il trattamento potrebbe presentare un rischio elevato, in assenza di misure adottate dal

titolare del trattamento per attenuare il rischio.

Art. 20 FASCICOLO SANITARIO ELETTRONICO (F.S.E.)

Il Fascicolo sanitario elettronico (F.S.E.) è l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici, riguardanti l'assistito e originati da diversi Titolari del trattamento (non solo ASL Napoli 3 Sud) operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (ad esempio Aziende sanitarie anche di altre Regioni, Laboratori clinici privati operanti nella medesima Regione o su un'Area più vasta).

Il F.S.E. è istituito dalla Regione, a cui è deputata la sua gestione tecnica e informatica, ed è disciplinato dall´art. 12, D.L. n. 179/2012, e dal D.P.C.M. n. 178/2015, nonché dall'art. 11 D.L. 19.05.2020, n. 34.

Le finalità che possono essere perseguite attraverso la costituzione del F.S.E. possono essere ricondotte esclusivamente a finalità di cura dell'Interessato e cioè di prevenzione, diagnosi e riabilitazione, finalità di ricerca (studio e ricerca scientifica in campo medico, biomedico ed epidemiologico) e finalità di governo (programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria).

Qualora attraverso il F.S.E. si intendano perseguire talune finalità amministrative connesse all'erogazione della prestazione sanitaria richiesta dall'interessato, i dati amministrativi devono essere separati dalle informazioni sanitarie, prevedendo profili diversi di abilitazione degli aventi accesso agli stessi, in funzione della differente tipologia di operazioni ad essi consentite.

Il F.S.E. è, in generale, alimentato, in maniera automatica, continuativa e tempestiva dai soggetti e dagli esercenti le professioni sanitarie che prendono in cura l'assistito con i dati degli eventi clinici relativi all'assistenza sanitaria da questo ricevuta.

Nel FSE sono contenuti tutti i dati e documenti sanitari relativi a referti, lettere di dimissione ospedaliera, prescrizioni, ecc., di eventi sanitari presenti e trascorsi. Per favorire un rapido inquadramento dello stato di salute dell'assistito al personale sanitario che lo prenderà in cura, nel F.S.E. è presente anche il cd. "profilo sanitario sintetico (Patient Summary)", in cui i dati sono inseriti e aggiornati dal medico di medicina generale/pediatra. Il F.S.E. contiene, altresì, informazioni relative a farmaci prescritti ed erogati all'interessato. Quest'ultimo potrà, altresì, inserire nel proprio FSE e precisamente alla sezione "Taccuino" ulteriori informazioni e documenti sanitari e renderli visibili agli esercenti le professioni sanitarie richieste.

Per rendere il F.S.E. accessibile per finalità di cura a tutti gli operatori che prenderanno in cura l'interessato,è necessario che lo stesso fornisca uno specifico consenso informato (consenso alla consultazione).

L'accesso al trattamento di dati personali effettuato attraverso il F.S.E. deve essere consentito unicamente da parte di soggetti operanti in ambito sanitario, secondo modalità tecniche di autenticazione che consentano di autorizzare l'accesso al F.S.E. da parte del medico curante, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche e organismiamministrativi anche operanti in ambito sanitario. Analogamente, l'accesso è precluso anche al personale medico nell'esercizio di attività medico-legale (es. visite per l'accertamento dell'idoneità lavorativa o alla guida).
Per rendere visibili agli operatori sanitari i dati relativi a prestazioni sanitarie rese in situazioni particolari (es. interruzione di gravidanza, violenza sessuale, uso di sostanze stupefacenti, stato di sieropositività, malattie sessualmente trasmesse, ecc.) dovrà essere richiesti ulteriore consenso specifico.
Qualora l'assistito non presti il proprio consenso al trattamento dei propri dati mediante il FSE o revochi il consenso prestato in precedenza (con le stesse modalità con le quali lo ha inizialmente fornito), il professionista e il personale sanitario di reparto/ambulatorio che lo prendono in cura avranno a disposizione le sole informazioni rese in quel momento dall'assistito e relative all'episodio per il quale questo è in cura,

nonché quelle relative alle eventuali precedenti prestazioni sanitarie erogate in passato a quel soggetto dallo stesso reparto/ambulatorio.
Un eventuale rifiuto alla costituzione del F.S.E. non avrà, pertanto, conseguenze negative sulla possibilità di usufruire delle prestazioni sanitarie richieste.

Si precisa che l'assistito ha la possibilità di non rendere visibili sul F.S.E. i dati relativi ad una prestazione ricevuta attraverso il cd "diritto di oscuramento". Tale diritto, che può essere esercitato chiedendo direttamente al personale sanitario al momento dell'erogazione della prestazione o successivamente a questa tramite accesso al F.S.E., avviene con modalità tali da garantire che nessun soggetto abilitato alla consultazione del F.S.E. per le finalità di cura venga a conoscenza del fatto che è stata effettuata tale sceltae che esistano dati oscurati.

L' oscuramento dell'evento clinico è revocabile nel tempo (oscuramento dell'oscuramento). Resta ferma la possibilità per il Titolare del trattamento di informare i soggetti abilitati ad accedere a tali strumenti che tutti i fascicoli cui hanno accesso possono non essere completi, in quanto l'Interessato potrebbe aver esercitato il suddetto diritto di oscuramento.

Le informative possono essere formulate distintamente per ciascuno dei Titolari del trattamento, in modo cumulativo, avendo comunque cura di indicare con chiarezza l'ambito entro il quale i singoli soggetti trattano i dati inseriti nel FSE.

Il Titolare deve valutare attentamente quali dati pertinenti, non eccedenti e indispensabili inserire nel F.S.E., in relazione alle necessità di prevenzione, diagnosi, cura e riabilitazione, anche mediante un'organizzazione modulare di tali strumenti, in modo da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni e, quindi, al modulo di dati indispensabili.

La particolare delicatezza dei dati personali trattati mediante il F.S.E. impone l'adozione di specifici accorgimenti tecnici, per assicurare idonei livelli di sicurezza.

Art. 21 INFORMATIVA

(artt. 12-14 Regolamento UE 2016/679)

Il Titolare del trattamento è tenuto a fornire all'Interessato tutte le informazioni previste dagli artt. 13 e 14 del Regolamento UE 2016/679 in forma concisa, trasparente, intelligibile e facilmente accessibile, ovvero con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate ai minori.
Lo scopo di tale adempimento è quello di mettere l'Interessato in condizioni di conoscere quale siano l'ambito e le conseguenze del trattamento.
L'informativa è fornita per iscritto, mediante idonei strumenti, quali:

a) moduli appositi da consegnare agli Interessati. Nel modulo sono indicati i soggetti a cui l'utente può rivolgersi per ottenere maggiori informazioni ed esercitare i propri diritti;
b) avvisi agevolmente visibili dal pubblico, posti nei locali di accesso delle strutture dell'Azienda, nelle sale d'attesa e in altri locali in cui ha accesso l'utenza o diffusi nell'ambito di pubblicazioni istituzionali e mediante il sito internet dell'Azienda;
c) avvertenza apposita inserita nei contratti o nelle lettere di affidamento al servizio del personale dipendente, del personale medico convenzionato, dei soggetti con i quali vengono instaurati rapporti di collaborazione o libero-professionali, degli specializzandi, tirocinanti, dei volontari, ecc. Per quanto riguarda i soggetti che hanno già instaurato rapporti con l'Azienda, l'informativa è fornita nei tempi e nei modi che saranno concordati tra il Referente aziendale privacy e i Designati altrattamento;
d) avvertenza resa in sede di pubblicazione dei bandi, all'affidamento di lavori o gare di forniture di beni e di servizi.

L'informativa contiene:

a) le finalità e le modalità del trattamento;
b) le basi giuridiche che giustificano e rendono lecito il trattamento;
c) le categorie di soggetti destinatari dei dati;
d) le informazioni per la costituzione del D.S.E. sulla base del consenso espresso dall'Interessato e possibilità di oscuramento di alcuni dati dello stesso;
e) l'indicazione e i dati identificativi del Titolare del Trattamento e del Responsabile per la protezione dei dati personali (DPO);
f) il trattamento dei dati in casi particolari;
g) l'indicazione dei diritti dell'Interessato;
h) il termine di conservazione dei dati personali e, qualora non fosse possibile, l'indicazione di criteri idonei a determinare tale termine;
i) l'ambito di comunicazione e diffusione dei dati, con specifica indicazione circa il trasferimento dei dati al di fuori del Sistema Economico UE e sull'esistenza delle dovute garanzie di protezione dei dati personali presso tali Paesi Terzi;
j) informazioni circa l'esistenza di un processo decisionale automatizzato, compresa la profilazione.

Qualora i dati siano raccolti da soggetti diversi dall'interessato, ex art 14 del Regolamento UE 2016/679, l'informativa conterrà tutte le informazioni di cui sopra, con l'aggiunta dell'indicazione della fonte di conoscenza delle informazioni stesse; tuttavia, il Titolare sarà esonerato da tale adempimento, qualora lo stesso risulti impossibile o comporterebbe uno sforzo sproporzionato, nonché qualora i dati debbano rimanere riservati conformemente a un obbligo di segreto professionale o altro obbligo di segretezza previsto dalla legge.

Tali informazioni possono altresì essere rese senza ritardo, successivamente alla prestazione, in caso di:

a) impossibilità fisica, incapacità, temporanea, di agire o incapacità, temporanea, di intendere o di volere dell'Interessato;
b) rischio grave, imminente ed irreparabile per la salute o l'incolumità fisica dell'interessato;
c) in caso di prestazione medica che può essere pregiudicata dal loro preventivo rilascio, in termini di tempestività o efficacia.

Nei bandi di gara, nei contratti/accordi/convenzioni, nei bandi di concorso pubblico, nelle segnalazioni di disservizio e reclami inviati all'U.O.C. Relazioni con il Pubblico, nonché in tutte le altre ipotesi di trattamento di dati personali è inserita la seguente clausola informativa:

"I dati personali acquisiti dall'Asl Napoli 3 Sud saranno trattati nel rispetto dei principi del Regolamento Ue n. 2016/679 e del d. lgs. n. 196 del 2003, nonché secondo le modalità, finalità e limiti indicati nel documento informativo pubblicato sul sito web istituzionale dell'Ente e/o in quello specificamente rilasciato nel momento in cui dati sono ottenuti".

Art. 22 CONSENSO AL TRATTAMENTO DEI DATI

(art. 7 Regolamento UE 2016/679)

Il consenso costituisce condizione di liceità del trattamento dei dati personali solo in via residuale rispetto alle altre condizioni individuate dal Regolamento Ue e dal Codice Privacy.

Qualora dalla mappatura delle attività di trattamento la base giuridica del trattamento sia individuata nel consenso, il Titolare deve essere in grado di dimostrare che l'Interessato abbia prestato il proprio consenso al trattamento dei propri dati personali.

Il consenso deve essere espresso mediante un atto positivo, inequivocabile, con il quale l'Interessato

manifesti l'intenzione libera, specifica e informata di accettare il trattamento dei dati personali che lo riguardano.

In particolare, il consenso deve essere reso dall'Interessato attraverso la compilazione dell'apposito modulo, previa consegna e presa d'atto della relativa informativa, recante la specifica indicazione della facoltà di revocare, in qualsiasi momento e con le medesime facilità, il consenso precedentemente accordato.

Se il consenso dell'Interessato è prestato nel contesto di una dichiarazione scritta che riguardi anche 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. La revoca del consenso precedentemente prestato non pregiudica la liceità dei precedenti trattamenti.

Il consenso ai sensi della normativa sulla protezione dei dati personali non deve essere confuso con il "consenso informato" di cui alla Legge 219/2017, necessario per poter sottoporre un paziente ad un determinato trattamento sanitario. In quest'ultima ipotesi, infatti, il paziente viene informato sul percorso diagnostico-terapeutico che gli viene proposto per poter decidere se sottoporsi a determinati accertamenti diagnostici, o trattamenti terapeutici, farmacologici o chirurgici.

Art. 23 COMUNICAZIONE DI DATI SANITARI ALL'INTERESSATO

I dati personali idonei a rivelare lo stato di salute possono essere resi noti:

a) all'Interessato;
b) ad un soggetto appositamente delegato per iscritto dall'Interessato.

Relativamente ai soggetti sprovvisti di capacità di agire, ovvero con limitazioni della stessa, nonché nei casi di incapacità naturale le informazioni possono essere rese a soggetti terzi che dimostrino, documentalmente, di essere portatori di interessi meritevole di tutela. All’Azienda è consentito, per il tramite dei propri dipendenti e a seguito di una valutazione fatta caso per caso, rifiutare la comunicazione delle informazioni di cui al presente articolo.

Art. 24 COMUNICAZIONI E NOTIZIE SULLO STATO DI SALUTE DEGLI UTENTI

Le comunicazioni e le informazioni sulle specifiche patologie dell'interessato possono essere rese a quest'ultimo solo per il tramite del medico dell'Azienda competente in relazione ai provvedimenti organizzativi aziendali, ovvero per il tramite del medico di fiducia dell'interessato da lui designato o del medico che ha prescritto il ricovero o gli accertamenti.

Il Designato al trattamento dei dati personali può autorizzare per iscritto gli esercenti le professioni sanitarie diversi dai medici che, nell'esercizio dei propri compiti, intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato. L'autorizzazione ne individua i limiti, le modalità e le cautele.

Nel caso in cui l'Interessato si trovi in stato di impossibilità fisica, di incapacità di agire o di incapacità naturale, le comunicazioni e le informazioni di cui ai commi 1 e 2 sono rese a chi dimostri, anche mediante autocertificazione resa ai sensi dell'art. 46 del D.P.R. 28.12.2000 n. 445, di esercitare legalmente la responsabilità genitoriale, di essere tutore dell’Interessato, di essere un prossimo congiunto, un familiare, un convivente.

È possibile fornire a soggetti terzi che ne facciano richiesta, previo consenso dell’interessato, informazioni sulla presenza dei pazienti quali ricoverati, nonché in merito alle condizioni di salute degli stessi.

Art. 25 PROCEDURE ORGANIZZATIVE A TUTELA DELLA RISERVATEZZA IN AMBIENTE SANITARIO

Presso tutti i presidi dell'Azienda, a cura del Direttore della struttura, anche quale incaricato delle funzioni datoriali, sono adottate procedure, quali l'adozione di opportuna segnaletica per delimitare le distanze di cortesia, atte a garantire la riservatezza degli utenti in occasione di richiesta o fruizione di prestazioni sanitarie (prenotazioni, esami diagnostici, visite mediche, certificazioni, etc.) o amministrative (rimborsi, indennità, ecc.).

Nella sale di attesa i pazienti non possono essere chiamati per nome.

I Designati e gli Autorizzati al trattamento sono tenuti ad adottare idonee misure atte a garantire che le informazioni sanitarie personali rese agli utenti verbalmente o tramite supporto cartaceo (documenti sanitari), non siano accessibili o percepibili da parte di terzi non espressamente autorizzati dagli interessati.

Le strutture ospedaliere possono fornire, fermo quanto previsto dall'art. 24 del presente Regolamento, informazioni sui degenti, anche tramite il centralino telefonico, relativamente alla loro presenza in ospedalee sulla loro collocazione all'interno della struttura, previo consenso dell'Interessato che dovrà indicare anchei soggetti ai quali possono essere date le informazioni.

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

Art. 26 PUBBLICITA' DEGLI ATTI E DIRITTO ALLA RISERVATEZZA

Salva diversa disposizione di legge, l'Azienda garantisce la riservatezza dei dati personali in sede di pubblicazione all'Albo online o di altri atti, mediante la non identificabilità dei soggetti cui tali dati si riferiscono, adottando gli opportuni accorgimenti in sede di predisposizione degli atti stessi e dei relativi allegati.

Laddove documenti e informazioni, oggetto di pubblicazione obbligatoria per finalità di trasparenza, contengano dati personali, questi ultimi devono essere pseudonimizzati.

Non è consentita la diffusione online di dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità, handicap fisici e/o psichici.

Nel caso in cui un documento, soggetto per legge a pubblicazione, riporti le informazioni rientranti nelle particolari categorie di dati, nonché relativi a relativi a condanne penali e reati, questi devono essere anonimizzati attraverso l'oscuramento totale del nominativo e delle altre informazioni, nel rispetto dei principi di necessità, pertinenza e non eccedenza.

Le predette categorie di dati sono sottratte all'indicizzazione e alla rintracciabilità tramite i motori di ricerca web esterni ed il loro riutilizzo.

L'Azienda applica in materia le disposizioni previste dal Provvedimento dell'Autorità Garante "*Linee Guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri Enti obbligati*" del15 maggio 2014, doc. web n. 3134436.

Art. 27 DIRITTO DI ACCESSO ALLA DOCUMENTAZIONE E RISERVATEZZA

Fatti salvi gli atti sottratti all'accesso a norma di legge o di regolamento, l'Azienda garantisce il diritto di accesso alla documentazione amministrativa nel rispetto dei limiti relativi alla tutela degli interessi giuridicamente rilevanti e nei limiti in cui sia strettamente indispensabile, nonché nell'esercizio dello svolgimento delle investigazioni difensive di cui alla legge 7 Dicembre 2000, n. 397.

L'istanza di accesso può essere negata per evitare un pregiudizio concreto alla protezione dei dati personali. Il limite riguarda solo alcuni dati o parti del documento richiesto, mentre deve essere consentito l'accesso agli altri dati che non comportino alcun pregiudizio per l'interessato.

Nel caso in cui l'istanza avanzata dal richiedente riguardi una documentazione contenete dati personali o categorie particolari di dati appartenenti a terzi, l'accesso è limitato alla sola visione dei dati la cui conoscenza sia necessaria per curare o difendere un proprio interesse giuridico, nel rispetto dei principi di pertinenza e di non eccedenza dei dati da visionare rispetto alle finalità per le quali è consentito l'accesso.

Qualora l'istanza di accesso riguardi documenti contenenti dati idonei a rivelare particolari categorie di dati, ovvero dati relativi a condanne penali e reati, l'accesso è consentito solo se la situazione giuridicamente rilevante che si intende tutelare in sede giudiziaria sia di rango almeno pari ai diritti del terzo, ovvero consista in un diritto della personalità o altro diritto o libertà fondamentale e inviolabile, sempre che le informazioni richieste siano pertinenti e non eccedenti le finalità per cui è richiesto l'accesso.

L'Azienda valuterà, caso per caso, la possibilità di concedere l'autorizzazione all'accesso ai documenti da parte di terzi e qualora autorizzi l'accesso dovrà effettuare un'attenta valutazione su quali informazioni debbano essere comunicate e quali invece siano eccedenti, rispetto allo scopo perseguito.

Si rimanda alla vigente regolamentazione aziendale in materia di accesso agli atti amministrativi (Deliberazione del Commissario Straordinario n. 100 del 18.02.2016) ed in materia di documentazione sanitaria (Deliberazione del Direttore Generale n. 273 del 22.03.2018).

Art. 28 RINVIO A PREVISIONI DI NORMATIVA SPECIALE

Restano fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa comunitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali e, in particolare:

- dall'art. 5, della Legge 5 giugno 1990, n. 135, come modificato dall'art. 178 del Codice, secondo cui la rivelazione statistica della infezione da HIV deve essere effettuata con modalità che non consentano l'identificazione della persona;
- dall'art. 11 della Legge 22 maggio 1978, n. 194, il quale dispone che l'ente ospedaliero, la casa di curao il poliambulatorio nei quali è effettuato un intervento di interruzione di gravidanza devono inviare alla Regione una dichiarazione che non faccia menzione dell'identità della donna;
- dall'art. 734-bis del Codice Penale, il quale vieta la divulgazione non consensuale delle generalità o dell'immagine della persona offesa da atti di violenza sessuale.

Restano altresì fermi gli obblighi di legge, salva giusta causa, che vietano la rivelazione e l'impiego, a proprio o altrui profitto, delle notizie coperte dal segreto professionale, nonché gli obblighi deontologici previsti; in particolare, quelli di cui al Codice di deontologia medica, adottato dalla Federazione nazionale degli ordini dei medici chirurghi e degli odontoiatri.

Art. 29 CARTELLA CLINICA E DOCUMENTAZIONE MEDICA

Il Responsabile dell'Unità Operativa che ha in carico il paziente risponde della regolarità nella redazione della Cartella clinica; essa deve essere conclusa con la diagnosi di dimissione e firmata dal Responsabile

sopracitato o da altro Dirigente medico a ciò appositamente delegato.

La cartella clinica è un atto pubblico di fede privilegiata che deve essere conservata per un periodo di tempo illimitato e risponde alle regole di cui alla delibera del Commissario Straordinario n. 4, del 12/01/2016.

La compilazione delle cartelle cliniche deve garantire la comprensibilità dei dati, in modo che siano distintii dati relativi al paziente da quelli eventualmente riguardanti altri Interessati, ivi comprese informazioni relative a nascituri.

Ai sensi dell'art. 7 del D.P.R. 128/1969 il primario è responsabile della regolare tenuta della compilazione delle cartelle cliniche, finché il paziente non sia dimesso; successivamente, quando il paziente è stato dimesso e le cartelle trasferite presso la struttura di degenza dell'archivio, sarà responsabile il Direttore Sanitario della struttura.

Eventuali richieste di presa visione o di rilascio di copia della cartella 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 viene effettuata in forma scritta, con firma autenticata nelle forme previste dalla legge, ed è giustificata dalla documentata necessità:

- di esercitare o difendere un diritto in sede giudiziaria ai sensi dell'articolo 9, paragrafo 2, lettera f), del Regolamento UE 679/2016, di rango pari a quello dell'interessato, ovvero consistente in un dirittodella personalità o in un altro diritto o libertà fondamentale;
- 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.

In ogni caso, il terzo dovrà produrre idonea documentazione, anche per il tramite dello strumento dell'autocertificazione, a riprova della propria qualità, che legittimi la presentazione dell'istanza in parola.

Nel caso di decesso dell'interessato, il richiedente può accedere ai dati personali presenti nella cartella clinica, qualora dimostri un interesse proprio a tutela del deceduto o per ragioni familiari meritevoli di protezione.

In ogni caso, l'Azienda dovrà effettuare, caso per caso, una concreta valutazione del "rango" del diritto che il terzo richiedente l'accesso alla documentazione sanitaria intende far valere sulla base della documentazione sanitaria stessa (cfr. Provvedimento generale del Garante sui diritti di pari rango del 9 luglio 2003).

Il Titolare, inoltre, dovrà agire nel rispetto dei principi di cui all'art. 13 del presente Regolamento.

L'accesso è normalmente consentito agli eredi che autocertifichino tale *status* ai sensi del D.P.R. 445/2000.

Il rilascio della cartella clinica o di referti clinici o di altra documentazione sanitaria è inoltre consentito a soggetti non intestatari della documentazione stessa nei seguenti casi:

a) richiesta da parte degli Organi Giudiziari;
b) richiesta del Direttore medico di Presidio ospedaliero e del legale rappresentante di altro Ospedale o Casa di cura, diversi da quelli presso i quali la documentazione sanitaria è conservata, qualora il paziente si trovi in esso ricoverato e sia necessario acquisire dati utili al trattamento dello stato morboso in atto, quindi per finalità di tutela della salute e dell'incolumità fisica del paziente, previa richiesta scritta, a firma del medico di reparto richiedente;
c) richiesta da parte del Consulente Tecnico d'Ufficio, previa esibizione dell'atto di nomina e di

autorizzazione del Giudice;

d) I.N.A.I.L., nei casi di infortunio o di malattia professionale occorso ad un assicurato, con delega sottoscritta dall'assistito (artt. 94 e 95 del D.P.R. 3.6.1965 n. 1124; art. 5 all. A al D.M. 15.3.1991);
e) I.N.P.S., con delega sottoscritta dall'assistito, nei casi in cui competano a questo le spese di spedalità per i pazienti dipendenti da aziende private (artt. 17 e 18 del D.P.R. n. 2316 del 1934);
f) Prefetture per spese di ricovero ospedaliero urgente di cittadini stranieri che dichiarino lo stato di indigenza, per i quali si richiede il rimborso del costo del ricovero direttamente all'AutoritàPrefettizia (Legge 17.7.1890 n. 6972; R.D. n. 99 del 5.2.1891, art. 114);
g) richiesta da parte di persona esercente la Responsabilità genitoriale, previa autocertificazione del relativo status;
h) Richiesta da parte del tutore del minore, nominato dal Giudice tutelare;
i) richiesta del medico di base, che ha in cura il paziente, con esplicitazione della indispensabilità di accedere a tali documenti per la tutela dell'incolumità fisica e della salute del paziente e mediante contestuale presentazione di documentazione idonea a dimostrare il consenso scritto dell'interessato;
j) richiesta da parte del tutore della persona interdetta, previa esibizione di documentazione probatoriae dichiarazione sostitutiva dell'atto di notorietà da cui risulti il relativo status;
k) dall'amministratore di sostegno previa esibizione della copia del decreto di nomina del Giudice Tutelare che certifichi il relativo *status*, qualora tale potere rientri nei suoi poteri.

La cartella clinica e la documentazione socio sanitaria possono essere consultate dal personale medico dell'Azienda, fermo restando che le cartelle cliniche dovranno essere conservate con tecniche di cifratura o mediante l'utilizzo di codici identificativi che rendano i dati temporaneamente non intelligibili, salvo la necessità degli operatori di accedere ai dati identificativi gli interessati, tenuto conto dell'attività espletata.

La consultazione delle cartelle cliniche per finalità di ricerca scientifica o statistica può essere effettuata sulla base di un atto motivato che ne giustifichi le finalità e deve essere autorizzata dalla Direzione sanitaria dell'Azienda. In questi casi i dati dovranno essere resi anonimi o comunicati in forma aggregata con modalità che rendono non identificabili i soggetti cui si riferiscono.

Si rimanda altresì alla vigente regolamentazione aziendale di cui alla deliberazione n. 273 del 22.03.2018.

Art. 30 RITIRO DEI REFERTI O ALTRA DOCUMENTAZIONE CONTENENTE DATI SANITARI

Il ritiro dei referti o altra documentazione contenente dati sullo stato di salute può essere effettuato, compilando apposito modulo.

a) dal diretto interessato;
b) da chi esercita la tutela, in caso di minore o di interdetto, ovvero dall'amministratore di sostegno se l'atto rientra tra i poteri conferitigli dal Giudice tutelare nel decreto di nomina, in caso contrario direttamente all'interessato;
c) dal delegato dell'interessato, se munito di delega, documento proprio e documento del delegante.

La consegna dei documenti deve essere effettuata in busta chiusa.

Non è possibile la comunicazione per via telefonica dei risultati delle analisi, salvo situazioni di assoluta necessità e urgenza a tutela dell'incolumità fisica dell'interessato.

Art. 31 VIDEOSORVEGLIANZA

Si rinvia a specifico Regolamento da adottarsi, previa predisposizione a cura della UOS Privacy con l'ausilio ed il supporto dei collaboratori interni e degli eventuali consulenti esterni nonché con la collaborazione delle articolazioni aziendali competenti in materia.

Art. 32 I DIRITTI DELL'INTERESSATO

(artt. 15-22 Regolamento UE 2016/679)

L'interessato è il soggetto, persona fisica, alla quale si riferiscono i dati oggetto del trattamento.

L'Azienda attua tutte le misure necessarie a facilitare l'esercizio dei diritti dell'interessato ai sensi degli artt. 12-22 del Regolamento UE 2016/679.

In particolare, l'interessato ha diritto ad ottenere tutte le informazioni di cui agli artt. 13 e 14 e le comunicazioni di cui agli artt. da 15 a 22 e all'articolo 34 (Regolamento UE 2016/679), relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplicee chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

Le informazioni sono fornite per iscritto o con altri mezzi, anche elettronici, purché gli stessi siano comprensibili dall'Interessato.

1) L'Interessato ha il diritto di ottenere 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 informazioni riguardanti:

a) le finalità del trattamento;
b) le categorie di dati trattati;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
d) il periodo di conservazione dei dati, ovvero, in mancanza, i criteri per determinare tale durata;
e) il diritto di chiedere 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 a un'autorità di controllo;
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) L'interessato ha diritto di ottenere una copia dei dati personali oggetto di trattamento. Qualora l'interessato faccia richiesta di ottenere più copie, il Titolare del trattamento può attribuire un contributo spese ragionevole tenendo conto dei costi amministrativi, come già determinati nel regolamento d'accesso agli atti. Se la richiesta dell'interessato perviene con mezzi elettronici, salvo diversa indicazione dell'interessato, le informazioni saranno rese in un formato elettronico di uso comune.

3) L'interessato ha il diritto di ottenere la rettifica/aggiornamento dei dati personali inesatti che lo riguardano, senza ingiustificato ritardo, nonché l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

4) L'interessato ha diritto di ottenere la cancellazione (diritto all'oblio) dei dati personali che lo riguardano, se trattati in violazione di legge, senza ingiustificato ritardo o quando ricorra uno dei motivi di cui all'art. 17 del Regolamento UE 2016/679. Nel caso in cui il Titolare del trattamento abbia reso pubblici i dati dell'interessato ed è obbligato a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure e tecniche ragionevoli per informare gli altri soggetti, a cui sono pervenuti i dati personali, della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. Tale diritto trova alcune limitazioni nell'art. 17, terzo paragrafo, del Regolamento UE 2016/679.

5) L'interessato ha diritto di ottenere l'attestazione che i suddetti interventi sui dati sono stati portati a conoscenza (anche per il contenuto) di coloro ai quali i dati sono stati comunicati.

6) L’interessato ha diritto di ottenere la limitazione del trattamento dei dati personali quando ricorre una delle ipotesi previste nell'art. 18 alla lett. a), b), c), d) del Regolamento UE 2016/679. A seguito dell'esercizio, da parte dell'interessato, del diritto di limitazione del trattamento i dati personali sono trattati, salvo che per la conservazione, solo con il consenso dello stesso o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria o per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.

7) L’interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, se tecnicamente fattibile e senza limitazioni, qualora: il trattamento si basi sul consenso o contratto e si svolga in forma automatizzata. Il diritto alla portabilità dei dati è derogabile nel caso in cui il trattamento dei dati sia necessario per l'esecuzione di un pubblico interesse o sia connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento. Tale diritto non deve ledere i diritti e le libertà altrui.

8) L’interessato ha diritto di proporre opposizione al trattamento dei dati. A seguito dell'esercizio del diritto di opposizione da parte dell'interessato, il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali, salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sui diritti, interessi e libertà dell'interessato.

I diritti di cui agli articoli da 12 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell’Interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

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.

Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo all'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione.

L'autorità di controllo a cui è stato proposto il reclamo informa il reclamante dello stato o dell'esito del reclamo, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78 del Regolamento UE 2016/679.

Fatto salvo ogni altro ricorso amministrativo o extragiudiziale disponibile, compreso il diritto di proporre reclamo a un'autorità di controllo ai sensi dell'articolo 77 del Regolamento UE 2016/679, ogni interessato ha il diritto di proporre un ricorso giurisdizionale effettivo qualora ritenga che i diritti di cui gode a norma del presente regolamento siano stati violati a seguito di un trattamento.

Art. 33 MODALITÀ DI ESERCIZIO DEI DIRITTI DELL'INTERESSATO

Per i diritti dell'Interessato in ordine all'accesso ed al trattamento dei suoi dati personali, si applicano le disposizioni previste dal Regolamento UE 2016/679 e dal Codice della Privacy.

Chiunque opera all’interno dell’organizzazione aziendale è tenuto a conoscere e porre in essere senza ritardo le azioni e gli accorgimenti specificamente individuati nella procedura appositamente elaborata e diffusa dall’Ente per la gestione dei diritti degli interessati.

La richiesta per l'esercizio dei diritti dell’Interessato di cui al presente Regolamento può essere fatta pervenire:

a) direttamente dall'Interessato, anche facendosi assistere da una persona di fiducia, con l'esibizione di un documento personale di riconoscimento o allegandone copia, ovvero anche con altre adeguate modalità o in presenza di circostanze atte a dimostrare l'identità personale dell'Interessato stesso (es. la conoscenza personale);
b) tramite altra persona fisica o associazione, a cui l'Interessato abbia conferito per iscritto delega o procura; in tal caso, la persona che agisce su incarico dell'Interessato deve consegnare copia della procura o della delega, nonché copia fotostatica non autenticata di un documento di riconoscimento del sottoscrittore;
c) tramite chi esercita la tutela, per i minori e gli incapaci interdetti;
d) in caso di persone decedute, tali diritti possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'Interessato o per ragioni familiari meritevoli di protezione.

L'Interessato può presentare o inviare la richiesta di esercizio dei diritti:

- al Titolare o Designato al trattamento che conserva e gestisce i dati personali dell'Interessato;
- al Responsabile della Protezione dei dati;
- all'Ufficio protocollo generale dell'Azienda o all' U.O.C. Relazioni con il Pubblico, che ne curano l'inoltro al Titolare del trattamento.

La richiesta per l'esercizio dei diritti, di cui al primo paragrafo, può essere esercitata dall'Interessato solo in riferimento alle informazioni che lo riguardano e non ai dati relativi ai terzi, eventualmente presenti all'interno dei documenti che lo riguardano.

Il Titolare del trattamento autorizza l'esibizione degli atti all'Interessato, ricorrendone le condizioni per l'accesso.

I soggetti competenti alla valutazione dell'istanza sono: il Titolare e/o il Designato rispetto al trattamento dei dati di cui si richiede l'accesso, la UOS Privacy, il Direttore U.O.C. Sistemi Informatici i quali congiuntamente decidono sull'ammissibilità della richiesta d'accesso e sulle modalità per consegnare/limitare/cancellare i dati all'interessato.

All'istanza deve essere dato riscontro entro 30 giorni dalla data di ricezione della stessa. I termini possono essere prolungati ad altri 30 giorni dalla data di ricezione, previa tempestiva comunicazione all'Interessato, qualora l'istanza avanzata dal richiedente sia di particolare complessità o ricorra un giustificato motivo.

L'accesso dell'Interessato ai propri dati personali può essere differito, a norma dell'art. 7 del D.P.R. 27 Giugno 1992, n.352, limitatamente al periodo strettamente necessario, durante il quale i dati stessi sono trattati esclusivamente per lo svolgimento di indagini difensive o per salvaguardare esigenze di riservatezza dell'Azienda.

L'accesso è tuttavia consentito agli altri dati personali dell'Interessato che non incidono sulle ragioni di tutela a base del differimento.

Art. 34 INDAGINI DIFENSIVE

Nel corso di un procedimento penale, il difensore, ai sensi della Legge 7 dicembre 2000, n. 397 e dell'art. 391-*quater* del Codice di Procedura Penale, ha facoltà di svolgere investigazioni per ricercare ed individuare elementi di prova a favore del proprio assistito.

Ai fini di tali indagini, il difensore può chiedere documenti in possesso dell'Azienda (e può estrarne copiaa proprie spese) anche se contengono dati personali di un terzo interessato.

Il rilascio è subordinato alla verifica che il diritto difeso sia di rango almeno pari a quello dell'Interessato,e cioè consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile.

Si fa rinvio al Regolamento aziendale sul Diritto di accesso di cui alla Deliberazione del Commissario Straordinario n. 100 del 18.02.2016.

Art. 35 FORMAZIONE DEL PERSONALE

(art. 29 Regolamento UE 2016/679)

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

Art. 36 MISURE DI SICUREZZA

(art. 32 Regolamento UE 2016/679)

L'Azienda, nel trattamento dei dati personali, garantisce l'applicazione di idonee e preventive misure di sicurezza che consentano 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.

Secondo la normativa vigente in materia, il Titolare e il Designato al trattamento, su proposta ed indicazione della UOS Privacy e del Responsabile protezione dati, mettono in atto misure e tecniche organizzative per garantire un livello di sicurezza adeguato al rischio, che comprendono:

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

Il Titolare e il Designato al trattamento fanno sì che chiunque agisca sotto la loro autorità ed abbia accessoai dati personali, non tratti tali dati se non sia istruito ed autorizzato a tale scopo.

Art. 37 TRASFERIMENTO DI DATI FUORI DALLO SPAZIO ECONOMICO EUROPEO

I dati personali potranno essere trasferiti fuori dallo SEE solo nei casi previsti dal Regolamento Ue agli artt. 45 (decisione di adeguatezza), 46 (garanzie adeguate), 47 (norme vincolanti di impresa), 49 purché siano trasferiti una sola parte dei dati limitatamente ai seguenti casi:
d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso.

I designati, con il supporto del RPD, procedono alla valutazione di ogni trasferimento. In particolare dovrà essere posta particolare attenzione alla valutazione del sistema giuridico del paese destinatario qualora si proceda in base agli artt. 46-47 (vedasi la Sentenza della Corte di Giustizia C 311/18).

Si ricorda che rendere accessibile a entità situati al di fuori dello SEE costituisce trasferimento aprescindere da dove siano conservati i dati. Unica eccezione è la pubblicazione su un sito internet posto nella Comunità Europea quando sia lecita tale pubblicazione.

Art. 38 MODULISTICA

All'interno dell'Azienda sono adottati modelli uniformi di informative, nomine e procedure che sono periodicamente aggiornati a cura della UOS Privacy, sentito il parere del D.P.O., in collaborazione con i Designati e gli Autorizzati al trattamento e sotto la supervisione del Titolare del trattamento.

Art. 39 RESPONSABILITÀ IN CASO DI VIOLAZIONE DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

(artt. 77-84 Regolamento UE 2016/679)

Il mancato rispetto delle disposizioni in materia di riservatezza dei dati personali è punito con sanzioni di natura amministrativa e di natura penale nelle ipotesi previste dal Regolamento Ue 2016/679 e dal Codice Privacy, nonché con sanzioni di natura disciplinare.

Il Titolare del trattamento risponde per il danno cagionato dal suo trattamento che violi la normativa vigente.

Il Designato al trattamento risponde per il danno causato dal trattamento, qualora non abbia adempiuto agli obblighi previsti nel presente Regolamento, a lui specificamente diretti, ovvero abbia agito in modo difforme o contrario rispetto alle legittime istruzioni impartitegli dal Titolare del trattamento.

Il Titolare o il Responsabile del trattamento sono esonerati da responsabilità se dimostrano che l'evento dannoso non gli è in alcun modo imputabile.

Art. 40 COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI

(art. 33 e 34 Regolamento UE 2016/679)

Quando si verifica un incidente sulla sicurezza dei dati personali, chiunque opera all'interno dell'organizzazione aziendale è tenuto a porre in essere senza ritardo le azioni e gli accorgimenti specificamente individuati nella procedura appositamente elaborata e diffusa dall'Ente per la gestione degli incidenti e delle violazioni.

La comunicazione dell'avvenuta violazione dei dati personali (*Data Breach*) è effettuata dal Titolare del trattamento senza ingiustificato ritardo.La notifica deve:

a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) comunicare il nome e i dati di contatto del responsabile 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.

Fermo quanto sopra esposto, qualora non sia possibile fornire le informazioni contestualmente, le stesse possono essere fornite in fasi successive, senza ulteriore ingiustificato ritardo.

La violazione è notificata, entro 72 ore, all'Autorità di controllo competente, salvo che sia improbabile chela violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo

Quando la violazione dei dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento comunica la violazione, altresì, all'Interessato, senza ingiustificato ritardo. La comunicazione all'Interessato descrive, con un linguaggio semplice e chiaro, la natura della violazione dei dati personali: tale comunicazione deve contenere tutte le informazioni di cui alla lettera b,c, e d, del presente articolo.

Non è richiesta la comunicazione qualora ricorra una delle seguenti condizioni:

- il Titolare del trattamento abbia messo in atto, preventivamente, le misure tecniche e organizzative di protezione adeguate e tali misure erano state applicate ai dati personali oggetto di violazione (ad esempio la cifratura);
- il Titolare del trattamento abbia successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà dell'interessato;
- la comunicazione richiederebbe sforzi sproporzionati, in tal caso si procede a una comunicazione pubblica o a una misura simile tramite la quale gli interessati sono informati con analoga efficacia.

Le violazioni dei dati trattati mediante Dossier sanitario elettronico devono essere comunicate entro le 48 ore al Garante Privacy, previa comunicazione senza ritardo all'Interessato delle operazioni di trattamento illecito effettuata sui suoi dati mediante il Dossier Sanitario Elettronico.

Il Titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio.

Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Art. 41 ACCERTAMENTI

Il Garante può disporre accessi a banche di dati, archivi o altre ispezioni e verifiche nei luoghi ove si svolge il trattamento o nei quali occorre effettuare rilevazioni comunque utili al controllo del rispetto della disciplina in materia di trattamento dei dati personali.

I controlli in parola sono eseguiti dal personale dell'Ufficio, con la partecipazione, se del caso, di componenti o personale di autorità di controllo di altri Stati membri dell'Unione europea.

Il Garante si avvale anche, ove necessario, della collaborazione di altri organi dello Stato per lo svolgimento dei suoi compiti istituzionali.

Ove l'accertamento venga effettuato presso il titolare del trattamento, viene redatto apposito verbale in contradditorio con le parti.

Art. 42 NORMA FINALE

Per quanto non previsto nel presente Regolamento, si rimanda all'applicazione delle norme e dei principi dettati dal Regolamento UE 2016/679, dal Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni ed integrazioni) e dai provvedimenti specifici del Garante per la protezione dei dati personali.

Il presente Regolamento sarà aggiornato a seguito di ulteriori modificazioni alla vigente normativa in

materia di riservatezza e protezione dei dati personali, a cura della UOS Privacy e del Responsabile della protezione dei dati.