Regolamento per la protezione dei dati personali presso l'Azienda Ospedaliero – Universitaria Ospedali Riuniti di Ancona

Distribuita elettronicamente nella Sezione "Certificazione e Qualità" del portale intranet e conservata in formato cartaceo presso Ufficio del Responsabile per la Protezione dei Dati Personali

INDICE

1. OGGETTO ..... ……3
2. SCOPO E CAMPO DI APPLICAZIONE 3
3. RIFERIMENTI NORMATIVI 3
4. ORGANIZZAZIONE AZIENDALE IN MATERIA DI TRATTAMENTO DATI PERSONALI.....4
5. PIANO OPERATIVO DI DISTRIBUZIONE DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATIPERSONALI.....8
6. FUNZIONI ATTRIBUITE IN MATERIA DI TRATTAMENTO DI DATI PERSONALI E CONSEGUENTI ADEMPIMENTI……9

Realizzata da: Dott.ssa Marianna Catalini	**Verifica** (RSGQI) Dr. Roberto Papa	**Approvazione** Direttore Generale Dott. Michele Caporossi Direttore Amministrativo Dott. Antonello Maraldo Direttore Sanitario Dr. Arturo Pasqualucci

Rev.	Data	Natura della revisione	Pag.
00	xx/06/2022	Emissione (con determina)	Tutte
01			

1. OGGETTO

L'obiettivo del presente Regolamento è quello di individuare e formalizzare per ciascuna attività prescritta dal Regolamento UE 2016/679, dal D.lgs. 196/2003 e s.m.i., dai provvedimenti dell'Autorità Garante per la protezione dei dati personali, le funzioni a ciascuno attribuite nell'ambito dell'assetto aziendale.
Ciascuno nel proprio ruolo e nello svolgimento delle proprie funzioni è tenuto a concorrere, a vario titolo, all'attuazione delle disposizioni di cui alla richiamata normativa.

2. SCOPO E CAMPO DI APPLICAZIONE

In particolare la complessità della gestione del trattamento dei dati personali in questa Azienda richiede la responsabilizzazione di ogni struttura aziendale e delle figure specificamente individuate per consentire al Titolare del trattamento dati l'effettivo raggiungimento delle finalità previste dalla normativa sopra citata.
Ciò richiede il coinvolgimento di tutte le strutture aziendali in conformità a quanto specificamente previsto dalle disposizioni contenute nella normativa di riferimento, in considerazione sia della pluralità delle attività di trattamento effettuate in Azienda sia della trasversalità delle azioni da attuarsi con riferimento ai diversi ambiti di trattamento dati.

3. RIFERIMENTI NORMATIVI

- 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.
- D. Lgs. 30 giugno 2003 n. 196 (Codice in materia di protezione dei dati personali) così come novellato dal D.Lgs. 10 agosto 2018 n. 101 e s.m.i.
- Manuale RPD: "Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e para pubblici per il rispetto del Regolamento Generale sulla protezione dei dati dell'UnioneEuropea", approvato dalla Commissione luglio 2019.

4. ORGANIZZAZIONE AZIENDALE IN MATERIA DI TRATTAMENTO DATI PERSONALI

L'organizzazione aziendale comprende tutte le strutture che nel compimento delle attività loro assegnate effettuano necessariamente trattamenti di dati personali.

Il Titolare del trattamento di dati personali è l'Azienda Ospedaliero Universitaria Ospedali Riuniti nella persona del legale rappresentante pro tempore.

Il Titolare è colui che stabilisce le finalità e i mezzi di trattamento dei dati personali sulla base anche delle specifiche disposizioni di legge che regolamentano alcune tipologie di trattamento di dati.

Il Titolare, pertanto, è tenuto a garantire la legittimità del trattamento e la riservatezza, disponibilità ed integrità dei dati personali trattati mettendo in essere misure tecniche ed organizzative adeguate sulla base della propria organizzazione e degli strumenti a disposizione allo stato dell'arte.

In particolare il Titolare del trattamento di dati personali può delegare e designare specifici soggetti per attribuire aree di competenza in materia di trattamento dati personali che tengano conto degli strumenti messi a disposizione dal Titolare medesimo.

Il Titolare del trattamento dati personali è sempre tenuto a vigilare sulla corretta attuazione delle deleghe e delle designazioni effettuate.

Il Titolare del trattamento ricorrendo i presupposti di cui all'art. 37 deve designare il DPO o RPD (*data protection officer* o responsabile protezione dati).

Il Titolare del trattamento dati personali, ai sensi dell'art. 2 quaterdecies, comma 1, D.lgs. 196/2003 e ss.mm.ii., può sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, assegnare specifici compiti e funzioni connessi al trattamento di dati personali ai soggetti che operano sotto la sua autorità.

Con riferimento alla materia della protezione dei dati personali in particolare sono attribuite specifiche funzioni ad alcune strutture aziendali o figure coinvolte direttamente nella realizzazione del sistema di protezione dei dati personali.

In particolare sono coinvolte le strutture nelle quali opera il RUP come definito dall'art. 30 del D.Lgs. n. 50/2016.

<u>SO Sistemi Informativi Aziendali (SO SIA)</u>

- Offre supporto tecnico al responsabile aziendale della privacy e all'ufficio del DPO;
- Definisce le regole del corretto uso dei sistemi informativi e delle apparecchiature informatiche nel rispetto della protezione dei dati personali;
- Definisce ed implementa le policy di sicurezza informatica in un'ottica di miglioramento continuo sulla base dell'evoluzione tecnologica e sulla base della normativa in materia di sicurezza informatica;
- Gestione affidamenti sevizi e forniture sotto soglia per attività che potrebbero comportare trattamenti di dati personali.

SOS Innovazione e ICT

- Assicura il corretto funzionamento ad aggiornamento degli applicativi e dei dispositivi in ambito sanitario;
- Progetta e cura l'implementazione del sistema informativo clinico sanitario;
- Valuta l'implementazione di soluzioni Blockchain, Big Data Analytics e Artificial Intelligence rivolte all'Healthcare;
- Supporta le analisi inerenti i processi standard IEC ISO 80001:2010;
- Partecipa al processo HTA aziendali e regionali in merito alle soluzioni informatiche e di telecomunicazione;
- Progetta e gestisce le soluzioni di telemedicina dell'Azienda

SOSD Qualità, rischio clinico, innovazione gestionale e tecnologica

- Supporta la direzione aziendale e le altre strutture di staff nella pianificazione, programmazione e controllo delle tecnologie sanitarie nonché nella ricerca della innovazione in tale settore;
- Partecipa alla Commissione Tecnica di Valutazione Aziendale dispositivi medici

SOD Direzione medica ospedaliera

- Cura l'alimentazione e la gestione dei flussi informativi sanitari, della documentazione sanitaria (cartelle cliniche) formata dell'Azienda.
- Gestione affidamenti sevizi e forniture sotto soglia per attività che potrebbero comportare trattamenti di dati personali.

Referente aziendale privacy

- Il Referente aziendale per la privacy individuato e nominato dal Titolare dei dati personali (D.Lgs.196/2003 ha inserito all'art. 2-quaterdecies la figura del "referente privacy", inteso come uno o più soggetti cui il Titolare delega specifiche attività relative alla normativa privacy) svolge, in nome e per conto dello stesso funzioni di gestione delle attività e degli adempimenti imposti al medesimo Titolare in materia di protezione dei dati personali dal Regolamento UE 2016/679, dal D.Lgs. n. 196/2003 e s.m.i. nonché dalla normativa in materia, in particolare per le attività di gestione incidenti sui sistemi informativi aziendali previste dal suddetto regolamento, il Referente aziendale per la privacy agisce con il supporto e la collaborazione della SO SIA

Responsabile per la Protezione dei Dati (RPD) o Data Protection Officer (DPO)

- Il DPO o RPD è figura espressamente prevista dal Regolamento Europeo 679/2016 qualora ricorrano le condizioni di cui all'art. 37.
- Per l'Azienda il DPO o RPD costituisce figura obbligatoria in quanto il trattamento di dati personali è effettuato da un'autorità pubblica, nel caso in esame una pubblica amministrazione ai sensi dell'art. 1, comma 3, del D.lgs. 165/2001, e qualora le attività principali del Titolare consistono nel trattamento su larga scala di categorie particolari di dati, nel caso in esame l'Azienda è un Ente del

Servizio Sanitario Regionale e specificamente un'Azienda Ospedaliero - Universitaria e tratta dati relativi allo stato di salute anche dati genetici di coloro che usufruisco delle prestazioni sanitarie che eroga l'Azienda.

- In particolare le funzioni attribuite al DPO sono funzioni previste per legge (art. 39 Reg. UE 679/2016) e vengono qui di seguito riportate:
  - 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 nonché da disposizioni previste dalla normativa europea e nazionali relative alla protezione dei dati personale;
  - sorvegliare l'osservanza della normativa europea e nazionali 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;
  - 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.

Il Titolare del trattamento coinvolge il DPO o RPD in tutte le questioni riguardanti la protezione dei dati personali e lo sostiene nell'esecuzione dei compiti come sopra individuati fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica, garantendo autonomia allo stesso nell'esecuzione dei suoi compiti.

Il DPO o RPD non può essere rimosso o penalizzato dal Titolare del trattamento per l'adempimento dei propri compiti; egli riferisce riferisce direttamente alla Direzione.

Il DPO o RPD è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità alle disposizoni europee e nazionali.

<u>Responsabile della transizione digitale</u>

- Il responsabile della transizione digitale svolge le funzioni ed i compiti attribuiti dall'art. 17 D. Lgs. 7 marzo 2005 n. 82 e s.m.i. ed è tenuto a garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione, rappresenta il principale interlocutore di AgID e della Presidenza del Consiglio dei Ministri per il monitoraggio e il coordinamento delle attività di trasformazione digitale, nonché per la partecipazione a consultazioni e censimenti previsti dal Piano triennale per l'informatica, in particolare si occupa del coordinamento strategico e dello sviluppo dei sistemi informativi di telecomunicazione e fonia, pianifica, coordina e monitora la sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, compie analisi per verificare la coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di

migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa e per procedere ad attività di revisione, pianifica e coordina il processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione, favorisce sistemi di pagamento informatici, implementazione di SPID, gestione documentale, apertura e pubblicazione dei dati, accessibilità, sicurezza, propone l'adozione di circolari e atti di indirizzo sulle materie di propria competenza

Responsabile della sicurezza informatica

- Il Responsabile della sicurezza informatica ha il compito di garantire la sicurezza delle infrastrutture ICT aziendali (PC, server, apparati di rete) e la sicurezza nella gestione degli accessi alle risorse aziendali.

Responsabile della gestione documentale

- Il Responsabile della gestione documentale si occupa della tenuta del protocollo informatico, dei flussi documentali e degli archivi ai sensi del DPCM 3 dicembre 2013.

Responsabile della conservazione documentale

- Il Responsabile della conservazione documentale definisce e attua le politiche complessive di un sistema di conservazione nella pubblica amministrazione utilizzate per l'archiviazione e la gestione documentale ai sensi del DPCM 3 dicembre 2013 art.7.

Direttori delle strutture organizzative aziendali

- I direttori delle strutture organizzative aziendali svolgono attività di gestione ed organizzazione operativa nell'ambito delle attività di trattamento di dati personali inerenti le funzioni loro affidate nella medesima struttura

Responsabili scientifici di progetti di ricerca e di studi clinici (Principal Investigator)

- I responsabili scientifici si occupano della gestione ed organizzazione operativa di attività di trattamento di dati personali inerenti la progettazione e conduzione di progetti di ricerca e studi clinici

Personale dell'Azienda

- Dipendenti, collaboratori, consulenti che svolgono nell'ambito di compiti loro assegnati attività di trattamento dati personali affidate alla struttura organizzativa aziendale cui afferiscono sulla base delle indicazioni specificamente ricevute

Ogni soggetto coinvolto nel trattamento dei dati personali sulla base della presente regolamentazione è tenuto ad informare il Titolare del trattamento, in relazione ad ogni questione che preveda la necessità di una valutazione diretta ad opera del Titolare del trattamento e che debba, quindi, essere specificamente autorizzata e valutata in quanto non ancora regolamentata, al fine di evitare trattamenti di dati personali che possano essere lesivi dei principi di cui al Reg. UE 679/2016 ed esporre il Titolare del trattamento a sanzioni ad opera dell'Autorità per la protezione dei dati personali.

5. PIANO OPERATIVO DI DISTRIBUZIONE DELLE COMPETENZE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Oggetto del presente regolamento è la definizione delle attività che l'Azienda deve compiere in attuazione della normativa vigente in materia di protezione dei dati personali, resta inteso che le attività qui descritte non esauriscono le misure che l'Azienda deve porre in essere in ambito di sicurezza IT, cybersicurity e conservazione digitale che sono regolamentate da altre ed ulteriori disposizioni e regolamenti.
Qui si intende, quindi, definire "il sistema privacy" in attuazione degli adempimenti connessi al sistema di gestione della protezione dei dati personali in attuazione di quanto prescritto dal Reg. UE 679/2016, nonché dal D. Lgs. 196/2003 e s.m.i. e dei provvedimento al riguardo adottati dall'Autorità per la Protezione dei Dati Personali.
Le attività sono state raggruppate in macrocategorie:

1. Tenuta ed Aggiornamento del Registro delle attività di trattamento effettuate in qualità di Titolare del trattamento
2. Tenuta ed Aggiornamento del Registro delle attività di trattamento effettuate in qualità di Responsabile del trattamento
3. Valutazione dei rischi e Data Protection Impact Assessment (DPIA)
4. Applicazione del principio di Privacy by Design e Privacy by Default
5. Formalizzazione di atti in materia di trattamento dati personali (accordi di contitolarità, nomina responsabile esterno, policy in materia di trattamento dati personali)
6. Nomina dei designati/autorizzati al trattamento dati personali e formalizzazione istruzioni
7. Gestione delle violazioni di dati personali (data breach)
8. Predisposizione informative e consensi
9. Gestione delle istanze degli interessati
10. Formazione e sensibilizzazione
11. Pareri e consulenze in materia di trattamento dati personali
12. Regolamenti e procedure in materia di trattamento dati personali
13. Gestione misure di sicurezza informatiche, dei dispositivi medici e delle tecnologie

Si rappresenta che le macroattività sopra sono, nella visione del GDPR e nell'implementazione delle stesse, strettamente correlate le une alle altre con la conseguenza di una loro trasversalità.

Tali attività debbono essere effettuate dal Titolare del trattamento e dai soggetti individuati dallo stesso sulla base dell'organizzazione che si è dato.

Di seguito per ciascuna delle macroattività sopra elencate, ferma l'attività di vigilanza in capo al Titolare del trattamento dei dati personali, sono individuati le strutture aziendali/figure tenute al compimento delle stesse e le specifiche competenze loro affidate.

Tale distribuzione delle competenze è stata elaborata sulla base della normativa, delle linee guida redatte dalle autorità competenti a livello europeo e nazionale e delle procedure interne in essere.

6. FUNZIONI ATTRIBUITE IN MATERIA DI TRATTAMENTO DI DATI PERSONALI E CONSEGUENTI ADEMPIMENTI

Sulla base delle strutture/figure individuate al precedente paragrafo 4) il Titolare attribuisce agli stessi le attività rientranti nelle macrocategorie elencate al precedente paragrafo 5).

Ogni struttura aziendale/figura coinvolta nell'attuazione della singola macroattività in materia di trattamento dati può assumere un ruolo diverso ed in particolare:

- preposto, se risulta essere la struttura aziendale competente della specifica attività; nel caso in cui l'esecuzione dell'attività richieda il convolgimento di altre strutture che ricoprono il ruolo di "collaboratore", la struttura "preposta" assume anche l'onere di coordinare il contributo proveniente dalle prime;
- collaboratore, se la struttura è tenuta a supportare quella preposta (competente a gestire la specifica attività) fornendo, ad esempio, informazioni ben precise;
- supervisore, ossia il DPO a cui è attribuita ex lege la funzione di controllo.

1. Aggiornamento del Registro delle attività di trattamento effettuate in qualità di Titolare

Riferimenti normativi:

- art. 30 GDPR: *"Ogni Titolare del trattamento […] tengono un registro delle attività di trattamento svolte sotto la propria responsabilità."*
- pag. 170 e ss. Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa: *"Il registro va considerato uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del Titolare del trattamento."*
- *pag. 204 e ss.* Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa: "*Il GDPR non impone in modo esplicito che il DPO sia coinvolto in ogni esercizio di valutazione dei rischi […]. Tuttavia, di fatto, è fortemente consigliabile, quantomeno, coinvolgere il DPO anche nelle attività connesse più in generale alla valutazione dei rischi di cui sopra. In pratica, l'esito di tale valutazione dipenderà spesso dal parere del DPO*"

Azienda (legale rappresentante)	D.P.O.	SO SIA	Referente Aziendale Privacy	Altre strutture
Titolare	*Preposto*	*Preposto*	*Preposto*	*Collaboratore*
	Provvede ad inserire, sulla base delle informazioni ricevute dalle diverse strutture aziendali, i trattamenti di dati personali in stretta collaborazione con il Referente Aziendale Privacy e le modifiche di quelli già in essere nel registro delle attività di trattamento ed effettua, se del caso, le proprie valutazioni.	Fornisce supporto tecnico per l'inserimento di nuovi trattamenti che prevedono l'utilizzo di applicativi e per l'aggiornamento di quelli esistenti.	Sottoscrive il registro in nome e per conto del Titolare e provvede alla sua tenuta in collaborazione con il DPO e garantisce per conto del Titolare l'inserimento dei trattamenti aziendali di dati personali collaborando in sinergia con il Referente Aziendale Privacy	I Direttori/Responsabili delle strutture aziendali hanno l'obbligo di comunicare la necessità di avviare un nuovo trattamento di dati personali o di modificarne uno già in essere al DPO e al Referente Aziendale Privacy come si evince dalle istruzioni che il Titolare ha impartito ai direttori SO/SOD/SOSD, autorizzati al trattamento dei dati personali ai sensi dell'art. 29 GDPR.

2. Aggiornamento del Registro delle attività di trattamento effettuate in qualità di Responsabile

Riferimenti normativi:

- art. 30 GDPR: "Ogni responsabile del trattamento […] tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un Titolare del trattamento."
- pag. 170 e ss. Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa: "Il registro va considerato uno degli strumenti che consentono al DPO di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del Titolare del trattamento."

Azienda (legale rappresentante)	D.P.O.	SO SIA	Referente Aziendale per la Privacy	Altre strutture
Titolare	*Preposto*	*Preposto*	*Preposto*	*Collaboratore*
	Provvede ad inserire, sulla base delle informazioni ricevute dalle diverse strutture aziendali, i trattamenti di dati personali in stretta collaborazione con il Referente Aziendale Privacy e le modifiche di quelli già in essere nel registro delle attività di trattamento ed effettua, se del caso, le proprie	Fornisce supporto tecnico per l'inserimento di nuovi trattamenti che prevedono l'utilizzo di applicativi e per l'aggiornamento di quelli esistenti.	Sottoscrive il registro in nome e per conto del Titolare e provvede alla sua tenuta in collaborazione con il DPO e garantisce per conto del Titolare l'inserimento dei trattamenti aziendali di dati personali collaborando in sinergia con il Referente Aziendale Privacy.	I Direttori/Responsabili delle strutture aziendali hanno l'obbligo di comunicare la necessità di avviare un nuovo trattamento di dati personali o di modificarne uno già in essere al DPO e al Referente Aziendale Privacy come si evince dalle istruzioni che il Titolare ha impartito ai direttori SO/SOD/SOSD, autorizzati al trattamento dei dati personali ai sensi dell'art. 29 GDPR.

	valutazioni.			Si tratta di attività che vengono affidate da Terzi all'Azienda nell'ambito delle attività afferenti la struttura.

3. Valutazione dei rischi e Data Protection Impact Assessment (DPIA)

Riferimenti normativi:

- art. 24 GDPR
- art. 35 GDPR: *"Quando un tipo di trattamento, allorchè 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, il Titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. […] Il Titolare del trattamento […] si consulta con il responsabile della protezione dei dati".*
- *art. 36* GDPR
- *art. 39* GDPR: "*Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti: […] fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35*".
- *pag. 204 e ss. Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa: "Il GDPR non impone in modo esplicito che il DPO sia coinvolto in ogni esercizio di valutazione dei rischi […]. Tuttavia, di fatto, è fortemente consigliabile, quantomeno, coinvolgere il DPO anche nelle attività connesse più in generale alla valutazione dei rischi di cui sopra. In pratica, l'esito di tale valutazione dipenderà spesso dal parere del DPO".*
- pag. 215 e ss. Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa: *"[…] spetta al Titolare del trattamento, e non al DPO, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati. Tuttavia, il DPO svolge un ruolo fondamentale e di grande utilità assistendo il Titolare nello svolgimento di tale DPIA."*

Azienda (legale rappresentante)	D.P.O.	SO SIA	Direttori/Responsabili strutture aziendali/Responsabili Scientifici/	Referente Aziendale per la Privacy
Titolare	*Supervisore*	*Preposto*	*Preposto*	*Preposto*
	Supporta nella valutazione del rischio dei singoli trattamenti anche con la collaborazione della SO SIA/Responsabile Transizione Digitale/Responsabile Sicurezza Sistemi informativi e fornisce pareri circa le misure da adottare per ridurre tale rischio. Fornisce, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e ne sorveglia lo svolgimento. Il manuale RPD sopra citato prevede che il Titolare consulti il DPO, sulla necessità di condurre o meno una DPIA, quale metodologia adottare per la sua conduzione, se condurla con risorse interne o esterne, quali salvaguardie applicare, comprese le misure tecniche e	Provvede alla valutazione del rischio dei trattamenti che richiedono l'utilizzo di applicativi informatici e ad individuare e implementare le misure tecniche necessarie per ridurre i rischi. Offre supporto tecnico per condurre la DPIA di trattamenti di dati personali che prevedono l'utilizzo di applicativi, in particolare per quanto concerne la valutazione dei rischi e l'individuazione delle misure da adottare per la mitigazione degli stessi.	Fornisce al Referente aziendale per la privacy e al DPO, tempestivamente, le informazioni e la documentazione necessaria per effettuare la valutazione dei rischi del trattamento e, se necessario, della valutazione di impatto anche sulla base di specifiche richieste.	Garantisce per conto del Titolare l'effettuazione della DPIA per i trattamenti che ne necessitano collaborando in sinergia con i Direttori/Responsabili strutture aziendali/Responsabili Scientifici Provvede ad attuare, se necessario con il supporto della SO SIA, le prescrizioni del DPO eventualmente fornite in sede di valutazione di impatto. Provvede per conto del Titolare in caso di non condivisione delle indicazioni del DPO a motivare la decisione di non conformarsi a tali indicazioni.

	organizzative, per attenuare i rischi per i diritti e gli interessi degli interessati, se la DPIA sia stata condotta correttamente o meno e se le conclusioni siano conformi al GDPR. Valuta la necessità di una consultazione preventiva e supporta il Titolare nella predisposizione della relativa istanza.			

4. Applicazione del principio di Privacy by Design e Privacy by Default

Riferimenti normativi:

- art. 25 GDPR
- Procurement Guidelines for cybersecurity in hospital (February 2020) della European Union Agency for Cybersecurity(ENISA)
- Guidelines 4/2019 on article 25 Data protection by Design and by Default Version 2.0 – Adopted on October 2020 del European Data Protection Board (EDPB)
- pag. 262 e ss. Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa

Azienda (legale rappresentante)	D.P.O.	SO SIA Ingegneria Clinica Responsabile transizione digitale Responsabile Sicurezza Informatica	Direttori/Responsabili strutture aziendali/DMO/Responsabili Scientifici	Referente Aziendale per la Privacy	Strutture nelle quali operano i RUP come definiti dall'art. 30 del D.Lgs. n. 50/2016/strutture che stipulano altri contratti, convenzioni e accordi
Titolare	*Supervisore*	*Preposto*	*Collaboratore*	*Preposto*	*Collaboratore*
	Fornisce pareri in merito a specifici quesiti posti dalle strutture preposte per l'implementazione di nuovi trattamenti o per il miglioramento di quelli esistenti indicando le attività necessariamente da compiersi.	Verificano con riferimento ai trattamenti che prevedono l'utilizzo di applicativi, dispositivi medici, sistemi di IA, da quando il trattamento di dati personali ha inizio fino al suo termine (privacy by default), che gli stessi siano conformi ai principi fondamentali applicabili al trattamento di dati personali (art. 5 GDPR). Monitorano l'efficacia delle misure tecniche adottate e da	Fornisce al Referente aziendale per la privacy/, al DPO, al Responsabile per la Transizione Digitale, Responsabile Sicurezza informatica, SO SIA e Ingegneria Clinica tempestivamente le informazioni e la documentazione necessaria per comprendere le finalità che si intendono soddisfare con lo specifico trattamento di dati personali e le caratteristiche dello stesso al fine di consentire le attività necessarie per l'avvio e la modifica dei trattamenti in modo conforme al GDPR, per la SOD DMO con particolare riferimento alla gestione della documentazione sanitaria	Verifica da quando il trattamento di dati personali ha inizio fino al suo termine (privacy by default) che lo stesso sia conforme ai principi fondamentali applicabili al trattamento di dati personali (art. 5 GDPR). Monitorando lo svolgimento sulla base di questo regolamento degli adempimenti necessari affinchè il trattamento sia conforme al GDPR. Monitora l'efficacia delle misure	Comunicano l'avvio della procedura per l'acquisizione di servizi e forniture che necessitano il trattamento di dati personali al DPO, al Referente Aziendale, alla SO SIA, all'Ingegneria Clinica per consentire di predisporre quanto necessario per l'avvio/modifica/miglioramento del trattamento in modo conforme al GDPR.

		adottarsi rispetto alla protezione dei dati personali mediante predisposizione di documentazione che sia in grado di accertare le attività in tal senso effettuate.		organizzative adottate e da adottarsi rispetto alla protezione dei dati personali.	

5. **Definizione dei ruoli (conTitolare, responsabile, Titolare autonomo/amministratori di sistema) in ambito di trattamento dati personali e formalizzazione del relativo atto giuridico**

Riferimenti normativi:

- artt. 26 e 28 GDPR
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 – Adopted on September 2020 del European Data Protection Board (EDPB)
- pag. 266 Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	SO SIA Responsabile transizione digitale Responsabile Sicurezza informatica	Referente Aziendale per la Privacy	~~Strutture nelle quali operano i RUP come definiti dall'art. 30 del D.Lgs. n. 50/2016/strutture che stipulano altri contratti, convenzioni e accordi/responsabili del procedimento~~
Titolare	*Supervisore*	*Collaboratore*	*Preposto*	*Preposto/collaboratore*
	Supporta nell'individuazione dei ruoli in ambito di trattamento dati e predispone modelli che regolamentano i diversi rapporti.	Supportano il DPO nella predisposizione di modelli/documentazione che regolamentano i diversi rapporti.	Verifica per conto del Titolare l'avvenuta formalizzazione delle diverse nomine.	Provvedono alla formalizzazione laddove necessario, sulla base dei modelli forniti, del rapporto individuato per quello specifico trattamento di dati personali con riferimento a quei trattamenti che afferiscono all'ambito di loro competenza.

6. **Nomina e istruzioni dei designati e degli autorizzati al trattamento**

Riferimenti normativi:

- art. 29 GDPR

- Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0 – Adopted on September 2020 del European Data Protection Board (EDPB)
- pag. 266 Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	SO Gestione del Personale	Referente Aziendale per la Privacy
Titolare	*Supervisore*	*Preposto*	*Preposto*
	Predispone i modelli aziendali per la nomina e l'istruzione dei **designati**.	Fa sottoscrivere all'atto del conferimento dell'incarico del direttore/responsabile di strutture aziendali la nomina, contenente le istruzioni, come designati al trattamento di dati personali sulla base del modello fornito e lo restituisce al Referente Aziendale per la Privacy	Acquisisce le nomine quali designati al trattamento di dati personali dei direttore/responsabile di SO/SOD/SOSD, provvede a farle sottoscrivere al legale rappresentante e le conserva.
Azienda (legale rappresentante)	D.P.O.	Direttori/Responsabili strutture aziendali	Referente Aziendale per la Privacy
Titolare	*Supervisore*	*Preposto*	*Preposto*
	Predispone i modelli aziendali per la nomina e l'istruzione degli autorizzati	Provvedono alla nomina e alla conservazione delle nomine degli autorizzati effettuate sulla base del modulo fornito, contenente le istruzioni, che potranno implementare sulla base dei specifici trattamenti di loro competenza.	Acquisisce e conserva l'elenco degli autorizzati.

7. Gestione delle violazioni di dati personali (*data breach*)*

Riferimenti normativi:

- art. 33 e 34 GDPR
- procedura aziendale
- linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679 – adottate a febbraio 2018
- pag. 239 e ss Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	Altre strutture	Gruppo per la gestione della violazione dei dati di cui alla procedura aziendale	Referente Aziendale per la Privacy
Titolare	*Supervisore*	*Collaboratore*	*Preposto*	*Preposto*
	Svolge funzioni di consulenza in caso si violazione di dati personali E funge anche da punto di contatto per l'autorità di controllo e per gli interessati e supporta il Titolare nella redazione dei documenti fornendo parere in merito alla struttura, amministrazione e impostazione della relativa documentazione. Supporta nel processo di notifica all'autorità di controllo e durante qualsiasi successiva indagine da parte della medesima autorità,	Qualunque struttura aziendale che riscontri una violazione o riceva una segnalazione dall'esterno è tenuta tempestivamente ad informare il Titolare, il referente aziendale per la privacy e il DPO, nonché il gruppo costituito per la gestione delle violazioni. La struttura aziendale coinvolta nel trattamento oggetto della violazione dovrà predisporre una breve relazione sulla base della procedura aziendale.	Raccoglie le segnalazioni di violazioni di dati e accerta con il DPO se si tratti effettivamente di una violazione. Valuta la natura della violazione dei dati personali e la gravità e la probabilità di conseguenze sui diritti e le libertà fondamentali degli interessati.	Provvede materialmente alla notifica all'Autorità per la protezione dei dati personali.

*Si rinvia in ogni caso alla specifica procedura aziendale per l'articolazione delle fasi di gestione delle violazioni.

8. Predisposizione informative e consensi

Riferimenti normativi:

- Artt. 7, 13 e 14GDPR
- pag. 266 Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	Altre strutture	Referente Aziendale per la Privacy
Titolare	*Supervisore*	*Collaboratore*	*Preposto*
	Provvede alla predisposizione/modifica dei modelli di informativa e di consenso. Fornisce, se richiesto, supporto per la redazione delle singole informative sulla base del modello.	Segnala l'eventuale necessità di predisporre/modificare una specifica informativa per uno specifico trattamento non rientrante tra quelli per i quali è già stato fornito un modello. Fornisce al DPO le informazioni necessarie sul trattamento indispensabili per redigere il modello di informativa.	Redige le informative per il trattamento dei dati personali tenendo conto dei modelli forniti dal DPO.

9. Gestione delle istanze degli interessati*

Riferimenti normativi:

- artt. 15 e ss GDPR
- procedura aziendale adottata con Determina del Direttore Generale n. 710 del 22 agosto 2019
- pag. 272 e ss Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	Referente Aziendale per la Privacy	Direttori e responsabili delle strutture
Titolare	*Supervisore e Preposto (eventuale)*	*Preposto*	*Collaboratore*
Riceve l'istanza dell'interessato.	Riceve l'istanza dell'interessato. Supporta nella gestione il referente aziendale per la privacy come previsto dalla procedura aziendale. Monitora che venga fornito riscontro agli interessati nei tempi fissati dalla normativa. In caso di inattività del referente privacy funge da punto di contatto per l'interessato. Verifica che le istanze gestite producano, se del caso, i cambiamenti necessari nelle prassi aziendali.	Riceve l'istanza dell'interessato. Gestione della richiesta dell'interessato supportato, ove necessario, dal DPO come previsto dalla procedura aziendale. Fornisce riscontro all'interessato nei termini.	Direttori e responsabili delle strutture delle strutture a cui afferiscono i trattamenti oggetto dell'istanza forniscono tutte le informazioni necessarie a fornire riscontro all'interessato in modo da consentire il rispetto dei termini di legge secondo quanto prescritto dalla procedura aziendale.

*Si rinvia in ogni caso alla specifica procedura aziendale per l'articolazione delle fasi di gestione delle violazioni.

10. Formazione e sensibilizzazione

Riferimenti normativi:
- art. 39 GDPR
- pag. 274 e ss Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	Referente Aziendale per la Privacy	Altre strutture
Titolare	*Preposto*	*Collaboratore*	*Collaboratore*
	Elabora note/circolari interne su specifici aspetti della protezione dei dati personali. Organizza eventi formativi per i dipendenti.	Suggerisce al DPO, se ritiene opportuno, alcune tematiche che dovrebbero essere oggetto di formazione. Supporta il DPO nell'attività di sensibilizzazione diffondendo le buone pratiche da questo elaborate.	Segnalano al DPO delle specifiche esigenze formative.

11. Pareri e consulenze

Riferimenti normativi:
- art. 39 GDPR
- pag. 274 e ss Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	Referente Aziendale per la Privacy	Altre strutture
Titolare	*Preposto*	*Collaboratore*	*Collaboratore*
	Offre pareri e consulenze in materia di trattamento di dati personali su specifiche tematiche non altrimenti trattate.	Supporta il DPO nell'attività di diffusione dei pareri e delle consulenze predisposte dal DPO.	Segnalano al DPO delle specifiche esigenze formative.

12. Regolamenti e procedure

Riferimenti normativi:
- art. 39 GDPR
- pag. 274 e ss Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa:

Azienda (legale rappresentante)	D.P.O.	Referente Aziendale per la Privacy	Altre strutture Responsabile per la transizione digitale Responsabile SIA Responsabile per la sicurezza informazione Responsabile gestione documentale e della conservazione/SOD DMO
Titolare	*Collaboratore*	*Preposto*	*Collaboratore*

	Supporta il Titolare nell'adozione di procedure e regolamenti aziendali su specifici aspetti in materia di trattamento di dati personali volti ad incrementare la *compliance* al GDPR	Supporta la direzione nel processo decisionale di approvazione delle procedure e regolamenti proposte sulla base delle finalità che il Titolare intende perseguire, nonché le modalità da adottarsi.	Supportano il DPO nella predisposizione delle procedure e regolamenti aziendali per le attività di loro competenza che richiedono conoscenze tecniche specifiche da implementare nei suddetti regolamenti e procedure.

13. **Gestione misure di sicurezza informatiche, dei dispositivi medici e delle tecnologie**

Riferimenti normativi:

- Art. 25 Reg. UE 679/2016
- pag. 129 e ss e pag. 262 e ss. Manuale RPD - Linee guida destinate ai responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento generale sulla protezione dei dati dell'Unione Europa
- D. Lgs. 7 marzo 2005 n. 82
- DPCM 3 dicembre 2013
- Provvedimenti Agid
- Regolamento UE 745/2017

Azienda (legale rappresentante)	D.P.O. e Referente aziendale privacy	Responsabile per la transizione digitale/ Responsabile per la sicurezza informazione Responsabile SIA/ Responsabile gestione documentale/ Qualità, rischio clinico, innovazione gestionale e tecnologica	Altre strutture
Titolare	*Collaboratore*	*Preposto*	*Collaboratore*
	Supporta il Responsabile per la transizione digitale/ Responsabile per la sicurezza informazione Responsabile SIA/ Responsabile gestione documentale/ Qualità, rischio clinico, innovazione gestionale e tecnologica	Supportano il Titolare nell'introduzione di misure tecniche ed organizzative idonee ed adeguate volte alla minimizzazione del rischio e al rispetto dei principi generali in materia di protezione di dati personali e all'adeguamento rispetto alla normativa di settore specifica (AGID. NSIS, Framework nazionali di Cybersecurity, normativa in materia di dispostivi medici)	Collaborano nel fornire informazioni specifiche richieste dai preposti per consentire l'adozione delle misure tecniche ed organizzative al Titolare