AZIENDA OSPEDALIERA
"SAN PIO" - BENEVENTO
di Rilievo Nazionale e di Alta Specializzazione
DEA di II Livello

Regolamento sulla protezione dei dati personali

INDICE

1. INTRODUZIONI GENERALI AL DOCUMENTO

La normativa Europea in merito alla protezione dei dati personali (Regolamento EU 2016/679 General Data Protection Regulation) è direttamente applicabile a tutti gli stati membri ed uno dei principi cardine esplicato è la responsabilizzazione di ciascun Titolare del Trattamento, i cui compiti verranno ripresi nei paragrafi successivi.
Al fine di soddisfare adeguatamente i requisiti prescritti ed evitare il rischio di trattamenti illeciti e le conseguenti sanzioni, ogni trattamento di dati personali effettuato dai Titolari o dai soggetti designati deve essere conforme alla normativa sopraindicata.

1.1 SCOPO DEL DOCUMENTO

Il presente documento definisce le regole generali al fine di disciplinare gli adempimenti normativi necessari in riferimento alle attività di trattamento dei dati personali effettuati dall'organizzazione e rimandando per i dettagli alle specifiche procedure, policy e linee guida. I contenuti descritti sono coerenti con le normative di riferimento in ambito privacy ed in particolare con il Regolamento Europeo sulla Protezione dei Dati (*GDPR - Regolamento EU 2016/679 "General Data Protection Regulation"*) e con il Codice in materia di Protezione dei Dati Personali (D.Lgs. 30 giugno 2003, n. 196), così come novellato dal D.Lgs. 10 agosto 2018, n. 101.

1.2 CAMPO DI APPLICAZIONE

Il presente documento si applica a tutte le strutture aziendali, ai dipendenti ed a tutti coloro che, a vario titolo, effettuano attività all'interno dell'AORN "San Pio".
Campo d'applicazione della procedura sono tutte quelle attività che rientrano nella definizione di trattamento di dati personali di cui alla normativa applicabile.
In particolare, ai sensi dell'art. 4 del GDPR, con l'espressione "trattamento di dati personali" s'intende "*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*", pertanto rientrano in tale definizione:

- la raccolta dei dati;
- la registrazione dei dati, ovvero il loro inserimento su supporti elettronici o in formato cartaceo;
- il processo di lavorazione che favorisca la fruibilità dei dati;
- la conservazione dei dati;
- l'adattamento o la modifica dei dati registrati in relazione a rettifiche o nuove acquisizioni;
- l'estrazione, ipotesi specifica che rientra nell'ipotesi più generale dell'elaborazione;
- la consultazione o l'uso;
- la comunicazione dei dati ad uno o più soggetti determinati, in qualunque forma;
- il raffronto o l'interconnessione, ovvero la messa in relazione di banche dati diverse e distinte fra loro al fine di compiere ulteriori processi di elaborazione, selezione, estrazione o raffronto;

- la limitazione;
- la cancellazione;
- la distruzione.

1.3 RIFERIMENTI

- Regolamento Europeo sulla Protezione dei Dati - (Regolamento EU 2016/679 “General Data Protection Regulation” – GDPR;
- D.Lgs. 30 Giugno 2003, n. 196, recante “Codice in materia di protezione dei dati personali”;
- D.Lgs. 10 agosto 2018, n. 101, rubricato “Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)”;
- Politiche, Policy e Linee Guida redatte in ambito Privacy il cui dettaglio è riportato nel paragrafo “Documentazione in ambito Privacy”.

1.4 DEFINIZIONI

Di seguito sono riportate le definizioni utilizzate nel documento:

Termine	Descrizione
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
Privacy By Design	Tecniche di protezione dei dati personali sia al momento della determinazione dei mezzi di trattamento sia all’atto di trattamento stesso
Privacy By Default	Tecniche atte a garantire che i dati trattati sono necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine
DPO	Data Protection Officer (Responsabile della Protezione dei Dati RPD)
Data Breach	Violazione dei Dati Personali

Tabella 1 – Definizioni

2. ATTORI DEL TRATTAMENTO

2.1 TITOLARE DEL TRATTAMENTO

Il Titolare del trattamento dei dati personali è, ai sensi dell'art. 4 del GDPR, "*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*". Alla luce di tale definizione, il Titolare del trattamento, per ciascuna delle attività di trattamento effettuate nell'ambito della struttura aziendale e mappate nel registro delle attività di trattamento, è l'A.O.R.N. "San Pio" (di seguito riportato come Titolare del Trattamento).

Il Titolare, quindi, è la struttura nel suo complesso ed agisce per mezzo del Direttore Generale, al quale i relativi poteri in materia di protezione di dati personali sono stati *pro tempore* attribuiti.

Al Titolare competono le scelte di fondo in merito alla raccolta e all'utilizzazione dei dati personali ed in particolare riguardo alla determinazione delle finalità e modalità del trattamento, ivi compreso il profilo della sicurezza.

L'art. 24 del GDPR stabilisce la responsabilità generale del Titolare per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. Il Titolare deve garantire la conformità e l'attuazione delle attività di trattamento secondo i principi indicati nel Regolamento GDPR. Tali misure di trattamento devono tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche. Inoltre, al fine di allineare con il Regolamento le azioni messe in atto, il Titolare deve adottare politiche interne e attuare misure che soddisfino requisiti previsti dal GDPR dalla fase di previsione delle garanzie a tutela dei diritti degli interessati (*privacy by design*) a quella di adozione di misure tecnico-organizzative di applicazione dei principi di protezione (*privacy by default*).

Il Regolamento prevede il potere di delega del Titolare nei confronti di alcuni soggetti, appositamente individuati, quali *Owner* del Trattamento, nonché le figure di Amministratore di Sistema, Referente Privacy, DPO, Delegati e Incaricati del Trattamento.

Il Titolare nomina, altresì, i Responsabili "esterni" del trattamento, ossia i soggetti esterni alla struttura aziendale che, nell'esecuzione di un servizio a favore del Titolare, trattano, per conto di quest'ultimo, dati personali. Il Titolare ha la responsabilità di individuare, al riguardo, soggetti che presentino garanzie sufficienti per mettere in atto le prescritte misure tecniche e organizzative adeguate.

In relazione alle attività di trattamento effettuate nell'ambito della propria struttura aziendale, il Titolare è tenuto a valutare, alla luce degli artt. 37 e ss. del Regolamento Europeo, la necessità o, quantomeno, l'opportunità di procedere alla nomina di un Responsabile della Protezione dei Dati (DPO). Laddove la nomina fosse ritenuta necessaria o opportuna, è compito del Titolare individuare e designare il DPO in funzione delle qualità professionali - e in particolare della conoscenza specialistica della normativa e della prassi in materia di protezione dei dati – dimostrate dallo stesso. Il DPO può essere individuato

nella persona di un soggetto interno all'organizzazione aziendale o di un soggetto esterno sulla base di apposito provvedimento di nomina, motivandone la scelta.

2.2 INTERESSATO

L'interessato è "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", destinataria della tutela predisposta dal GDPR in relazione alle operazioni di trattamento dei dati che la riguardano.

All'interessato vengono accordate particolari tutele diritti dettagliati nel Capo III del Regolamento UE 679/2016.

2.3 DATA PROTECTION OFFICER

Il DPO (responsabile della protezione dei dati) risulta essere un supervisore indipendente a garanzia dell'applicazione delle disposizioni in materia di trattamento dei dati e punto di riferimento nella realtà organizzativa e per l'Authority garante della Privacy. L'art. 37, paragrafo 1 del Regolamento GDPR sancisce le modalità di designazione del DPO in diversi ambiti:

- in ambito *pubblico*, la nomina del DPO è sempre obbligatoria, fatta eccezione per l'autorità giurisdizionali in esercizio delle loro funzioni;
- in ambito *privato*, la nomina del DPO è obbligatoria quando il Titolare effettua trattamenti regolari e sistematici, su larga scala, o inerenti a dati relativi a condanne penali o reati (come definito dall'art. 10 del Regolamento).

L'articolo 39 del Regolamento sancisce i compiti assegnati al DPO, tra quali:

- informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
- sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

- cooperare con l'autorità di controllo;
- fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Per consentirgli di svolgere appieno il compito affidatogli, il Titolare dovrà fornire al DPO la struttura e le risorse necessarie, permettergli l'accesso ai dati ed alle operazioni del trattamento, assicurarsi che eventuali altri compiti gli consentano, in ordine di tempo e di possibilità, di adempiere alla responsabilità alla quale è chiamato e non interferiscano con essa.

2.4 DELEGATO/RESPONSABILE INTERNO DEL TRATTAMENTO

All'interno dell'Azienda Ospedaliera, in ragione della sua articolazione, il Titolare del Trattamento provvede, mediante atto deliberativo, alla nomina dei Delegati/Responsabili interni del trattamento nelle persone dei Direttori/Responsabili di Unità Operativa, dei Presidenti/Coordinatori degli Organismi Collegiali, chiamati a svolgere, per conto del titolare, funzioni di gestione, coordinamento e controllo delle attività di trattamento svolte nell'ambito della rispettiva sfera di competenza, al fine di ottemperare agli adempimenti previsti dal GDPR 2016/679 ed a quelli fissati a livello aziendale con Linee Guida, Procedure, Piani di Sicurezza e Data Protection Impact Assessment (DPIA).
Spetta ai Delegati procedere alla designazione dei propri collaboratori come incaricati del trattamento, in ragione dello svolgimento materiale delle operazioni sui dati personali.
Il Titolare del Trattamento individua tra i Delegati il Referente Aziendale Privacy, chiamato in ragione delle specifiche competenze e conoscenze di natura giuridico-amministrativa a coadiuvarlo nelle attività di programmazione, coordinamento, attuazione e controllo degli interventi in materia di trattamento dei dati.

2.5 AUTORIZZATO AL TRATTAMENTO

Ai fini del trattamento dei Dati Personali è possibile definire, all'interno della struttura aziendale, i soggetti interni da autorizzare a compiere operazioni di trattamento di dati personali contenuti in banche dati elettroniche o cartacee.
Tali soggetti rivestono il ruolo di "*Incaricati al Trattamento*" per conto del Titolare del Trattamento o dei suoi Delegati. Quest'ultimo/ultimi provvede/ono alla definizione di un opportuno obbligo legale di riservatezza da sottoporre ai soggetti Autorizzati al Trattamento al fine di proteggere le informazioni trattate.

L'attuale orientamento dell'Autorità Garante conferma la compatibilità di tale figura con quanto definito dal GDPR, nonostante la normativa europea non preveda formalmente tale figura/ruolo, parlando semplicemente di soggetti autorizzati al trattamento.
L' Autorizzato al Trattamento effettua operativamente le attività di trattamento dei dati personali attinenti alla propria attività lavorativa. Pertanto, ogni dipendente o collaboratore del Titolare che, per le mansioni assegnate, debba trattare dati personali, è autorizzato nell'ambito dei compiti che gli sono affidati ad accedere alle banche dati necessarie per lo svolgimento di tali mansioni.
L'Autorizzato al Trattamento è indentificato nell'ambito della propria struttura di afferenza e deve attenersi strettamente alle istruzioni impartite dal Titolare o dal suo Delegato in relazione alle specifiche finalità e modalità di utilizzo dei dati a cui lo stesso abbia accesso.

2.6 RESPONSABILI "ESTERNI" DEL TRATTAMENTO

Il Titolare, per effetto della conclusione ed esecuzione di specifici contratti, può demandare alcuni servizi che prevedono il trattamento di dati personali a soggetti esterni. In tali casi, tali soggetti esterni sono nominati Responsabili "esterni" del trattamento, intesi, ai sensi dell'art. 4 del GDPR, come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".
Il Responsabile "esterno" del trattamento deve essere nominato con apposito contratto o atto giuridico.
Secondo la normativa vigente, il Responsabile "esterno" è tenuto a presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato.
Il Responsabile "esterno", inoltre, non può ricorrere ad un altro Responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare. In caso di autorizzazione, il Responsabile esterno è tenuto a nominare il sub Responsabile del trattamento e ad imporre allo stesso, tramite contratto o atto giuridico, i medesimi doveri in materia di protezione dei dati personali che il Titolare gli ha prescritto.
Il contratto o l'atto giuridico tra il Titolare ed il Responsabile "esterno" del trattamento deve prevedere la materia disciplinata, la durata del trattamento, la natura e le finalità del trattamento nonché il tipo di dati personali e le categorie di interessati a cui gli stessi dati si riferiscono.

2.7 CONTITOLARI

Ai sensi dell'art. 26 del GDPR, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. In tali circostanze, il GDPR richiede che tali soggetti determinino in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali derivanti dalla normativa applicabile, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive

funzioni di comunicazione delle informative di cui agli artt. 13 e 14 del GDPR, salvo che le rispettive responsabilità siano già determinate per legge.
L'accordo di riparto costituisce un obbligo per i contitolari, definendo i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
La contitolarità va ravvisata nella decisione condivisa delle finalità e dei conseguenti mezzi di trattamento tra titolati distinti.

2.8 AMMINISTRATORE DI SISTEMA

L'Amministratore di sistema, figura professionale non prevista dal GDPR, ma originariamente contemplata nel D.Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) e recuperata dal Garante nel Provvedimento del 27.11.2008, modificato dal Provvedimento del 26.06.2009, è il "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l´utilizzazione".
Ha specifiche competenze tecniche, che gli consentono di gestire i sistemi informatici e telematici e le banche dati, adoperandosi per la loro protezione e sicurezza.

3. DISPOSIZIONI GENERALI IN MATERIA DI DATI PERSONALI

In merito al trattamento dei dati personali, sono presenti una serie di disposizioni generali appositamente regolamentate dal GDPR, meglio descritte di seguito.

3.1. PRINCIPI GENERALI DEL TRATTAMENTO

Il trattamento dei dati personali deve essere effettuato nel rispetto delle norme di legge, delle disposizioni di cui alla presente Politica, nonché delle istruzioni di volta in volta impartite dal Titolare o, se del caso, dal DPO.
Le funzioni coinvolte nelle attività di raccolta, conservazione ed utilizzo di dati personali operano nel rispetto del sistema normativo interno e del sistema di poteri e responsabilità, nonché in piena conformità con tutte le leggi ed i regolamenti vigenti.

In virtù di quanto detto, i dati personali oggetto di trattamento, ai sensi dell'art. 5 del GDPR, sono:

- trattati in modo lecito, corretto e trasparente nei confronti dell'Interessato (principio di "liceità", "correttezza" e "trasparenza");
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (principio di "limitazione della finalità");
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di "minimizzazione dei dati");
- esatti e, se necessario, aggiornati; devono pertanto 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");
- 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 (principio di "limitazione della conservazione");
- 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 accidentale (principio di "integrità e riservatezza");

Il Titolare, in virtù del principio di "responsabilizzazione" o "accountability", è competente in materia di trattamento dei dati e risponde della corretta applicazione della normativa.
Ogni trattamento dei dati personali deve svolgersi nel rispetto dei diritti e delle libertà fondamentali e della dignità dell'Interessato, con particolare riferimento alla riservatezza, all'identità personale ed al diritto alla protezione dei dati personali, in coerenza con i principi normativi previsti per il loro esercizio.
Laddove necessario, il Titolare collabora con l'Autorità garante per la protezione dei dati personali, anche con riferimento specifico ad eventuali casi di notifica per violazioni ovvero in relazione alla valutazione preliminare per il trattamento di taluni dati, allo scopo di garantire il pieno rispetto dei diritti dell'Interessato e di fornire tutte le informazioni necessarie.

Ogni attività di trattamento dei dati personali deve essere avviata in maniera trasparente, rendendo all'Interessato idonea informativa in merito alle finalità, tempistiche, comunicazione e diffusione del Trattamento stesso e acquisendone, in tutti i casi previsti dalla legge, il consenso in maniera formale, scritta e libera.

Si precisa inoltre che:

- il trattamento deve essere effettuato dagli Incaricati del Trattamento per gli scopi determinati nelle rispettive mansioni di lavoro;
- i dati personali raccolti e/o trattati in violazione dei principi enunciati nei precedenti punti non possono essere ulteriormente oggetto di trattamento;
- i dati personali oggetto del trattamento devono essere conservati per un periodo non eccedente a quello necessario per le finalità per cui gli stessi sono stati raccolti e trattati;
- in nessun caso i dati personali possono essere utilizzati per scopi illeciti o incompatibili con i fini per i quali sono stati raccolti e registrati.

3.2. TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI PERSONALI

L'articolo 9 del GDPR definisce dati personali appartenenti a categorie particolari quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, quelli biometrici volti ad identificare in modo univoco una persona fisica e quelli relativi alla salute, alla vita o all'orientamento sessuale della persona.
Il trattamento di tali dati personali deve essere effettuato tenendo conto di ulteriori cautele e, in particolare, per quanto in questa sede rileva:

(i) con il consenso esplicito dell'Interessato;
(ii) se necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'Interessato in materia di diritto del lavoro, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri;
(iii) se il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
(iv) se il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria.

In ogni caso, gli Incaricati del Trattamento devono assicurarsi che i dati personali di natura particolare siano oggetto unicamente di trattamenti strettamente necessari per il perseguimento delle finalità per le quali sono raccolti e siano destinati ai soli soggetti autorizzati.

4. MODALITÀ DI GESTIONE DEI DATI PERSONALI

In merito alla protezione dei dati personali, in linea con quanto definito dal GDPR e dalle normative Nazionali in materia di protezione dei dati, sono attuati una serie di macro-processi descritti di seguito.

4.1. REGISTRO DEI TRATTAMENTI

Il GDPR impone ai Titolari del Trattamento, con limitate eccezioni, di tenere un Registro delle attività di trattamento svolte sotto la propria responsabilità (il "Registro").
L'articolo 30 del GDPR recita infatti *"Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità".*
Ai sensi dello stesso articolo 30 del GDPR, il Registro deve contenere, almeno, le seguenti informazioni:

- il nome ed i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del Trattamento, nonché del DPO e del rappresentante del Titolare;
- le finalità del trattamento;
- una descrizione delle categorie di Interessati e delle categorie di dati personali trattati;
- le categorie di terzi/destinatari a cui i dati personali sono stati o saranno comunicati;
- eventuali trasferimenti di dati personali verso un paese terzo o organizzazioni internazionali;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati personali;
- una descrizione generale delle misure di sicurezza tecniche ed organizzative adottate.

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e del responsabile della protezione dei dati;
- i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale;
- le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
- una descrizione generale delle misure di sicurezza tecniche e organizzative

I registri sono tenuti in forma scritta, anche in formato elettronico e su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento, mettono il registro a disposizione dell'autorità di controllo.
In conformità a quanto previsto dal GDPR, nell'AORN è stato predisposto un apposito registro, nel quale sono dettagliate, come da norma, tutte le informazioni relative alle attività di trattamento.

4.2. DATA PROTECTION IMPACT ASSESSMENT

Il GDPR ha introdotto l'obbligo per il Titolare del trattamento di eseguire, al ricorrere di determinate condizioni, una valutazione d'impatto sulla protezione dei dati (*DPIA - Data Protection Impact Assessment*).
Ai sensi dell'art. 35 del GDPR, è previsto in capo al Titolare l'onere di procedere ad una valutazione d'impatto sulla protezione dei dati personali *"quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*
Nello specifico, lo svolgimento della DPIA è in particolare richiesto nei seguenti casi:

- valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basato su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- trattamento su larga scala di Dati particolari o Dati giudiziari;
- sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione d'impatto sulla protezione dei dati personali risponde al principio di *accountability*, in quanto permette al Titolare di valutare e dimostrare di aver adottato le misure idonee a garantire il rispetto delle prescrizioni dettate dal GDPR relativamente alla gestione dei rischi per i diritti e le libertà delle persone fisiche interessate. In particolare, la DPIA ha lo scopo di valutare, in ottica prudenziale, la probabilità e la gravità dei rischi connessi a un'attività di trattamento per i diritti e le libertà degli interessati, con lo scopo di individuare le misure di sicurezza, sia tecniche sia organizzative, necessarie a garantire un livello di sicurezza adeguato al rischio identificato, assicurando al contempo la protezione dei dati personali trattati.
Per tali ragioni, la valutazione deve essere effettuata prima di procedere al trattamento.
Il GDPR riconosce tuttavia la possibilità per il Titolare di svolgere una singola valutazione al fine di esaminare un insieme di trattamenti simili che presentato rischi elevati analoghi.
L'adempimento dell'obbligo di DPIA è in carico al Titolare, nello specifico, la valutazione circa la necessità o quantomeno l'opportunità di provvedere o meno allo svolgimento di una DPIA deve essere condotta, ogniqualvolta sia implementato un nuovo servizio, sia impiegata una nuova tecnologia nell'ambito di attività di trattamento già effettuate, ovvero siano effettuate nuove attività di trattamento.
Laddove risultasse necessario o quantomeno opportuno procedere con la DPIA, tale valutazione deve contenere:

- una descrizione sistematica dei trattamenti previsti e delle rispettive finalità, nonché, ove applicabile, l'eventuale interesse legittimo del Titolare;
- una valutazione sulla necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati;

- le misure previste per affrontare tali rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento.

Qualora dall'esito del processo di DPIA risultasse che il trattamento, nonostante le contromisure di sicurezza identificate, presenti un rischio alto e/o comunque rilevante per i diritti e le libertà delle persone fisiche, il Titolare del Trattamento è tenuto a consultare l'Autorità di controllo che provvederà a fornire un proprio parere in merito.
L'AORN, con Delibera n. 71 del 05.02.2020, si è dotata di un'apposita linea guida per la conduzione delle attività di Data Protection Impact Assessment, al fine di garantire l'adozione di un approccio rigoroso basato sul rischio ed in linea con i requisiti del Regolamento Europeo.

4.3. INFORMATIVA AL TRATTAMENTO DEI DATI PERSONALI

Il Titolare e/o i Delegati e/o gli Incaricati e/o i Responsabili esterni, prima di procedere a qualsiasi attività di trattamento, sono tenuti obbligatoriamente a fornire apposita informativa agli Interessati in merito ai loro diritti e alle caratteristiche del trattamento, in particolare per ciò che concerne le finalità e le modalità del trattamento dei dati stessi, in accordo a quanto previsto dalle disposizioni di legge in materia.
L'obbligo di fornire l'informativa all'Interessato risponde alla necessità di riconoscere a quest'ultimo il diritto di avere conoscenza dell'ambito di circolazione dei propri dati, al fine di poter procedere ad un consapevole esercizio dei poteri allo stesso riconosciuti (ad es. esprimere o negare il consenso, opporsi al trattamento, etc.).
Sul portale dell'Azienda Ospedaliera, nell'apposita sezione *Privacy*, sono disponibili *on line* tutti i documenti relativi.

4.4. RACCOLTA, UTILIZZO E CONSERVAZIONE DEI DATI

Il Titolare e/o i Delegati e/o gli Incaricati e/o i Responsabili esterni, prima di procedere alla raccolta dei dati presso l'interessato, forniscono allo stesso le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento e del suo rappresentante;
- i dati di contatto del responsabile della protezione dei dati (DPO);
- le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- i legittimi interessi perseguiti dal titolare del trattamento o da terzi, qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f);
- gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;

- l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza.

Per quanto attiene ai termini per la conservazione dei dati, ci si riporta ai seguenti principi fissati dal GDPR:

- l'art. 39 del GDPR, il quale illustra *"l'obbligo di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica".*
- l'art. 65 del GDPR, secondo il quale *"Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati personali qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria"*
- l'art. 5, paragrafo 1, lettera e), che stabilisce che i dati personali sono *"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, 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»)".*
- l'art. 13, paragrafo 2, in virtù del quale *"nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo".*

Pertanto, deve essere garantita l'adozione di misure tecnico - organizzative necessarie affinché i dati personali siano conservati per un periodo di tempo adeguato alle finalità e alle richieste dell'Interessato. A tal file, nel momento in cui i dati personali sono ottenuti, il Titolare e/o i Delegati e/o gli Incaricati e/o i Responsabili esterni, per garantire un trattamento corretto e trasparente, forniscono all'interessato le seguenti ulteriori informazioni:

- il periodo di conservazione dei dati personali o, qualora non sia possibile, i criteri utilizzati per determinare tale periodo;

- l'esistenza del diritto dell'interessato di chiedere l'accesso ai dati personali, la rettifica, la cancellazione, la limitazione del trattamento o di opporsi al trattamento stesso, oltre del diritto alla portabilità dei dati;
- l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento avvenuto sulla scorta del consenso prestato, qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a);
- il diritto di proporre reclamo a un'autorità di controllo;
- la riconducibilità della comunicazione di dati personali ad un obbligo legale o contrattuale oppure alla necessità di fornirli per la conclusione di un contratto, e le possibili conseguenze del trattamento e/o della mancata comunicazione di tali dati;
- l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, le informazioni significative sulla logica utilizzata.

5. DIRITTI DELL'INTERESSATO

Il Titolare del Trattamento, attraverso i Delegati e/o gli Incaricati e/o i Responsabili esterni, garantisce l'esercizio dei diritti dell'interessato, come previsto dal GDPR, attraverso un processo di gestione delle richieste effettuate dagli interessati, con riferimento ai seguenti diritti:

- **ricevere un'informativa** contenente tutti gli elementi indicati negli articoli 13 e 14, GDPR sia nel caso in cui i dati siano forniti direttamente dall'Interessato stesso al Titolare che nel caso in cui questi siano ottenuti da terzi (artt. 13 e 14, GDPR);
- **revocare**, in qualsiasi momento, il **consenso**, senza alcun condizionamento e con la stessa facilità con cui è stato prestato (art. 7, GDPR);
- **garantire l'accesso**, consistente nella facoltà di ottenere dal Titolare la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso a tali dati – compresa una copia degli stessi – ed alle informazioni elencate all'articolo 15, GDPR (art. 15, GDPR);
- **operare una rettifica**, consistente nella possibilità di ottenere dal Titolare la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e/o l'integrazione dei dati personali incompleti (art. 16, GDPR);
- **chiedere la cancellazione** (c.d. **diritto all'oblio**), consistente nella facoltà di ottenere dal Titolare la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo nel rispetto delle condizioni del GDPR (art. 17, GDPR);
- **limitare il trattamento**, consistente nella possibilità di ottenere dal Titolare la limitazione (temporanea) del trattamento al ricorrere di una delle ipotesi elencate dall'articolo 18, GDPR e salve le deroghe ivi previste (art. 18, GDPR);
- **ottenere la comunicazione**, da parte del Titolare ai destinatari, di eventuali rettifiche, cancellazioni o limitazioni del trattamento, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato per il titolare stesso. Inoltre, l'interessato ha diritto di ottenere la comunicazione di tali destinatari (art. 19, GDPR)
- **chiedere la portabilità dei dati**, consistente nella facoltà – nei soli casi in cui il trattamento si basa sul consenso o su un contratto ed è effettuato con mezzi automatizzati – di ricevere dal Titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti dall'Interessato stesso. Inoltre, qualora tecnicamente possibile, il diritto alla portabilità dei dati consente di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro (art. 20, GDPR);
- **fare opposizione**, consistente nel diritto di opporsi, alle condizioni e nel rispetto dei limiti previsti dal GDPR, al trattamento dei dati personali che lo riguardano qualora il trattamento degli stessi fosse: (i) necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri; (ii) fondato sull'interesse legittimo del titolare; (iii) finalizzato ad attività di marketing diretto svolte sulla base del legittimo interesse del Titolare; (iv) finalizzato alla ricerca scientifica o storica o con fini statistici (art. 21, GDPR);

- **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, salvo che la decisione sia necessaria per la conclusione o l'esecuzione di un contratto tra l'Interessato e il Titolare; sia autorizzata dal diritto dell'Unione Europea e/o dalla legge nazionale cui è sottoposto il Titolare; si basi sul consenso esplicito dell'Interessato (art. 22, GDPR).

In ogni caso, l'articolo 12 del GDPR, prevede che tutte le informazioni ed i riscontri debbano essere forniti all'interessato con le seguenti modalità:

- in una forma concisa, trasparente, intelligibile e con un linguaggio semplice e chiaro;
- per iscritto, o con mezzi elettronici, se la richiesta è stata effettuata con mezzi elettronici, essendo consentita la risposta orale solo su domanda espressa dall'interessato;
- senza ingiustificato ritardo e, al più tardi, entro un mese dal ricevimento della richiesta, salva la possibilità di prorogare tale termine di due mesi nei particolari casi previsti e fermo restando l'obbligo di informare comunque l'interessato del ritardo e dei motivi dello stesso ritardo, notiziandolo, comunque, della possibilità di proporre reclamo ad un'autorità di controllo e ricorso giurisdizionale;
- gratuitamente. Può essere addebitato un contributo ragionevole, o negata la soddisfazione della richiesta, solo nel caso di richieste manifestamente infondate o eccessive, anche per la loro ripetitività;
- dopo aver verificato l'identità dell'interessato, eventualmente anche domandando informazioni aggiuntive a quelle già raccolte.

6. PRINCIPI DI PRIVACY BY DESIGN E PRIVACY BY DEFAULT

L'articolo 25 del GDPR pone l'obbligo al Titolare del Trattamento di mettere in atto le seguenti misure tecniche ed organizzative adeguate a:

- proteggere i dati personali sia al momento della determinazione dei mezzi di trattamento sia all'atto del trattamento stesso (principio di "Privacy by Design");
- garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari al perseguimento delle specifiche finalità per cui sono raccolti e per il periodo strettamente necessario a tale fine (principio di "Privacy by Default").

I principi trasversali di Privacy by Design and Privacy by Default hanno l'obiettivo di definire le logiche di protezione dei dati personali, attraverso l'individuazione dei potenziali rischi di non conformità in materia di privacy e delle conseguenti misure tecniche-organizzative per la riduzione degli stessi sin dalla fase di progettazione e lungo tutto il ciclo di vita del trattamento dei dati.

6.1. PRIVACY BY DESIGN

La Privacy by Design trova fondamento nell'obbligo, in capo al Titolare, di configurare il trattamento, prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti previsti dal GDPR a tutela dei diritti degli interessati. Il titolare dovrà tenere conto del contesto complessivo ove il trasferimento dei dati si colloca e dei rischi per i diritti e le libertà dei soggetti interessati al trattamento.

6.2. PRIVACY BY DEFAULT

La Privacy by Default trova fondamento nell'obbligo, in capo al Titolare/ Delegato al Trattamento, di adottare misure tecniche-organizzative adeguate a garantire l'applicazione dei principi di protezione dei dati come impostazione di default. Tale attività ha l'obiettivo di definire le azioni da intraprendere, al fine di assicurare che vengano trattati solo i dati personali necessari al perseguimento delle specifiche finalità del trattamento.

7. IL DATA BREACH

Il GDPR definisce Data Breach "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".

Eventi di Data Breach possono riguardare sia la diffusione di dati relativi a un singolo individuo, che situazioni più critiche di furto o perdita di intere basi dati, quali, a titolo esemplificativo, l'anagrafica dei clienti del Titolare, o le informazioni relative ai dipendenti.

Il Regolamento prevede che, nel caso in cui una organizzazione rilevi una violazione dei Dati personali trattati (c.d. *Data Breach*), la stessa:

- sia tenuta a informare l'Autorità di controllo (Garante per la Protezione dei Dati Personali) entro e non oltre le 72 ore successive all'avvenuta conoscenza della violazione – a meno che sia del tutto improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati
- nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, debba informare senza ritardo anche gli Interessati stessi.

Al fine di adempiere alle indicazioni del Regolamento, è, altresì, importante che tutti coloro che nell'ambito della propria attività quotidiana trattano dati personali partecipino attivamente a tale processo, segnalando tempestivamente ogni caso di violazione di cui siano venuti a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione.

Al fine di definire le regole di riferimento finalizzate ad assicurare il rispetto di leggi, regolamenti o normative di riferimento è stata predisposta una specifica procedura *Procedura per la Gestione del Data Breach,* di cui alla Delibera n. 71 del 05.02.2020.

8. IL SISTEMA SANZIONATORIO

La riforma globale del contesto normativo sulla protezione dei dati personali introdotta dal GDPR prevede, tra i propri pilastri fondamentali, un rafforzamento dei poteri destinati a far rispettare le disposizioni previste in materia.

Il Titolare del Trattamento deve garantire l'efficace tutela dei dati personali delle persone fisiche. Allo stesso tempo, le Autorità di controllo, e tra queste, per quanto maggiormente rilevante ai fini della Procedura, l'Autorità Garante, sono dotate dei poteri necessari per garantire che i principi del GDPR e i diritti delle persone interessate siano rispettati conformemente al dettato e alla ratio del Regolamento Europeo.

Nello specifico, sono previste sanzioni a carico di chi dovesse violare il dettato normativo e i diritti e le libertà degli Interessati.

Alla luce di quanto sopra, tutti gli operatori aziendali sono tenuti a cooperare con il Titolare, affinché sia garantito il rispetto delle disposizioni del presente Regolamento e dei diritti e libertà riconosciuti all'Interessato alla luce dell'innovato contesto normativo.

A tal fine, a ciascuna funzione aziendale, ed in particolare, a ciascun Delegato e/o Incaricato e/o Responsabile esterno è richiesto di rispettare pedissequamente e di porre in essere quanto previsto all'interno del presente documento e in tutte le procedure ad esso correlate.

9. NORMA DI RINVIO

Per tutto quanto non espressamente previsto nel presente Regolamento, si rinvia alle vigenti disposizioni normative in materia ed alle Politiche, Linee Guida, Procedure e DPIA già adottate dall'AORN San Pio con le Delibere n. 71 del 05.02.2020, n. 505 del 09.09.2021 e n. 599 del 15.11.2021.