REGIONE CAMPANIA
AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE E DI ALTA SPECIALIZZAZIONE
"SANT'ANNA E SAN SEBASTIANO"
CASERTA

Deliberazione del Direttore Generale N. 113 del 01/02/2024

Proponente: Il Direttore UOC SERVIZI INFORMATICI AZIENDALI

Oggetto: Applicazione Atto Aziendale di cui al D.G.R.C. n.654/2023 – Adozione Regolamento Sistema di Protezione e Sicurezza dei Dati

PUBBLICAZIONE
In pubblicazione dal 01/02/2024 e per il periodo prescritto dalla vigente normativa in materia (art.8 D.Lgs 14/2013, n.33 e smi)

ESECUTIVITA'
Atto immediatamente esecutivo

TRASMISSIONE
La trasmissione di copia della presente Deliberazione è effettuata al Collegio Sindacale e ai destinatari indicati nell'atto nelle modalità previste dalla normativa vigente. L'inoltro alle UU. OO. aziendali avverrà in forma digitale ai sensi degli artt. 22 e 45 D.gs. n° 82/2005 e s.m.i. e secondo il regolamento aziendale in materia.

UOC AFFARI GENERALI
Direttore Eduardo Chianese

ELENCO FIRMATARI

Gaetano Gubitosa - DIREZIONE GENERALE

Giovanni Sferragatta - UOC SERVIZI INFORMATICI AZIENDALI

Angela Annecchiarico - DIREZIONE SANITARIA

Amalia Carrara - DIREZIONE AMMINISTRATIVA

Per delega del Direttore della UOC AFFARI GENERALI, il funzionario Pasquale Cecere

Oggetto: Applicazione Atto Aziendale di cui al D.G.R.C. n.654/2023 – Adozione Regolamento Sistema di Protezione e Sicurezza dei Dati

Direttore UOC SERVIZI INFORMATICI AZIENDALI

A conclusione di specifica istruttoria, descritta nella narrazione che segue e i cui atti sono custoditi presso la struttura proponente, rappresenta che ricorrono le condizioni e i presupposti giuridico-amministrativi per l'adozione del presente provvedimento, ai sensi dell'art. 2 della Legge n. 241/1990 e s.m.i. e, in qualità di responsabile del procedimento, dichiara l'insussistenza del conflitto di interessi, ai sensi dell'art. 6 bis della legge 241/90 e s.m.i.

Premesso che
- con Deliberazione n. 411 del 14.06.2018 è stato adottato il regolamento del Sistema di Protezione e Sicurezza dei Dati;

Considerato che
- con Deliberazione di Giunta Regionale della Campania n. 654 del 16.11.2023 ad oggetto "Atto Aziendale AORN Sant'Anna e San Sebastiano di Caserta è stato approvato il nuovo Atto Aziendale di quest'azienda;
- con Deliberazione n. 1080 del 30.11.2023 quest'azienda ha preso atto dell'approvazione regionale dell'Atto Aziendale;
- il D.C.A. n.18 del 18.02.2013 dispone, tra l'altro, da parte delle aziende del SSR, in occasione dell'approvazione di un nuovo atto aziendale, la riadozione di una serie di regolamenti obbligatori, nonché di regolamenti ritenuti necessari, tra cui si può includere anche la riadozione del regolamento del Sistema di Protezione e Sicurezza dei Dati;
- che lo stesso Atto Aziendale, al paragrafo 1.3, prevede, tra gli altri, l'aggiornamento del regolamento del sistema di protezione e sicurezza dei dati;

Ritenuto
- di dover, quindi, procedere, per le motivazioni che precedono, all'aggiornamento del regolamento del sistema di protezione e sicurezza dei dati in attuazione del nuovo Atto aziendale;

Visti
- il D.C.A. n.18 del 18.02.2013;
- la D.G.R.C. n. 654 del 16.11.2023;

Attestata la legittimità della presente proposta, che è conforme alla vigente normativa in materia;

PROPONE

1. di adottare il nuovo *Regolamento del Sistema di Protezione e Sicurezza dei Dati* come da documento allegato che costituisce parte integrante e sostanziale del presente atto, in attuazione di quanto previsto dal nuovo Atto aziendale approvato con DGRC 654/2023;
2. di demandare alla U.O.C. Affari Generali la trasmissione di copia del presente atto:
   - al Collegio Sindacale,
   - alla UOC Gestione Economico Finanziaria,
   - al Responsabile della Prevenzione della Corruzione e della Trasparenza per la pubblicazione nell'apposita sezione del sito web aziendale;
3. di rendere la presente deliberazione immediatamente eseguibile, stante i tempi di attuazione previsti per legge.

IL DIRETTORE GENERALE
Dr. Gaetano Gubitosa
individuato con D.G.R.C. n. 465 del 27/07/2023
immesso nelle funzioni con D.P.G.R.C. n. 80 del 31/07/2023

Vista la proposta di deliberazione che precede, a firma del Direttore UOC Servizi Informatici Aziendali, Dr. Giovanni Sferragatta;

Acquisiti i pareri favorevoli del Direttore Sanitario e del Direttore Amministrativo in modalità telematica sotto riportati:

Il Direttore Sanitario	D.ssa Angela Annecchiarico	Favorevole
Il Direttore Amministrativo	Avv. Amalia Carrara	Favorevole

DELIBERA

per le causali in premessa, che qui si intendono integralmente richiamate e trascritte, di prendere atto della proposta di deliberazione che precede e, per l'effetto di:

1. **ADOTTARE** il nuovo *Regolamento del Sistema di Protezione e Sicurezza dei Dati*, come da documento allegato che costituisce parte integrante e sostanziale del presente atto, in attuazione di quanto previsto dal nuovo Atto aziendale approvato con DGRC 654/2023;
2. **DEMANDARE** alla U.O.C. Affari Generali la trasmissione di copia del presente atto:
   - al Collegio Sindacale,

- alla UOC Gestione Economico Finanziaria,
- al Responsabile della Prevenzione della Corruzione e della Trasparenza per la pubblicazione nell'apposita sezione del sito web aziendale;

3. **RENDERE** la presente deliberazione immediatamente eseguibile, stante i tempi di attuazione previsti per legge.

Il Direttore Generale
Gaetano Gubitosa

REGIONE CAMPANIA - AZIENDA OSPEDALIERA DI RILIEVO NAZIONALE

E DI ALTA SPECIALIZZAZIONE

"SANT'ANNA E SAN SEBASTIANO" DI CASERTA

REGOLAMENTO AZIENDALE

SISTEMA DI PROTEZIONE E SICUREZZA DEI DATI

SOMMARIO

1. INTRODUZIONE

1.1. ARTICOLO 1): PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali (così detta "privacy") è uno strumento di applicazione del vigente D.lgs. 30 giugno 2003, n. 196 (cosiddetto "Codice sulla privacy" come novellato dal recente D.lgs. 10 agosto 2018 n. 101) e, in particolare, del nuovo Regolamento Europeo n. 2016/679, anche conosciuto come "GDPR"), nell'ambito dell'organizzazione dell'Azienda Ospedaliera "Sant'Anna e San Sebastiano" di Caserta.

A far data dal 25 maggio 2018 ha trovato diretta ed immediata applicazione, sul territorio nazionale, il nuovo Regolamento Europeo n. 2016/679 (così detto GDPR ossia "General Data Protection Regulation") sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 04 maggio 2016.

Ciò ha comportato il superamento, a far data dal 25 maggio 2018, delle disposizioni legislative di cui al previgente Codice della privacy (D.lgs. 196/2003 come successivamente modificato dal Legislatore italiano con il D.lgs. 101 del 10 agosto 2018 di adeguamento al GDPR), così come delle norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, nella misura in cui le norme nazionali risultino contrastanti o incompatibili con quelle europee.

Il principio cardine, di matrice anglosassone, introdotto dal nuovo Regolamento Europeo è quello della "responsabilizzazione" (accountability nell'accezione inglese) che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della "conformità" o compliance nell'accezione inglese); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento UE.

Nell'ottica del Legislatore europeo, quindi, in materia di privacy ciascun Titolare può scegliere autonomamente il modello organizzativo e gestionale che ritiene più adatto alla propria realtà e dotarsi delle misure di sicurezza che ritiene più efficaci in quanto Egli risponde delle proprie azioni e deve essere in grado, in qualsiasi momento, di darne conto verso l'esterno (il termine accountability, infatti, rinvia letteralmente al concetto di "resa di conto").

Il "sistema aziendale privacy" adottato dall'Azienda Ospedaliera di Caserta, in attuazione del principio europeo dell'accountability, è oggi infatti interamente fruibile nel sito internet (www.ospedale.caserta.it) di questa Azienda, nell'apposita pagina web denominata "PROTEZIONE DEI DATI PERSONALI" (www.ospedale.caserta.it/gdpr/gdpr.htm).

La pagina di cui si tratta contiene diverse "sezioni" rispondenti alle esigenze concrete e quotidiane dei propri operatori.

Il presente Regolamento aziendale si rende necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di carattere aziendale che nazionale, in tema di trattamento dei dati personali, al fine darne collocazione sistematica nel contesto di questa Azienda.

Il presente Regolamento è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

1.2. ARTICOLO 2): PREMESSA DI CARATTERE ORGANIZZATIVO

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

Il diritto alla privacy costituisce, anche secondo il Legislatore europeo, un vero e proprio diritto inviolabile dell'essere umano, 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 del singolo individuo.

Per questi motivi, la "cultura della privacy" necessita di divenire un vero e proprio elemento cardine dell'organizzazione di questa Azienda, che deve impegnarsi perché la cultura di cui si tratta possa crescere e rafforzarsi, principalmente fra gli operatori della sanità, in quanto solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo, nel trattamento dei 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 ed alla implementazione del "processo di umanizzazione" in corso di realizzazione, nell'ambito di questa Azienda, oramai da molti anni.

2. DISPOSIZIONI GENERALI

2.1. ARTICOLO 3): OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno dell'Azienda, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto dal Codice in materia di protezione dei dati personali (Decreto Legislativo del 30/06/2003 n. 196 e ss.mm.ii.) ed in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

2.2. ARTICOLO 4): FINALITÀ' DEL REGOLAMENTO

L'Azienda Ospedaliera di Caserta garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea.)

2.3. ARTICOLO 5): SENSIBILIZZAZIONE

L'Azienda Ospedaliera di Caserta 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 tale riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, 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 introdotte dal nuovo Regolamento europeo, e di conseguenza dal presente nuovo Regolamento aziendale, questa Azienda ha pubblicato sul proprio sito istituzionale www.ospedale.caserta.it tutti i documenti citati nel presente regolamento.

2.4. ARTICOLO 6): DEFINIZIONI

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare aziendale si intende per:

a) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può esser identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo

online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

b) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

c) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

d) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

e) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

f) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

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

h) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

i) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

j) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

k) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di

detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

l) «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;

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

A proposito delle tipologie di "dati" sopra indicate, si fa rinvio, per la disciplina di dettaglio, alle disposizioni di cui al D.lgs. 101 del 2018 che ha novellato il D.lgs. 196/2003 (vedasi, in particolare, il Titolo 1° della Parte 1^, rubricato "Disposizioni generali").

n) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;

Quelle sopra riportate, di cui si è data evidenza, rappresentano le "definizioni" su cui ha inciso maggiormente il nuovo Regolamento europeo: per le altre "definizioni" si fa espresso rinvio al testo dell'articolo n. 4 del Regolamento Europeo n. 2016/679 ed al D.lgs. 196/2003.

2.5. ARTICOLO 7): PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del Regolamento Europeo n. 2016/679, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»). A tale proposito, il Regolamento UE ricalca i principi sostanziali di "necessità, pertinenza, indispensabilità e non eccedenza" (rispetto alle finalità del trattamento) contenuti nel D.lgs. 196/2003;

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente

regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

Come stabilito dal Regolamento UE, il Titolare del trattamento, ovvero il Delegato Titolare del Trattamento dei Dati è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'«accountability» o «responsabilizzazione»).

2.6. ARTICOLO 8): TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Detta disposizione non si applica, secondo il Regolamento UE, quando incorrono alcune condizioni, riportate al summenzionato articolo n. 9, tra le quali si evidenzia quella di cui alla lettera "h", applicabile a questa Azienda, ai sensi della quale "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 ovvero gestione dei sistemi e servizi sanitari sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (..)", nonché quella di cui alla lettera "i", anch'essa applicabile a questa Azienda, ai sensi della quale "il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale".

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

Posto quanto sopra, si fa integrale rinvio agli articoli 2-sexies, 2-septies e 2-octies del D.lgs.196/2003 (come novellato dal D.lgs. 101/2018) contenenti specifiche disposizioni relative al trattamento delle categorie particolari di dati personali ed alle "misure di garanzia" per il trattamento dei dati genetici, biometrici e relativi alla salute.

2.7. ARTICOLO 9): TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del Regolamento Europeo n. 2016/679, "il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."

Posto quanto sopra, si fa integrale rinvio all'articolo 2-octies del D.lgs. 196/2003 (come novellato dal D.lgs. 101/2018) dedicato al trattamento dei dati relativi a condanne penali e reati.

2.8. ARTICOLO 10): COMUNICAZIONE DI DATI VERSO L'ESTERNO

La comunicazione di dati sensibili e giudiziari da parte di un soggetto pubblico ad altro soggetto pubblico, è ammessa quando è prevista da una norma di legge o regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi in gioco.

2.9. ARTICOLO 11): FASCICOLO SANITARIO ELETTRONICO

Il Fascicolo Sanitario Elettronico (abbreviato "FSE"), la cui istituzione è prevista dalla Legge, è l'insieme dei dati e dei documenti digitali di tipo sanitario e socio-sanitario, generati da eventi clinici presenti e trascorsi, riguardanti l'assistito.

L'avvento della digitalizzazione ha infatti rivoluzionato il mondo dei servizi, contribuendo a sviluppare nuove modalità con cui le istituzioni possono rispondere efficacemente ai bisogni dei cittadini. Questo vale anche per l'ambito sanitario: a tale proposito, la Regione Campania, in collaborazione con le aziende sanitarie ed ospedaliere sta portando avanti la realizzazione del Fascicolo Sanitario Elettronico (FSE), ovvero lo strumento digitale nel quale in futuro tutti i dati relativi alla storia sanitaria di un paziente (ricette farmaceutiche e specialistiche, referti di laboratorio, etc.) saranno raccolti, organizzati e resi accessibili allo stesso paziente e, solo per il tempo necessario e nel pieno rispetto della privacy, a chi lo prenderà in cura.

L'obiettivo è quello di abbattere tempi e costi, perché con la digitalizzazione, ove possibile, saranno i dati a spostarsi e non più le persone. Si tratta di un primo passo verso un mondo in cui, grazie alle tecnologie digitali, i dati e i servizi relativi alla salute siano sempre più facilmente disponibili, aggiornati, completi e rapidamente accessibili.

Il FSE è alimentato in maniera continuativa, previo consenso libero e informato dell'assistito, dai soggetti che lo prendono in cura nell'ambito del Servizio Sanitario Nazionale (SSN) e dei Servizi Sanitari Regionali - anche fuori dalla regione di residenza - e può essere da essi consultato, previo ulteriore consenso dell'assistito stesso.

L'accesso al FSE permette agli operatori del SSN e dei Servizi Sanitari Regionali, che hanno in cura l'assistito, di visualizzare tanto i dati sanitari più recenti, quanto l'intera storia clinica.

L'alimentazione dei dati del FSE, quindi, ha lo scopo di documentare la storia clinica dell'assistito, al fine di ottimizzare le procedure di cura. Il FSE si basa su tecnologie digitali che permettono di migliorare e semplificare le modalità di intervento sanitario.

Questa Azienda è impegnata nel processo di implementazione del FSE sulla base delle indicazioni regionali e nazionali. A tale riguardo si rinvia al Portale Salute del Cittadino della Regione Campania, disponibile al seguente indirizzo internet: sinfonia.regione.campania.it

2.10. ARTICOLO 12): CENSIMENTO DEI TRATTAMENTI

Questa Azienda evidenzia la necessità di avvalersi di un censimento dei trattamenti dei dati personali utile sia come strumento di lavoro e di disciplina della materia, sia come mezzo per implementare il contenuto del nuovo "Registro elettronico delle attività di trattamento" (vedasi il successivo articolo n. 25 del presente Regolamento).

3. DIRITTI DELL'INTERESSATO

3.1. ARTICOLO 13): CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

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

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

3.2. ARTICOLO 14): DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo 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 di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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 ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento, o il delegato, fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento, o il delegato, può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed organizzativo, il diritto di accesso, si fa rinvio alle vigenti diposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale e regionale nonché dal Garante per la privacy, con particolare riferimento all'ambito sanitario ed ospedaliero.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di "accesso documentale", di "accesso civico" e di "accesso generalizzato", come disciplinate dal Regolamento aziendale sul diritto di accesso, tempo per tempo vigente.

Nel dare evidenza del fatto che, presso questa Azienda, la competenza sulla materia de quo è affidata al Responsabile aziendale della Trasparenza e della Prevenzione della Corruzione si rinvia al contenuto delle schede informative pubblicate sul sito internet aziendale (www.ospedale.caserta.it), dedicate all'argomento e, in particolare alla pagina: www.ospedale.caserta.it/gdpr/gdpr.htm

3.3. ARTICOLO 15): DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di ottenere la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

3.4. ARTICOLO 16): DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del Regolamento Europeo n. 2016/679, in capo all'interessato è riconosciuto il diritto "all'oblio", che si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata.

Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di

cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del Regolamento UE).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

3.5. ARTICOLO 17): DIRITTO DI LIMITAZIONE AL TRATTAMENTO

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, è esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì anche se l'interessato chiede la rettifica dei dati.

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la limitazione è vietato a meno che ricorrano determinate circostanze (consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante).

Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di determinazioni ulteriori.

3.6. ARTICOLO 18): DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste specifiche condizioni per il suo esercizio; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati "forniti" dall'interessato (si veda il considerando 68 del Regolamento UE).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

3.7. ARTICOLO 19): DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del Regolamento Europeo n. 2016/679, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni.

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 sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

3.8. ARTICOLO 20): PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

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

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

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

4. SOGGETTI

4.1. ARTICOLO 21): TITOLARE DEL TRATTAMENTO

Il "Titolare" del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della privacy, è l'Azienda Ospedaliera di Caserta, nella persona del suo Direttore generale, in qualità di legale rappresentante dell'Azienda stessa, con sede in via F. Palasciano a Caserta.

Con deliberazione del Direttore Generale n. 125 del 2023 è stata effettuata la nomina delle seguenti figure:

a) Delegato del Titolare del Trattamento
b) Responsabile della Protezione dei Dati (DPO)
c) Referente Privacy

4.2. ARTICOLO 22): DELEGATO INTERNO ALLA GESTIONE DELLE ATTIVITA' DI TRATTAMENTO DEI DATI

Il D.lgs. 196/2003, come novellato dal recente D.lgs. 101/2018 di armonizzazione del Codice italiano della privacy alle novità del GDPR Europeo n. 2016/679, stabilisce, al nuovo articolo 2-quaterdecies, comma 1, che il Titolare può "prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la propria autorità".

L'Azienda Ospedaliera di Caserta, in qualità di Titolare del trattamento di dati personali (di seguito "Azienda" o "Titolare"), cioè quale soggetto che determina le finalità e i mezzi dei trattamenti dei dati effettuati nel proprio ambito, è tenuta a delineare al proprio interno un'adeguata ed efficace articolazione delle responsabilità al fine di assicurare il rispetto delle disposizioni vigenti in materia, e ciò sulla base del principio europeo di accountability, che prevede il coinvolgimento e la responsabilizzazione, ad ogni livello, delle strutture dell'azienda nel percorso di adeguamento ai precetti europei.

Ciò detto, si rende necessario attribuire le deleghe di cui si tratta ai dirigenti di questa Azienda che, per il ruolo ricoperto ed in virtù dei poteri di organizzazione e gestione già conferiti da questa stessa Azienda, risultano possedere i requisiti necessari per essere delegati

all'esercizio delle funzioni di gestione, coordinamento e controllo delle attività di trattamento dei dati personali svolte nell'ambito delle rispettive strutture nonché dei correlati adempimenti previsti dal GDPR.

Tenuto conto del grado di complessità che caratterizza questa Azienda Ospedaliera, che consta, al 31.12.2023, 1.788 dipendenti a tempo indeterminato, si reputa opportuno individuare i soggetti da "designare", ai sensi del D.lgs. 101/2018, a ricoprire le funzioni di "Responsabile interno del trattamento dei dati".
Detti soggetti, oggi definiti dal D.lgs. 101/2018 come "Delegati interni alla gestione delle attività di trattamento dei dati personali e degli adempimenti previsti dal Regolamento UE n. 2016/679" sono individuabili, in base al vigente Atto Aziendale, nelle seguenti, specifiche figure:

a) I Direttori delle UOC (unità operative complesse) e delle UOS (unità operative semplici) dell'area della Direzione Amministrativa;

b) I Direttori delle UOC, delle UOSD (unità operative semplici dipartimentali) e delle UOS dell'area della Direzione Sanitaria.

Per quanto riguarda, invece, la maggior parte dei lavoratori, già in servizio presso questa Azienda, le "istruzioni" sono pubblicate nella pagina web aziendale dedicata alla "Protezione dei Dati Personali" raggiungibile attraverso il seguente collegamento: www.ospedale.caserta.it/gdpr/gdpr.htm

4.3. ARTICOLO 23): RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

Nell'ambito della Azienda Ospedaliera di Caserta, sono inoltre individuati quali Responsabili "esterni" del trattamento dei dati personali, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con l'Azienda, trattino dati di cui è titolare l'Azienda medesima e qualora siano in possesso dei requisiti previsti dalla vigente normativa (esperienza, capacità ed affidabilità).

In ottemperanza all'articolo 28 del Regolamento Europeo 2016/679, i Responsabili esterni verranno nominati con la sottoscrizione di un apposito "Accordo per la nomina a Responsabile Esterno del trattamento dei dati personali", il cui modello aziendale è pubblicato sul sito web aziendale nell'apposita pagina web dedicata alla "Privacy Europea".

L' "accordo di nomina" sottoscritto da parte del Titolare del trattamento, ovvero dal delegato e controfirmato per accettazione da parte del Responsabile esterno: il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di 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.

5. SICUREZZA DEI DATI PERSONALI E MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

5.1. ARTICOLO 24): PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del Regolamento Europeo n. 2016/679 introduce il criterio sintetizzato dall'espressione inglese "data protection by default and by design", ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25, paragrafo 1 del Regolamento UE) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

5.2. ARTICOLO 25): REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO

Tutti le Aziende, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del Regolamento UE), devono tenere un registro delle operazioni di trattamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle dimensioni e della complessità che caratterizzano questa Azienda, non può che avere forma elettronica, e deve essere esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

Il Registro dei Trattamenti di questa Azienda è disponibile sul Sito Aziendale nella pagina "Protezione Dei Dati Personali" raggiungibile attraverso il seguente collegamento: www.ospedale.caserta.it/gdpr/gdpr.htm

5.3. ARTICOLO 26): PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" del trattamento (articolo 32, paragrafo 1 del Regolamento UE).

Per lo stesso motivo, secondo il Regolamento UE non potranno sussistere dopo il 25 maggio 2018 obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Si richiama l'attenzione anche sulla possibilità di utilizzare l'adesione a specifici codici di condotta o a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

5.4. ARTICOLO 27): NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

A partire dal 25 maggio 2018, tutti i titolari, e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi, dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza e "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del Regolamento UE); questa procedura va sotto il nome di "Data Breach".

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare.

Se la probabilità di tale rischio è elevata, si dovrà informare delle violazioni anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento.

Con deliberazione del Direttore Generale n. 522 del 29/07/2019 è stata effettuata la nomina del Comitato Data Breach a cui è stato delegato il compito di verificare l'analisi e la classificazione del Data Breach, identificandone la classe di rilevanza e di intraprendere le idonee azioni consequenziali.

5.5. ARTICOLO 28): CODICE DI COMPORTAMENTO DEI DIPENDENTI E COLLABORATORI DELL'AZIENDA

Si fa rinvio alle disposizioni di cui al Codice aziendale tempo per tempo vigente, che disciplina la materia di cui si tratta pubblicato sul sito web Aziendale con deliberazione del Direttore Generale n. 916 del 09/10/2023.

5.6. ARTICOLO 29): ENTRATA IN VIGORE E PUBBLICITA'

Il presente Regolamento entra in vigore dalla data di adozione con atto deliberativo del Direttore Generale.

Il Regolamento verrà pubblicato sul sito internet aziendale nell'apposita sezione dedicata ai Piani Aziendali e Regolamenti, disponibile a partire dalla pagina principale del sito al seguente collegamento: www.ospedale.caserta.it/regolamenticentri.htm

5.7. ARTICOLO 30): DISPOSIZIONE FINALE RELATIVA AI DOCUMENTI TECNICI CITATI NEL REGOLAMENTO: RINVIO AL SITO WEB AZIENDALE

Per la consultazione di tutti i modelli e documenti tecnici citati nel testo del presente Regolamento, si fa espresso ed integrale rinvio alla sezione dedicata alla "Protezione dei Dati Personali" contenuta nel sito web aziendale, all'interno della quale è pubblicata tutta la documentazione relativa alla materia in rilievo, disponibile al seguente collegamento: https://www.ospedale.caserta.it/gdpr/gdpr.htm

***