DETERMINA DEL DIRETTORE GENERALE AZIENDA SANITARIA TERRITORIALE DI ASCOLI PICENO

n. 46 del 27 febbraio 2025

Oggetto: **Approvazione Regolamento Aziendale in materia di Protezione dei Dati Personali.**

VISTO il documento istruttorio riportato in calce alla presente determina di cui costituisce parte integrante e sostanziale e dal quale si rileva la necessità di provvedere a quanto in oggetto specificato;
RITENUTO, per i motivi riportati nel predetto documento istruttorio, di adottare il presente atto;
ACQUISITI i pareri favorevoli del Direttore Amministrativo, del Direttore Sanitario e del Direttore socio-sanitario AST;
VISTA l'attestazione del Direttore f.f. U.O.C. Supporto Area Contabilità Bilancio e Finanza.

DETERMINA

1. Di approvare il Regolamento Aziendale in materia di Protezione dei Dati Personali della AST di Ascoli Piceno che si allega al presente atto quale sua parte integrante e sostanziale (Allegato n.1) comprensivo degli allegati di seguito indicati:
   - Allegato A) Linee guida per conduzione attività di *Data protection impact*;
   - Allegato B) Politica di protezione dei dati personali;
   - Allegato C) Il Registro delle attività di trattamento;
   - Allegato D) Modulo di richiesta di esercizio dei diritti dell'interessato;
   - Allegato E) Informativa navigatori siti internet aziendali;
   - Allegato F) Informativa utenti ex artt.13-14 Regolamento UE 2016/679;
   - Allegato G) Atto di nomina designato al trattamento con Compiti ed Istruzioni;
   - Allegato H) Atto di nomina autorizzato al trattamento dei dati con Istruzioni;
   - Allegato I) Istruzioni specifiche personale sanitario designati ed autorizzati;
   - Allegato J) Modello nomina Responsabile del trattamento ex Art.28 REG.(UE) 2016/679.

2. Di riservarsi la possibilità di apportare eventuali modifiche/integrazioni al Regolamento in oggetto nonché alla documentazione allo stesso allegata in relazione alle necessità manifestate dal DPO ASTAP in sede di applicazione dello stesso, nonché alla riorganizzazione in atto della AST AP a seguito dell'adozione della proposta di atto aziendale ed alla prossima implementazione del nuovo sito internet aziendale;

3. Di nominare, ai sensi e per gli effetti di cui all'art.2 *quaterdecies* del D.Lgs.n.196/2003 e ss.mm.ii., quali soggetti "Designati" al trattamento dei dati personali dell'Azienda Sanitaria Territoriale Ascoli Piceno, i titolari dei seguenti incarichi:
   - Direttori di Struttura Complessa (ovvero Titolari di incarichi di "sostituzione" nei termini previsti dai CC.NN.LL. delle Aree contrattuali di riferimento);
   - Responsabili di Struttura Semplice Dipartimentale;
   - Altro personale designato ai fini dello svolgimento di funzioni previste da specifiche normative di settore (RSPP, Medico competente, etc.).;

4. Di dare atto che, sulla base della previsione normativa di cui al precedente Punto 3) del dispositivo, ai professionisti "Designati" vengono assegnati – in ragione del proprio ruolo di responsabilità organizzativa all'interno dell'Azienda – specifici compiti e funzioni di vigilanza sul rispetto e attuazione delle disposizioni in tema di trattamento di dati personali all'interno delle strutture rispettivamente dirette;

5. Di dare, altresì atto che, in caso di vacanza degli incarichi di cui al precedente Punto 3) del dispositivo e nelle more del relativo conferimento, le correlate responsabilità in tema di protezione dei dati personali sono in capo al Direttore del Dipartimento, ove presente, ovvero al Direttore Sanitario e al Direttore Amministrativo a seconda dello specifico ambito organizzativo;

6. Di trasmettere, per il tramite dell'Ufficio determine presso la Direzione Generale AST, il presente atto a ciascun "Designato" al trattamento dei dati personali, unitamente alle relative istruzioni fornite dal Titolare cui i "Designati" medesimi sono tenuti ad attenersi nell'effettuare le attività di trattamento rientranti nelle rispettive funzioni istituzionali e che si allegano alla presente determina (Allegato G);

7. Di dare atto che, in linea con le previsioni di cui agli artt.4 n.10) e 29 del GDPR, tutto il Personale in servizio all'interno delle diverse Unità Operative aziendali è "Autorizzato" al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza; ciò sotto la diretta autorità e vigilanza da parte dei soggetti "Designati" al trattamento e attenendosi alle istruzioni allegate alla presente determina (Allegato H), fatte salve le responsabilità di natura personale correlate all'autonomia professionale di specifiche categorie di professionisti;

8. Di approvare - ad integrazione dei contenuti delle istruzioni di cui ai precedenti punti 6 e 7 del dispositivo - le istruzioni specifiche per il trattamento dati da parte del personale sanitario, destinate sia ai "Designati" che a tutti gli "Autorizzati" al trattamento, che si allegano alla presente determina (Allegato I);

9. Di dare atto che, fino alla completa implementazione e messa a regime del Regolamento in parola e della relativa modulistica, permangono in vigore le nomine dei designati ed autorizzati effettuate ai sensi della previgente regolamentazione e modulistica in uso.

10. Di dare mandato alla U.O.C Gestione risorse umane di provvedere tempestivamente a formale comunicazione al RPD in ordine al vigente assetto degli incarichi di cui al precedente punto 3) del dispositivo, nonché al relativo aggiornamento, onde consentire allo stesso RPD l'espletamento degli adempimenti in tema di protezione dei dati personali;

11. Di dare mandato ai professionisti "Designati" al trattamento di produrre – secondo modalità da comunicarsi a cura del RPD - apposita attestazione comprovante l'avvenuta comunicazione dei contenuti del presente atto al Personale in servizio che effettua trattamenti di dati personali presso le Unità Operative rispettivamente dirette, ciò al fine di rendere edotti i medesimi in merito al contesto di riferimento ed alle richiamate specifiche istruzioni;

12. Di dare mandato alla U.O.C Gestione Risorse Umane di provvedere - in sede di conferimento di incarichi di direzione/responsabilità di struttura complessa ovvero di struttura semplice dipartimentale - all'inserimento di specifica clausola contrattuale ove il professionista venga nominato quale soggetto "Designato" al trattamento dei dati per la rispettiva Struttura, fornendo al medesimo le relative istruzioni di cui all'Allegato G ed anche all'Allegato I (solo per i professionisti sanitari);

13. Di dare, altresì, mandato alle suddette Strutture competenti in materia di gestione delle risorse umane di provvedere - in sede di assunzione in servizio di nuove unità di Personale - all'inserimento di specifica clausola contrattuale contenente la nomina del neo assunto quale soggetto "Autorizzato" al trattamento, fornendo allo stesso le relative istruzioni di cui all'Allegato H e anche all'Allegato I (solo per i professionisti/operatori sanitari);

14. Di dare mandato alla U.O.C Formazione ovvero alla U.O.C Direzione Medica di Presidio in relazione all'attuale riparto funzionale nell'ambito dell'assetto organizzativo della AST, di provvedere - in sede di autorizzazione alla frequenza delle strutture aziendali da parte di volontari, tirocinanti, studenti e specializzandi - all'inserimento di specifica clausola contenente la nomina delle predette figure in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato H e anche all'Allegato I (solo per i frequentatori di strutture/servizi sanitari);

15. Di dare mandato alla U.O.C. D.A.T di provvedere, in sede di reclutamento di personale convenzionato (Medici dell'Emergenza Sanitaria Territoriale, Medici Specialisti Ambulatoriali e Medici del Ruolo Unico di Assistenza Primaria a Rapporto Orario), all'inserimento di specifica clausola contenente la nomina dei predetti professionisti in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato H e all'Allegato I;

16. Di dare atto che con successivo provvedimento la Direzione generale AST procederà alla costituzione del c.d. Gruppo multidisciplinare di supporto al DPO ai sensi dell'art.29 dell'approvando Regolamento aziendale in materia di protezione dei dati personali;

17. Di dare mandato alla U.O.C. SIA di procedere entro 60 (sessanta) giorni dall'adozione del presente atto alla predisposizione di nuova regolamentazione AST per l'Utilizzo di Strumenti e Servizi IT (Information & Tecnology), fermo restando, nelle more di quanto sopra, la piena operatività del Regolamento approvato dalla soppressa ASUR Marche, ai sensi della DGR Marche n.1718/2022;

18. Di dare mandato alla U.O.C SIA di verificare la possibilità di acquisire ai sensi della vigente normativa apposito applicativo al fine di consentire, in un'ottica di efficienza ed efficacia, la gestione dinamica del Registro del trattamento dei dati;

19. Di dare che dal presenta atto non derivano oneri economici a carico del bilancio della AST di Ascoli Piceno;

20. Di dare atto che la presente determina non è sottoposta a controllo ai sensi dell'art.4 della Legge 412/91 e dell'art.39 della L.R.n.19/2022;

21. Di dare atto che, a norma dell'art.39, comma 8, della L.R. 19/2022, la presente determina è efficace dalla data di pubblicazione all'Albo on line aziendale.

Il Direttore Generale F.F. AST
(Dr.ssa Maria Bernadette Di Sciascio)

per i pareri infrascritti

Il Direttore Amministrativo	**Il Direttore Socio Sanitario**	**Il Direttore Sanitario**
(Dr.ssa Paola D'Eugenio)	(*Dr.ssa Sonia Carla Cicero*)	*(Dr.ssa Maria Bernadette Di Sciascio)*

Documento informatico firmato digitalmente

DOCUMENTO ISTRUTTORIO
U.O.C. Affari Generali e Contenzioso AST

Normativa ed altri atti di riferimento:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 (GDPR) "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)";
- Decreto Legislativo 30 giugno 2003, n.196 e ss.mm.ii. "Codice in materia di protezione dei dati personali" (aggiornato con le modifiche introdotte dal D.Lgs. 10 agosto 2018, n. 101);
- Legge Regionale 08 agosto 2022, n.19 "Organizzazione del Servizio Sanitario Regionale";
- Determina n.349/DG ASUR del 30/05/2018;
- Determina n.350/DG ASUR del 01/06/2018;
- Determina DG ASUR n.177 del 22/04/2020 aveva adottato il Regolamento per l'Utilizzo di Strumenti e Servizi IT (Information & Tecnology) all'interno dell'azienda ASUR Marche;
- DGR Marche n.1718 del 19/12/2022 "Adempimenti funzionali previsti dagli art.42 e 43 della L.R. 8 agosto 2022, n.19 (Organizzazione del servizio sanitario regionale) e DGRM 1385/2022";
- DGR Marche n.1703/2024 "D. Lgs. 171/2016 e L. R. 19/2022 - Definizione degli obiettivi dei Direttori Generali degli Enti del Servizio Sanitario Regionale e del DIRMT per l'anno 2024 e approvazione dei criteri relativi alla procedura di valutazione dei risultati conseguiti dagli stessi per l'anno 2024"
- Determina DG n.23/ASTAP del 31/01/2025 recante ad oggetto "Proposta di Atto Aziendale dell'Azienda Sanitaria Territoriale di Ascoli Piceno. Approvazione."

Motivazione:

- Il 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 - GDPR), è entrato in vigore il 24 maggio 2016 e trova applicazione dal 25 maggio 2018. Il Decreto Legislativo n.101/2018 - emanato in attuazione dell'art.13 della Legge di delegazione europea 2016-2017 (Legge 25 ottobre 2017 n.163) - reca disposizioni per l'adeguamento della normativa nazionale alle disposizioni del succitato Regolamento (UE) 2016/679.

- L'ASUR Marche con Determina n.349/DG del 30/05/2018 approvava il Regolamento organizzativo privacy aziendale successivamente integrato ai sensi della Determina n.350/DG ASUR del 01/06/2018.

- Con Legge Regionale 8 agosto 2022, n.19 recante ad oggetto "Organizzazione del servizio sanitario regionale", è stata soppressa, al 31 dicembre 2022, l'Azienda Sanitaria Unica Regionale (ASUR) e dal 01 gennaio 2023 sono state costituite e diventate operative le Aziende Sanitarie Territoriali, che sono subentrate all'ASUR Marche senza soluzione di continuità.

- Ai sensi dell'art.18 ("Normazione interna") dell'Allegato A) alla DGR Marche n.1718 del 19/12/2022 (recante ad oggetto "Adempimenti funzionali previsti dagli art. 42 e 43 della L.R. 8 agosto 2022, n.19 (Organizzazione del servizio sanitario regionale) e DGRM 1385/2022"), le AST sono tenute a garantire, nella fase di prima operatività e sino a successive nuove determinazioni in merito da parte del Legale Rappresentante della AST di pertinenza, la validità ed efficacia della normazione interna (Regolamenti, Atti Generali, Codici, Accordi Sindacali, Circolari e relative disposizioni di attuazione) allo stato vigenti presso le Aziende soppresse.

- Per quanto concerne la protezione dei dati personali trattati, l'Azienda Sanitaria Territoriale di Ascoli Piceno, quale Titolare del trattamento ex art.4 n.7) del Regolamento UE 2016/679 (GDPR), è tenuta - nella logica della piena applicazione del principio di *accountability* di cui all'art.24 del GDPR stesso - a mettere in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che i trattamenti di dati personali siano effettuati conformemente ai principi di cui al citato Regolamento UE 2016/679.

- Considerato che, nell'ottica del Legislatore europeo, 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 lo stesso risponde delle proprie azioni e deve essere in grado, in qualsiasi momento di darne conto verso l'esterno.

- Il Direttore Generale della AST di Ascoli Piceno, in ottemperanza alle disposizioni dell'art.37 del Regolamento (UE) 2016/679 ed ai provvedimenti dell'Autorità del Garante, ha nominato, con Determina n.40/ASTAP del 14/02/2024, il Responsabile Aziendale per la Protezione dei Dati personali (RPD/DPO) nella persona dell'Avv. Bruno Antonio Malena;

- Questa Amministrazione, sentito il DPO della AST, ha ritenuto indispensabile ed opportuno avviare ogni utile ed opportuna iniziativa per prevenire i rischi derivanti dal trattamento dei dati personali e sensibili mediante l'adozione di un nuovo Regolamento aziendale per la protezione dei dati personali in ottemperanza alle disposizioni di cui al Regolamento UE 2016/679.

- Con specifico riferimento all'ambito delle misure organizzative da adottare, stante l'attuale fase di ristrutturazione del proprio l'assetto, questa AST necessita, quindi, d'implementare una nuova architettura del sistema privacy, quale modello organizzativo in grado di assicurare la più efficace applicabilità delle disposizioni normative in materia di protezione dei dati; ciò nelle more della completa definizione e realizzazione del predetto processo di riorganizzazione a seguito dell'adozione e conseguente attuazione dell'Atto aziendale.

- Per quanto sopra il Dirigente della proponente U.O.C, sentito il Direttore della UOC Governo clinico e gestione del rischio e il Dirigente della U.O.C Sistema Informativo aziendale, di concerto con il DPO della AST di Ascoli Piceno, ha proceduto alla redazione di un nuovo modello di regolamento per la protezione dei dati personale e relativi allegati, compresa la predisposizione di nuovi modelli ai sensi dell'art.2 - quaterdecies del D.Lgs.n.196/2003 e s.m.i. e dell'art.29 del Regolamento UE 2016/679 per la nomina dei soggetti "designati" ed "autorizzati" al trattamento dei dati personali dell'AST di Ascoli Piceno.

- Ad esito di reiterati scambi di corrispondenza il predetto DPO ASTAP, con nota e-mail del 26/09/2024 e da ultimo con comunicazione del 26/02/2025 (acquisita al protocollo AST con nota prot.n.18154 del 26/02/2025), il DPO della AST di AP ha espresso parere positivo in ordine alla stesura finale del Regolamento per la protezione dei dati della AST comprensivo di tutti gli allegati al presente provvedimento.

- Questa AST, considerata la complessità delle proprie funzioni istituzionali e la necessità di continuare a garantire a tutti i livelli la più efficace applicabilità dei precetti in materia di privacy, ritiene necessario continuare a designare i Responsabili interni del trattamento dei dati personali, conferendo l'incarico di designato ai dirigenti apicali che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti dell'approvando Regolamento e garantisca la tutela dei diritti dell'interessato.

- Pertanto, il Titolare del trattamento - in ragione della complessità ed eterogeneità delle funzioni in capo all'Azienda e dell'esigenza di rendere tempestiva ed efficace la vigilanza sui trattamenti e sulla protezione dei dati a livello di tutte le Unità Operative che la costituiscono - nell'ottica di presidiare il sistema privacy mediante una strutturazione interna articolata sui diversi livelli di responsabilità, ritiene, in conformità al vigente quadro normativo di riferimento, di nominare quali soggetti "Designati" al trattamento dei dati personali i titolari, presso l'Azienda stessa, dei seguenti incarichi:
  - Direttori di Struttura Complessa (ovvero Titolari di incarichi di "sostituzione" nei termini previsti dai CC.NN.LL. delle Aree contrattuali di riferimento);
  - Responsabili di Struttura Semplice Dipartimentale;
  - Altro personale designato ai fini dello svolgimento di funzioni previste da specifiche normative di settore (RSPP, Medico competente, etc.).

- E' opportuno evidenziare che ai professionisti "Designati" al trattamento dei dati personali vengono assegnati da parte del Titolare - in ragione del proprio ruolo di responsabilità organizzativa all'interno dell'Azienda – specifici compiti e funzioni volti ad assicurare la corretta applicazione delle disposizioni in materia di protezione dei dati personali nell'ambito delle strutture rispettivamente dirette, sulla base di

specifiche istruzioni fornite dal Titolare stesso e in coerenza con il quadro disciplinare di cui all'art. 2–quaterdecies del D.Lgs.n.196/2003 e ss.mm.ii., il quale contempla che: *"1. Il titolare o il responsabile possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità*".

- In linea con il quadro normativo vigente in materia, ovvero con le previsioni di cui agli artt.4 n.10) e 29 del GDPR, tutto il Personale a vario titolo in servizio all'interno delle diverse Unità Operative aziendali è "Autorizzato" al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza; ciò sotto la diretta autorità e vigilanza dei soggetti "Designati" al trattamento, attenendosi alle istruzioni impartite ed in conformità all'art.32 comma 4 del GDPR il quale, appunto, prevede che il Titolare del trattamento fa sì che chiunque agisca sotto la sua autorità e abbia accesso a dati personali non li tratti se non è in tal senso istruito dal Titolare medesimo.

- Da ultimo in data 13/02/2025, si è tenuto un incontro con il DPO AST, il Direttore della U.O.C Governo clinico e gestione del rischio e il Dirigente analista della U.O.C SIA nel corso del quale sono state affrontate alcune problematiche connesse all'adozione del nuovo Regolamento aziendale in materia di protezione dei Dati personali.

- Per quanto di riferimento alla policy aziendale ed alle misure di sicurezza tecniche ed organizzative di cui all'art.30 del Regolamento (UE) 2016/679, si precisa che la soppressa ASUR Marche con Determina DG ASUR n.177 del 22/04/2020 aveva adottato il *Regolamento per l'Utilizzo di Strumenti e Servizi IT (Information & Tecnology) all'interno dell'azienda ASUR Marche*. Detta regolamentazione, nelle more dell'adozione di nuova specifica regolamentazione da parte della AST di Ascoli Piceno, è tutt'ora vigente ai sensi di quanto disposto dal punto 18) dell'allegato "A" della DGRM n.1718/2022, secondo cui le AST sono tenute a garantire, nella fase di prima operatività e sino a successive nuove determinazioni in merito da parte del Legale Rappresentante, la validità ed efficacia della normazione interna (Regolamenti, Atti generali, Codici, Accordi sindacali, Circolari e relative disposizioni di attuazione), vigente presso la soppressa Azienda Sanitaria Unica Regionale.

- Con riferimento alle predette misure di sicurezza la AST di Ascoli Piceno, insieme alle altre Aziende Sanitarie Territoriale delle Marche, entro la portata delle risorse esistenti, sta avviando alcune azioni operative prioritarie ed urgenti nell'ambito delle strategie sulla Cybersicurezza presenti nel Piano Regionale. Le attività previste sono finalizzate a:
  - innalzamento del livello di sicurezza generale dell'infrastruttura digitale della sanità regionale a supporto dei DEA di primo e secondo livello;
  - iniziative urgenti di rafforzamento della sicurezza cibernetica dei sistemi a maggior criticità in termini di impatto, diretto o indiretto, sui Dipartimenti di Emergenza e Accettazione, anche al fine di mitigare l'esposizione ai rischi di attacchi cibernetici.

  Il piano va nella direzione del soddisfacimento dei fabbisogni di potenziamento immediato della resilienza cyber delle Aziende sanitarie regionali sede di DEA di primo e secondo livello, utilizzando "tecnologie allo stato dell'arte" ed agendo, al contempo, su tutti i sistemi potenzialmente esposti (*IT, MD, MIoT e OT*) e sui principali processi di *governance*, programmazione e gestione della cybersicurezza che riguardano gli "asset critici" con l'obiettivo di ottenere in tempi rapidi il massimo rapporto costo/efficacia nella riduzione dei rischi cyber, *data protection* e *safety*. Parallelamente al Piano Operativo Regionale, questa Amministrazione sta valutando ulteriori iniziative da attivare al fine di:
  - Implementare misure organizzative e tecniche anche attraverso l'utilizzo di metodologie e tecnologie integrate di sicurezza informatica, in grado di assicurare pratiche di *governance*, conformità normativa, sicurezza e resilienza;
  - Acquistare un servizio di risposta agli incidenti (SOC) che supporti i sistemi IT, IoT, OT e medicali dell'AST AP e di supervisione, monitoraggio e supporto alla realizzazione del complesso delle azioni relative alla sanità digitale.

- In ragione di quanto sopra esposto si ritiene di dover procedere all'adozione del nuovo Regolamento in materia di protezione dei dati personali della AST di Ascoli Piceno anche al fine di garantire il raggiungimento degli obiettivi previsti dalla DGR Marche n.1703/2024 con riferimento al percorso di autorizzazione all'esercizio delle strutture sanitarie, socio-sanitarie e sociali, secondo le indicazioni attuative comunicate dal Direttore generale facente funzione AST e dal Direttore della UOC Governo clinico e gestione del Rischio con rispettive note prot.n.ID.2140111 del 25/02/2025 e prot.ID.n.2140414

del 26/02/2025. Nello specifico la missiva ID.n.2140414/2025 del Direttore della UOC Governo clinico e gestione del Rischio stabilisce l'adozione a cura della U.O.C Affari generali e contenzioso del predetto Regolamento entro il termine del 28/02/2025.

Per tutte le motivazioni sopra precisate si propone al Direttore Generale f.f. della AST di Ascoli Piceno l'adozione della presente proposta di determina:

1. Di approvare il Regolamento Aziendale in materia di Protezione dei Dati Personali della AST di Ascoli Piceno che si allega al presente atto quale sua parte integrante e sostanziale (Allegato n.1) comprensivo degli allegati di seguito indicati:
   - Allegato A) Linee guida per conduzione attività di *Data protection impact*;
   - Allegato B) Politica di protezione dei dati personali;
   - Allegato C) Il Registro delle attività di trattamento;
   - Allegato D) Modulo di richiesta di esercizio dei diritti dell'interessato;
   - Allegato E) Informativa navigatori siti internet aziendali;
   - Allegato F) Informativa utenti ex artt.13-14 Regolamento UE 2016/679;
   - Allegato G) Atto di nomina designato al trattamento con Compiti ed Istruzioni;
   - Allegato H) Atto di nomina autorizzato al trattamento dei dati con Istruzioni;
   - Allegato I) Istruzioni specifiche personale sanitario designati ed autorizzati;
   - Allegato J) Modello nomina Responsabile del trattamento ex Art.28 REG.(UE) 2016/679.

2. Di riservarsi la possibilità di apportare eventuali modifiche/integrazioni al Regolamento in oggetto nonché alla documentazione allo stesso allegata in relazione alle necessità manifestate dal DPO ASTAP in sede di applicazione dello stesso, nonché alla riorganizzazione in atto della AST AP a seguito dell'adozione della proposta di atto aziendale ed alla prossima implementazione del nuovo sito internet aziendale;

3. Di nominare, ai sensi e per gli effetti di cui all'art.2 *quaterdecies* del D.Lgs.n.196/2003 e ss.mm.ii., quali soggetti "Designati" al trattamento dei dati personali dell'Azienda Sanitaria Territoriale Ascoli Piceno, i titolari dei seguenti incarichi:
   - Direttori di Struttura Complessa (ovvero Titolari di incarichi di "sostituzione" nei termini previsti dai CC.NN.LL. delle Aree contrattuali di riferimento);
   - Responsabili di Struttura Semplice Dipartimentale;
   - Altro personale designato ai fini dello svolgimento di funzioni previste da specifiche normative di settore (RSPP, Medico competente, etc.);

4. Di dare atto che, sulla base della previsione normativa di cui al precedente Punto 3) del dispositivo, ai professionisti "Designati" vengono assegnati – in ragione del proprio ruolo di responsabilità organizzativa all'interno dell'Azienda – specifici compiti e funzioni di vigilanza sul rispetto e attuazione delle disposizioni in tema di trattamento di dati personali all'interno delle strutture rispettivamente dirette;

5. Di dare, altresì atto che, in caso di vacanza degli incarichi di cui al precedente Punto 3) del dispositivo e nelle more del relativo conferimento, le correlate responsabilità in tema di protezione dei dati personali sono in capo al Direttore del Dipartimento, ove presente, ovvero al Direttore Sanitario e al Direttore Amministrativo a seconda dello specifico ambito organizzativo;

6. Di trasmettere, per il tramite dell'Ufficio determine presso la Direzione Generale AST, il presente atto a ciascun "Designato" al trattamento dei dati personali, unitamente alle relative istruzioni fornite dal Titolare cui i "Designati" medesimi sono tenuti ad attenersi nell'effettuare le attività di trattamento rientranti nelle rispettive funzioni istituzionali e che si allegano alla presente determina (Allegato G);

7. Di dare atto che, in linea con le previsioni di cui agli artt.4 n.10) e 29 del GDPR, tutto il Personale in servizio all'interno delle diverse Unità Operative aziendali è "Autorizzato" al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza; ciò sotto la diretta autorità e vigilanza da parte dei soggetti "Designati" al trattamento e attenendosi alle istruzioni allegate alla presente determina (Allegato H), fatte salve le responsabilità di natura personale correlate all'autonomia professionale di specifiche categorie di professionisti;

8. Di approvare - ad integrazione dei contenuti delle istruzioni di cui ai precedenti punti 6 e 7 – le istruzioni specifiche per il trattamento dati da parte del personale sanitario, destinate sia ai "Designati" che a tutti gli "Autorizzati" al trattamento, che si allegano alla presente determina (Allegato I);

9. Di dare atto che, fino alla completa implementazione e messa a regime del Regolamento in parola e della relativa modulistica, permangono in vigore le nomine dei designati ed autorizzati effettuate ai sensi della previgente regolamentazione e modulistica in uso.

10. Di dare mandato alla U.O.C Gestione risorse umane di provvedere tempestivamente a formale comunicazione al RPD in ordine al vigente assetto degli incarichi di cui al precedente punto 3) del dispositivo, nonché al relativo aggiornamento, onde consentire allo stesso RPD l'espletamento degli adempimenti in tema di protezione dei dati personali;

11. Di dare mandato ai professionisti "Designati" al trattamento di produrre – secondo modalità da comunicarsi a cura del RPD - apposita attestazione comprovante l'avvenuta comunicazione dei contenuti del presente atto al Personale in servizio che effettua trattamenti di dati personali presso le Unità Operative rispettivamente dirette, ciò al fine di rendere edotti i medesimi in merito al contesto di riferimento ed alle richiamate specifiche istruzioni;

12. Di dare mandato alla U.O.C Gestione Risorse Umane di provvedere - in sede di conferimento di incarichi di direzione/responsabilità di struttura complessa ovvero di struttura semplice dipartimentale - all'inserimento di specifica clausola contrattuale ove il professionista venga nominato quale soggetto "Designato" al trattamento dei dati per la rispettiva Struttura, fornendo al medesimo le relative istruzioni di cui all'Allegato G ed anche all'Allegato I (solo per i professionisti sanitari);

13. Di dare, altresì, mandato alle suddette Strutture competenti in materia di gestione delle risorse umane di provvedere - in sede di assunzione in servizio di nuove unità di Personale - all'inserimento di specifica clausola contrattuale contenente la nomina del neo assunto quale soggetto "Autorizzato" al trattamento, fornendo allo stesso le relative istruzioni di cui all'Allegato H e anche all'Allegato I (solo per i professionisti/operatori sanitari);

14. Di dare mandato alla U.O.C Formazione ovvero alla U.O.C Direzione Medica di Presidio in relazione all'attuale riparto funzionale nell'ambito dell'assetto organizzativo della AST, di provvedere - in sede di autorizzazione alla frequenza delle strutture aziendali da parte di volontari, tirocinanti, studenti e specializzandi - all'inserimento di specifica clausola contenente la nomina delle predette figure in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato H e anche all'Allegato I (solo per i frequentatori di strutture/servizi sanitari);

15. Di dare mandato alla U.O.C. D.A.T di provvedere, in sede di reclutamento di personale convenzionato (Medici dell'Emergenza Sanitaria Territoriale, Medici Specialisti Ambulatoriali e Medici del Ruolo Unico di Assistenza Primaria a Rapporto Orario), all'inserimento di specifica clausola contenente la nomina dei predetti professionisti in qualità di "Autorizzati" al trattamento, fornendo loro le relative istruzioni di cui all'Allegato H e all'Allegato I;

16. Di dare atto che con successivo provvedimento la Direzione generale AST procederà alla costituzione del c.d. Gruppo multidisciplinare di supporto al DPO ai sensi dell'art.29 dell'approvando Regolamento aziendale in materia di protezione dei dati personali;

17. Di dare mandato alla U.O.C. SIA di procedere entro 60 (sessanta) giorni dall'adozione del presente atto alla predisposizione di nuova regolamentazione AST per l'Utilizzo di Strumenti e Servizi IT (Information & Tecnology), fermo restando, nelle more di quanto sopra, la piena operatività del Regolamento approvato dalla soppressa ASUR Marche, ai sensi della DGR Marche n.1718/2022.

18. Di dare mandato alla U.O.C SIA di verificare la possibilità di acquisire ai sensi della vigente normativa apposito applicativo al fine di consentire, in un'ottica di efficienza ed efficacia, la gestione dinamica del Registro del trattamento dei dati;

19. Di dare che dal presenta atto non derivano oneri economici a carico del bilancio della AST di Ascoli Piceno;

20. Di dare atto che la presente determina non è sottoposta a controllo ai sensi dell'art.4 della Legge 412/91 e dell'art.39 della L.R.n.19/2022;

21. Di dare atto che, a norma dell'art.39, comma 8, della L.R. 19/2022, la presente determina è efficace dalla data di pubblicazione all'Albo on line aziendale.

Si attesta l'avvenuta verifica circa l'insussistenza di situazioni, anche potenziali, di conflitto di interessi ai sensi dell'art.6-*bis* della L.n.241/1990 e ss.mm.ii.
Si richiede la pubblicazione all'*Albo on line*:
[x] INTEGRALE

Il Funzionario Istruttore
(Dott. Marco Tempera)

ATTESTAZIONE DEL DIRIGENTE UOC Affari Generali e contenzioso AST
Il Dirigente della U.O.C. proponente condivide in fatto e in diritto il documento istruttorio e attesta che dalla presente determina non derivano spese a carico del bilancio della AST di Ascoli Piceno.

Il Dirigente U.O.C. Affari Generali e contenzioso
(Dott. Silvio Maria Liberati)

Documento informatico firmato digitalmente

ALLEGATI

Allegato n.1 – "*Regolamento della protezione dei dati personali*" comprensivo dei seguenti allegati:

- Allegato A) Linee guida per conduzione attività di *Data protection impact*;
- Allegato B) Politica di protezione dei dati personali;
- Allegato C) Il Registro delle attività di trattamento;
- Allegato D) Modulo di richiesta di esercizio dei diritti dell'interessato;
- Allegato E) Informativa navigatori siti internet aziendali;
- Allegato F) Informativa utenti ex artt.13-14 Regolamento UE 2016/679;
- Allegato G) Atto di nomina designato al trattamento con Compiti ed Istruzioni;
- Allegato H) Atto di nomina autorizzato al trattamento dei dati con Istruzioni;
- Allegato I) Istruzioni specifiche personale sanitario designati ed autorizzati;
- Allegato J) Modello nomina Responsabile del trattamento ex Art.28 REG.(UE) 2016/679

Allegato 1)

ASCOLI PICENO
MARCHE

REGOLAMENTO AZIENDALE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

INDICE

PREMESSA

A - DISCIPLINA QUADRO

- Il Regolamento Europeo 2016/679 "Regolamento Generale sulla Protezione dei dati relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE" - d'ora innanzi denominato "GDPR" rivisita completamente la prospettiva della disciplina sulla privacy, istituendo un quadro normativo incentrato sui doveri e la responsabilizzazione del Titolare del trattamento (principio di "accountability"). La nuova disciplina impone a tale soggetto di garantire il rispetto dei principi in essa contenuti e al contempo di essere in grado di comprovarlo; ciò adottando una serie di strumenti che lo stesso GDPR indica, partendo da un'attenta valutazione di rischi e impatti e con una pianificazione di attività tali da poter incidere significativamente sotto il profilo culturale, organizzativo e tecnologico.
  Con il D.Lgs.n.101 del 10 agosto 2018, il Legislatore ha modificato la normativa nazionale rappresentata dal Decreto Legislativo n.196/2003 (Codice in materia di protezione dei dati) adeguando le parti incompatibili o contrastanti con il GDPR.
- In particolare, l'art.2 quaterdecies del D.Lgs.n.196/2003, introdotto dal D.Lgs.n.101/2018, conferisce ai titolari e responsabili del trattamento la possibilità di prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità; da ciò discende la necessità, soprattutto per sistemi complessi quali le Aziende Sanitarie ed Ospedaliere, di strutturare un'articolata architettura in grado di definire i rispettivi ruoli di professionisti e operatori.
- All'interno di tale contesto, quindi, il presente Regolamento costituisce lo strumento attraverso il quale l'AST di Ascoli Piceno rappresenta il proprio modello organizzativo e gestionale per il trattamento dei dati personali in linea ed in costante adeguamento rispetto al quadro normativo sopra richiamato.

B-PRINCIPALE NORMATIVA E ATTI DI RIFERIMENTO

- Legge n. 241/1990 e ss.mm.ii. "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi" e ss.mm.ii;

- D.Lgs.n.196/2003 "Codice in materia di protezione dei dati personali", integrato con le modifiche introdotte dal D.Lgs. n. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";

- D.Lgs.82/2005 e ss.mm.ii. "Codice dell'Amministrazione Digitale";

- Deliberazione del Garante per la protezione dei dati personali n. 243 del 14/06/2007 "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico";

- Provvedimento del Garante per la protezione dei dati personali del 27/11/2008, modificato con Provvedimento del 25/06/2009 "Misure e accorgimenti prescritti ai titolari

dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";

- Deliberazione del Garante per la protezione dei dati personali n. 36 del 19/11/2009 "Linee guida in tema di referti on-line – 19 novembre 2009";

- D.L. n. 179/2012, art. 12, comma 5 "Ulteriori misure urgenti per la crescita del paese";

- D.Lgs. n. 33/2013 e ss.mm.ii. "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle publiche amministrazioni";

- DPCM dell'08/08/2013 "Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali";

- Deliberazione del Garante per la protezione dei dati personali n. 243 del 15/05/2014 "Linee guida del Garante per la Protezione dei Dati Personali in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri Enti obbligati";

- Deliberazione del Garante per la protezione dei dati personali n. 331 del 04/06/2015 "Linee Guida in materia di Dossier Sanitario";

- Provvedimento del Garante per la protezione dei dati personali n. 393 del 02/07/2015 "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche";

- DPCM n.178 del 29/09/2015 "Regolamento in materia di fascicolo sanitario elettronico";

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46 CE (regolamento generale sulla protezione dei dati);

- Provvedimento del Garante per la protezione dei dati personali n. 512 del 19/12/2018 "Regole deontologiche relative al trattamento di dati personali effettuati per svolgere investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria pubblicate ai sensi dell'art.20, comma 4, del d.lgs. 10 agosto 2018, n. 101";

- Provvedimento del Garante per la protezione dei dati personali n.55 del 07/03/2019 "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario";

- Provvedimento del Garante per la protezione dei dati personali n.146 del 05/06/2019 "Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, del d.lgs. 10 agosto 2018 n. 101";

- D.L.n.34/2020 "Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19";

- Decreto del Dirigente del Servizio Sanità della Regione Marche n. 6 del 22/03/2021 "Art. 11 D.L. 19.05.2020 n.34 – Misure urgenti in materia di Fascicolo Sanitario Elettronico – Aggiornamento modulistica";

- Provvedimento del Garante per la protezione dei dati personali n. 186 del 29/04/2021 "Documento di indirizzo su designazione, posizione e compiti del Responsabile della protezione dei dati (RPD) in ambito pubblico";

- Determina DG ASUR n.177 del 22/04/2020 "*Regolamento per l'Utilizzo di Strumenti e Servizi IT (Information & Tecnology) all'interno dell'azienda ASUR Marche*".

C-DEFINIZIONI

Si richiamano, di seguito, alcune delle definizioni contenute nell'art. 4 del GDPR:
«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;
«limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
«profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;
«pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile; - «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;
«titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
«responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;
«destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è

conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
«terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;
«consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;
«violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
«dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;
«dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;
«dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
«autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art.51 del GDPR.

TITOLO I- IL TRATTAMENTO DEI DATI PERSONALI

Art.1- Oggetto ed ambito di applicazione

1. Il presente Regolamento disciplina il sistema di gestione dei dati personali all'interno dell'Azienda, nel rispetto di quanto previsto dal GDPR e dal quadro normativo nazionale di riferimento in tema di protezione dei dati personali.
2. La protezione delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale riconosciuto dalla Unione Europea e a tal fine l'Azienda mette in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato conformemente alla normativa vigente, tenuto conto della relativa natura, ambito di applicazione, contesto e finalità di trattamento e possibile rischio di lesione dei diritti e delle libertà degli interessati.
3. Il trattamento dei dati personali - nell'ambito di ogni articolazione organizzativa dell'Azienda - viene effettuato garantendo a chiunque il rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati stessi.

Art 2- Principi applicabili al trattamento dei dati personali

1. Al trattamento dei dati personali si applicano i principi di cui all'art.5 del GDPR. Ai sensi del citato art.5 del GDPR, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità («limitazione della finalità»);
c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);
d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);
f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).
2. Il Titolare del trattamento, attraverso la complessiva struttura organizzativa aziendale, è competente in ordine al rispetto e all'applicazione dei citati principi ed in grado di comprovarlo verso l'esterno («responsabilizzazione»).

Art.3 – Base giuridica del trattamento

a) Le condizioni di liceità - in presenza delle quali si effettuano operazioni di trattamento di dati personali – sono quelle indicate all'art.6 del GDPR, come di seguito riportate: l'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del Titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'Interessato è un minore. Tale condizione non si applica al trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Art. 4 – Categorie di dati personali

1. Ai sensi di quanto previsto all'art.4 del GDPR, l'Azienda effettua il trattamento dei soli dati necessari rispetto alle finalità per le quali vengono raccolti o trattati, tra cui:
   - dati personali comuni, quali nome, cognome, residenza, cittadinanza, recapito telefonico, codice fiscale;
   - categorie particolari di dati personali (art.9 del GDPR);

- dati economici, quali retribuzione, compensi, benefici, agevolazioni;
- dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza (art. 10 del GDPR);
- dati sanitari (art.9, par. 2, lett. h e par.3; C.53), (art.9, par. 2, lett. i; C54)

2. I dati personali trattati dall'Azienda, nelle forme e nei limiti di quanto previsto dalla vigente normativa, sono raccolti:
   - prioritariamente presso l'Interessato o anche presso persone diverse nei casi in cui questi sia minorenne o incapace o non sia in grado di fornirli;
   - presso enti del SSN, presso altri enti e amministrazioni pubbliche o terzi, presso pubblici registri o presso altri esercenti le professioni sanitarie.

Art.5 – Categorie di soggetti interessati

1. Per soggetto interessato è da intendersi la persona fisica cui i dati trattati si riferiscono.
2. L'Azienda tratta i dati personali relativi, principalmente, a:
   - utenti, assistiti, pazienti e loro familiari e/o accompagnatori;
   - personale sanitario, amministrativo, tecnico e professionale, con rapporto di dipendenza, consulenza o collaborazione;
   - soggetti che per motivi di studio, tirocinio, stage o volontariato frequentano le strutture aziendali, quali specializzandi, studenti, tirocinanti, volontari;
   - soggetti che intrattengono rapporti contrattuali con l'Azienda stessa ai fini della fornitura di beni e servizi, attività di assistenza o consulenza, esecuzione di opere edilizie, interventi di manutenzione su software o dispositivi medici o altre prestazioni;
   - soggetti e imprese partecipanti a bandi di gara o di pubblico concorso.

Art.6 – Categorie di trattamenti

1. In conformità all'art.4, n.2) del GDPR, per trattamento si intende qualunque operazione, o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicati a dati personali o insiemi di dati personali, quali:
   - la raccolta dei dati;
   - la registrazione dei dati, ovvero il loro inserimento su supporti, automatizzati o manuali, al fine di rendere i dati disponibili per successivi trattamenti;
   - l'organizzazione dei dati, cioè il processo di lavorazione finalizzato a favorirne la fruibilità attraverso l'aggregazione, la disaggregazione, l'accorpamento, la catalogazione;
   - la conservazione dei dati;
   - l'adattamento o la modifica in relazione a variazioni o a nuove acquisizioni;
   - l'estrazione;
   - la consultazione;
   - l'uso;
   - la comunicazione dei dati mediante trasmissione ad uno o più soggetti determinati, in qualunque forma, anche mediante messa a disposizione o consultazione; la comunicazione dei dati avviene solo nei casi previsti da norme di legge o regolamento;
   - la comunicazione dei dati mediante diffusione, ovvero il dare conoscenza dei dati personali a soggetti indeterminati;
   - la limitazione, cioè il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;
   - la cancellazione;

- la distruzione.

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

Art.7 - Finalità del trattamento

1. Il trattamento di dati personali effettuato dall'Azienda è finalizzato principalmente:
   - allo svolgimento dei compiti del Servizio Sanitario Nazionale di rilevante interesse pubblico e all'espletamento delle funzioni istituzionali previste dalla normativa vigente;
   - all'erogazione di prestazioni sanitarie specialistiche (comprensive di tutte le necessarie attività di supporto) volte alla tutela della salute e dell'incolumità fisica degli utenti, di terzi e della collettività;
   - allo svolgimento di attività di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria;
   - allo svolgimento di attività amministrative connesse e correlate all'erogazione di prestazioni sanitarie;
   - all'esecuzione di adempimenti amministrativi, gestionali e contabili connessi e correlati alle proprie funzioni istituzionali delle Aziende e/o ad obblighi di legge;
   - alla tutela della sicurezza e della salute dei lavoratori e sorveglianza igienico sanitaria delle proprie strutture;
   - alla gestione delle proprie risorse umane, tecnologiche, strumentali e patrimoniali;
   - medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali ("finalità di cura") sulla base del diritto dell'Unione/Stati membri o conformemente al contratto con un professionista della sanità, effettuati da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona anch'essa soggetta all'obbligo di segretezza (art. 9, par. 2, lett. h e par. 3; C.53).

Art. 8 - Categorie particolari di dati personali

1. L'attività dell'Azienda nell'ambito dell'assistenza sanitaria comporta il trattamento di dati personali appartenenti alle categorie particolari di cui all'art.9 del GDPR, tra cui dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, dati che rivelino l'origine razziale o etnica, le convinzioni religiose o l'appartenenza sindacale, dati genetici. Il trattamento di tali categorie di dati è consentito qualora si verifichi uno dei casi indicati al paragrafo 2 del citato art. 9 del GDPR, qui di seguito richiamati:
   a) l'Interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche [...];
   b) il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'Interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale [...];
   c) il trattamento è necessario per tutelare un interesse vitale dell'Interessato o di un'altra persona fisica qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali […];
e) il trattamento riguarda dati personali resi manifestamente pubblici dall'Interessato;
f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale;
i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato.

2. In conformità a quanto previsto dall'art. 2-sexies, comma 1, del D.Lgs.n.196/2003 e s.m.i., i trattamenti delle categorie particolari di dati personali, necessari per motivi di interesse pubblico rilevante ai sensi dell'art.9, paragrafo 2, lettera g) del GDPR, sono ammessi qualora siano previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'Interessato. Il citato articolo individua, altresì, i motivi di interesse pubblico rilevante che consentono il trattamento di categorie particolari di dati personali.
3. I dati rientranti nelle categorie particolari sono trattati dall'Azienda qualora essenziali e necessari allo svolgimento delle attività istituzionali ad essa assegnate e nel caso in cui tali attività non possano essere eseguite mediante il trattamento di dati anonimi o di dati personali di diversa natura.

Art.9 - Il trattamento dei dati dei lavoratori

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

a) per adempiere a specifici obblighi previsti da leggi, regolamenti o contratti collettivi ai fini dell'instaurazione, gestione ed estinzione del rapporto di lavoro, nonché ai fini del riconoscimento di agevolazioni ovvero dell'erogazione di contributi, dell'applicazione della normativa in materia di previdenza, di igiene e sicurezza del lavoro, nonché in materia fiscale e sindacale;
b) anche fuori dei casi di cui alla lettera a) - in conformità alla legge e per scopi determinati e legittimi - ai fini della tenuta della contabilità o della corresponsione di stipendi, assegni, premi, altri emolumenti o benefici accessori;
c) per perseguire finalità di salvaguardia della vita o dell'incolumità fisica del lavoratore o di un terzo;
d) per far valere o difendere un diritto, anche da parte di un terzo, in sede giudiziaria, nonché in sede amministrativa o nelle procedure di arbitrato e di conciliazione, nei casi previsti dalle leggi, dalla normativa dell'Unione europea, dai regolamenti o dai contratti collettivi, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
e) per adempiere ad obblighi derivanti da contratti di assicurazione finalizzati alla copertura dei rischi connessi alla responsabilità del datore di lavoro in materia di salute e sicurezza del lavoro e di malattie professionali o per i danni cagionati a terzi nell'esercizio dell'attività lavorativa o professionale;
f) per garantire le pari opportunità nel lavoro;
g) per perseguire scopi determinati e legittimi individuati dagli statuti di associazioni, organizzazioni, federazioni o confederazioni rappresentative di categorie di datori di lavoro o dai contratti collettivi, in materia di assistenza sindacale ai datori di lavoro. L'Azienda adotta adeguate misure nel trattamento dei dati personali dei dipendenti idonei a rivelare lo stato di salute, le abitudini sessuali, l'origine razziale ed etnica, le convinzioni politiche o d'altro genere.

3. I dati che rivelano le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni od organizzazioni a carattere religioso o filosofico sono trattati esclusivamente in caso di fruizione di permessi in occasione di festività religiose o, nei casi previsti dalla legge, per l'esercizio dell'obiezione di coscienza.
4. I dati che rivelano le opinioni politiche o l'appartenenza sindacale, o l'esercizio di funzioni pubbliche e incarichi politici, di attività o di incarichi sindacali sono trattati esclusivamente ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o dai contratti collettivi anche aziendali, nonché per consentire l'esercizio dei diritti sindacali compreso il trattamento dei dati inerenti alle trattenute per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali.

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

Art.10 - Periodo di conservazione dei dati personali

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

- smaltire gli apparati hardware o supporti rimovibili di memoria con modalità che non rendano possibile accedere ad alcun dato personale di cui è titolare l'Azienda stessa;
- procedere al riutilizzo degli apparati di memoria o hardware con modalità tali da garantire che non sia possibile accedere ad alcun dato personale.

Art.11 - Categorie di destinatari

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

Art.12 - Comunicazione dei dati all'interessato

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

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

1. L'Azienda applica le disposizioni ed i principi di cui all'art.59 del D.Lgs.196/2003 e ss.mm.ii. in materia di accesso a documenti amministrativi contenenti dati personali disciplinato dalla Legge n.241/90 e s.m.i. e di accesso civico (semplice e generalizzato) disciplinato dal D. Lgs. 33/2013 e s.m.i.
2. In osservanza delle richiamate disposizioni l'Azienda valuta caso per caso, anche con riguardo ad altre regolamentazioni specifiche, la possibilità da parte di terzi di accedere ai documenti contenenti dati di cui agli artt.9 e 10 del GDPR.
3. Ai sensi dell'art.60 del D. Lgs. 196/2003 e ss.mm.ii., qualora il trattamento concerna dati genetici, relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'Interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale.

Art.14 - Accesso alle cartelle cliniche

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

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

Art.15 - Certificato di assistenza al parto

1. Ai fini della dichiarazione di nascita, il certificato di assistenza al parto è sempre sostituito da una semplice attestazione contenente i soli dati richiesti nei registri di nascita.
2. In caso di madre che abbia dichiarato di non voler essere nominata si applicano le disposizioni di cui all'art.93, commi 2 e 3, del D.Lgs.196/2003 e ss.mm.ii., ovvero:
   - il certificato di assistenza al parto o la cartella clinica, ove comprensivi dei dati personali che rendano identificabile la madre che abbia dichiarato di non voler essere nominata, possono essere rilasciati in copia integrale a chi vi abbia interesse, in conformità alla legge, decorsi cento anni dalla formazione del documento;
   - durante il periodo di cui al precedente punto, la richiesta di accesso al certificato o alla cartella può essere accolta relativamente ai dati della madre che abbia dichiarato di non voler essere nominata, osservando le opportune cautele per evitare che quest'ultima sia identificabile.

Art.16 – Fascicolo Sanitario Elettronico Regionale (FSE)

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

Art.17 – Dossier Sanitario

1. Il Dossier Sanitario è l'insieme dei dati personali generati da eventi clinici presenti e trascorsi originati all'interno dell'Azienda riguardanti l'interessato, che vengono condivisi tra i professionisti sanitari che lo assistono presso un´unica struttura sanitaria (ad es. ospedale, casa di cura privata, prestazioni di laboratorio, visite ambulatoriali, accessi al Pronto Soccorso, ricoveri, ecc..).
2. Il Dossier Sanitario persegue la finalità di rendere più efficienti i processi di diagnosi e cura del paziente erogati dall'Azienda stessa, consentendo ai diversi professionisti che vi operano di accedere a tutte le informazioni cliniche relative ai precedenti eventi clinici.
3. Il Dossier Sanitario può essere attivato unicamente previa acquisizione del consenso del paziente, raccolto dall'operatore sanitario che ne effettua il primo trattamento. Il mancato consenso al trattamento mediante Dossier Sanitario in ogni caso non incide sulla possibilità di accedere alle prestazioni di cura richieste.
4. Al Dossier Sanitario può accedere, in forma protetta e riservata, solamente personale sanitario, autorizzato al trattamento, che svolga la propria attività presso le strutture dell'Azienda e sia a vario titolo direttamente coinvolto nel percorso di cura del paziente.
5. Il Dossier Sanitario consente ai professionisti che prendono in cura il paziente di disporre di un quadro di informazioni e dati sanitari al fine di fornire un livello di assistenza il più completo e adeguato possibile.

Art.18 – Videosorveglianza

1. L'installazione di sistemi di videosorveglianza è autorizzata dall'Azienda nel rispetto delle disposizioni vigenti in materia, solo quando ciò sia strettamente indispensabile per garantire la sicurezza di dipendenti, pazienti e la tutela del patrimonio aziendale e per assicurare il monitoraggio di determinate categorie di pazienti che necessitano di continuo controllo delle condizioni di salute.
2. Il trattamento dei dati personali effettuato tramite sistemi di videosorveglianza avviene nel rispetto della dignità e dell'immagine delle persone, delle norme a tutela dei lavoratori (art.4, Legge n.300/1970 e ss.mm.ii.) e dei Provvedimenti adottati in materia dall'Autorità Garante per la protezione dei dati personali.

TITOLO II - I SOGGETTI DEL TRATTAMENTO

Art.19- Il Titolare del trattamento

1. Il Titolare del trattamento, nella persona del Legale rappresentante pro - tempore dell'Azienda, è definito all'art.4 del GDPR come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali", e, "quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".
2. Al Titolare competono, anche unitamente ad altro Titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza.
3. Il Titolare è il soggetto su cui grava la responsabilità generale del trattamento, adempie alle prescrizioni contenute nelle varie disposizioni del GDPR e dimostra che il trattamento

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

4. Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, quali la pseudonimizzazione e la cifratura dei dati personali, la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati.
5. Gli artt.24 e 25 del GDPR individuano gli obblighi generali in capo al Titolare del trattamento, mentre obblighi specifici sono contenuti in varie altre disposizioni del GDPR stesso. In particolare, il Titolare:
   - designa il Responsabile della protezione dei dati di cui all'art. 37 del GDPR;
   - nomina con proprio atto i responsabili del trattamento dei dati personali di cui all'art.28 del GDPR impartendo agli stessi - per la corretta gestione e tutela dei dati personali - i compiti e le necessarie istruzioni in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, all'esercizio dei diritti dell'interessato di cui al Capo III del GDPR;
   - attribuisce, nell'ambito dell'assetto organizzativo aziendale, specifici compiti e funzioni connessi al trattamento dei dati ai soggetti designati secondo quanto previsto dall'art. 2-quaterdecies, comma 1, del D. Lgs. 196/2003 e ss.mm.ii.;
   - individua le modalità più opportune per autorizzare al trattamento dei dati le persone che operano sotto la propria diretta autorità, ai sensi dell'art. 2-quaterdecies, comma 2, del D. Lgs. 196/2003 e ss.mm.ii.;
   - tiene il registro delle attività di trattamento svolte sotto la propria responsabilità secondo quanto previsto dall'art.30 del GDPR;
   - in caso di violazione dei dati personali provvede alla notifica al Garante per la protezione dei dati personali senza ingiustificato ritardo secondo le modalità e i contenuti di cui all'art.33 del GDPR;
   - svolge, nei casi previsti dall'art. 35 del GDPR, una valutazione d'impatto sulla protezione dei dati consultandosi con il Responsabile della protezione dei dati e procede, qualora necessario, alla consultazione preventiva di cui all'art. 36 del GDPR.
6. Il Titolare può dimostrare il rispetto degli obblighi a suo carico anche attraverso l'adesione a codici di condotta o a meccanismi di certificazione di cui agli artt.40 e 42 del GDPR.
7. Il Titolare del trattamento adotta misure tecniche ed organizzative adeguate onde perseguire le seguenti finalità:
   - garantire, ed essere al contempo in grado di dimostrare, che il trattamento è effettuato in conformità al GDPR; ciò comportando l'attuazione di adeguate politiche in materia di protezione dei dati;
   - proteggere i dati fin dalla fase di ideazione e progettazione del trattamento o di un sistema e nel corso del trattamento stesso (c.d. "Privacy by design"), ad esempio mediante tecniche di pseudonimizzazione (art.25 del GDPR);
   - assicurare che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni singola finalità del trattamento (c.d. "Privacy by default") rendendo inaccessibili i dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica, e ciò con riferimento alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione ed all'accessibilità (art.25 del GDPR).
8. Nell'individuazione delle misure tecniche ed organizzative adeguate, il Titolare del trattamento tiene conto dei seguenti elementi:

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

Art.20 - Contitolari del trattamento

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

Art.21 - Interessato e soggetti terzi

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

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

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

organizzative adeguate in modo tale che il trattamento soddisfi i requisiti di legge e garantisca la tutela dei diritti dell'Interessato.

4. L'atto di designazione viene predisposto secondo schema tipo redatto in conformità alle disposizioni di cui all'art.28 del GDPR.
5. Tale atto di designazione/contratto - stipulato in formato elettronico - vincola il Responsabile al Titolare del trattamento in particolar modo per quanto riguarda la durata, la natura, la finalità del trattamento, il tipo di dati trattati, le categorie di interessati, gli obblighi ed i diritti del Titolare del trattamento.
6. Nel caso in cui il Responsabile del trattamento ricorra, previa specifica autorizzazione, ad un Sub – Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto dell'Azienda, a tale Sub – Responsabile sono imposti, mediante un contratto, gli stessi obblighi a cui è stato sottoposto il Responsabile. Qualora il Sub - Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile del trattamento conserva nei confronti dell'Azienda l'intera responsabilità dell'adempimento degli obblighi del Sub– Responsabile.
7. Nel rispetto delle istruzioni operative impartire dal Titolare, spetta al Direttore/Dirigente Responsabile del procedimento di acquisizione di determinato servizio curare l'istruttoria finalizzata alla formalizzazione dell'atto di designazione del soggetto esterno in qualità di Responsabile del trattamento; ciò avvalendosi anche del supporto consulenziale del Responsabile della protezione dei dati.
8. Il Titolare del trattamento può delegare il Direttore/Dirigente Responsabile del procedimento alla nomina del Responsabile del trattamento ex art.28 del GDPR.

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

1. L'art. 2-quaterdecies, comma 1, del D. Lgs. 196/2003 e ss.mm.ii. conferisce al Titolare del trattamento la possibilità di prevedere che – nell'ambito del proprio assetto organizzativo - specifici compiti e funzioni connesse al trattamento dei dati personali siano attribuiti a persone fisiche espressamente designate operanti sotto la sua autorità.
2. Ai sensi del richiamato art.2-quaterdecies, comma 1, del D. Lgs. 196/2003 e ss.mm.ii., l'Azienda, in considerazione della complessità e dell'eterogeneità delle proprie attività e compiti istituzionali e della necessità di assicurare nei diversi livelli la più efficace applicabilità delle disposizioni in materia di protezione dei dati personali, tenuto conto altresì delle disposizioni di natura organizzativa e gestionale e dei relativi provvedimenti attuativi, designa quali Responsabili "interni" del trattamento i titolari dei seguenti incarichi:
    - Direttori di Struttura Complessa (ovvero Titolari di incarichi di "sostituzione" nei termini previsti dai CC.NN.LL. delle Aree contrattuali di riferimento)
    - Responsabili di Struttura Semplice Dipartimentale;
    - Altro personale dirigenziale assegnato allo svolgimento di funzioni previste da specifiche normative di settore (RSPP, Medico competente, etc.)

   ciascuno in riferimento ai trattamenti rientranti nell'espletamento delle funzioni/attività istituzionali e gestionali assegnate in ragione delle specifiche competenze, professionalità e responsabilità.
3. I soggetti designati in qualità di Responsabili "interni" del trattamento, in ragione dell'incarico ricoperto all'interno dell'Azienda, svolgono compiti e funzioni di vigilanza sul rispetto e attuazione delle istruzioni privacy da parte del personale autorizzato al trattamento di dati personali in servizio presso le strutture rispettivamente dirette.
4. I soggetti designati in qualità di Responsabili "interni" del trattamento sono nominati con determina del Direttore Generale – oggetto di periodico aggiornamento - e

nell'effettuare i compiti di cui al comma 3 del presente articolo si attengono – a loro volta – alle specifiche istruzioni loro fornite dal Titolare del trattamento. In caso di vacanza della titolarità degli incarichi di cui al precedente comma 2 e nelle more del relativo conferimento (anche interno), le correlate responsabilità gestionali in tema di applicazione delle misure privacy sono in capo al Direttore del Dipartimento, ove presente, ovvero al Direttore Sanitario e al Direttore Amministrativo a seconda dello specifico ambito organizzativo.

5. La U.O.C Gestione Risorse Umane - in sede di conferimento di nuovi incarichi di direzione/responsabilità di struttura complessa ovvero di struttura semplice dipartimentale - provvede all'inserimento di specifica clausola contrattuale contenente la designazione del titolare di incarico in qualità di Responsabile "interno" del trattamento e fornendo al medesimo le relative istruzioni.

Art.24 – Gli Autorizzati al trattamento

1. Ai sensi dell'art. 2-quaterdecies, comma 2, del D. Lgs. 196/2003 e ss.mm.ii. e dell'art. 29 del GDPR, tutto il Personale in servizio a diverso titolo all'interno delle Unità Operative aziendali è autorizzato – sulla base della determina del Direttore Generale dell'Azienda di approvazione del presente documento – al trattamento dei dati personali nell'ambito dello svolgimento delle attività istituzionali presso le strutture di rispettiva afferenza.
2. Gli Autorizzati si attengono con scrupolo e diligenza alle istruzioni impartite dal Titolare e loro fornite dal designato in qualità di Responsabile "interno" del trattamento della struttura di appartenenza, il quale deve garantirne il rispetto e l'attuazione attraverso attività di vigilanza.
3. La UOC Gestione Risorse Umane - in sede di assunzione in servizio di nuove unità di Personale – provvede all'inserimento di specifica clausola contrattuale contenente l'autorizzazione del neo assunto ad effettuare il trattamento di dati personali nell'ambito dello svolgimento delle proprie attività istituzionali e fornendo contestualmente le relative istruzioni sulla cui osservanza e rispetto è tenuto, appunto, a vigilare il designato in qualità di Responsabile "interno" del trattamento della rispettiva struttura. In analogia con quanto sopra procederà U.O.C. D.A.T in sede di reclutamento di personale convenzionato;
4. Sono, altresì, Autorizzati al trattamento soggetti quali volontari, tirocinanti, studenti, specializzandi che prestino la loro opera, anche in via temporanea, all'interno delle strutture dell'Azienda in attività comportanti il trattamento di dati personali dell'Azienda stessa.
5. Sempre in analogia alle modalità previste al comma 3 del presente articolo, la U.O.C alla UOC Formazione ovvero alla UOC Direzione Medica di Presidio in relazione all'attuale riparto funzionale nell'ambito dell'assetto organizzativo della AST - in sede di autorizzazione alla frequenza delle strutture aziendali da parte di volontari, tirocinanti, studenti e specializzandi – provvedono all'inserimento di specifica clausola contenente l'autorizzazione delle predette figure ad effettuare il trattamento di dati personali nell'ambito della frequenza delle strutture aziendali e fornendo, parimenti, le relative istruzioni sulla cui osservanza e rispetto è tenuto a vigilare il designato in qualità di Responsabile "interno" del trattamento della rispettiva struttura.

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

1. Il GDPR, ai sensi dell'art.37, comma 1, lett.a), prevede l'obbligo per il Titolare del trattamento di designare il Responsabile della protezione dei dati "quando il trattamento

è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali".

2. Al fine di dare attuazione alle disposizioni di cui al GDPR onde assicurare lo svolgimento delle funzioni e dei compiti stabiliti dagli artt.38 e 39, l'Azienda – con apposito atto pubblicato sul sito web istituzionale - ha individuato i recapiti del Responsabile della protezione dei dati.
3. Il Responsabile della protezione dei dati costituisce il punto di contatto tra il Titolare che lo ha designato e l'Autorità Garante Privacy, con la quale deve cooperare per tutte le questioni connesse al trattamento dei dati personali, consultandola anche preventivamente quando necessario.
4. Il Responsabile della protezione dei dati, comunque tenuto al rispetto delle norme in materia di segreto o riservatezza, deve in ogni modo facilitare l'accesso, da parte dell'Autorità Garante, ai documenti e alle informazioni necessarie per l'adempimento dei suoi compiti istituzionali, compresi quelli finalizzati all'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi.
5. Il Responsabile della protezione dei dati è preposto allo svolgimento – in ambito aziendale – delle seguenti funzioni e compiti stabiliti dall'art.39 del GDPR:
   a) informare e fornire consulenza al Titolare del trattamento, nonché al personale aziendale che esegue attività di trattamento dati, in merito agli obblighi derivanti dal GDPR e dalla relativa normativa di attuazione;
   b) sorvegliare l'osservanza della normativa privacy e delle politiche aziendali sempre in materia di protezione dei dati, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
   c) fornire, se richiesto, parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del GDPR;
   d) cooperare con l'Autorità di controllo;
   e) fungere da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art.36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.
6. In riferimento ai compiti di cui al punto b), rientrano - in particolare - la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità e l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e dei soggetti preposti al trattamento dei dati personali nel contesto aziendale; ciò anche mediante la realizzazione di audit interni sotto il coordinamento del RPD stesso, onde assicurare la compliance dell'organizzazione ai principi ed alle disposizioni vigenti in materia.
7. Nell'eseguire i propri compiti il Responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.
8. Il Responsabile della protezione dei dati provvede, altresì:
   - a supportare il Titolare nel monitoraggio del Registro delle attività di trattamento di cui all'art.30 del GDPR;
   - alla formalizzazione della documentazione privacy quali istruzioni, informative, modulistica, procedure, nonché ogni altra opportuna ed adeguata misura organizzativa;
   - al coordinamento del Gruppo multidisciplinare di supporto al RPD stesso eventualmente costituito;

- a supportare le Unità Operative aziendali per gli ambiti e le materie di cui al GDPR;
- a gestire i contatti con gli interessati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal GDPR.

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

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

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

Art.27 - Ruolo della UOC Sistema Informativo aziendale e del Servizio di Ingegneria Clinica

1. Nell'ambito del sistema di Data Protection Governance Aziendale, per quanto attiene gli specifici aspetti della sicurezza informatica, la UOC Sistema Informativo aziendale ed il servizio di Ingegneria Clinica – in ragione degli ambiti di rispettiva competenza – provvedono a:

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

Art.28 - Gli Amministratori di Sistema

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

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

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

Art.30 – Referente/i Privacy

1. In ragione della complessità delle funzioni istituzionali svolte e della quantità e natura dei dati trattati, oltreché della necessità di garantire l'adozione di misure organizzative armoniche presso ciascuna Struttura/Servizio/Ufficio, il modello di *Data Protection Governance* aziendale contempla l'individuazione di uno o più Referenti Privacy onde assicurare un presidio coordinato delle operazioni di trattamento sulla base di una corretta circolazione di flussi informativi in materia di protezione dei dati personali tra tutti i soggetti coinvolti (Titolare, Responsabile della protezione dei dati, designati in qualità di Responsabili "interni" del trattamento, UOC SIA, Ingegneria Clinica, ecc.);
2. Il Referente privacy - c.d. *Privacy Manager aziendale* - è una figura interna con specifica esperienza maturata nel settore privacy e formazione avanzata in materia di privacy e protezione dei dati personali nonché in possesso di abilità informatiche tali da poter garantire un adeguato supporto al DPO aziendale;
3. Il Referente Privacy, già autorizzato al trattamento sulla base di quanto previsto all'art.24 del presente Regolamento, opera sotto la vigilanza del soggetto designato in qualità di Responsabile interno/delegato del trattamento e, in particolare, per quanto concerne la tematica della protezione dei dati personali, è tenuto a:
   - curare che le comunicazioni/informazioni da parte del Titolare o del Responsabile della protezione dei dati vengano capillarmente e adeguatamente trasmesse all'interno dell'articolazione organizzativa stessa;
   - fornire supporto ai designati in qualità di Responsabili "interni" del trattamento nell'applicazione e attuazione delle istruzioni e misure impartite dal Titolare o dal Responsabile della protezione dei dati;

- gestire i contatti con il Responsabile della protezione dei dati in ordine alla soluzione di specifiche problematiche formulando anche proposte.

4. Il/I Referente/i Privacy viene, altresì, coinvolto dal Responsabile della protezione dei dati nell'esecuzione dei diversi adempimenti quali gestione *data breach*, aggiornamento Registro delle attività di trattamento, valutazioni di impatto.
5. Il/I nominativo/i del/i Referente/i Privacy di struttura viene/vengono formalmente comunicato/i al Responsabile della protezione dei dati.

TITOLO III- I DIRITTI DELL'INTERESSATO

Art.31 - Informazioni sul trattamento dei dati personali

1. L'Azienda - quale Titolare del trattamento - è dotata di un sistema documentale relativamente alle informazioni sul trattamento da fornire al soggetto interessato. Tali informazioni, in linea con i principi contenuti nel GDPR, sono rese all'utente in forma coincisa, trasparente, intelligibile e con un linguaggio semplice e chiaro.
2. L'Azienda – in relazione ai diversi ambiti di attività istituzionale – ha adottato specifiche Informative sul trattamento dei dati personali che riportano le seguenti informazioni stabilite dall'art.13 del GDPR:
   - l'identità e i dati di contatto del Titolare del trattamento e del Responsabile della protezione dei dati;
   - le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
   - i legittimi interessi perseguiti dal Titolare del trattamento o da terzi (nel caso di trattamenti basati sull'art. 6, par. 1, lettera f) del GDPR);
   - gli eventuali destinatari, o categorie di destinatari, cui possono essere comunicati i dati;
   - ove applicabile, l'intenzione del Titolare di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione UE, nei termini previsti da GDPR;
   - il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   - l'esistenza del diritto dell'Interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
   - qualora la liceità del trattamento dei dati sia basata sul preventivo rilascio del consenso, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
   - il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali; se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali, nonché le possibili conseguenze della mancata comunicazione di tali dati;
   - l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

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

Art.32 - Consenso al trattamento dei dati

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

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

Art.33 - Diritto di accesso

1. Ai sensi dell'art.15 del GDPR l'Interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:
   a) le finalità del trattamento;
   b) le categorie di dati personali in questione;
   c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
   d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
   e) l'esistenza del diritto dell'Interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
   f) il diritto di proporre reclamo al Garante della protezione dei dati;
   g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
   h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.
2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate relative al trasferimento.
3. L'Azienda fornisce una copia dei dati personali oggetto di trattamento.
4. Nell'addebitare i costi sostenuti per il rilascio di copie all'interessato, l'Azienda applica quanto previsto sul punto dalla vigente regolamentazione in materia di accesso a documenti, dati e informazioni richiamata in premessa e a cui si fa espresso rinvio. Se l'Interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.
5. Il diritto di ottenere una copia dei dati personali non deve ledere i diritti e le libertà altrui.

Art.34 - Diritto di rettifica

1. Ai sensi dell'art.16 del GDPR l'Interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'Interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

Art.35 Diritto alla cancellazione

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

Art.36 - Diritto di limitazione di trattamento

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

5. Se il trattamento è limitato, i dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante.
6. L'Interessato che ha ottenuto la limitazione del trattamento è informato dal Titolare del trattamento prima che detta limitazione sia revocata.

Art.37 - Diritto alla portabilità dei dati

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

Art.38 - Diritto di opposizione

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

Art.39 - Reclamo all'Autorità Garante per la protezione dei dati personali

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

Art.40 - Diritti riguardanti le persone decedute

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

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

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

TITOLO IV- MISURE TECNICHE ED ORGANIZZATIVE

Art.42 - Misure di sicurezza di carattere generale

1. L'Azienda, nell'effettuare attività di trattamento dei dati personali, garantisce l'applicazione di idonee e preventive misure di sicurezza che consentono di ridurre al minimo i rischi di distruzione o perdita - anche accidentale - dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta.
2. Nell'ambito dell'Azienda il sistema gestionale privacy rappresenta un requisito indispensabile di qualità, per assicurare il quale, l'Azienda stessa adotta tutte le misure tecniche ed organizzative necessarie a far sì che la protezione dei dati personali e la loro tenuta in sicurezza siano non solo il rispetto di un obbligo normativo ma anche l'occasione di una crescita organizzativa e culturale.

3. In conformità ai principi contenuti agli artt. 24, 25 e 32 del GDPR, il Titolare del trattamento – attraverso i designati in qualità di Responsabili "interni" del trattamento, il personale autorizzato ed in particolare mediante il supporto del Responsabile della protezione dei dati, della UOC Sistema Informativo aziendale e del servizio Ingegneria Clinica – mette in atto misure e tecniche organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono:
   - la pseudominizzazione e la cifratura dei dati personali trattati;
   - procedure per assicurare, in modo permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
   - modalità per garantire il ripristino tempestivo nell'accesso ai dati personali in caso di incidente fisico o tecnico;
   - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
   - Il Titolare e i soggetti designati in qualità di Responsabili "interni" del trattamento fanno sì che chiunque agisca sotto la loro autorità e ha accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare e dai Responsabili medesimi.
4. L'accesso ad ogni sistema informatizzato è consentito solo se necessario e coerente rispetto al trattamento dei dati per il quale si è stati formalmente autorizzati ed è consentito soltanto utilizzando apposite credenziali di autorizzazione fornite dall'Azienda, strettamente personali e della cui riservatezza risponde personalmente il singolo soggetto autorizzato al trattamento dei dati personali.
5. I relativi processi di assegnazione di credenziali di accesso ai predetti sistemi sono gestiti – a seconda dei rispettivi ambiti di competenza – dalla UOC Sistema Informativo aziendale e del servizio di Ingegneria Clinica che provvedono ad elaborare specifiche policy finalizzate ad assicurare la sicurezza dei trattamenti, con il coinvolgimento del Responsabile della protezione di dati.
6. Tutti i soggetti autorizzati al trattamento sono tenuti a trattare i soli dati essenziali per svolgere l'attività istituzionale, riducendo al minimo l'utilizzo di dati identificativi, in modo da escludere il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante l'utilizzo di dati anonimi o mediante modalità che consentano di identificare l'Interessato unicamente in caso di necessità.
7. I dati su supporto cartaceo devono essere conservati in luoghi e contenitori atti ad evitare perdite, sottrazioni, danneggiamenti, distruzioni e l'accesso a soggetti diversi dal personale autorizzato al relativo trattamento, nel rispetto, peraltro, del principio della tutela della riservatezza di terzi.
8. Gli atti e i documenti devono essere conservati in archivi ad accesso protetto ed i soggetti autorizzati al trattamento sono tenuti a conservarli e restituirli al termine delle operazioni effettuate.
9. Nel caso di trattamenti di categorie particolari di dati personali, di cui agli artt. 9 e 10 del GDPR, oltre a quanto previsto, debbono essere osservate le seguenti ulteriori misure:
   - gli atti e i documenti sono conservati in locali o contenitori muniti di serratura, fino alla loro eventuale distruzione nel rispetto dei limiti temporali previsti dalla normativa in tema di scarto degli atti d'archivio;
   - l'accesso agli archivi è oggetto di controllo nel rispetto delle procedure aziendali vigenti.
10. Il trattamento dei dati – anche appartenenti alle categorie particolari – effettuato mediante strumenti elettronici è assoggettato all'osservanza delle seguenti misure di carattere generale predisposte e messe in atto dalla UOC Sistema Informativo aziendale e/o del servizio Ingegneria Clinica, in funzione degli ambiti di rispettiva competenza:

- autenticazione informatica, secondo le specifiche procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito al personale autorizzato ed agli addetti alla gestione o manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati e ad accessi non consentiti;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati rientranti nelle categorie particolari di cui all'art. 9 del GDPR.

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

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

1. Gli archivi che custodiscono i dati di cui è Titolare del trattamento l'Azienda, cartacei o digitali, devono essere collocati in locali idonei in ossequio alle disposizioni generali in materia di sicurezza e a quelle specifiche per la protezione del patrimonio informativo aziendale.
2. La documentazione archiviata, anche digitalmente, contenente i dati personali è conservata secondo le modalità e i tempi previsti dalla legge ed è poi sottoposta a scarto di archivio o a distruzione come da vigente normativa.
3. I designati in qualità di Responsabili "interni" del trattamento e gli Autorizzati, attenendosi alle istruzioni ricevute, attivano meccanismi necessari a garantire l'accesso selezionato ai dati e l'accesso controllato ai locali dove questi sono collocati mediante registrazione degli accessi ed esclusione degli stessi fuori dell'orario di servizio dell'archivio medesimo.
4. I supporti contenenti dati personali diversi dal cartaceo (supporti informatici, magnetici, videoregistrazioni effettuate nell'ambito dell'attività clinica, immagini iconografiche, ecc.), sono conservati e custoditi secondo le modalità e i termini previsti dalla normativa vigente.
5. Gli archivi cartacei e digitali sono oggetto di trattamento da parte di personale autorizzato e adeguatamente formato in materia di protezione dei dati, che deve assicurarne la riservatezza, protezione ed integrità per tutto il tempo in cui ne mantiene la disponibilità.
6. L'Azienda assicura l'adozione di misure e procedure attraverso le quali:
   - si proceda alla distruzione di documenti in formato cartaceo e digitale, una volta terminato il limite di conservazione degli stessi e dei dati ivi riportati,
   - siano smaltiti apparati hardware o supporti rimovibili di memoria con modalità che impediscano di accedere ad alcun dato personale; ciò anche in caso di riutilizzo degli stessi.

7. Relativamente agli archivi informatizzati contenenti dati personali adotta idonee procedure di sicurezza, quali:
   - salvataggio periodico dei dati;

- misure di contenimento dei virus/malware informatici e di protezione perimetrale da cyber attacchi alle infrastrutture ICT aziendali;
- *disaster recovery* e continuità operativa;
- conservazione sostitutiva come da vigente normativa.

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

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

Art.45 - Sensibilizzazione e formazione

1. L'Azienda promuove al suo interno ogni iniziativa di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.
2. In tale ambito, una delle iniziative di sensibilizzazione è costituita dall'attività formativa ed informativa rivolta al personale in tema di privacy; ciò allo scopo di garantire un aggiornamento formativo costante sulla normativa tecnica in continua evoluzione involgente problematiche connesse alla relativa applicazione e attuazione nel contesto operativo e gestionale, onde assicurare il corretto

funzionamento del sistema privacy e favorire una crescita culturale sull'importanza della protezione dei dati personali.

3. In riferimento alle anzidette finalità e nell'ottica della valorizzazione e mantenimento delle professionalità interne, specie in una fase di così complessa e delicata transizione verso sistemi e modelli gestionali del tutto innovativi e di rilevanza strategica, il Responsabile della protezione dei dati promuove – nell'ambito della pianificazione annuale delle attività formative aziendali – la realizzazione di eventi formativi su tematiche inerenti la privacy all'UOC Formazione che è tenuta ad espletarli.
4. L'Azienda – allo scopo di diffondere la conoscenza del sistema di governance della privacy in ambito istituzionale - alimenta l'apposita Sezione "Privacy" del sito web con policy, Informative redatte ex art.13 del GDPR, procedure, modulistiche e atti organizzativi.

Art.46 - Il Registro delle attività di trattamento

1. Il Titolare del trattamento tiene un Registro delle attività di trattamento svolte sotto la propria responsabilità contenente le informazioni di cui all'art. 30, paragrafo 1, del GDPR:
   a) il nome e i dati di contatto del Titolare del trattamento e del Responsabile della protezione dei dati;
   b) le finalità del trattamento;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
   e) i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
   f) i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
   g) una descrizione generale delle misure di sicurezza tecniche e organizzative.
2. Il Titolare, nell'ottica della piena applicazione del principio di accountability - su eventuale proposta del Responsabile della protezione dei dati - si riserva la facoltà di integrare i campi informativi del Registro con ulteriori informazioni rispetto a quelle obbligatorie riportate nell'elenco di cui al precedente comma. Il Registro delle attività di trattamento dell'Azienda - quale parte integrante del complessivo sistema di gestione dei dati personali - si fonda sulla mappatura dei dati trattati nonché sulla ricognizione di tutti gli elementi rilevanti di un trattamento di dati personali.
3. Il Registro delle attività di trattamento dell'Azienda è strutturato attraverso un percorso metodologico che riconduce alla responsabilità organizzativa dei soggetti designati in qualità di Responsabili "interni" del trattamento – di cui all'art. 23 del presente Regolamento - i corrispondenti trattamenti di dati personali effettuati presso la Struttura/Servizio/Ufficio diretti; ciò secondo una logica che prende a riferimento le macro attività istituzionali proprie della mission aziendale e l'articolata trasversalità e interconnessione dei diversi processi mediante i quali vengono erogate sia prestazioni sanitarie che di carattere amministrativo e tecnico.
4. Il Titolare, avvalendosi del supporto e della consulenza del Responsabile della protezione dei dati, assicura la gestione, l'aggiornamento e la conservazione del Registro su formato elettronico.
5. Il Registro delle attività di trattamento - stante la sua natura fortemente dinamica ed evolutiva – viene, altresì, adeguato in funzione dei futuri sviluppi, anche applicativi, del complessivo quadro normativo di riferimento oltreché dei possibili mutamenti degli assetti organizzativi aziendali.

6. Dietro richiesta, si provvede a mettere il Registro delle attività di trattamento a disposizione dell'Autorità Garante per la protezione dei dati personali.

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

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

Art.48 - La violazione dei dati personali

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

fisiche interessate, il Titolare del trattamento predispone la notificazione all'Autorità Garante in ottemperanza alle prescrizioni di cui al richiamato art. 33 del GDPR.

11. Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone fisiche interessate, queste ultime devono essere informate senza ingiustificato ritardo al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali pregiudizi derivanti dalla violazione.

12. Il Responsabile della protezione dei dati, ove richiestone, supporta il Titolare del trattamento nella predisposizione della comunicazione all'interessato/agli interessati, da inviarsi nei tempi e con le modalità che il Titolare stesso - sempre attraverso la funzione consulenziale del Responsabile della protezione dei dati - individuerà come più opportune, anche tenendo conto di eventuali indicazioni all'uopo fornite dall'Autorità Garante. La comunicazione descriverà con linguaggio semplice e chiaro la natura della violazione dei dati personali, le probabili conseguenze derivanti dalla stessa, oltreché le relative misure individuate per porvi rimedio.

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

TITOLO V – NORME FINALI

Art.49 – Disposizioni finali

1. Per tutto quanto non previsto dal presente Regolamento, si fa espresso rinvio alle disposizioni normative di livello comunitario e nazionale vigenti in materia di protezione di dati personali, nonché agli specifici provvedimenti dell'Autorità Garante.
2. Dalla data di approvazione del presente Regolamento cessa di avere efficacia ogni disposizione regolamentare ed organizzativa in contrasto con quanto dallo stesso disciplinato, salva la vigenza degli atti con esso compatibili.
3. Il presente Regolamento è pubblicato sul sito web istituzionale alla Sezione "Amministrazione Trasparente" – sottosezione "Disposizioni Generali" e alla Sezione "Privacy".
4. I diversi atti, quali, modulistica, procedure, Informative, adottati dall'Azienda relativamente alla tematica della protezione dei dati sono consultabili nel sito web istituzionale.

Allegati:

- Allegato A) Linee guida per conduzione attività di *Data protection impact*;
- Allegato B) Politica di protezione dei dati personali;
- Allegato C) Il Registro delle attività di trattamento;
- Allegato D) Modulo di richiesta di esercizio dei diritti dell'interessato;
- Allegato E) Informativa navigatori siti internet aziendali;
- Allegato F) Informativa utenti ex artt.13-14 Regolamento UE 2016/679;
- Allegato G) Atto di nomina designato al trattamento con Compiti ed Istruzioni;
- Allegato H) Atto di nomina autorizzato al trattamento dei dati con Istruzioni;
- Allegato I) Istruzioni specifiche personale sanitario designati ed autorizzati;
- Allegato J) Modello nomina Responsabile del trattamento ex Art.28 REG.(UE) 2016/679.

ALLEGATO A)

LINEE GUIDA PER LA CONDUZIONE DELLE ATTIVITÀ DI DATA PROTECTION IMPACT ASSESSMENT

Sommario

CAPITOLO 1 - GENERALITÀ

Il *Data Protection Impact Assessment* (DPIA) o "Valutazione di impatto sulla protezione dei dati" rappresenta una delle fondamentali attività previste dal Regolamento UE 679/2016, di seguito sinteticamente indicato come "Regolamento" o "GDPR", relativamente agli obblighi dei Titolari (cfr.art.35), nell'ambito della gestione del rischio correlato al trattamento di dati personali.

La DPIA è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per ridurli.

La valutazione d'impatto sulla protezione dei dati è uno strumento importante di responsabilizzazione in quanto sostiene il titolare del trattamento non soltanto nel rispettare i requisiti del Regolamento, ma anche nel dimostrare che sono state adottate misure appropriate.

La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione del Garante per la protezione dei dati personali laddove richiesto (articolo 36, paragrafo 3, lettera e), possono comportare sanzioni.

In linea con l'approccio basato sul rischio adottato dal Regolamento, è necessario realizzare un DPIA quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"; risulta pertanto fondamentale svolgere un'analisi preliminare per individuare tali trattamenti e dotarsi di principi e metodologie comuni per lo svolgimento delle attività di valutazione.

1.1 FINALITÀ DEL DOCUMENTO

Questo documento espone le linee guida per la conduzione delle attività di *Data Protection Impact Assessment* attuate dalla Struttura Sanitaria al fine di garantire l'adozione di un approccio rigoroso basato sul rischio ed in linea con i requisiti del Regolamento.

1.2 AMBITO DI APPLICAZIONE

Gli indirizzamenti definiti nel presente documento si applicano a quei trattamenti della Struttura Sanitaria che il Titolare, confrontatosi con il DPO, ritiene dover sottoporre ad una DPIA e sono da ritenersi estese anche ai Responsabili e agli eventuali Sub-responsabili del trattamento di dati personali, nei modi e nei termini definiti nell'art.28 del GDPR.

1.3 DOCUMENTI DI RIFERIMENTO

[1] Regolamento (UE) 2016 del Parlamento Europeo e del Consiglio, del 27 Aprile 2016, relativo alla protezione delle persone con riguardo al trattamento dei dati personali – Regolamento Generale sulla Protezione dei Dati (GDPR) e ss.mm.ii.

[2] D.lgs 10 agosto 2018, n. 101. "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)"

[3] D.Lgs. 30 Giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" e s.m.i.
[4] ISO/IEC 27001:2013 "Information Security Management Systems", 01/10/2013
[5] ISO/IEC 27002:2013 "Code of practice for information security controls", 01/10/2013
[6] ISO/IEC 27005: 2011 "Information technology — Security techniques — Information security risk management, Second edition 2011-06-01
[7] ISO/IEC 29134:2017€ "Information technology – Security techniques – Guidelines for privacy impact assessment", First edition 2017-06
[8] ISO/IEC 29100:2011 "Privacy Framework"
[9] ISO/IEC 29151:2017 "Code of practice for personally identifiable information protection"
[10] "Accountability on the ground Part II: Data Protection Impact Assessments & Prior Consultation", European Data Protection Supervisor, Febbraio2018
[11] "Privacy Impact Assessment (PIA) Methodology", Autorità francese per la protezione dei dati (CNIL), Febbraio 2018
[12] "Privacy Impact Assessment (PIA) Knowledge Bases", Autorità francese per la protezione dei dati (CNIL), Febbraio 2018
[13] WP29 Gruppo istituito ai sensi dell'art. 29 della direttiva 95/46 CE (dal 25 Maggio prende il nome di EDPB – European Data Protection Board)
[14] "Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE)
2016/679", WP 248 rev.01, 04/04/2017
[15] "Linee guida sui responsabili della protezione dei dati", WP 243 rev. 01, 05/04/17

1.4 ACRONIMI E DEFINIZIONI

Categorie particolari di dati personali	Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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.
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.
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

Dati 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.
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dati relativi alla salute	I dati personali attinenti alla salute fisica mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o 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 4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/33 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.
Dossier sanitario	Il dossier sanitario è l´insieme dei dati personali generati da eventi clinici presenti e trascorsi riguardanti l´interessato, che vengono condivisi tra i professionisti sanitari che lo assistono presso un´unica struttura sanitaria (ad es. ospedale, casa di cura privata, ecc.). Inoltre, il dossier sanitario serve a rendere più efficienti i processi di diagnosi e cura del paziente all´interno di un´unica struttura sanitaria, consentendo ai diversi professionisti che vi operano di accedere a tutte le informazioni cliniche relative ai precedenti interventi (ricoveri, visite ambulatoriali, accessi in pronto soccorso)

	effettuati dall´assistito presso quella stessa struttura.
DPIA	Data Protection Impact Assessment (art. 35 del GDPR).
DPO/RDP	Data Protection Officer/Responsabile della Protezione dei Dati.
FSE	Il fascicolo sanitario elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito *(art.12, comma 1, d.l. n. 179/2012)*, generati oltre che da strutture sanitarie pubbliche anche da quelle private.
GDPR	Regolamento Generale per la Protezione dei Dati.
IaaS	Infrastructureas a Service.
SaaS	Software as a Service
PaaS	Platform as a Service.
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Pseudonimizzazione	Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Rappresentante	La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'art.27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento.
Referto online	Possibilità di accedere al referto tramite modalità digitali (Fascicolo sanitario elettronico, sito Web, posta elettronica anche certificata, supporto elettronico).

Responsabile del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento trattamento.
RPO	Recovery Point Objective.
RTO	Recovery Time Objective.
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.
Titolare del trattamento	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.
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.
Trattamento transfrontaliero	a) Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; *oppure* b) Trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

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.

1.5 RUOLI E RESPONSABILITÀ

La responsabilità di condurre un DPIA è assegnata al Titolare del trattamento in base all'art. 35, par.1 del Regolamento.
Nello svolgimento di tale attività, il Titolare è assistito e supportato dal Responsabile della Protezione dei Dati (RDP/DPO) con il quale si consulta chiedendo, se necessario, un parere in merito al DPIA e di sorvegliarne lo svolgimento ai sensi dell'art.35 del Regolamento. In particolare, il Titolare si consulta con il RPD/DPO sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e le libertà degli interessati;
- se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano in linea con il Regolamento.

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni.
In ogni caso, il RDP sorveglia lo svolgimento delle attività di DPIA al fine di rilevare eventuali difformità da quanto previsto dal Regolamento e/o dalle presenti Linee guida e funge da punto di contatto con il Garante per la protezione dei dati personali in caso di consultazione preventiva di cui all'art.36 del GDPR. Tutte le UU.OO. della Struttura Sanitaria, ognuno per il proprio ambito di competenza in relazione al trattamento, incluse la U.O.C all'interno della quale è incardinata la funzione privacy, la U.O.C SIA e l'U.O.C. che si occupa di apparecchiature elettromedicali, supportano il titolare ed il RDP nello svolgimento delle valutazioni di impatto.
Qualora il trattamento venga eseguito in toto o in parte da un responsabile esterno del trattamento dei dati, quest'ultimo deve assistere il titolare del trattamento nell'esecuzione del DPIA e fornire tutte le informazioni necessarie.

CAPITOLO 2 - PRINCIPI CHE INDIRIZZANO LE ATTIVITÀ DI DPIA

Nella conduzione delle attività di DPIA è necessario garantire la scrupolosa osservanza dei seguenti principi guida:

- i criteri per valutare il rischio e definire la strategia di trattamento devono essere mantenuti aggiornati e devono tenere in opportuna considerazione i valori, gli obiettivi e le risorse della Struttura Sanitaria, ma anche il contesto normativo di riferimento;
- successive DPIA devono produrre risultati coerenti, validi e confrontabili fra loro;
- per le diverse fasi della DPIA devono essere assegnati ruoli e responsabilità specifiche e deve essere garantito un forte *commitment* sul tema;

- la metodologia operativa della DPIA deve essere mantenuta aggiornata in linea con le evoluzioni normative, tecnologiche e di contesto;
- il programma delle attività di DPIA deve essere formulato con frequenza almeno annuale e comunque rivisto ad ogni cambiamento avente impatti sul contesto o su valutazioni già effettuate;
- nello svolgimento del DPIA occorre tenere in debito conto il rispetto di codici di condotta eventualmente approvati, di cui all'art.40 del GDPR, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati;
- le informazioni raccolte e/o elaborate durante la DPIA devono essere documentate in modo che queste siano agevolmente rintracciabili dalle persone autorizzate ed accessibili solo a queste ultime.

CAPITOLO 3 - CONDUZIONE DELLE ATTIVITÀ DI DPIA

Nei paragrafi successivi sono descritte le linee guida da adottare per ognuna delle seguenti fasi della DPIA:

1. Valutazione preliminare di necessità della DPIA;
2. Preparazione della DPIA;
3. Esecuzione della DPIA;
4. Eventuale consultazione del Garante per la protezione dei dati personali.

3.1 VALUTAZIONE PRELIMINARE DI NECESSITÀ DELLA DPIA

In base al Regolamento (art. 35), una DPIA è obbligatoria quando il 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. In particolare, il Regolamento prescrive la valutazione di impatto per i trattamenti che:

- prevedono una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- prevedono il trattamento, su larga scala, di categorie particolari di dati personali (art.9 GDPR) o di dati relativi a condanne penali e a reati (art. 10 GDPR);
- prevedono la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Lo stesso Regolamento individua anche i seguenti casi per i quali non è invece obbligatorio eseguire una DPIA:

a) il trattamento appartiene ad una o più tipologie incluse in un elenco ufficiale di tipologie di trattamenti non soggetti al requisito di DPIA ai sensi del paragrafo 1 del art.5 del GDPR, qualora pubblicato dall'autorità di controllo (Garante per la protezione dei dati personali);
b) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art.6, par. 1, lettera c) o per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art.6, par. 1 lettera e), inoltre il trattamento trova nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare è soggetto una base

giuridica, tale diritto disciplina il trattamento specifico o l'insieme di trattamenti in questione, ed è già stato effettuato una DPIA nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

Tutto ciò premesso, per determinare la necessità di eseguire una DPIA, la Struttura Sanitaria deve adottare i seguenti criteri decisionali:

- trattamenti che sottintendono un rischio elevato di violazione dei diritti e delle libertà delle persone fisiche (interessati);
- trattamenti che non rientrano nei casi di cui ai punti a) e b) del precedente elenco;
- trattamenti che rientrano in una o più delle casistiche riportate nella seguente tabella.

Tabella 1 – Criteri per la valutazione di necessità della DPIA

Valutazione di profilazione o scoring	Tutti quei trattamenti che prevedono la valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato.
Decisioni automatizzate	Tutti quei trattamenti che prevedono un processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente (trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che hanno effetti giuridici o che incidono in modo analogo significativamente su dette persone fisiche).
Monitoraggio sistematico	Tutti quei trattamenti utilizzati per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Categorie particolari di dati personali e/o dati personali relativi a condanne penali e reati	Tutti quei trattamenti che si riferiscono a categorie particolari di dati personali o dati personali relativi a condanne penali o reati.

Trattamento di dati su larga scala	Tutti i trattamenti che gestiscono dati personali su larga scala, in relazione ai seguenti fattori: 1. numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; 2. volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; 3. durata ovvero la persistenza dell'attività di trattamento; 4. portata geografica dell'attività di trattamento.
Combinazioni o raffronto di insieme di dati	Tutti quei trattamenti nei quali è prevista la creazione di corrispondenze o combinazione di insiemi di dati, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato.
Dati relativi a interessati vulnerabili	Tutti quei trattamenti in cui la tipologia delle informazioni trattate determina uno squilibrio fra interessato e titolare, nel senso della mancanza del potere, in capo al primo, di acconsentire o di opporsi al trattamento. Si inseriscono in questa categoria i dati dei minori, dei dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.).
Uso innovativo o applicazione di nuove soluzioni tecnologiche ed organizzative	Tutti quei trattamenti che utilizzano tecnologie o tecniche innovative per la raccolta o l'utilizzo dei dati personali, dato che il livello di conoscenza tecnologica, in un dato momento storico, non è in grado valutare il livello di rischio connesso all'innovazione.
Trattamenti che impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto	Tutti quei trattamenti che impediscono agli interessati di esercitare un diritto, di avvalersi di un servizio o di un contratto, ossia tutti i trattamenti dai quali l'interessato non può esimersi qualora volesse accedere a detto servizio o concludere detto contratto.

Il titolare può comunque decidere di svolgere una DPIA anche per trattamenti che non soddisfano i suddetti criteri o che li soddisfano solo in parte, ma che da valutazioni preliminari potrebbero determinare rischi elevati.
Pertanto, al momento della definizione del Registro dei Trattamenti o del suo aggiornamento, il titolare valuta, per ogni trattamento, se le sue modalità di attuazione o i dati trattati soddisfano i suddetti criteri, e non si configurano eccezioni (individuate all'interno di elenchi che dovranno essere redatti dalle autorità di controllo degli Stati Membri), registrando la necessità di svolgere la DPIA in apposito campo del Registro. I criteri per la valutazione di necessità della DPIA possono essere anche utilizzati per la definizione delle priorità di svolgimento delle valutazioni di impatto.

3.2 PREPARAZIONE DELLA DPIA

Una volta individuata la necessità di effettuare una o più DPIA, occorre definire:

- l'ambito della DPIA;
- le risorse (umane ed economiche) necessarie per lo svolgimento delle attività;
- il Gruppo di lavoro, identificando i referenti interni ed esterni necessari, tenendo presente i ruoli e le responsabilità;
- Gli *stakeholders* ossia coloro che possono trattare dati personali o possono essere impattati dal trattamento (attori coinvolti), consultandoli ove ritenuto opportuno/necessario;
- le priorità per lo svolgimento delle DPIA, qualora il numero sia rilevante in relazione alle risorse disponibili;

Per quanto riguarda l'ambito, una DPIA può riguardare una singola operazione di trattamento dei dati oppure un insieme di trattamenti simili che presentano rischi elevati analoghi. Si può ad esempio ricorrere ad una singola DPIA per trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi oppure nel caso si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità.
Per quanto riguarda la pianificazione, coerentemente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita, la DPIA deve essere effettuata prima possibile nella fase di progettazione del trattamento anche se alcune delle operazioni di trattamento non sono ancora note e comunque prima di avviare il trattamento. La DPIA deve infatti essere considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento, sia prima del trattamento, sia nel corso del trattamento, soprattutto quando esso è dinamico ed è soggetto a variazioni continue.

3.3 PROCEDURA OPERATIVA PER LA ESECUZIONE DEL DPIA

La fase di esecuzione della DPIA deve seguire i seguenti passi principali:

- definizione del contesto;
- valutazione di necessità e proporzionalità del trattamento;
- valutazione dei rischi;
- definizione delle modalità di trattamento dei rischi;
- redazione e approvazione del piano di azione della DPIA.

Durante l'esecuzione della DPIA la Struttura Sanitaria può avvalersi di strumenti automatici o semiautomatici purché siano conformi alle presenti linee guida.

3.3.1 DEFINIZIONE DEL CONTESTO

La definizione del contesto deve consentire una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, nonché degli strumenti a supporto, pertanto, occorre individuare:

- finalità del trattamento;
- categoria di interessati (evidenziando se trattasi di minori);
- Se il trattamento soddisfa uno o più criteri tra quelli riportati in Tabella 1;
- Responsabilità del trattamento (titolare del trattamento, contitolare del trattamento, RDP, eventuali referenti interni, eventuali Enti terzi/Responsabili del trattamento);
- Gli *asset* (risorse e strumenti) a supporto del trattamento;
- Le informazioni (categorie di dati personali) trattate ed il flusso informativo identificando le principali operazioni di trattamento svolte.

Nell'individuare gli *asset* a supporto occorre censire e descrivere quelli afferenti alle seguenti principali categorie:

- organizzazione (strutture organizzative preposte al trattamento);
- asset IT on premise (applicativi/data base gestiti presso il Data Center della Struttura Sanitaria o presso Data Center di fornitori);
- servizi in Cloud (distinguendo tra: *Software as a Service - SaaS, Platform as a Service - PaaS, Infrastructureas a Service – IaaS*);
- facility (Data Center, Uffici ove si effettuano le operazioni di trattamento, Archivi preposti alla conservazione di documentazione cartacea contenente dati personali, etc.);
- documentazione cartacea (tipologia di documentazione cartacea contenente dati personali oggetto di trattamento).

Nel descrivere le informazioni trattate, eventualmente aggregandole per categorie omogenee, occorre:

- descrivere la tipologia di dati personali (dati anagrafici, dati sanitari contenuti in referti medici, dati sanitari contenuti in cartella sanitaria, etc.);
- identificare se l'informazione è soggetta a trasferimento verso paesi terzi o organizzazioni internazionali, ed in tal caso identificare il paese terzo o l'organizzazione internazionale e le condizioni per il trasferimento;
- identificare se l'informazione è trattata all'interno del Fascicolo Sanitario Elettronico o Dossier Sanitario Elettronico, attraverso servizi web, app mediche e/o Referto on line;
- definire i termini di cancellazione dell'informazione;
- identificare i destinatari;
- identificare l'Unità Organizzativa preposta al trattamento dell'informazione.

Per quanto riguarda la tipologia di dati occorre specificare se trattasi di:

- categorie particolari di dati personali (art. 9 GDPR);
- dati personali relativi a condanne penali e reati (art.10 GDPR);
- dati sanitari;
- dati biometrici;

- dati genetici;

Nello svolgimento di tale attività è necessario prendere come riferimento anche le informazioni contenute nel Registro dei Trattamenti predisposto della Struttura Sanitaria.

3.3.2 VALUTAZIONE DI NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO

Un punto fondamentale della DPIA è la descrizione delle modalità adottate per garantire la necessità e la proporzionalità del trattamento in relazione alle finalità. Nello specifico, occorre:

- illustrare perché le finalità del trattamento sono specifiche, esplicite e legittime;
- presentare le basi giuridiche del trattamento (ad esempio: consenso dell'interessato, esecuzione di misure precontrattuali, esecuzione di un contratto, adempimenti di obblighi legali del titolare, salvaguardia di interessi vitali, esercizio di un interesse pubblico, legittimo interesse del titolare);
- spiegare perché i dati raccolti sono necessari per le finalità del trattamento;
- descrivere quali sono le misure adottate per assicurare l'accuratezza dei dati;
- spiegare perché la durata dell'archiviazione è giustificata da requisiti legali e/o necessità di trattamento.

3.3.3 VALUTAZIONE DEI RISCHI

Definito il contesto e la valutazione di necessità e proporzionalità del trattamento occorre passare alla valutazione dei rischi. Un "rischio" è uno scenario che descrive un evento e le sue conseguenze. La valutazione dei rischi deve identificare gli "scenari di rischio" e, per ognuno di essi, stimare il "livello di rischio effettivo" per i diritti e le libertà dell'interessato connesso al trattamento in esame con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento.

I principali scenari di rischio da prendere in considerazione sono:

- perdita di riservatezza - accesso illegittimo ai dati personali;
- perdita di integrità - modifica non autorizzata dei dati personali;
- perdita di disponibilità - perdita, furto, cancellazione non autorizzata di dati personali.

Il livello di rischio è inteso come la probabilità che una minaccia possa sfruttare le vulnerabilità di un asset o di un gruppo di asset a supporto del trattamento e quindi causare un danno all'interessato.

Il criterio utilizzato per la conduzione dell'analisi dei rischi, derivato con alcuni adattamenti dallo standard ISO/IEC 27001:2017e dalla Norma DS/ISO/IEC 29134:2017 (Annex A) e dal documento "Privacy Impact Assessment" della Commission nationale de l'informatique et des libertés 2015, si basa sulla correlazione fra la gravità (**G**) di un rischio (definita in relazione all'ampiezza degli impatti potenziali sugli interessati, tenendo conto delle misure esistenti) e la probabilità (**P**) di accadimento dell'evento minaccia che provoca il danno (definita in relazione alle vulnerabilità dei supporti interessati e alla capacità delle fonti di rischio di sfruttarle, tenendo conto delle misure esistenti).

A tal riguardo, si è definito l'indice o fattore di rischio **R** come funzione della probabilità di accadimento delle minacce e l'Indice di gravità del danno:

R = f (P, G)

In tale ottica la valutazione del livello di rischio deve pertanto essere stimato in termini di:

- "impatto/gravità (**G**)" potenziale sull'interessato nel caso in cui si concretizzi ognuno degli scenari di rischio e relativa probabilità di accadimento dello scenario di impatto;
- "probabilità delle minacce (**P**)" che dipende principalmente dal livello di vulnerabilità delle risorse di supporto e dalle minacce in grado di sfruttarle.

A tal fine la fase di valutazione del rischio deve prevedere le seguenti sotto-fasi:

- analisi degli impatti sui diritti e le libertà dell'interessato e della probabilità di accadimento degli scenari di impatto;
- analisi delle minacce applicabili al contesto di trattamento;
- definizione delle misure necessarie a contrastare le minacce identificate;
- valutazione della probabilità di accadimento delle minacce determinata secondo un criterio relazionale inversamente proporzionale al livello di efficienza delle misure identificate nel contrastarle, efficienza determinata in funzione dell'applicabilità dei controlli a sostegno delle misure definite ed alla robustezza degli stessi;
- valutazione del rischio effettivo.

I principi dettagliati per lo svolgimento delle suddette attività sono descritti nei successivi paragrafi. Per valutare al meglio l'analisi delle minacce applicabili al contesto del trattamento, particolare attenzione deve essere prestata qualora il titolare del trattamento, ricorra a Responsabili del trattamento che, ai sensi dell'art.28 del Regolamento UE 2016/679 (GDPR), devono presentare garanzie sufficienti affinché il trattamento soddisfi i requisiti previsti dalla normativa vigente e garantisca la tutela dei diritti dell'interessato. Nello specifico il GDPR prevede che ogni Responsabile e i suoi eventuali sub-responsabili per il trattamento dei dati, in relazione alle specifiche attività di trattamento svolte per conto del Titolare, per garantire un livello di sicurezza adeguato in conformità all'art.32 del GDPR, debba mettere in atto e mantenere in essere appropriate misure tecniche ed organizzative, controlli interni e processi di sicurezza intesi a proteggere i dati da perdita accidentale, distruzione o alterazione, da accessi o da diffusione non autorizzati o da illegale distruzione.

Pertanto, atteso che tra i compiti del Responsabile, ai sensi del citato art.28 par.3 lett. h), vi è quello di mettere a disposizione del Titolare tutte le informazioni necessarie a dimostrare il rispetto degli obblighi e delle disposizioni previste dal succitato Regolamento, è necessario che tra le suddette informazioni vi sia il presupposto di una eventuale DPIA condotta dal Responsabile o, in alternativa, della disponibilità, nel caso di utilizzo di strumenti informatici o telematici, delle rispettive certificazioni di conformità al GDPR validate dai preposti organismi e agenzie nazionali ed europei.

3.3.3.1 ANALISI DEGLI IMPATTI SUI DIRITTI E LE LIBERTÀ DELL'INTERESSATO

L'analisi degli impatti potenziali sui diritti e le libertà dell'interessato deve essere condotta considerando le seguenti dimensioni di analisi:

- scenario di perdita di Riservatezza, Integrità e Disponibilità;
- categoria di impatto.

Le categorie di impatto devono includere le seguenti:

- impatto fisico - tutti i danni fisici che gli interessati potrebbero subire a seguito di violazioni dei dati personali;
- impatto materiale - tutti i danni materiali che gli interessati potrebbero subire a seguito di violazioni dei dati personali;
- impatto psicologico - tutti i danni psicologici che gli interessati potrebbero subire a seguito di violazioni dei dati personali.

Per ogni scenario e per ogni categoria d'impatto occorre identificare un "livello di impatto (G)", espresso secondo una scala di valutazione qualitativa discreta (N.A.= Non Applicabile, 1=Trascurabile, 2=Limitato, 3=Significativo, 4=Massimo), descritta nella seguente tabella.

LIVELLI DI IMPATTO PER CATEGORIA				
Livello		Impatto Fisico	Impatto materiale	Impatto psicologico
N.A.	**Non Applicabile**	Gli interessati non subirebbero alcun impatto.	Gli interessati non subirebbero alcun impatto.	Gli interessati non subirebbero alcun impatto.
1	**Trascurabile**	Gli interessati potrebbero incontrare qualche inconveniente fisico, superabile senza difficoltà (ad es. mal di testa)	Gli interessati potrebbero incontrare qualche inconveniente materiale, superabile senza difficoltà (ad es. perdita di tempo)	Gli interessati potrebbero incontrare qualche inconveniente psicologico, superabile senza difficoltà (ad es. semplice fastidio)
2	**Limitato**	Gli interessati potrebbero sperimentare inconvenienti fisici superabili nonostante alcune difficoltà (ad es. malattia lieve).	Gli interessati potrebbero avere inconvenienti materiali, superabili nonostante alcune difficoltà (ad es: costi aggiuntivi o mancato accesso ad un servizio).	Gli interessati potrebbero avere inconvenienti psicologici, superabili nonostante alcune difficoltà (ad es. disturbo psicologico minore ma oggettivo, intimidazione sui social network).

3	**Significativo**	Gli interessati potrebbero subire conseguenze fisiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad es. malattia a lungo termine)	Gli interessati potrebbero subire conseguenze materiali significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad es. perdita di opportunità non ricorrenti).	Gli interessati potrebbero subire conseguenze psicologiche significative, che dovrebbero essere in grado di superare, ma con notevoli difficoltà (ad es. significativo disturbo psicologico, esposizione a ricatti, cyberbullismo)
4	**Massimo**	Gli interessati potrebbero sperimentare gravi conseguenze fisiche, anche irrimediabili, che potrebbero non superare (ad es. malattie permanenti o decesso)	Gli interessati potrebbero subire gravi conseguenze materiali, anche irrimediabili, che potrebbero non superare (ad es. indebitamento ingente, impossibilità di lavorare)	Gli interessati potrebbero subire gravi conseguenze psicologiche, anche irrimediabili, che potrebbero non superare (ad es. perdita di legami familiari, disturbo psicologico permanente o a lungo termine).

Figura 1 – Livelli di impatto per categoria

3.3.3.2 ANALISI DELLE MINACCE APPLICABILI

L'analisi delle minacce deve essere basata su un "catalogo di minacce" derivanti da standard e *best practices* di riferimento, ognuna delle quali è caratterizzata da:

- uno o più scenari di rischio che la minaccia può determinare (accesso illegittimo ai dati, modifica non autorizzata dei dati, perdita dei dati);
- la tipologia di asset sulla quale può agire;
- uno o più agenti di minaccia che possono attuarla (fonti umane interne/esterne o fonti non umane).

Tra queste minacce occorre identificare quelle applicabili allo specifico trattamento in esame.

3.3.3.3 VALUTAZIONE DELLA PROBABILITÀ DI ACCADIMENTO DELLE MINACCE

Per ogni minaccia identificata come applicabile al trattamento in esame, occorre valutare la probabilità (**P**) di accadimento espressa su una scala di valutazione qualitativa discreta di 4 livelli (Trascurabile, Limitata, Significativa, Massima) prendendo in considerazione i tre scenari di rischio relativi alla perdita di riservatezza, integrità e disponibilità.

A tal fine, la probabilità viene derivata secondo un principio inversamente proporzionale al livello di efficienza delle misure predisposte per contrastarle e quindi dal livello di attuazione dei controlli posti in essere a protezione del trattamento relativamente ai seguenti ambiti:

- requisiti del Regolamento;
- requisiti derivanti dalla normativa e dai pronunciamenti del Garante per la protezione dei dati personali;
- requisiti derivanti da standard e best practices internazionali di sicurezza e privacy.

Nello specifico per ogni minaccia applicabile sono individuate le misure ritenute necessarie a contrastarla e per ogni misura l'insieme dei controlli che la costituiscono.
Ciò richiede che i controlli siano strutturati in "classi funzionali", ciascuna delle quali individua funzionalità omogenee di sicurezza e privacy in grado di contrastare le minacce applicabili, ovvero la misura che esse configurano.
Ogni controllo inoltre deve essere caratterizzato da un livello di robustezza su una scala ordinale a tre valori; il livello ordinale e quindi cardinale di implementazione "asis" dei controlli deve essere valutato, sia tramite intervista che autovalutazione, utilizzando la seguente nomenclatura convenzionale:

- "Si": il controllo è coperto da una o più contromisure pienamente e correttamente applicate (100%);
- "Parziale": una o più contromisure coprono solo parzialmente il controllo espresso (più del 50% ma non ancora il 100%);
- "No": il controllo non è coperto da alcuna contromisura oppure è solo parzialmente implementato (<50%);
- "N.A.": il controllo non è applicabile al contesto di riferimento.

Come già detto la probabilità di accadimento di una minaccia è inversamente proporzionale alla efficienza delle misure predisposte a contrastarla e quindi alla copertura e alla robustezza dell'insieme dei controlli a sostegno delle suddette misure.
Nello specifico, sulla base dei requisiti derivanti dalla normativa e dai pronunciamenti del Garante per la protezione dei dati personali, dei requisiti derivanti da standard e *best practices* internazionali di sicurezza e privacy e dei riferimenti di cui al precedente punto 1.3, si identificano i controlli a sostegno della misura desiderata ed in funzione della esistenza o meno e del livello di robustezza di ognuno di essi, si determina in un range da 0 a 100 l'efficienza (E) della misura in oggetto (100 = massima efficienza) e di conseguenza la probabilità (P) di accadimento della minaccia in un range da 0 a 100: P= (100 – E; 0 = probabilità nulla). La scala di valutazione qualitativa discreta secondo 4 livelli della probabilità di accadimento delle minacce si ottiene rapportando i valori percentuali secondo il seguente criterio: 0-25% = 1 Trascurabile; 25-50% = 2 Limitata; 26-75% = 3 Significativa; 75-100% = Massima.

3.3.3.4 VALUTAZIONE DEL RISCHIO EFFETTIVO

Il rischio effettivo per i diritti e le libertà degli interessati connesso al trattamento in esame deve essere valutato per ogni scenario di rischio e per ogni minaccia, in base a:
- i valori di impatto rilevati, pesati con la probabilità degli scenari di impatto;

- la probabilità di accadimento delle minacce. I livelli di rischio rilevati devono essere espressi secondo una scala di valutazione qualitativa discreta a 4 livelli (1=Trascurabile, 2=Limitato, 3=Significativo, 4=Massimo), applicando i criteri espressi dalla matrice di rischio rappresentata nella figura seguente.

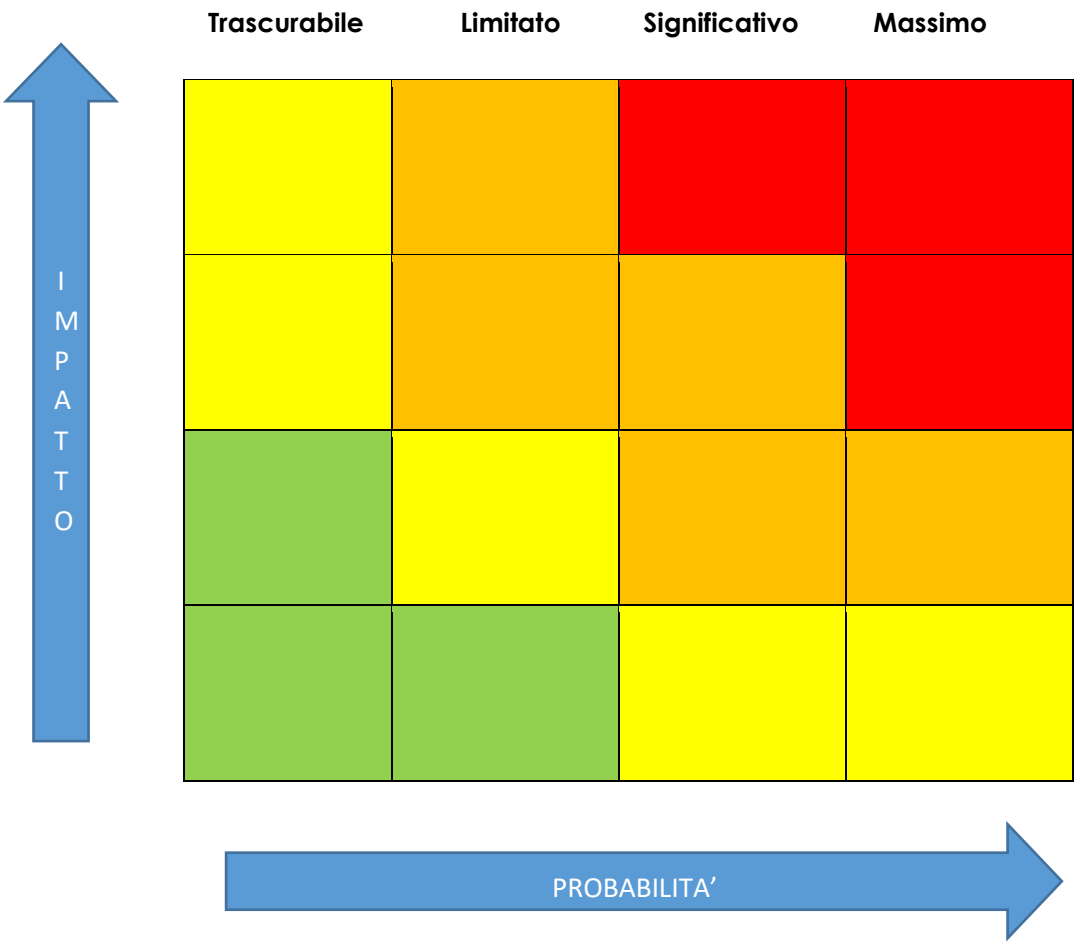

Figura 2 - Matrice livello di rischio

3.3.4 DEFINIZIONE DELLE MODALITÀ DI TRATTAMENTO DEI RISCHI

A conclusione delle attività fin qui descritte occorre definire ed individuare la strategia di gestione del rischio per i diritti e le libertà degli interessati della struttura sanitaria.
Tale strategia scaturisce dalla identificazione degli asset tecnici, organizzativi e logistici che presentano criticità elevate e pertanto, controlli non adeguati a contrastare le eventuali minacce per il trattamento dei dati a cui essi sono rivolti. Tali asset, o meglio i relativi controlli a sostegno, vanno formalmente catalogati in documenti di analisi sulla base dei quali dovranno essere successivamente formulati, quali parte integrante della documentazione a corredo della DPIA, i piani di sicurezza/azione temporali e strutturali relativi alla pianificazione degli interventi da mettere in atto per la implementazione o il potenziamento delle misure necessarie a raggiungere i livelli di sicurezza prefissati. Tali piani di azione vanno poi sottoposti all'attenzione del Titolare che, valutato il livello di rischio effettivo, identifica quale tra le seguenti opzioni per il trattamento del rischio ritiene di adottare:
- evitare il rischio, rinunciando, ad esempio, alle attività che lo generano;

- condividere il rischio con un'altra parte in grado di gestire il rischio in modo più efficace, come ad esempio assicuratori e fornitori;
- ridurre il rischio ad un livello ritenuto accettabile, attraverso l'implementazione delle contromisure necessarie al raggiungimento di tale soglia
- accettare il rischio se non si ritiene opportuna alcuna delle precedenti opzioni.

In tal senso, la Struttura Sanitaria, nella persona del titolare, adotta, in funzione del livello di rischio effettivo riscontrato, l'approccio sintetizzato nella seguente tabella:

Livello di rischio effettivo		Strategia di trattamento del rischio			
		Evitare	Condividere	Ridurre	Accettare
4	**Massimo**	**X**	**X**	**X**	
3	**Significativo**	**X**	**X**	**X**	
2	**Limitato**			**X**	**X**
1	**Trascurabile**				**X**

Come si evince dalla tabella, la soglia di accettabilità del rischio è stabilita ad un livello di rischio "Limitato", conseguentemente tutti gli altri casi, richiedono un trattamento al fine di ridurlo, trasferirlo o evitarlo. In ogni caso, anche quando il livello di rischio effettivo risulta limitato, la Struttura Sanitaria deve valutare i costi di una eventuale riduzione, rispetto ai benefici per l'interessato e quindi valutare l'opportunità di ridurre tale rischio.

In generale, nel caso in cui si optasse per il trattamento di riduzione, il rischio di riferimento sarà quello ritenuto accettabile dal titolare.

Quando il livello di rischio risulta essere Massimo o Significativo, è consigliabile prendere in considerazione:

- l'opzione evitare in caso di gravi violazioni di legge o di pericolo per le incolumità delle persone;
- l'opzione condividere quando, scartata l'opzione precedente, il costo di tale condivisione, in termini di tempi e costi, è minore di quello associato all'implementazione delle contromisure di sicurezza per la riduzione del rischio;
- l'opzione ridurre, anche congiuntamente a quella di condividere, quando il titolare ritiene opportuno l'implementazione delle contromisure necessarie al raggiungimento di un livello di soglia ritenuto accettabile.

Se la strategia di trattamento approvata prevede la riduzione, occorre valutare il livello di rischio residuo che si raggiungerà a valle della applicazione della strategia scelta ed i requisiti da attuare per il suo conseguimento, che saranno successivamente dettagliati all'interno di specifici piani di sicurezza. In base al livello di rischio residuo ed ai tempi previsti per il suo raggiungimento, il titolare valuta la necessità di consultare il Garante.

In ogni caso, a prescindere dal livello di rischio effettivo valutato, occorre definire una strategia di trattamento mirata a soddisfare tutti i requisiti normativi, non coperti o parzialmente coperti.

3.3.5 REDAZIONE E APPROVAZIONE DEL RAPPORTO DI DPIA/PIANO DI AZIONE

Tutto quanto fin qui indicato deve essere, come già in precedenza accennato, racchiuso in un rapporto generale della DPIA con relativo piano di sicurezza che ne costituisce parte integrante; tale rapporto deve contenere almeno i seguenti argomenti (art.37 par.7 GDPR):

- la descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
- la valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- i risultati della valutazione dei rischi per i diritti e le libertà degli interessati in linea con l'art. 5 par.1 del Regolamento;
- le misure previste per affrontare i rischi e dimostrare la conformità al Regolamento;
- la descrizione della strategia di gestione del rischio che si intende adottare.

Il documento deve essere approvato dal titolare e riportare i nominativi di chi ha contribuito alla redazione ed alla revisione del documento (RDP, responsabili del trattamento, etc.).
Il titolare può prendere in considerazione, in taluni casi, la pubblicazione di alcune parti del rapporto di DPIA.
Il documento pubblicato non deve comunque contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza o divulgare informazioni riservate. In queste circostanze, la versione pubblicata può consistere soltanto in una sintesi delle principali risultanze del DPIA, nella conclusione del DPIA o addirittura soltanto in una dichiarazione nella quale si afferma che la DPIA è stata condotta.

3.4 EVENTUALE CONSULTAZIONE PREVENTIVA DEL GARANTE

In linea con le prescrizioni del Regolamento (cfr.art.35), il titolare, prima di procedere al trattamento, deve consultare il Garante per la protezione dei dati personali qualora la DPIA indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio (rischio residuo elevato).
In caso di consultazione, il titolare del trattamento deve comunicare al Garante le seguenti informazioni:

- ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento;
- le finalità e i mezzi del trattamento previsto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del Regolamento;
- i dati di contatto del responsabile della protezione dei dati;
- la valutazione d'impatto sulla protezione dei dati;
- ogni altra informazione richiesta dal Garante.

Il Garante, se ritiene che il trattamento violi il Regolamento, in particolare qualora il titolare del Trattamento non abbia identificato o attenuato sufficientemente il rischio, fornisce, entro un termine prestabilito, dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento.
A fronte di tale parere, il titolare deve pianificare tutte le attività necessarie a recepire quanto segnalato dal Garante.

CAPITOLO 4 - NORME FINALI E DI RINVIO

4.1 DISPOSIZIONI FINALI

La presente procedura è stata adottata dal Titolare del trattamento. Suddetta procedura entra in vigore il giorno successivo alla sua approvazione. Il suo contenuto è soggetto ad aggiornamento periodico. La sua pubblicizzazione, secondo norma, avverrà attraverso il sito aziendale. È fatto obbligo a chiunque spetti di osservarlo.

4.2 NORMA DI RINVIO

Per quanto non espressamente previsto dal presente regolamento, si applicano le disposizioni di legge e i provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali che regolamentano la materia in oggetto.

Allegato B)

Politica di protezione dei dati personali

TITOLARE DEL TRATTAMENTO:	AST ASCOLI PICENO
Sede:	Via degli Iris, 63100 Ascoli Piceno AP
Tel./FAX:	0736.358691/93
PEO:	direzionegenerale.ast.ap@sanita.marche.it
PEC:	ast.ascolipiceno@emarche.it
Sito web:	*http://www.asur.marche.it*

Sommario

INTRODUZIONE

L'AZIENDA SANITARIA TERRITORIALE DI ASCOLI PICENO (di seguito azienda) riconosce l'importanza della protezione dei dati personali trattati e riferiti ai propri utenti, poiché direttamente legata alla tutela della dignità, della libertà e della eguaglianza delle persone.
Questo documento illustra la Politica di protezione dei dati personali adottata dall'azienda e manifesta la volontà di rispettare e proteggere i dati personali di ogni individuo, conformemente a quanto previsto dalle norme europee, in particolare dal Regolamento Generale sulla Protezione dei Dati UE n.2016/679 (in inglese General Data Protection Regulation o GDPR), e da quelle nazionali come il D.lgs. n.196/2003 e il D.lgs.n.101/2018 (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento). In aggiunta all'Informativa e al fine di assicurare la massima trasparenza, la Politica di protezione dei dati personali ha l'obiettivo di far conoscere a tutte le persone coinvolte (autorizzati e interessati) le tipologie di dati trattati, le modalità di raccolta, utilizzo, conservazione, condivisione, protezione e soprattutto i diritti previsti dal Regolamento e le modalità di esercizio.
Da notare che la Politica di protezione dei dati personali è, e sarà, un documento in continuo miglioramento, legato da un lato alla conformità normativa e dall'altro all'evoluzione delle modalità di trattamento connesse con i servizi erogati. È possibile verificare eventuali modifiche dal numero di Revisione e dalla data di aggiornamento posta in fondo ad ogni pagina.
Al fine di allineare i comportamenti di tutti gli attori impegnati nel trattamento dei dati personali, la presente Politica di protezione dei dati personali è presente presso la sede del Titolare nella versione aggiornata e pubblicata sul sito web istituzionale.

LE DEFINIZIONI

Ai fini della Politica di protezione dei dati personali si intende per:
«interessato»: persona fisica identificata o identificabile a cui si riferiscono i dati personali trattati, quindi studenti, genitori, tutori, personale docente e non docente, fornitore di servizi, partner, subappaltatore, candidato e, più in generale, chiunque sia in contatto con noi (di seguito: "tu" o "tuo").
«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

«Titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;
«Responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, individuato dallo stesso, a cui viene esternalizzata un'attività e che, pertanto, effettua per conto del Titolare dei trattamenti su dati personali. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione europea o degli Stati membri.
«Autorizzato al trattamento»: Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

IL CAMPO DI APPLICAZIONE

Il Campo di applicazione della Politica di protezione dati personali definisce il perimetro entro il quale questo documento ha l'obiettivo di operare. Nella pratica è lo stesso del Regolamento, che all'art.2 "Ambito di applicazione materiale" recita: "… si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi."
Per meglio comprendere il Campo di applicazione è necessario fare riferimento alla definizione di 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". Quindi il Campo di applicazione previsto nella presente Politica di protezione dati personali riguarda tutti i trattamenti automatizzati o cartacei effettuati dall'organizzazione o per conto di essa.

LO SCOPO DEL DOCUMENTO

La massima trasparenza nelle modalità di trattamento e gestione della sicurezza dei Suoi dati personali è la condizione essenziale ai fini della conformità a quanto previsto dall'art. 24 del Regolamento. La Politica di protezione dati personali è il documento in cui l'organizzazione si impegna a rispettare le "regole del gioco" previste dal Regolamento e dalle successive integrazioni e modificazioni normative.

I DESTINATARI

I destinatari di questo documento sono tutte le persone coinvolte nelle attività svolte dal Titolare o da soggetti che svolgono la propria attività per conto dello stesso, sia interni sia esterni alla sua struttura.

LE NORMATIVE DI RIFERIMENTO

- D.lgs. n.196/2003 Codice in materia di protezione dei dati personali
- GDPR dell'UE 2016/679 Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio Europeo 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. n. 101/2018 Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

I PRINCIPI APPLICATI

L'AST DI ASCOLI PICENO è il TITOLARE DEL TRATTAMENTO dei dati personali che l'interessato comunica o consegna con la modulistica cartacea o tramite gli strumenti del web per tutta la durata dei servizi erogati, delle prestazioni effettuate, degli incarichi conferiti, del rapporto di lavoro o delle forniture.

Il TITOLARE determina, singolarmente o insieme ad altri, le finalità e i mezzi per il trattamento dei dati personali; per questo motivo è anche responsabile delle informazioni che Lei condivide con noi.

Le modalità di trattamento dei dati personali sono conformi a quanto previsto dal Regolamento Europeo (UE) 2016/679 (GDPR), dalla disciplina nazionale vigente in materia e dalle successive modificazione e integrazioni, che nell'insieme definiscono le regole di protezione dei dati personali. In particolare, l'impegno è rivolto a:

a) trattare i Suoi dati personali in modo lecito, corretto e trasparente («liceità, correttezza e trasparenza»);
b) raccogliere i Suoi dati personali per finalità determinate, esplicite e legittime, e successivamente trattarli in modo che compatibile con tali finalità;
c) minimizzare i Suoi dati rendendoli adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti e trattati;
d) adottare tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);
e) conservare 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 («limitazione della conservazione»);
f) proteggere i dati personali con adeguate misure di sicurezza tecniche e organizzative rispetto a trattamenti non autorizzati o illeciti, dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

I DATI PERSONALI RACCOLTI, MODALITÀ DI UTILIZZO E FINALITÀ

Sempre nell'ottica della massima trasparenza, il registro delle attività di trattamento presente in azienda illustra nel modo più chiaro possibile, quali dati personali trattiamo, come, perché e in base a quali norme. La raccolta dei dati può avvenire in diversi modi, tramite moduli cartacei o digitali, via posta elettronica o attraverso gli strumenti del web. I campi obbligatori sono contrassegnati appositamente e nel caso non si fornisca il dato richiesto, potrebbe risultare impossibile proseguire nel procedimento e erogare il servizio prescelto.

L'accesso ai nostri servizi come anche dei nostri siti web, prevede la comunicazione dei Suoi dati personali in diverse modalità sia dirette (moduli, applicazioni, servizi o altro ancora) che indirette o completamente trasparenti, come ad esempio con i cookie impiegati al fine di comprendere come utilizza i nostri servizi e poterli migliorare. Altre volte i dati che La riguardano o che permettono di identificarla, possono provenire da altri Enti Pubblici o organizzazioni, essere comunicati o condivisi con altre aziende che svolgono queste attività per nostro conto, comunque nominate **Responsabili Esterne** e istruite a trattare i dati in massima sicurezza.

CONSENSO

Il Regolamento prevede che un trattamento è considerato lecito se ricorre almeno una delle basi giuridiche individuate, ovvero se:

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

  Quando non sussistono nessuna delle precedenti condizioni di liceità, il trattamento è considerato legittimo soltanto se l'interessato esprime il consenso al trattamento dei propri dati personali per una o più specifiche finalità. Per questi motivi la maggior parte dei trattamenti che effettua l'azienda non richiede di prestare il consenso dell'interessato. Soltanto in alcuni casi risulta necessario per la raccolta, l'uso o la divulgazione dei Suoi dati personali o dei Suoi familiari o se è necessario acquisire informazioni relative a dati particolari (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), per i quali è necessario che:
- l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;

- il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
- il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo (…);
- il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
- il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
- il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, (…);
- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (…);
- 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 (…); - il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (…).

COMUNICAZIONE

Alcuni Suoi dati personali potranno o dovranno essere condivisi con altri Contitolari, con soggetti esterni alla struttura o con i fornitori di servizi (ad esempio degli applicativi software) che svolgono queste attività per nostro conto, e che comunque sono nominati Responsabili Esterni ed istruiti a trattare i dati in massima sicurezza. Nelle clausole contrattuali è ben definito il perimetro del trattamento, per cui è assicurato che i Suoi dati personali non siano utilizzati per nessun'altra finalità ed è previsto che siano adottate tutte le misure tecnico organizzative adeguate alla protezione del patrimonio informativo.
Inoltre, sono forniti solo i sottoinsiemi di informazioni effettivamente necessari a svolgere i servizi appaltati a soggetti terzi.
I Suoi dati possono essere comunicati a enti pubblici, rispettando gli obblighi previsti dalle leggi e dai regolamenti. Oltre le ipotesi sopra descritte, i Suoi dati non saranno comunicati senza il Suo consenso. I Suoi dati non saranno mai diffusi.
I Suoi dati non saranno trasferiti in Paesi terzi non appartenenti all'Unione Europea e con normative di protezione dei dati personali non allineate al Regolamento.

Ad ogni modo, sono fornite all'esterno solo le informazioni effettivamente necessarie a svolgere l'eventuale attività richiesta.

CONSERVAZIONE

Tutti i dati personali sono conservati nel rispetto delle normative vigenti in materia di protezione dei dati.
Gli archivi cartacei correnti sono posizionati negli uffici preposti ai trattamenti a cui i faldoni si riferiscono. Gli archivi di deposito e storici sono posizionati solitamente presso apposite stanze-archivio ad accesso ristretto.
L'elaborazione dei dati avviene utilizzando applicazioni software su personal computer e server collegati in rete. Per alcuni trattamenti utilizziamo anche il cloud ma con i data center posizionati in Italia o comunque in UE. Soltanto il personale autorizzato dal titolare può accedere per effettuare le operazioni di trattamento o di manutenzione dei sistemi.
Gli eventuali outsourcer che operano sulla nostra strumentazione tecnologica, considerato il livello di accesso e i possibili impatti sulla riservatezza delle informazioni, sono nominati Responsabili (esterni) del trattamento. Il personale tecnico che abbia accesso a livello rete, sistema, database e applicativo è nominato amministratore di sistema ai sensi delle prescrizioni del Garante della protezione dei dati personali "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) (modificato in base al provvedimento del 25 giugno 2009)".
I Responsabili (esterni) provvedono alla nomina e alla comunicazione degli elenchi del personale specificatamente nominato Amministratore di Sistema per i sistemi aziendali gestiti in outsourcing.

TEMPISTICHE DI CONSERVAZIONE (RETENTION)

Il periodo di conservazione dipende fortemente dalla finalità ma l'intento è conservare solo i dati personali necessari e per il solo tempo utile al conseguimento delle finalità per cui sono stati raccolti. In alcuni casi si applicano le norme nazionali in tema di conservazione, che tendono ad allungare i tempi.
Nei casi particolari e nel momento di raccolta dei dati, il personale fornirà indicazioni sulle ragioni di prolungamento del periodo di conservazione e sulla durata prevista.

PROTEZIONE

La sicurezza delle informazioni riguarda gli aspetti di:

Riservatezza	Solo gli autorizzati possono accedere alle informazioni necessarie
Integrità	I dati sono protetti contro alterazioni o danneggiamenti, tutelando l'accuratezza e la completezza dei dati
Disponibilità	Le informazioni sono rese disponibili quando occorrono e nell'ambito di un contesto pertinente

La protezione degli asset digitali è basata sul paradigma previsto dal framework della National Institute of Standards and Technology (NIST), ripreso dalla Direttiva del Presidente

del Consiglio dei ministri 1° agosto 2015 - Misure minime di sicurezza ICT per le Pubbliche Amministrazioni, che prevede le seguenti attività a supporto della sicurezza:

IDENTIFICARE	Conoscere la propria infrastruttura per ridurre al minimo i rischi per sistemi, risorse e dati
PROTEGGERE	Progettare misure di sicurezza per limitare l'impatto di potenziali eventi su servizi e infrastrutture critici
INDIVIDUARE	Implementare attività per identificare il verificarsi di un evento di sicurezza informatica
REAGIRE	Adottare le misure appropriate dopo aver appreso di un evento di sicurezza
RECUPERARE	Pianificare la resilienza e il tempestivo recupero della capacità e dei livelli di servizio compromessi

L'impegno rappresentato nella presente Politica di protezione dei dati personali è quello di conservare in massima sicurezza i Suoi dati adottando le misure tecnico organizzative a seguito della valutazione dei rischi, che necessita di periodiche revisioni ogni qualvolta variano le circostanze, i contesti, le tecnologie e le normative.
L'obiettivo è garantire che non avvengano accessi non autorizzati, divulgazioni, perdite o distruzione dei Suoi dati personali, in ottemperanza alle leggi ma nel rispetto della dignità, della libertà e della eguaglianza delle persone. I fornitori di servizi che gestiscono i Suoi dati personali per nostro conto sono contrattualmente obbligati a fare altrettanto.

DIRITTI

Il legislatore europeo ha confermato i diritti previsti dal Codice privacy (la precedente normativa nazionale in tema di protezione dei dati personali) ed ha aggiunto dei nuovi.
I diritti di seguito riportati sono esercitabili su iniziativa dell'interessato, sempre che siano presenti delle limitazioni previste dalla normativa vigente. Ogni eventuale delucidazione potrà essere fornita su motivata richiesta. I suoi diritti sono:

Accesso e di informazione	Ha il diritto di essere informato in modo conciso, trasparente, intelligibile e facilmente accessibile sulle modalità con cui vengono trattati i Suoi dati personali. Ha anche il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che La riguardano e, in tal caso, di accedere a tali dati personali e di ottenerne una copia.
Rettifica	Ha il diritto di ottenere la rettifica dei Suoi dati personali non esatti. Ha anche il diritto di ottenere l'integrazione dei dati personali incompleti.
Cancellazione (Diritto all'oblio)	in alcuni casi, ha il diritto di ottenere la cancellazione dei tuoi dati personali quando non sono presenti basi giuridiche o legittimi motivi per conservare tali dati personali.
Limitazione del trattamento	Ha il diritto di ottenere la limitazione del trattamento dei Suoi dati personali, sempre che non siano presenti basi giuridiche o legittimi motivi che impediscano l'esercizio di questo diritto.

Portabilità dei dati	Ha il diritto di ricevere i Suoi dati personali, in un formato strutturato, di uso comune e leggibile da dispositivo automatico; ha il diritto di richiedere la trasmissione di tali dati a un altro titolare del trattamento. Questo diritto è applicabile solo per i trattamenti effettuati con strumenti informatici.
Opposizione	Ha il diritto di opporsi in qualsiasi momento al trattamento dei Suoi dati personali, sempre che non siano presenti basi giuridiche o legittimi motivi che impediscano l'esercizio di questo diritto.
Revoca del consenso	Ha il diritto di revocare in qualsiasi momento il Suo consenso a un trattamento (basato sul consenso). La revoca del consenso non ha validità retroattiva.
Proporre reclamo all'autorità di controllo	Ha il diritto di presentare reclamo al Garante per la protezione dei dati personali in merito alle modalità di trattamento adottate nella protezione dei dati personali.

PUNTO DI CONTATTO

Nel caso di dubbi, questioni sul trattamento dei Suoi dati personali o se desidera esercitare i diritti riportati nella tabella precedente, La preghiamo di contattarci ai numeri o indirizzi di seguito riportati:

TITOLARE DEL TRATTAMENTO: **AST ASCOLI PICENO**
Sede: Via degli Iris, 63100 Ascoli Piceno AP
Tel. / FAX: 0736.358691/93
e-mail: direzionegenerale.ast.ap@sanita.marche.it
PEC: ast.ascolipiceno@emarche.it
Sito web: http://www.asur.marche.it

RESPONSABILE PROTEZIONE DATI: **Avv. Bruno Antonio Malena**
e-mail/PEC: info.dataprotectionofficer@gmail.com
avv.brunoantoniomalena@ordineavvocatibopec.it

ALLEGATO C)

IL REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

SOMMARIO

CAPITOLO 1 - INTRODUZIONE

Il General Data Protection Regulation (di seguito, "GDPR") è un Regolamento, redatto dalla Commissione Europea e pubblicato sulla "Gazzetta Ufficiale" dell'Unione Europea in data 04 Maggio 2016, che ha il fine di armonizzare all'interno dell'UE le norme relative alla gestione dei dati personali. Il presente documento s'inquadra nel contesto degli aspetti inerenti alla gestione del Registro delle Attività di Trattamento, con lo scopo di descrivere le attività necessarie alla sua compilazione e successiva gestione. Il Registro dei trattamenti dei dati è considerato il cardine centrale degli adempimenti nei modelli privacy che l'azienda dovrà adottare; esso è lo strumento di rappresentazione verso l'autorità garante del progetto privacy adottato e, pertanto, occorrerà porre massima attenzione nella sua predisposizione e compilazione. Esso deve offrire una fotografia dei trattamenti eseguiti presso un'organizzazione ed è fondamentale, perché costituisce la base per identificare e procedere a tutti gli altri adempimenti, serve a definire a tutto tondo l'organizzazione del Titolare sotto il profilo della protezione dei dati. Naturalmente, redatto una prima volta, deve essere aggiornato, affinché ne sia mantenuta l'aderenza all'effettiva realtà organizzativa. Inoltre, non bisogna dimenticare che il Registro anche se sostanzialmente rappresenta un documento a valenza esterna (deve essere esibito su richiesta del Garante per documentare l'adempimento delle misure prescritte dal Regolamento e dalle altre disposizioni dell'ordinamento giuridico in materia di *data protection*), ha anche un ruolo interno di tipo sistemico in quanto, quale modello organizzativo "privacy", definisce le procedure per la condivisione delle informazioni in esso contenute tra i vari collaboratori/autorizzati, che debbono poter gestire con la dovuta consapevolezza le varie operazioni relative ai trattamenti assegnati.

In sede di prima applicazione della presente regolamentazione si premette che - in relazione al precedente assetto organizzativo – la ex Area Vasta n.5 (ora AST di Ascoli Piceno) è dotata di *Registro delle attività di trattamento* che, predisposto nel rispetto della vigente normativa, sarà oggetto di aggiornamento e/o modifica in relazione ai principi espressi nel presente documento, anche mediante apposito applicativo al fine di consentire, in un'ottica di efficienza ed efficacia, la gestione dinamica dello stesso. Detto registro è visionabile previo accesso agli atti ai sensi della Legge n.241/1990 e s.m.i.

1.1 FINALITA' DEL DOCUMENTO

Il GDPR introduce la necessità da parte del Titolare del trattamento e, ove applicabile, del proprio rappresentante, di avere un Registro delle Attività di Trattamento (di seguito Registro dei Trattamenti) svolte sotto la propria responsabilità (Art.30). Scopo del presente documento è quello di fornire le linee guida per facilitare la redazione e l'aggiornamento del Registro dei Trattamenti da parte della struttura sanitaria come richiesto dal Regolamento Europeo. Il Titolare del trattamento dati ha la responsabilità di mettere in atto misure tecniche ed organizzative adeguate per garantire ed essere in grado di dimostrare la conformità al GDPR (art.32 Regolamento UE 679/2016). Tali misure vanno aggiornate e riesaminate se necessario, devono essere preventive e devono tener conto dello stato dell'arte e dei costi di attuazione. A tale proposito il Titolare del trattamento, in ottica di *accountability*, deve rivedere ed aggiornare i sistemi di gestione e gli strumenti informatici in uso rendendoli conformi al Regolamento UE 2016/679. Ciò richiede che tutte le UU.OO. della Struttura Sanitaria, ognuno per il proprio ambito di competenza in relazione al trattamento dovranno supportare il titolare ed il RDP/DPO nello svolgimento delle valutazioni di conformità al GDPR. La redazione del Registro dei trattamenti è uno dei

principali adempimenti di *accountability* previsti dal Regolamento UE 2016/679; i contenuti di tale Registro sono elencati nelle lettere da a) a g) dell'art.30 comma 1.

1.1.1 DOCUMENTI DI RIFERIMENTO

Il presente paragrafo contiene la lista dei documenti di riferimento.

- Regolamento (UE) 2016/679 (GDPR)

1.2 GLOSSARIO

Acronimo/Definizione	Descrizione
GDPR	General Data Protection Regulation
RAT	Registro delle Attività di Trattamento
DPIA	Data Protection Impact Analysis
DPO	Data Processor Officer
RPD	Responsabile della Protezione dei Dati
UOC/UOSD	Unità Operativa Complessa/Unità Operativa Semplice Dipartimentale
Designato interno al Trattamento dati	Soggetto interno all'Amministrazione, formalmente individuato, cui il Titolare attribuisce compiti e funzioni specificamente individuati nell'ambito delle operazioni di trattamento effettuate nell'ambito della struttura di diretta competenza.

CAPITOLO 2 - REGISTRO DELLE ATTIVITA' DI TRATTAMENTO

Il Registro dei trattamenti è uno strumento fondamentale non soltanto per disporre di un quadro aggiornato dei trattamenti in essere all'interno di una organizzazione, ma è anche la fonte primaria di riferimento per lo svolgimento delle attività di analisi e valutazione degli impatti sulla privacy e sui rischi di sicurezza delle informazioni trattate. Redigerlo implica l'esecuzione di una mappatura dei trattamenti di dati che consenta di acquisire le informazioni su finalità dei trattamenti, tipologie di interessati, categorie di dati personali e di destinatari dei medesimi (a vario titolo e, se del caso, anche in Paesi extra-UE) e - dove possibile, come precisa la disposizione - anche quelle concernenti i termini di cancellazione dei dati nonché una descrizione generale delle misure di sicurezza (tecniche ed organizzative) adottate per la loro protezione. Ciò premesso, si comprende bene come la redazione del Registro dei trattamenti richiede tutta una serie di attività che vanno ben oltre quelle degli adempimenti legali e procedurali previsti dal Regolamento UE 2019/679 e che, affinché possano fotografare i singoli trattamenti posti in essere dal Titolare, necessitano di analisi, studi e riscontri puntuali. Fotografare i singoli trattamenti vuol dire anche analizzare il proprio sistema gestionale dei dati sia in termini di organizzazione e processi che in termini di applicazioni e infrastrutture al fine di valutare – per ogni trattamento gestito – i gaps rispetto alle richieste del GDPR e alla eventualità che un trattamento possa rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche e quindi la necessità di disporre una DPIA (valutazione d'impatto) dello stesso. Tutto questo richiede:

- Individuazione dei trattamenti posti in essere all'interno dell'Azienda;
- Analisi delle problematiche legate al trattamento dei dati personali;

- Individuazione dei trattamenti su server e su postazioni stand alone;
- Responsabilizzazione del singolo designato alla titolarità del trattamento dati;
- Verifica della sussistenza delle misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato ai rischi;
- Compilazione del Registro dei trattamenti dati come sommatoria dei trattamenti delle singole unità operative;
- Supporto e formazione sull'attività di manutenzione del Registro;
- Individuazione delle banche dati interessate dalle diverse attività di trattamento con il responsabile dei sistemi informativi aziendali e con il DPO;
- Supporto al DPO per il monitoraggio della continua rispondenza tecnica delle misure di sicurezza.

I Designati interni al trattamento dati (Direttori UU.OO.CC. e UU.OO.SS.DD.) sono tenuti a collaborare, per la mappatura dei trattamenti, anche ai fini del successivo aggiornamento. Tutte le strutture dell'Azienda, ciascuna per il proprio ambito di competenza in relazione al trattamento effettuato, supportano il Titolare, il/i Referente/i privacy e il DPO nello svolgimento delle valutazioni di conformità al GDPR. I Delegati segnalano le proposte di adeguamento necessarie a seguito di eventuali modifiche relative alle attività di trattamento, nonché degli eventuali mutamenti organizzativi o tecnici che riguardano i trattamenti di competenza effettuati, le modalità di svolgimento degli stessi, nonché le eventuali esternalizzazioni. Ogni ulteriore trattamento posto in essere, o le eventuali modifiche intervenute (nei termini sopra indicati), deve essere pertanto comunicato al Titolare, al RPD/DPO e al/i Referente/i privacy al fine di aggiornare il predetto Registro previa valutazione dell'impatto privacy. La U.O.C. che si occupa della gestione dei sistemi IT, nello specifico provvede a riscontrare la conformità dell'utilizzo delle risorse IT e a verificare la conformità al GDPR dei software applicativi utilizzati e le modalità di accesso alle banche dati interessate, parallelamente procede per quanto di propria competenza il servizio di Ingegneria clinica. Il suddetto percorso consente al Titolare, con cadenza periodica - mediante attività di ricognizione - di verificare, per il tramite dei Delegati Interni al trattamento, l'attualità del registro alle attività di trattamento svolte.

Le modalità operative secondo le quali tali attività dovranno svolgersi sono:

1) Analisi comparativa tra i trattamenti teoricamente individuati sulla base delle attività istituzionali della azienda e quelli da censire realmente sul campo. A tale proposito si avrà:
   - lo svolgimento di appositi incontri/interviste con i referenti aziendali responsabili delle unità operative decisionali, il DPO e il/i Referente/i privacy finalizzati al raggiungimento della definizione di un elenco di trattamenti consolidato e completo che fotografi in maniera realistica i trattamenti di dati personali svolti in Azienda;
   - la predisposizione di uno schema del Registro dei trattamenti elaborato sulla base delle informazioni raccolte nell'attività precedente.
2) Raccolta sul campo delle informazioni necessarie alla verticalizzazione del Registro nel contesto specifico dell'Azienda, al fine di individuare tutti gli elementi informativi necessari alla compilazione del Registro dei trattamenti. Questa attività sarà condotta attraverso:
   - la stretta collaborazione con il DPO e il/i Referente/i privacy con i quali condividere i criteri e gli eventuali strumenti utilizzati per la rilevazione dei dettagli informativi richiesti per la costruzione del Registro dei Trattamenti, come previsto dall'art.30 del Regolamento.

Secondo il Regolamento (art.30 par.1), il Registro delle Attività di Trattamento deve contenere perlomeno le seguenti informazioni:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, par.1.

Nello specifico il Registro dei Trattamenti viene prodotto in *Formato Microsoft Excel* e verrà gestito con l'ausilio di un applicativo software proprietario, semplice e intuitivo che offre tutta una serie di facilitazioni e suggerimenti per una sua corretta compilazione, che ne consentirà, in relazione al relativo carattere di dinamicità, ogni variazione derivante dalle attività di aggiornamento e dai mutamenti organizzativi in relazione al processo di aziendalizzazione in atto presso la AST di Ascoli Piceno. Tale software utilizza come data-Input l'"Elenco Base dei Trattamenti" censiti durante le attività di ricognizione e mappatura prime descritte, corredato da tutta una serie di tabelle da cui selezionare le definizioni opportune. Elenco base e tabelle sono a loro volta strutture in formato Excel che il software in questione gestisce come tabelle a tendina da cui selezionare le definizioni opportune. Ovviamente sarà sempre possibile accettare ex-novo eventuali definizioni non previste nelle liste predefinite. Il Registro dei Trattamenti in formato Excel che verrà generato è strutturato come di seguito descritto nelle seguenti sezioni:

1. Informazioni generali
2. Elenco dei Trattamenti.

2.1 INFORMAZIONI GENERALI

Questa sezione è propedeutica alla compilazione vera e propria del Registro e oltre ai dati del Titolare comprende una serie di parametri relativi alla release, ai dati dell'autore e dei soggetti preposti alla valutazione e validazione. Una volta validato il documento Excel che rappresenta il Registro verrà bloccato e protetto da apposita password di dominio del soggetto che opera la validazione.

Eventuali modifiche o aggiornamenti del Registro dei Trattamenti, precedentemente validato, verranno gestiti come versioni successive, mantenendo inalterate le versioni precedenti; un apposito campo "Motivazioni" potrà servire per descrivere i motivi della redazione di una nuova versione.

Tale modalità consentirà al Titolare del trattamento di dimostrare in continuità la conformità al GDPR (art.32 Regolamento UE 679/2016), ma principalmente di disporre di un quadro aggiornato dei trattamenti in essere all'interno della sua organizzazione. Nello specifico nella prima sezione sono esplicitate alcune informazioni generali quali:

- **Dati del Titolare:** devono essere indicati i dati identificativi del Titolare (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali) e i suoi dati di contatto;

- **Dati del Referente/i Privacy** (qualora nominato): devono essere indicati i dati identificativi del Responsabile dell'Ufficio Privacy (persona fisica nominata dal Titolare con la responsabilità di svolgere i compiti a lui assegnati) e i suoi dati di contatto;
- **Dati del DPO** (qualora nominato): devono essere indicati i dati identificativi del Responsabile della Protezione dei Dati (RPD o DPO) e i suoi dati di contatto;
- **Data di inizio validità**: deve essere indicata la data di creazione del Registro dei Trattamenti;
- **Data di aggiornamento**: deve essere indicata l'ultima data in cui il Registro dei Trattamenti è stato aggiornato.

2.2 ELENCO DEI TRATTAMENTI

Il Registro dei trattamenti è uno degli adempimenti cogenti previsti dal GDPR e deve essere tenuto in forma scritta o anche in formato elettronico e messo a disposizione dell'autorità di controllo qualora richiesto. Il Registro dei Trattamenti, corretto ed aggiornato nel tempo, costituisce una significativa evidenza della responsabilizzazione del Titolare, e costituisce l'elemento basilare per un approccio razionale ed esaustivo alla gestione della privacy, in quanto fornisce un quadro sinottico dei trattamenti posti in essere dall'organizzazione, da utilizzare come fonte di riferimento per ogni attività di valutazione degli impatti e dei rischi privacy. È importante riportare nel registro**:**

- Denominazione del trattamento
- Finalità del trattamento
- Descrizione workflow processo
- Categorie di interessati
- Categoria di dati personali
- Descrizione categoria di dati
- Unità operativa
- Delegati del titolare
- Base giuridica del trattamento
- Tipologia di dati
- Modalità di raccolta dei dati
- Modalità di gestione dei dati
- Modalità di archiviazione dei dati
- Periodo di conservazione
- Soggetti a cui possono essere comunicati i dati
- Responsabile del titolare/Contitolare
- Modalità di consenso
- Paesi terzi extra Ue verso i quali possono essere trasferiti dati
- Garanzie adottate per il trasferimento
- Ubicazione dei dati cartacei
- Tipo di software gestionali
- Ubicazione dei server
- Misure di sicurezza organizzative
- Misure di sicurezza tecnica
- Necessità DPIA

2.2.1 DENOMINAZIONE TRATTAMENTO

Si definisce "trattamento" (art.4) "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".
In questo campo deve essere riportato l'identificativo del Trattamento selezionandolo dall'"Elenco Base dei Trattamenti" censiti durante le attività di ricognizione e mappatura prime descritte, oppure, laddove non presente in tale elenco, può essere a compilazione libera. In tal caso, a completamento delle informazioni ad esso associate, verrà aggiunto all'elenco base.

2.2.2 FINALITA' DEL TRATTAMENTO

In questo campo deve essere inserita una breve descrizione delle finalità del trattamento. Il campo è attinto anch'esso dall'elenco base dei trattamenti con possibilità di modifica o compilazione libera.
Ovviamente quando si tratta di un nuovo Trattamento che si aggiunge all'elenco suddetto, la finalità specificata verrà salvata insieme al trattamento.
Esempi finalità:
-Rilascio esenzione
-Gestione del personale
-Prevenzione frodi
-Contabilità
-Gestione del contenzioso

2.2.3 DESCRIZIONE WORKFLOW PROCESSO

In questo campo deve essere inserita una breve descrizione del trattamento ed in particolare del processo con cui questo viene gestito. Il campo è a compilazione libera.

2.2.4 CATEGORIE DI INTERESSATI

In questo campo deve essere riportata la categoria di interessati del trattamento. L'interessato è una persona fisica identificata o identificabile, direttamente o indirettamente, con delle informazioni quali il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o con uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.
Esempi categorie di interessati:
-Pazienti
-Familiari
-Dipendenti
-Fornitori

2.2.5 CATEGORIA DI DATI PERSONALI

In questo campo deve essere riportata la categoria di dati utilizzata nel trattamento (es. anagrafica, dati sanitari, dati finanziari). Il campo è attinto anch'esso dall'elenco base dei trattamenti.
Esempi categoria di dati personali:
-Dati personali di identificazione
-Dati che rivelano l'origine etnica
-Dati che rivelano opinioni politiche
-Dati genetici
-Dati biometrici

-Dati finanziari
-Descrizione fisica
-Dati professionali

2.2.6 DESCRIZIONE CATEGORIA DI DATI

In questo campo deve essere descritta con maggiore dettaglio la categoria inserita nel campo precedente, indicando i dati personali che la compongono (es. nome, cognome, indirizzo, diagnosi clinica, numero conto corrente). Il campo è a compilazione libera.

2.2.7 UNITA' OPERATIVA

In questo campo deve essere inserita l'Unità Organizzativa dell'azienda, il servizio o il Presidio in cui viene svolto il Trattamento. Anche per questo campo è prevista una lista, nella fattispecie, dell'organigramma aziendale dalla quale selezionare la o le UU.OO. che effettuano il trattamento in questione (più unità Operative possono effettuare lo stesso trattamento, come ad esempio il trattamento di Degenza). In tale campo vanno indicate tutte le altre UU.OO. che concorrono al trattamento.

2.2.8 DELEGATI DEL TITOLARE

In questo campo vanno indicati i responsabili (Delegati interni del Titolare) delle UU.OO. che concorrono al trattamento in questione. Anche a questo campo è associata la lista dell'organigramma aziendale. Ovviamente esso, come anche quello precedente, possono essere a compilazione libera qualora la tabella dell'organigramma aziendale dovesse essere non aggiornata.

2.2.9 BASE GIURIDICA DEL TRATTAMENTO

In questo campo devono essere riportati i principi di liceità del trattamento come previsto dall'art.6 par. 1, dall'Art. 9 e dall'art.10 del GDPR.
Esempi:
-Consenso dell'interessato
-Legittimo interesse del titolare
-Ricerca storica/statistica
-Interesse pubblico per sanità pubblica
-Esecuzione di un contratto

2.2.10 TIPOLOGIA DI DATI

I dati personali sono classificati nelle seguenti tipologie:

Dati personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (vedi Art.4 par.1).

Dati particolari (o sensibili): 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.

Dati giudiziari: quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

2.2.11 MODALITA' DI RACCOLTA DEI DATI

In questo campo deve essere riportato il formato con il quale vengono raccolti i dati del trattamento.

Esempi:
-Cartaceo
-Digitale
-Cartaceo e digitale.

2.2.12 MODALITA' DI GESTIONE DEI DATI

In questo campo deve essere riportata la modalità con la quale vengono gestiti i dati del trattamento.

Esempi:
-Automatizzata
-Non automatizzata
-Semiautomatizzata.

2.2.13 MODALITA' DI ARCHIVIAZIONE DEI DATI

In questo campo deve essere riportato il formato con il quale vengono archiviati i dati del trattamento.

Esempi:
-Cartaceo
-Digitale
-Cartaceo e digitale.

2.2.14 PERIODO DI CONSERVAZIONE

In questo campo, a compilazione libera, devono essere riportati i termini ultimi previsti per la cancellazione dei dati personali trattati. Il periodo di conservazione dei dati deve essere strettamente correlato allo scopo perseguito con il trattamento, ovvero deve rispettare i termini di legge qualora esistenti.
L'AST di Ascoli Piceno fa riferimento alla Determina ASUR del 21-07-2017 n.466, nella quale sono indicati per ciascuna area e fattispecie, i relativi termini di conservazione.

2.2.15 SOGGETTI A CUI POSSONO ESSERE COMUNICATI I DATI

Si definisce destinatario, l'insieme dei quali costituisce l'ambito di comunicazione: "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". In questo campo deve essere riportata la categoria di destinatari a cui i dati personali sono stati o saranno comunicati.

Esempi:
-Amministrazioni pubbliche

-ANAC
-Istituti di previdenza
-Organi di giustizia e di polizia.

2.2.16 RESPONSABILE DEL TITOLARE/CONTITOLARE

Il GDPR definisce Responsabile (ex art.28) "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento". In questo campo devono essere riportati i dati identificativi e di contatto del/i Responsabile/i eventualmente presente/i per lo specifico trattamento o dell'ente terzo, persona fisica o giuridica che tratta dati per contro del titolare del trattamento ma che non viene nominato Responsabile. In tale campo, qualora il soggetto in questione si configura secondo l'art.26 del GDPR ("*1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento*.") va annotata chiaramente la condizione di contitolarità. E ciò in quanto essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt.13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. In questo campo devono essere riportati i dati identificativi e di contatto del/i contitolare/i eventualmente presente/i per lo specifico trattamento.

2.2.17 MODALITA' DI CONSENSO

Si definisce "consenso" (art.4): "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".
In questo campo devono essere riportate le caratteristiche del consenso.
Esempi:
-Espresso
-Per iscritto
-comportamentale

2.2.18 PAESI TERZI EXTRA UE VERSO I QUALI POSSONO ESSERE TRASFERITI I DATI

In questo campo deve essere indicato il paese terzo o l'organizzazione internazionale Extra UE verso cui si ha l'eventuale trasferimento dei dati. Il campo è a compilazione libera. A tale proposito si chiarisce che il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, anche se Extra UE, è ammesso se la Commissione UE ha stabilito che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato (Art.45 comma 1 Capo V del Regolamento GDPR). In tal caso il trasferimento non necessita di autorizzazioni. Nel caso contrario invece, ovvero in assenza di parere positivo da parte della Commissione UE, occorre che il Responsabile Esterno che effettua il trasferimento, fornisca in proprio le garanzie adeguate e venga assicurato che gli interessati possano esercitare i propri diritti utilizzando mezzi di ricorso effettivi. Le garanzie necessarie vanno indicate al successivo campo.

2.2.19 GARANZIE ADOTTATE PER IL TRASFERIMENTO

In questo campo vanno indicate le garanzie, secondo la Commissione Europea per la Protezione dei Dati, offerte dal paese terzo in questione.
Esempi:
-Consenso dell'interessato
-Motivi di interesse pubblico
-Clausole standard
-Regole aziendali vincolanti

2.2.20 UBICAZIONE DATI CARTACEI
In questo campo devono essere riportate la ubicazione degli ambienti e la descrizione dei dispositivi fisici dove vengono custoditi e archiviati i dati cartacei (armadi con o senza chiusura, scaffali, etc.)

2.2.21 TIPO DI SOFTWARE GESTIONALI
In questo campo deve essere riportato il nome del data base nel quale sono memorizzati i dati relativi al trattamento e l'applicativo che li elabora.

2.2.22 UBICAZIONE SERVER
In questo campo deve essere riportato l'allocazione fisica dei server dove risiedono i DB e gli applicativi software.

2.2.23 MISURE DI SICUREZZA ORGANIZZATIVE
Il campo in questione e quello successivo hanno lo scopo di rispondere all'art.32 del GDPR, ovvero: "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento."

In questo campo devono essere riportate, ove possibile, le misure di sicurezza organizzativa adottate a protezione del trattamento.
Esempi:
-Casseforti con chiavi
-Dati cartacei conservati in buste sigillate
-Formazione del personale

2.2.24 MISURE DI SICUREZZA TECNICA
In questo campo devono essere riportate, ove possibile, le misure di sicurezza tecnica adottate a protezione del trattamento.
Esempi:
-Autenticazione con User e Password

-Autenticazione con caratteristiche biometriche
-Autenticazione con Badge magnetico
-Istallazione sistemi antivirus

2.2.25 NECESSITA' DPIA

L'art.35 cita: "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, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno".

Esempi:
-Non richiesta
-Da avviare
-Terminata

2.2.26 NOTE

In questo campo è possibile riportare le eventuali note in riferimento ad uno qualsiasi dei campi precedenti ovvero i riferimenti a documenti che supportano quanto inserito.

ALLEGATO D)

MODULO DI RICHIESTA DI ESERCIZIO DEI DIRITTI DA PARTE DELL'INTERESSATO

Gentile Interessato, il Regolamento Generale sulla protezione dei dati dell'Unione Europea (GDPR) prevede la possibilità di esercitare sui dati personali che La riguardano i seguenti diritti:

- **Accesso** ovvero chiedere conferma che sia o meno in corso un trattamento (art. 15) e conoscere alcune notizie sul trattamento come:
  - le finalità del trattamento;
  - le categorie di dati personali in questione;
  - 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;
  - il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
  - tutte le informazioni disponibili sulla loro origine qualora i dati non siano raccolti presso l'interessato;
  - l'esistenza di un processo decisionale automatizzato, compresa la profilazione (art. 22 paragrafi 1 e 4,) e le conseguenze di tale trattamento previste per l'interessato.
- **Rettifica** degli eventuali dati personali inesatti o incompleti (art.16)
- **Cancellazione** dei dati personali o applicazione del cosiddetto «diritto all'oblio» (art. 17)
- **Limitazione** ovvero ridurre il trattamento dei dati personali (art.18)
- **Portabilità** dei dati (art. 20) ovvero ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali oppure, se possibile tecnicamente, ottenere la trasmissione diretta tra titolari
- **Opposizione** al trattamento dei dati personali (artt.21 e 22).

È sufficiente compilare il presente modulo e inviarlo al:

TITOLARE DEL TRATTAMENTO:	**AST di Ascoli Piceno**
Sede:	Via degli Iris, 63100 Ascoli Piceno
Tel. / FAX:	0736.358691/93
PEO:	direzionegenerale.ast.ap@sanita.marche.it
PEC:	ast.ascolipiceno@emarche.it
Sito web:	http://www.asur.marche.it/
RESPONSABILE PROTEZIONE DATI:	**Avv. Bruno Antonio Malena**
Tel.:	3803674364
e-mail/PEC:	info.dataprotectionofficer@gmail.com avv.brunoantoniomalena@ordineavvocatibopec.it

Le rammentiamo di inviare una copia di un documento di identità allegata al modulo.

Daremo riscontro dell'avvenuto ricevimento della Sua richiesta e Le risponderemo entro un mese.

Il sottoscritto Interessato:

Nome e cognome	
Codice fiscale	
Luogo e data di nascita	
Indirizzo postale	
Numero di telefono	
Indirizzo e-mail/PEC	

RICHIEDE

☐ Accesso ☐ Limitazione

☐ Rettifica ☐ Portabilità

☐ Cancellazione ☐ Opposizione

Relativamente a:

Dati personali	
Categorie di dati	
Trattamenti	

per le seguenti motivazioni:

Note:

Ascoli Piceno, li _____ Firma _____

INFORMATIVA AI SENSI DELLA VIGENTE NORMATIVA IN TEMA DI PROTEZIONE DEI DATI PERSONALI
(artt. 15-22 del Regolamento UE 2016/679)

Gentile Interessato,

L'AST Ascoli Piceno, in qualità di titolare del trattamento di dati personali connesso alla procedura avviata con la presente modulistica, precisa che il trattamento è finalizzato a riconoscere e garantire i benefici previsti dalla normativa comunitaria e nazionale in ordine alla protezione dei dati personali, con particolare riferimento ai diritti previsti dagli articoli 15 e seguenti del Regolamento (UE) 2016/679, come attuati nell'ordinamento italiano dalla vigente normativa in materia.

COSA FACCIAMO CON I VOSTRI DATI (Categorie dati, obbligo legale/contrattuale, requisito necessario)

Il trattamento potrebbe coinvolgere, oltre a dati personali e dati di contatto, anche categorie particolari di dati personali ai sensi dell'art. 9 del Regolamento (UE) 2016/679, ivi compresi dati personali che rivelino l'origine 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, dat i relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, eventualmente forniti o acquisiti dalla ns. Azienda nell'ambito del rapporto con Lei.

PERCHÉ TRATTIAMO I VOSTRI DATI (Finalità e base giuridica)

Al fine di tutelare la riservatezza dei dati comunicati, di offrire loro un'adeguata protezione e al fine di minimizzare i dati oggetto di trattamento, i dati personali comunicati saranno oggetto di registrazione, conservazione e trattamento nel rispetto delle misure di sicurezza adottate dalla ns. Azienda. Tali modalità sono tese a porre in atto le misure idonee a tutelare i diritti e le libertà degli interessati da eventuali accessi di soggetti non autorizzati.

DOVE E A CHI FINISCONO I VOSTRI DATI (Comunicazione a terzi e categorie di destinatari)

I dati comunicati non saranno ceduti a terzi né saranno oggetto di trasferimenti verso paesi al di fuori dello spazio UE e non saranno comunicati a soggetti terzi, a meno di esplicita Sua richiesta in tal senso, nell'esercizio, ove ipotizzabile, del diritto alla portabilità ai sensi dell'art. 22 del GDPR, come attuato nella normativa nazionale vigente. I dati personali non saranno oggetto di profilazione o altri processi decisionali automatizzati.

COME TRATTIAMO I VOSTRI DATI E CON QUALI MEZZI (Modalità di trattamento)

Il Trattamento è effettuato sulla base degli obblighi di legge previsti dal Regolamento (UE) 2016/679 (così come attuato nella normativa nazionale vigente), pertanto, in mancanza dei dati richiesti o laddove siano integrate le ipotesi di limitazione all'esercizio dei diritti stessi, potrebbe non essere possibile garantire il completo esercizio dei Suoi diritti.

QUANTO TEMPO CONSERVIAMO I VOSTRI DATI (Periodo di conservazione)

I dati oggetto della presente domanda rimarranno conservati presso l'Amministrazione aziendale sino alla definizione della procedura connessa all'esercizio dei diritti suddetti, in ossequio alle finalità perseguite dalla legge, mentre saranno oggetto di cancellazione, laddove, al termine della procedura, non sussistano interessi da salvaguardare in procedure giudiziali o extragiudiziali.

QUALI SONO I VOSTRI DIRITTI

In aggiunta all'esercizio dei suddetti diritti, resta fermo il diritto per l'interessato di proporre reclamo innanzi all'Autorità Garante per la Protezione dei Dati Personali avverso il trattamento dei propri dati effettuato dalla ns. Azienda.

ALLEGATO E)

Informativa navigatori siti internet aziendali[1]

Articolo 13, Regolamento (UE) n.2016/679

PERCHÉ QUESTE INFORMAZIONI

Il Regolamento (UE) 2016/679 (di seguito "Regolamento") prevede che Lei Utente (o Interessato) sia informato sulle modalità di trattamento dei dati personali raccolti durante la consultazione dei siti web delle AST accessibili al seguente indirizzo Internet: *www.asur.marche.it*

Le informazioni riportate non riguardano i siti web, pagine o servizi online raggiungibili tramite link ipertestuali eventualmente pubblicati all'indirizzo www.asur.marche.it.

CHI SIAMO

La AST DI ASCOLI PICENO è il **TITOLARE DEL TRATTAMENTO** dei dati relativi a persone fisiche identificate o identificabili trattati a seguito della consultazione dei siti web sopra elencati.

TITOLARE DEL TRATTAMENTO:	**AST DI ASCOLI PICENO**
Sede:	Via degli Iris, 63100 Ascoli Piceno (AP)
Tel:	0736-358691/93
PEO:	direzionegenerale.ast.ap@sanitamarche.it
PEC:	ast.ascolipiceno@emarche.it
Sito web:	https://www.asur.marche.it
RESPONSABILE PROTEZIONE DATI:	**Avv. Bruno Antonio Malena**
Tel.:	3803674364
e-mail/PEC:	info.dataprotectionofficer@gmail.com avv.brunoantoniomalena@ordineavvocatibopec.it

PERCHÉ POSSIAMO TRATTARE I VOSTRI DATI (Base giuridica o condizione di liceità)

I dati personali indicati in questa pagina sono trattati dall'AST ASCOLI PICENO nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, inclusi i compiti istituzionali di informazione, promozione della salute, prevenzione, diagnosi, cura, riabilitazione e ricerca.

---

[1] **Si precisa che il presente allegato sarà oggetto di variazioni in relazione alla implementazione del nuovo sito aziendale**

PERCHÉ TRATTIAMO I VOSTRI DATI (Finalità, scopo della raccolta e dell'elaborazione dei dati)

I dati degli Utenti sono raccolti ed utilizzati per consentire la corretta navigazione nel Sito web, per migliorare l'esperienza di navigazione, nonché per rispondere ad eventuali richieste e comunicazioni da parte degli Utenti.

COSA FACCIAMO CON I VOSTRI DATI (Categorie dati, requisito necessario)

Dati di navigazione

I sistemi informatici e le procedure software preposte al funzionamento di questo sito web acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet.

In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer e dei terminali utilizzati dagli utenti, gli indirizzi in notazione URI/URL (Uniform Resource Identifier/Locator) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente.

Tali dati, necessari per la fruizione dei servizi web, vengono anche trattati allo scopo di:

- ottenere informazioni statistiche sull'uso dei servizi (pagine più visitate, numero di visitatori per fascia oraria o giornaliera, aree geografiche di provenienza, ecc.);
- controllare il corretto funzionamento dei servizi offerti.

I dati di navigazione sono conservati per non più di sette giorni (salve eventuali necessità di accertamento di reati da parte dell'Autorità giudiziaria).

Dati comunicati dall'utente

L'invio facoltativo, esplicito e volontario di messaggi agli indirizzi di contatto di AST ASCOLI PICENO, i messaggi privati inviati dagli utenti ai profili/pagine istituzionali sui social media (laddove questa possibilità sia prevista), nonché la compilazione e l'inoltro dei moduli presenti sui siti aziendali, comportano l'acquisizione dei dati di contatto del mittente, necessari a rispondere, nonché di tutti i dati personali inclusi nelle comunicazioni.

Nel caso di erogazione di ulteriori servizi non illustrati in questa pagina, sarà nostra cura pubblicare le informative integrative nei rispettivi siti delle AST.

Cookie e altri sistemi di tracciamento

In questo sito web non sono utilizzati cookie di profilazione degli utenti.

Viene effettuato il trattamento dati per la produzione di statistiche sulla navigazione nei siti aziendali mediante la piattaforma Web Analytics Italia (WAI) *https://webanalytics.italia.it/*, la piattaforma nazionale di raccolta e analisi dei dati statistici relativi al traffico dei siti e servizi digitali della Pubblica Amministrazione italiana.

Sono invece utilizzati i cosiddetti cookie di sessione (non persistenti) in modo strettamente limitato a quanto necessario per la navigazione sicura ed efficiente dei siti. La memorizzazione dei cookie di sessione nei terminali o nei browser è sotto il controllo dell'utente; sui sistemi server le informazioni relative ai cookie, una volta terminate le sessioni HTTP, restano registrate nei log dei servizi con tempi di conservazione comunque non superiori ai sette giorni, al pari degli altri dati di navigazione.

DOVE E A CHI FINISCONO I VOSTRI DATI (Destinatari dei dati)

I dati personali raccolti sono trattati dal personale di AST ASCOLI PICENO, che opera sulla base di specifiche istruzioni fornite in ordine a finalità e modalità del trattamento medesimo.

QUALI SONO I VOSTRI DIRITTI E COME POTETE ESERCITARLI

Ogni Interessato ha il diritto di ottenere da AST ASCOLI PICENO, nei casi previsti, l'accesso ai propri dati personali, la rettifica, la cancellazione degli stessi o la limitazione del trattamento che li riguarda. L'interessato ha, altresì, diritto di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza deve essere presentata contattando il Responsabile della protezione dei dati agli indirizzi sopra riportati, fermo restando il diritto di proporre un reclamo all'Autorità Garante per la Protezione dei Dati Personali (come previsto dall'art.77 del Regolamento) o, eventualmente, adire le opportune sedi giudiziarie (art.79 del Regolamento).

AGGIORNAMENTI

L'Informativa è lo strumento previsto dal Regolamento per applicare il principio di trasparenza e agevolare Lei (interessato) nella gestione delle informazioni che trattiamo e che La riguardano. Al variare delle modalità di trattamento, della normativa nazionale o europea, l'Informativa potrà essere revisionata e integrata; in caso di cambiamenti importanti, sarà data notizia nella home page del sito web istituzionale.

ALLEGATO F)

Informativa Utenti
(articolo 13-14, Regolamento UE n. 2016/679)

CHI SIAMO

TITOLARE DEL TRATTAMENTO:	**AST di Ascoli Piceno**
Sede:	Via degli Iris 63100 Ascoli Piceno
Tel./FAX:	0736.358691/93
PEO:	direzionegenerale.ast.ap@sanita.marche.it
PEC:	ast.ascolipiceno@emarche.it
Sitoweb:	http://www.asur.marche.it/
RESPONSABILE PROTEZIONE DATI:	**Avv. Bruno Antonio Malena**
Tel.:	3803674364
e-mail/PEC:	info.dataprotectionofficer@gmail.com avv.brunoantoniomalena@ordineavvocatibopec.it

L'AST di Ascoli Piceno è il **TITOLARE DEL TRATTAMENTO** dei dati personali che La riguardano e che potranno essere gestiti in modalità cartacea o attraverso i sistemi informatici.
Il RESPONSABILE della PROTEZIONE dei DATI *(o Data Protection Officer -DPO)* è il Suo punto di contatto per qualsiasi questione o problema legati all'applicazione del Regolamento sulla privacy (GDPR 679/2016).

COSA FACCIAMO CON I VOSTRI DATI (Categorie dati, requisito necessario)

Di solito trattiamo soltanto dati personali "comuni"; in alcuni casi è necessario trattare anche dati "particolari" quelli, cioè che "*rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, 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*".
Sarà cura del personale comunicarLe tutte le informazioni necessarie.
Le ricordiamo tuttavia che fornire i Suoi dati personali è necessario per poter usufruire dei servizi forniti dall'AST DI ASCOLI PICENO. In assenza dei Suoi dati potranno esserle erogati i servizi sanitari solo nei casi e con le modalità previste dalla Legge.

PERCHÉ TRATTIAMO I VOSTRI DATI (Finalità, base giuridica)

Trattiamo i Suoi dati per lo svolgimento delle funzioni istituzionali dell'AST DI ASCOLI PICENO quali la diagnosi, la cura, la prevenzione, la riabilitazione. Oltre a queste ci occupiamo di

igiene e sanità pubblica, assistenza farmaceutica, ricerca clinica ed epidemiologica e attività di carattere sociale e amministrativo-contabile correlate al perseguimento dei predetti fini istituzionali, comprese la valutazione della qualità dei servizi erogati, gli obblighi di natura precontrattuale, contrattuale, legale, le comunicazioni di servizio, la gestione dei reclami e infine per il riscontro delle richieste di informazioni inoltrate.
Trattiamo i Suoi dati anche per funzioni di carattere pubblico di competenza dell'azienda, come la fornitura di beni e servizi all'utente per la salvaguardia della salute, l'attività certificatoria, l'adempimento degli obblighi di legge come le norme civilistiche, fiscali, contabili, di gestione amministrativa e di sicurezza. I Suoi dati personali, anche se raccolti da uno specifico ufficio o presidio, potranno essere utilizzati dal Titolare anche per esigenze di altri settori, purché il trattamento sia sempre connesso al perseguimento delle finalità istituzionali.
Per tutto ciò, non è necessario richiedere il Suo consenso.

QUANDO CHIEDIAMO IL SUO CONSENSO (Attività facoltative rispetto alle precedenti)

Il Suo **Consenso** è richiesto, invece, quando il trattamento dei dati riguarda delle finalità considerate importanti per l'azienda, ma che non rientrano nelle funzioni istituzionali previste dalle norme nazionali, ovvero:

1. Per effettuare le Comunicazioni del Suo stato di salute a Suoi familiari o conoscenti;
2. Per effettuare le Comunicazioni del Suo stato di salute al Suo medico curante;
3. Per costituire un Dossier Sanitario Elettronico, ovvero un servizio utile a tenere traccia dei Suoi episodi clinici, presenti e passati, trattati nella nostra azienda;
4. Per permetterle di Consultare gratuitamente ed estrarre i Suoi referti via web, nel pieno rispetto della sicurezza dei Suoi dati, invece che ritirarli all'apposito sportello;
5. Per autorizzare l'AST AP a trattare i Suoi dati sanitari per fini di ricerca scientifica, sperimentazione e farmacovigilanza.

COME TRATTIAMO I SUOI DATI E CON QUALI MEZZI (Modalità di trattamento)

Nel trattare i Suoi dati, adottiamo tutte le misure tecniche e organizzative utili ad evitare accessi non autorizzati, divulgazione, modifica o distruzione. Per alcuni trattamenti utilizziamo anche il cloud con i data center posizionati esclusivamente in Europa. Soltanto il personale autorizzato dal Titolare può accedere per effettuare le operazioni di trattamento o di manutenzione dei sistemi.
Non sono utilizzati sistemi di decisione automatica, compresa la profilazione.

DOVE FINISCONO I SUOI DATI (Comunicazione a terzi e categorie di destinatari)

In alcuni casi è possibile che i Suoi dati personali siano comunicati a soggetti esterni che svolgono attività per nostro conto. Questi tuttavia vengono nominati Responsabili e istruiti a trattare i dati in massima sicurezza.
I Suoi dati personali sono altresì comunicati ad altri enti pubblici solo per obblighi previsti da leggi e regolamenti. Ove necessario, potranno essere comunicati ad altre aziende sanitarie per fini strettamente correlati al miglior esito delle attività di diagnostica e di terapia.
I Suoi dati non saranno mai diffusi.

In caso di trasferimento verso Paesi terzi non appartenenti all'Unione Europea, essi verranno protetti con idonee misure di sicurezza e comunicati solo verso Paesi con normative di protezione dei dati personali allineate al Regolamento Europeo.

QUANTO TEMPO CONSERVIAMO I SUOI DATI (Periodo di conservazione)

I Suoi dati personali sono conservati solo per il tempo necessario al perseguimento delle finalità sopra riportate, a meno che la Legge non preveda un periodo di conservazione più lungo.
Le norme nazionali sulla conservazione prevedono che i Suoi dati personali continuino ad essere memorizzati per tutto il tempo necessario al perseguimento delle finalità sopra riportate e per il tempo di conservazione previsto per la cartella clinica.

DA CHI RICEVIAMO I SUOI DATI (Fonte dei dati)

Laddove possibile, raccogliamo i dati personali direttamente, ma se le Sue condizioni di salute non ce lo permettono ci rivolgiamo a:

- chi esercita legalmente la rappresentanza;
- un prossimo congiunto, familiare, convivente o unito civilmente, o, infine, a un fiduciario.

In loro assenza, nel rispetto delle misure per la tutela dei diritti e delle libertà dell'interessato, ci rivolgiamo al responsabile della struttura presso cui Lei dimora o al medico da Lei designato a trattare i suoi dati personali idonei a rivelare lo stato di salute.

QUALI SONO I SUOI DIRITTI

Può richiedere direttamente al Titolare del trattamento di vedere, correggere, cancellare o limitare i dati che trattiamo e che La riguardano. In alcuni casi, può anche opporsi o revocare il Suo consenso al trattamento; ha anche il diritto alla portabilità dei dati e quindi in qualsiasi momento può richiedere una copia digitale degli stessi o il trasferimento automatico tra enti pubblici. Può anche richiedere l'applicazione del diritto all'Oblio ma solo per i trattamenti per i quali Le abbiamo richiesto il consenso.

COME PUÒ ESERCITARE I SUOI DIRITTI

A volte l'evoluzione tecnologica non ci facilita il compito di proteggere i Suoi dati.
Se ha dei dubbi che stiamo conservando Suoi dati errati, incompleti o se pensa che Li abbiamo gestiti male, La preghiamo di contattare il Responsabile della Protezione dei Dati (RPD/DPO) oppure inviare una richiesta utilizzando il modulo di Richiesta di Accesso ai dati, scaricabile dal sito dell'ASUR MARCHE sotto riportato. Il nostro Responsabile della Protezione dei Dati (RPD/DPO) esaminerà la Sua richiesta e La contatterà per risolvere al più presto il problema. Altrimenti ha il diritto di proporre un reclamo all'Autorità Garante per la Protezione dei Dati Personali. Ulteriori informazioni sul trattamento dei dati, sull'esercizio dei sui diritti e sulla disciplina normativa in materia sono disponibili ai seguenti indirizzi web:

Pagina web GDPR	*http://www.asur.marche.it/gdpr*
Modulo di richiesta di accesso ai dati	*http://www.asur.marche.it/gdpr/RichiestaAccessoaiDati.pdf*

Regolamento (UE) 2016/679	*http://www.asur.marche.it/gdpr/Regolamento.pdf*
Glossario GDPR	*http://www.asur.marche.it/gdpr/GlossarioGDPR.pdf*
Garante italiano della protezione dei dati personali	*http://www.garanteprivacy.it*
Pagina informativa GDPR-GPDP	*https://www.garanteprivacy.it/regolamentoue*
Guida all'applicazione del regolamento UE 2016/679	*https://www.garanteprivacy.it/documents/10160/0/ Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf*

AGGIORNAMENTI

L'Informativa è lo strumento previsto dal Regolamento per applicare il principio di trasparenza e agevolare la gestione delle informazioni che trattiamo e che La riguardano. Al variare delle modalità di trattamento, della normativa nazionale o europea, l'Informativa potrà essere revisionata ed integrata; in caso di cambiamenti importanti, comunque, sarà data notizia nella home page del sito web istituzionale.

ALLEGATO G)

ATTO DI NOMINA DESIGNATO TRATTAMENTO DEI DATI PERSONALI
(DIRETTORE U.O.C./U.O.S.D./altro)
(art. 2-quaterdecies, D.Lgs.n.196/2003 e art.29, Reg.UE 679/2016)
(Personale interno - Modello specifico per compiti e funzioni)

AL DIRETTORE
SEDE

OGGETTO: Atto di nomina del Designato al Trattamento ai sensi di quanto statuito dall'art.29 Regolamento UE 2016/679 e relativi compiti.

Il Direttore Generale della AST di Ascoli Piceno

Al fine di procedere alla nomina, ai sensi del Regolamento Aziendale per la protezione dei dati personali, approvato con Determina n. _____/ASTAP del _____, dei Responsabili interni del trattamento dei dati personali ("designati") nell'ambito dell'AST di Ascoli Piceno i Direttori di UOC/Responsabili UOSD/altro, in possesso dei requisiti di esperienza, capacità, e affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia del trattamento dei dati, ivi compreso il profilo relativo alla sicurezza, per l'ambito di attribuzioni, funzioni e competenze declinate per ciascuno di essi dal richiamato regolamento come di seguito specificati:

NOMINA

ai sensi di quanto statuito (art.2-quaterdecies, D.Lgs.n.196/2003 e art.29, Reg.UE 679/2016), il Dott._____, C.F._____, nato/a a_____, doc. id. n._____, quale (Direttore di Dipartimento/Dirigente/Responsabile della U.O.C./U.O.S.D) _____, persona designata al trattamento dei dati personali (Responsabile interno) che in relazione all'incarico ricoperto offre idonea garanzia circa il pieno rispetto delle vigenti disposizioni in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza.

Nella sua qualità le viene affidata l'organizzazione, la gestione e la supervisione di tutte le operazioni di trattamento dei dati personali che la nostra Azienda effettua presso la struttura da lei diretta.

In particolare è tenuto ad osservare oltre che le disposizioni di legge in tale materia anche le istruzioni allegate (allegato n. 1), quale parte integrante e sostanziale del presente atto di nomina.

Si precisa che la presente nomina ha efficacia fino alla data di cessazione a qualsiasi titolo dell'incarico da lei ricoperto.

Ascoli Piceno, il

Il Direttore Generale AST

Per accettazione
(Direttore U.O.C./U.O.S.D)

Allegato 1 - Compiti e istruzioni ai professionisti "Designati" al trattamento dei dati personali nell'ambito dell'organizzazione dell'Azienda Sanitaria Territoriale di Ascoli Piceno

Lei nella sua qualità di Direttore UOC/UOSD deve attenersi alle seguenti istruzioni.

PRINCIPI GENERALI

In conformità ai contenuti dell'art.5 del Regolamento Europeo 2016/679 (GDPR) che prescrive i "*principi applicabili al trattamento dei dati personali*", il professionista "Designato" al trattamento dei dati personali è tenuto a garantire che ciascuna attività di trattamento dati - effettuata nell'ambito della struttura dallo stesso diretta - avvenga in osservanza dei seguenti principi di ordine generale:

- **liceità**, vale a dire nel rispetto delle Leggi, comprese quelle che regolano specifici settori;
- **correttezza**, vale a dire nel rispetto delle reciproche esigenze dell'Azienda e dell'Interessato, oltre agli obblighi derivanti dal quadro normativo;
- **trasparenza**, nel senso di assicurare la piena consapevolezza dell'Interessato, con particolare riferimentoall'obbligo di rendere conoscibili all'utenza le modalità con cui i dati sono raccolti, utilizzati e consultati attraverso informazioni e comunicazioni facilmente accessibili, utilizzando un linguaggio semplice e chiaro.

I dati devono essere raccolti solo per **scopi**:

- **determinati,** vale a dire che non è consentita la raccolta come attività fine a sé stessa;
- **espliciti**, nel senso che il soggetto interessato va informato sulle finalità del trattamento;
- **legittimi**, ossia, oltre al trattamento, anche il fine della raccolta dei dati deve essere lecito;
- **compatibili** con il presupposto per il quale sono inizialmente trattati, specialmente nelle operazioni di comunicazione degli stessi.

I dati devono, inoltre, essere:

- **esatti**, ossia, precisi e rispondenti al vero e, se necessario, **aggiornati**;
- **pertinenti**, ovvero, il trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, inrelazione all'attività che viene svolta;
- **non eccedenti** in senso quantitativo rispetto allo scopo perseguito; ovvero devono essere raccolti solo idati che siano al contempo strettamente necessari e sufficienti in relazione al fine ed in mancanza dei quali non sia possibile il perseguimento del fine stesso;
- **conservati** per un periodo non superiore a quello necessario per gli scopi del trattamento e comunque in base alle specifiche disposizioni di Legge cui è tenuto il Titolare. Trascorso detto periodo i dati vanno resi anonimi o cancellati e la loro comunicazione non è più consentita. In particolare, i dati idonei a rivelarelo **stato di salute** o la **vita sessuale devono** essere accuratamente conservati;
- **sicuri,** cioè deve essere garantita la sicurezza nel trattamento, compresa la protezione mediante misure tecniche e organizzative adeguate, atte a impedirne la perdita, distruzione o danno accidentale (integritàe riservatezza).

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dai principi fondamentali di **integrità, riservatezza** e **rispetto della dignità della persona fisica dell'interessato**, ovvero deve essere effettuato eliminando ognirischio di impropria conoscibilità dei dati da parte di terzi e di perdita o distruzione del dato.

COSA SAPERE

1. Deve trattare soli i dati necessari per lo svolgimento del suo incarico e, quando possibile e compatibile con lo scopo, utilizzarli in forma anonima.
2. Deve teneri i dati che tratta aggiornati e completi e conservali per il tempo necessario al compimento del trattamento.

3. Deve conoscere i trattamenti di dati personali che effettua, i sistemi informatici e gli archivi informatici e/o cartacei necessari per lo svolgimento delle attività di sua competenza.
4. Deve nello svolgimento dei suoi compiti prestare attenzione a quelle attività che comportano il trattamento di dati personali e in particolare di quei dati idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale e i dati giudiziari, deve, quindi, non diffondere tali dati e comunicarli solo alle persone autorizzate o istituzionalmente tenute a conoscerli.

COSA FARE
1. Nominare come soggetti autorizzati al trattamento dei dati personali, utilizzando la lettera di nomina predisposta dall'Azienda, le persone che nella struttura organizzativa da Lei diretta trattano i dati personali. Se necessario può personalizzare la lettera di nomina in base ai compiti assegnati ai singoli.
2. Conservare all'interno della propria struttura organizzativa le lettere di nomina in originale dei soggetti autorizzati da esibire all'Autorità di controllo (Garante per la protezione dei dati personali) in caso di richiesta della stessa Autorità.
3. Comunicare i nominativi delle persone autorizzate e le eventuali modifiche al/ai Referente/i Privacy aziendale, al DPO e anche al Responsabile dei sistemi informativi aziendali per specificare i profili di autorizzazione all'uso dei sistemi informativi aziendali.
4. Fornire le istruzioni alle persone nominate quali autorizzate (incaricati) circa il rilascio dell'informativa, l'acquisizione del consenso degli interessati (pazienti, dipendenti, candidati, fornitori), l'utilizzo degli strumenti informatici per garantire la sicurezza dei dati, circa la gestione degli archivi cartacei, nonché circa l'indicazione delle misure più idonee a salvaguardare la riservatezza dei dati personali dell'interessato.
5. Conservare i documenti cartacei in archivi protetti vale a dire o in armadietti chiusi a chiave o, in alternativa, in locali chiusi a chiave con accesso esclusivo alle persone autorizzate.
6. Utilizzare e far utilizzare al personale assegnato i sistemi informativi secondo le regole organizzative e tecniche stabilite dal SIA come indicate nel Regolamento aziendale dei sistemi informativi pubblicato nel sito istituzionale.
7. Partecipare all'attività formativa promossa dall'Azienda su tali argomenti.

COSA COMUNICARE
1. Trasmettere al Direttore Generale e al/ai Referente/i Privacy aziendale nonché al DPO qualunque richiesta presentata dagli interessati, come quelle relative all'esercizio dei diritti (ad esempio diritto di accesso ai propri dati personali, diritto di rettifica, diritto alla cancellazione, diritto alla limitazione, eccetera).
2. Avvisare il Direttore Generale e il/i Referente/i Privacy aziendale nonché il DPO in ordine ad ogni richiesta/ordine/attività di controllo proveniente dall'autorità di controllo o dall'autorità giudiziaria.
3. Comunicare al/ai Referente/i Privacy aziendale e al DPO se vi sono soggetti terzi esterni ai quali sono attribuite delle attività nella sua struttura organizzativa (soggetti diversi dal personale a voi assegnato) e che per questo trattano i dati per conto dell'Azienda, al fine di predisporre la documentazione necessaria.
4. Comunicare immediatamente al Direttore Generale e/o al Responsabile per la protezione dei dati (DPO) eventuali violazioni di dati (ad esempio distruzione, perdita, comunicazione e/o divulgazione illecita o accesso non autorizzato) e a comunicare anche eventuali sottrazioni di apparecchiature informatiche e/o documenti cartacei per le obbligatorie denunce all'Autorità di controllo (Garante per la protezione dei dati personali).

5. Avvisare il Direttore Generale, il/i Referente/i Privacy aziendale e il Responsabile per la protezione dei dati (DPO) se risulta necessario introdurre un nuovo trattamento di dati (ad esempio uso di una nuova tecnologia, di un nuovo macchinario che contiene dati personali) per consentire all'Azienda di valutarne l'impatto ed attivare le procedure di sicurezza necessarie.

In caso di dubbi su questioni relative al trattamento dei dati personali può rivolgersi al Referente aziendale privacy e/o al Responsabile per la protezione dei dati (DPO) i cui contatti sono reperibili sul sito istituzionale.

ALLEGATO H)

Egr. Sig./Gent.mo
U.O.C.

Referente/i Privacy AST/DPO ASTAP
LORO SEDI

OGGETTO: Nomina autorizzato al trattamento dei dati della U.O.C. - "Decreto legislativo n.101/2018 e GDPR 679/2016"

Il/La sottoscritto/a Dr./Dr.ssa _____ della U.O.C. _____, nella sua qualità di Responsabile del trattamento dati, giusta nomina ai sensi dall'art.29 Regolamento UE 679/2016 GDPR, tenuto conto della rilevazione dei trattamenti riferita alla propria struttura organizzativa

NOMINA

il/i destinatario Il/La signor/a_____, c.f._____, nato/a a _____, doc. id. n._____, della presente quale soggetto autorizzato al trattamento dei dati personali ai sensi dell'art. art 2-quaterdecies del D.Lgs. 101/2018 per i trattamenti di seguiti indicati

la raccolta	x	la registrazione	x	l'organizzazione	x	la conservazione	x
la consultazione	x	l'elaborazione	x	la modificazione		la selezione	x
l'estrazione	x	il raffronto	x	l'utilizzo	x	l'interconnessione	x
il blocco		La comunicazione	x	la cancellazione		la distruzione di dati	

La nomina è strumentale all'effettuazione delle operazioni di trattamento dei dati personali che sono indispensabili per l'espletamento delle attività assegnate, con possibilità di reciproca sostituzione in ipotesi di più incaricati.

In ottemperanza dell'art.2-quaterdecies del Decreto Legislativo n.101/2018 e dall'art.29 Regolamento UE 679/2016 a ciascun soggetto autorizzato sono affidati i compiti riconducibili a quanto specificato nell'allegato 1) alla presente lettera di nomina, oltre ai seguenti (*eventuale)* ulteriori compiti/istruzioni (*in base al settore di afferenza*)_____

In caso di allontanamento, anche temporaneo, dal posto di lavoro, il soggetto autorizzato dovrà verificare che non vi sia possibilità da parte di terzi, anche se dipendenti, di accedere a dati personali per i quali sia in corso un qualunque tipo di trattamento, sia cartaceo che informatizzato.

Nessun dato potrà essere comunicato a terzi o diffuso senza la preventiva autorizzazione del Responsabile del trattamento.

Ascoli Piceno lì, _____

Il DESIGNATO AL TRATTAMENTO DEI DATI

PERSONALI
Direttore U.O.C.
Dr./Dr.ssa
_____

Autorizzato per presa visione e ricevuta copia: _____

Allegato 1 - Istruzioni agli "Autorizzati" al trattamento dei dati personali all'interno dell'organizzazionedell'Azienda Sanitaria Territoriale di Ascoli Piceno

PRINCIPI GENERALI

Al fine di una corretta applicazione dei principi e delle disposizioni contenute nel Regolamento Europeo 2016/679 (GDPR) in materia di protezione dei dati personali, il soggetto "Autorizzato" è tenuto – nell'ambito delle attività di trattamento effettuate presso la struttura di appartenenza sotto la diretta autorità e vigilanza del "Designato" al trattamento - ad osservare le seguenti istruzioni impartite dal "Designato" medesimo, ovvero:

☐ effettuare le operazioni di trattamento dei dati personali (ivi compresi i dati sensibili e giudiziari) strettamente necessarie allo svolgimento delle attività cui si è preposti nell'ambito della struttura di assegnazione;

☐ trattare tutti i dati personali di cui si viene a conoscenza nell'ambito dello svolgimento delle proprie funzioni secondo liceità e correttezza e, comunque, in modo tale da garantire, in ogni operazione di trattamento, la massima riservatezza;

☐ verificare che i dati trattati siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccoltio successivamente trattati;

☐ accedere unicamente alle banche dati presenti presso la struttura in cui si presta la propria attività lavorativa;

☐ mantenere assoluto riserbo sui dati personali di cui si viene a conoscenza nell'esercizio delle proprie funzioni;

☐ evitare l'uso di strumenti informatici personali e del telefono cellulare per il trattamento di dati personali e sensibili acquisiti durante l'attività di servizio; ciò vale anche in caso di rilascio pareri e consulenze;

☐ utilizzare il PC, internet e la posta elettronica attenendosi alle indicazioni e prescrizioni fornite dalla U.O.C. Sistema Informatico aziendale;

☐ attenersi alle disposizioni aziendali in tema di conservazione ed archiviazione dei dati e di accesso agli archivilocali e centralizzati di raccolta dei dati.

Il personale "Autorizzato" effettua le attività di trattamento dei dati nell'ambito della struttura di appartenenza sotto la diretta autorità e vigilanza del professionista "Designato" al trattamento, fatte salve le responsabilità di natura personale correlate all'autonomia professionale di specifiche categorie di professionisti.

PER I TRATTAMENTI EFFETTUATI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

- I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave);
- I documenti contenenti dati personali prelevati ed estratti dagli archivi per lo svolgimento dell'attività quotidianadevono esservi riposti a fine giornata;
- I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro. In caso diallontanamento - anche temporaneo - dal posto di lavoro, adottare le misure in atto a propria disposizione (secondo le istruzioni ricevute) per evitare l'accesso ai dati personali trattati o in trattamento, da parte di soggetti terzi, anche dipendenti, non autorizzati;
- I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento);
- Qualora sia necessario eliminare documenti contenenti dati personali, questi devono essere distrutti utilizzandogli appositi apparecchi "distruggi documenti" o, in assenza, devono essere frammentati in maniera tale da non essere più ricomponibili;
- I documenti che contengono dati sensibili e/o giudiziari devono essere controllati e custoditi dagli "Autorizzati"al trattamento, i quali devono impedire l'accesso a persone prive di autorizzazione;
- L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari deve avvenire in locali ad accessocontrollato, utilizzando armadi o cassetti chiusi a chiave.

PER I TRATTAMENTI EFFETTUATI CON L'AUSILIO DI STRUMENTI ELETTRONICI

- Il trattamento di dati personali con strumenti elettronici è consentito soltanto agli "Autorizzati" dotati di credenziali che permettano il superamento di una procedura di autenticazione relativa a uno specifico trattamentoo a un insieme di trattamenti. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'"Autorizzato" associato a una parola chiave riservata conosciuta solamente dal medesimo;
- La password deve essere modificata dall'"Autorizzato" almeno ogni 90 giorni solari;
- La password deve essere composta da almeno 12 (dodici) caratteri comprendenti lettere

maiuscole e minuscole, numeri e caratteri speciali;

- Nel digitare la password accertarsi che non ci sia nessuno che osservi e sia in grado di vedere od intuire i caratteri digitati sulla tastiera;
- Aver cura di non scrivere le proprie password su supporti facilmente rintracciabili e soprattutto in prossimità della postazione di lavoro utilizzata;
- In presenza di ospiti occorre lasciare attendere questi ultimi in luoghi in cui non siano presenti informazioni riservate o dati personali;
- Non si deve lasciare incustodito e accessibile lo strumento elettronico (p.c.) durante una sessione di trattamento. In caso di allontanamento, anche temporaneo, dal posto di lavoro, occorre attivare adottare la procedura c.d. "salva schermo";
- Se nell'ambito dell'utilizzo del sistema informatico attraverso il quale viene effettuata attività di trattamento di dati si rileva una problematica tale da compromettere la sicurezza dei dati stessi, l'"Autorizzato" è tenuto a darne immediata comunicazione al professionista "Designato" al trattamento;
- Si deve accedere unicamente alle banche dati presenti presso l'Unità Organizzativa in cui si presta la propria attività lavorativa;
- Evitare di creare banche dati nuove senza espressa autorizzazione del Titolare o del designato in qualità di Responsabile "interno" del trattamento;
- È fatto assoluto divieto di comunicare o diffondere i dati personali provenienti da banche dati aziendali in assenza dell'autorizzazione del Titolare o del designato in qualità di Responsabile "interno" del trattamento;
- Accertarsi che sul proprio *personal computer* sia sempre operativo un programma antivirus, aggiornato e con la funzione di monitoraggio attiva;
- Sottoporre a controllo mediante il programma antivirus installato sul proprio *personal computer* tutti i supportidi provenienza esterna prima di eseguire *file* in essi contenuti;
- Non è consentito l'uso e l'installazione di *software* non aziendali senza l'autorizzazione della competente UOC Servizio Informatico;
- Assicurarsi sempre della provenienza dei messaggi di posta elettronica contenenti allegati; in caso di dubbio procedere alla cancellazione del messaggio senza aprire gli allegati;
- La connessione ad Internet deve essere utilizzata esclusivamente per lo svolgimento dei propri compiti istituzionali;
- Informare il professionista "Designato" al trattamento in caso di incidenti di sicurezza o di eventuali anomalie che coinvolgono i dati personali all'interno della struttura di afferenza;
- Osservare tutte le misure tecniche, organizzative e di sicurezza adottate a livello aziendale, oltre le eventuali ulteriori istruzioni che verranno comunicate dal Titolare, dal "Designato" al trattamento o dal Responsabile dellaprotezione dei dati.

ALLEGATO I)

Istruzioni specifiche per il personale sanitario destinate sia ai "Designati" che agli "Autorizzati" al trattamento dei dati personali

Indice

PREMESSA

Le presenti istruzioni – specifiche per il personale sanitario che svolge la propria attività lavorativa in contesti, quali, l'ambito ospedaliero, ambulatori, distretti, strutture territoriali, ecc. - hanno lo scopo di chiarire e diffondere regole/misure comportamentali, organizzative e tecniche cui i professionisti "Designati" e gli "Autorizzati" al trattamento devono attenersi nello svolgimento delle operazioni di trattamento dei dati personali all'interno dell'organizzazione aziendale, al fine di ridurre e contenere i rischi di danneggiamento, dispersione o perdita di dati a causa di un uso non corretto o illecito dei sistemi informatici e degli archivi cartacei.

1. ISTRUZIONI GENERALI

1.1. Segreto professionale o d'ufficio

I "Designati" e gli "Autorizzati" al trattamento sono tenuti a mantenere la necessaria riservatezza sulle informazioni di cui vengono a conoscenza nello svolgimento della propria attività lavorativa e professionale e nel corso delle operazioni di trattamento, evitando di comunicare informazioni e dati a terzi.

Tutto il personale del comparto e della dirigenza – appartenente al ruolo medico, sanitario, tecnico - e chiunquepresti la propria attività lavorativa in ambito sanitario (anche in veste di consulente, libero/professionista, tirocinante, volontario, specializzando, personale convenzionato) presso le strutture dell'Azienda è tenuto al segreto professionale o al segreto d'ufficio, ossia a non rivelare e/o agevolare in qualsiasi modo, senza giusta causa, la conoscenza di notizie, dati o banche dati di cui - in ragione e in occasione del proprio stato o ufficio - sia venuto a conoscenza. L'eventuale violazione di tale obbligo può comportare l'applicazione di sanzioni di naturadeontologica e disciplinare, nonché una responsabilità di natura amministrativa, civile e penale, secondo quantoprevisto dalla legge.

1.2. Tutela della dignità della persona

Deve essere sempre tutelata la dignità di tutti i soggetti che usufruiscono di prestazioni sanitarie, con particolareriguardo alle fasce deboli (ad es. disabili fisici o psichici, minori e anziani), pazienti sieropositivi o affetti da infezione da HIV, pazienti sottoposti a trattamenti medici invasivi, soggetti particolarmente vulnerabili (ad es. interruzione volontaria di gravidanza o vittime di atti di violenza sessuale o di genere).

Nelle terapie intensive o nei reparti che consentono la visione dei pazienti anche attraverso sistemi di videosorveglianza sanitaria devono essere utilizzati paraventi o altri accorgimenti che limitino la visibilità dell'interessato, durante l'orario di visita, ai soli familiari e conoscenti.

1.3. Riservatezza nei colloqui e nel corso di prestazioni sanitarie

Durante i colloqui con l'interessato o con soggetti dallo stesso individuati, o durante l'esecuzione di prestazioni sanitarie, vanno adottate opportune cautele per evitare che le informazioni sulla salute possano essere conosciuteda terzi. Analoghe cautele vanno adottate in occasione della raccolta di dati anamnestici, qualora ciò avvenga in situazioni di promiscuità.

Tutti i professionisti e operatori devono evitare di discutere sulle condizioni cliniche dei pazienti in pubblico, nei luoghi comuni (es. corridoi, bar, ascensore), in presenza di estranei o mediante o utilizzando altre modalità - quali social network, videoconferenza pubblica - ricorrendo a riferimenti che rendano direttamente o indirettamente identificabile la persona.

1.4. – Comunicazioni sulla presenza del Paziente in Ospedale

Utilizzando la modulistica appositamente predisposta, l'interessato – se cosciente e capace – all'atto del ricoveroo dell'accesso in Pronto Soccorso deve essere informato e posto in condizione di fornire indicazioni circa i soggettiche possono ricevere notizie sul suo stato di salute e/o sulla sua presenza presso le diverse strutture dell'Azienda.Deve essere rispettata l'eventuale decisione dell'interessato di non rendere nota la sua presenza in ospedale.

1.5. - Comunicazione all'interessato o a terzi legittimati

La comunicazione al paziente di informazioni sul suo stato di salute deve essere effettuata solo da personale medico o da altro operatore sanitario che intrattenga rapporti diretti con il paziente (ad esempio personale infermieristico purché autorizzato dal responsabile della Struttura).

Le informazioni sullo stato di salute possono essere fornite a soggetti diversi dall'interessato solo se espressamente individuati dal medesimo, mediante la modulistica in uso, oppure nei casi previsti dalla legge.

Pertanto, prima di dare informazioni a terzi legittimati (ad esempio: coniuge, convivente, figli, genitori, fratelli,ecc.) occorre verificare che il paziente non abbia espresso volontà contraria o abbia identificato solo particolarisoggetti destinatari dell'informazione, accertandosi - per quanto possibile - dell'identità dei soggetti richiedenti. Nel caso di pazienti minori con genitori separati con affidamento esclusivo, la comunicazione di notizie al genitore non affidatario può avvenire solo previo consenso esplicito di quello affidatario.

Con specifico riferimento alle categorie particolari di dati personali, le notizie da fornire, specie se destinate a soggetti terzi (es. medico di famiglia), devono limitarsi ai soli elementi pertinenti e necessari per le finalità di cura.

1.6. Rilascio notizie a mezzo telefono o ad organi di stampa

E' vietato fornire dati e informazioni di carattere sanitario tramite telefono ad eccezione dei pazienti e delle persone da questi autorizzate e solo se si abbia certezza assoluta dell'identità del chiamante.

Nel caso in cui giungano richieste telefoniche di dati sanitari da parte dell'Autorità Giudiziaria o degli organi di polizia occorre verificare preliminarmente l'identità del soggetto richiedente richiamando, in caso di dubbio, l'interlocutore al numero da questi comunicato.

È fatto divieto di comunicare dati personali o sanitari agli organi di stampa; le eventuali richieste di informazionidevono essere inoltrate alla Direzione Generale per il tramite dell'URP.

1.7. Distanze di cortesia

Tutti i punti di accettazione e front office devono rispettare una distanza di cortesia, evidenziata da una striscia gialla di segnalazione posta a terra e da un avviso o cartello per l'utenza, sia per operazioni amministrative allo sportello (prenotazione, accettazione, ritiro referti), sia per l'acquisizione di dati personali comuni e relativi alla salute.

1.8. Ordine di chiamata

Gli utenti in attesa di visita o di accertamenti (ad es. analisi cliniche o indagini di radiologia) non devono essere chiamati direttamente per nome o cognome ma mediante chiamata non nominativa (eliminacode, numero di prenotazione CUP o attribuzione di un codice numerico o alfanumerico al momento dell'accettazione).

1.9. Liste di pazienti

E' vietata l'affissione di liste di pazienti nei locali destinati all'attesa o comunque aperti al pubblico, con o senza la descrizione del tipo di patologia sofferta.

1.10. Cartella clinica e documentazione sanitaria

In caso di trasferimento interno dei pazienti ricoverati tra i diversi Presidi o Strutture o nel caso di consulenza o accertamenti diagnostici, la documentazione sanitaria del paziente deve essere riposta in buste o raccoglitori chiusi e non trasparenti, in modo da non permettere la lettura dei dati sensibili da parte di personale non autorizzato.

La documentazione deve essere presa in custodia dal personale sanitario incaricato e da questi consegnata al personale medico ovvero al personale autorizzato dallo stesso personale medico della struttura di destinazione.

I documenti e i supporti elettronici portati in visione dal paziente devono essere conservati rispettando le regoledel rispetto del segreto professionale e, al momento della dimissione o alla conclusione della visita, riconsegnati al paziente.

1.11. Ritiro referti

Qualsiasi documento relativo ad attività sanitarie (quali referti di esami di laboratorio o di esami strumentali, referti di Pronto Soccorso e di visite ambulatoriali, lettere di dimissione) deve essere consegnato in busta chiusadirettamente all'Interessato.

Il ritiro della documentazione sanitaria è ammesso anche da parte di persona diversa dall'interessato purché munita di delega scritta e con consegna in busta chiusa.

Per gli accertamenti HIV non è consentito il ritiro mediante delega.

1.12. - Attestazione di presenza in ospedale

Le dichiarazioni attestanti la visita, l'esame o il ricovero effettuati (es. giustificativo per il datore di lavoro) devonoessere formulate in maniera tale che dalle stesse non possano derivare, per gli estranei, informazioni riguardantilo stato di salute della persona interessata. L'attestazione deve essere generica e non deve riportare indicazioni sulla Unità operativa di erogazione, né il timbro con la specializzazione del sanitario o ogni altra informazione da cui si possa evincere la patologia trattata, ovvero l'Unità operativa presso la quale è stata eseguita la prestazione.

2. DOCUMENTAZIONE CARTACEA E SANITARIA

2.1. Tenuta e custodia

I documenti contenenti dati personali o dati relativi alla salute del Paziente, devono essere custoditi dai "Designati"e dagli "Autorizzati" al trattamento in modo da non essere accessibili a persone prive di autorizzazione (es. localinon accessibili al pubblico, armadi o cassetti chiusi a chiave).

I documenti contenenti dati personali o dati relativi alla salute del Paziente non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

In caso di locali aperti al pubblico, le cartelle e i fascicoli devono essere tenuti sulla propria scrivania curando che i dati non siano visibili a persone non autorizzate.

In caso di assenza o allontanamento, anche temporaneo, dalla postazione di lavoro, è vietato lasciare incustoditi fascicoli, cartelle o documenti cartacei contenenti dati relativi alla salute del Paziente. In tal caso occorre chiuderela propria stanza, qualora rimanga incustodita senza personale all'interno, oppure riporre la documentazione in un armadio o cassetto chiuso a chiave.

2.2. Comunicazione e trasmissione

I documenti contenenti dati personali non devono essere condivisi, comunicati o inviati a colleghi che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se tali professionisti o operatori sono a loro volta "Autorizzati" al trattamento).

I documenti contenenti dati personali devono essere consegnati ai destinatari utilizzando buste chiuse o raccoglitori sigillati a garanzia dell'integrità - oppure effettuando la consegna personalmente - in modo da ridurreal minimo la possibilità che soggetti terzi non autorizzati possano prendere visione del contenuto.

La trasmissione di documentazione sanitaria al domicilio del paziente - su richiesta dello stesso - deve avvenire in busta chiusa ed evitando di riportare sulla busta esterna riferimenti a specifici servizi/strutture dell'Azienda che possano rivelare lo stato di salute dell'interessato o il tipo di patologia e, quindi, in busta recante il solo logo dell'AST;

Nel trasporto della documentazione tra un ufficio e l'altro, occorre adottare precauzioni per evitare la visibilità dei dati personali da parte di estranei (ad es. carpette o faldoni anonimi).

In caso di dati riservati o relativi alla salute occorre accertarsi che il tipo di spedizione sia idoneo a garantire l'integrità della documentazione e la ricezione certa da parte del destinatario, fermo restando quanto sopra specificato con riferimento alle indicazioni contenute all'esterno della busta.

E' proibito trasportare all'esterno del posto di lavoro qualsiasi documentazione contenente dati personali comuni e appartenenti a categorie particolari, salvo motivate esigenze di servizio e fermi restando gli obblighi di custodia.

2.3. Archiviazione e distruzione

I documenti cartacei contenenti dati sensibili e/o giudiziari devono essere utilizzati dai "Designati" e dagli "Autorizzati" al trattamento solo per il tempo necessario allo svolgimento dei relativi compiti istituzionali e poi riposti in archivi o locali ad accesso controllato o, nei casi previsti, affidati al servizio di archiviazione.

Qualora sia necessario disfarsi di documenti cartacei contenenti dati personali, questi devono essere distrutti utilizzando gli appositi distruggidocumenti o, in loro assenza, strappandoli manualmente in modo da non essere più ricomponibili, leggibili o comprensibili.

3. UTILIZZO DI STRUMENTI INFORMATICI

3.1. *User*-id e password

• L'accesso alle risorse informatiche dell'Azienda (PC, applicativi, banche dati, posta elettronica, ecc.) è consentitoai "Designati" e agli "Autorizzati" al trattamento dotati di credenziali di autenticazione formate da un codice di accesso (*user-id* o *username*) e da una parola chiave riservata (password) conosciuta solamente dal medesimo.

• Solamente i professionisti "Designati" al trattamento autorizzano - mediante apertura *ticket* con *mail* ad all'*HelpDesk* del Servizio Informatico o all'Amministratore del Sistema - il rilascio delle credenziali utente in favore del personale assegnato alle strutture rispettivamente dirette; ciò laddove il Servizio Informatico è Amministratore di Sistema. Nella richiesta di rilasciocredenziali devono essere riportati obbligatoriamente i recapiti di telefono aziendale fisso e di telefono personale,generalità, Codice Fiscale, reparto/servizio di appartenenza dell'utente assegnatario della nuova *user-id*, riconducibile ad una singola persona. L'*help desk* provvederà all'abilitazione creando una *password* temporanea da modificare alla prima connessione.

• La *password* scelta dall'utente deve essere complessa, composta da almeno 12 (dodici)[1] caratteri alfanumerici, caratteri speciali (,.!?-=:;), lettere maiuscole, lettere minuscole e numeri.

• La *password* deve essere cambiata periodicamente almeno ogni 3 (tre) mesi o secondo le specifiche scadenze appositamente comunicate. Va inoltre cambiata in ogni caso di sospetto utilizzo o conoscenza da parte di terzi.

• La password deve essere conservata con la massima attenzione e segretezza e non deve essere collocata a vista o in prossimità sulle postazioni di lavoro, non deve essere comunicata a terzi o lasciata in luoghi accessibilia terzi.

• *User-id* e *password* sono personali e non devono mai essere condivise tra più utenti anche se autorizzati al trattamento.

3.2. Posta elettronica

• Ogni utente deve utilizzare la posta elettronica messa a disposizione dall'Azienda esclusivamente per necessitàdi lavoro e lo scambio di corrispondenza tra l'interessato e i propri familiari, amici e conoscenti deve essere assolutamente limitato nel tempo e nella quantità.

• La casella di posta elettronica è assegnata in maniera nominale ed univoca ad una persona fisica, pertanto ogni utente è direttamente responsabile sia da un punto di vista disciplinare che giuridico del suo utilizzo e del contenuto dei messaggi inviati.

• Nell'invio di una *e-mail* occorre prestare massima attenzione alla corretta digitazione dell'indirizzo deldestinatario, specie in caso di comunicazioni riservate o relative alla salute.

• L'indirizzo di posta elettronica aziendale non deve essere utilizzato per l'iscrizione a servizi (social network, gruppi di discussione, servizi telefonici, bancari, assicurativi di tipo personale etc.) non strettamente correlati allapropria attività istituzionale.

• L'utente non deve aprire o rispondere a comunicazioni *e-mail* inattese e/o di provenienza incerta o sospetta (anche se sembrano provenire da un mittente affidabile), contrassegnate come indesiderate (spam), contenentiallegati o

[1] Come indicato dalle "Linee guida funzioni crittografiche – Conservazione delle password redatte dal Garante Privacy e l'Agenzia per la cybersicurezza nazionale

link di cui non si conosce la natura e l'origine (estensione *.com .exe .vbs .scr .pif* ecc.), che possono contenere *file* o programmi dannosi capaci di diffondere virus o programmi malevoli nell'infrastruttura aziendaleo costituire attività di "phishing" mirate al furto di dati personali.

• E' vietato – ad eccezione di motivate esigenze di servizio - l'accesso alla casella di posta elettronica aziendale da computer pubblici in quanto alcuni dati potrebbero essere temporaneamente memorizzati nel disco locale e recuperati da un altro utente.

• E', altresì, vietato l'accesso alla casella di posta elettronica aziendale mediante *wifi*-pubblici (ad es. aeroporti, hotel, ristoranti, ecc.) o altre reti non protette che espongono a rischi per la sicurezza dei dati.

• Ogni utente deve periodicamente cancellare o archiviare la posta elettronica in modo da evitare il riempimento della quota disco assegnata.

• Ogni utente deve predisporre, nell'ambito dell'apposita area "Preferenze" -> "Firme" della *webmail*, la firma infondo ai messaggi avendo cura di dettagliare identità, reparto/servizio di appartenenza, numeri di telefono di contatti.

3.3. Personal computer

• Il PC in dotazione deve essere utilizzato esclusivamente per ragioni di lavoro e per conto dell'Azienda.

• E' vietato connettere alla rete dati aziendale personal *computer* personali.

• In caso di necessità i dipendenti possono utilizzare un PC aziendale diverso da quello in dotazione, entrando in rete con la propria *username* e *password* di dominio AST.

• Durante la sessione di lavoro è necessario evitare che persone estranee e non autorizzate possano visualizzare la schermata del PC posizionando, se del caso, lo schermo in modo da limitarne la visibilità.

• Durante una sessione di lavoro non si deve lasciare il PC incustodito o accessibile da soggetti estranei: in casodi allontanamento - anche temporaneo - dalla postazione di lavoro occorre bloccare la postazione o disconnettere la sessione di lavoro.

• I programmi devono essere chiusi secondo appropriate misure di sicurezza per evitare la perdita dei dati.

• Il PC deve essere spento al termine della sessione lavorativa o in caso di assenza dalla postazione di lavoro.

• Gli unici addetti autorizzati ad installare *software*, apportare modifiche alle impostazioni di sicurezza o di configurazione del PC (es. antivirus) sono i tecnici di *Help Desk* del Servizio Informatico. Nessun utente è autorizzato ad installare *software* o *hardware* diversi da quelli forniti dall'Azienda senza formale autorizzazione del Servizio Informatico.

L'uso di *software* contraffatto, ovvero con licenza d'uso contraffatta, costituisce un illecito penale e civile, secondo quanto previsto dalla normativa sul diritto d'autore.

• Ogni utente è tenuto a non interrompere le operazioni di aggiornamento pianificate del sistema operativo edegli antivirus, procedendo al salvataggio dei dati ed al riavvio del PC, qualora richiesto.

• I dati e i documenti elettronici contenenti dati sensibili devono essere archiviati sul *server* centrale dell'Azienda ed eliminati dall'*hard disk* del PC in dotazione.

• E' vietata la condivisione di documenti contenenti dati personali particolari su *cloud* (*dropbox, google drive, onedrive, wetransfer.com*, ecc.) e server non aziendali.

3.4. Dispositivi portatili e supporti di memoria

• I dispositivi portatili (*notebook*, *tablet*, smartphone ecc.) e i supporti di memoria rimovibili (ad es. CD, DVD, *pen drive*, memorie USB, ecc.) devono essere conservati in un luogo sicuro (stanze, armadi o cassetti chiusi a chiave) e mailasciati incustoditi.

• E' vietato l'uso di dispositivi portatili e memorie al di fuori dall'Azienda contenenti dati sensibili. L'utilizzatore è personalmente consapevole dei rischi per la protezione dei dati e delle conseguenti responsabilità in caso di perdita o violazione degli stessi.

• Salvo motivate esigenze, è tassativamente vietato trasferire, anche solo temporaneamente, copie di dati personali

particolari (es. dati sanitari) su qualsiasi dispositivo portatile o memoria rimovibile.

• Nel caso in cui vi sia la motivata necessità di memorizzare dati relativi alla salute su dispositivi portatili o memorie rimovibili, l'archiviazione deve avvenire mediante impiego di idonei sistemi di crittografia e copie di backup.

• In sede di rimozione dei dispositivi di memoria occorre seguire le procedure di disconnessione sicura.

• E' obbligatorio assicurarsi che i dispositivi non vengano utilizzati da terzi e che non siano infettati da virus (procedere alla scansione del supporto).

• E' vietata - ad eccezione di motivate esigenze di servizio - la connessione dei dispositivi aziendali a *wifi*-pubblici(ad es. aeroporti, hotel, ristoranti, ecc.) o altre reti non protette, in quanto comportano rischi per la sicurezza deidati.

• In caso di riutilizzo/dismissione dei dispositivi portatili e dei supporti di memoria, l'utente deve assicurarsi che si proceda, prima dello smaltimento, all'eliminazione permanente delle informazioni e dei dati memorizzati affinché questi non possano essere in alcun modo recuperati.

3.5.* – Sistemi server e *Backup

• E' obbligatorio utilizzare le cartelle *Home* utenti di rete e le cartelle di scambio di servizio/reparto per deteneredati aziendali necessari alle continuità di servizio.

• E' consigliato verificare almeno settimanalmente la presenza e consistenza dei dati contenuti nelle cartelle e comunicare tempestivamente eventuali errate cancellazioni dei medesimi. Il sistema informatico possiede una *data retention* per i dati utenti di 7 giorni. In caso di cancellazione di *file* con tempo superiore sarà impossibile recuperare i backup dei medesimi.

3.6. - Fotocopiatrici, stampanti e fax

• E' obbligatorio assicurarsi di non lasciare incustodite le stampe contenenti dati sensibili, specie se la stampante o la fotocopiatrice è condivisa con più utenti e si trova a distanza dalla postazione informatica. Le copie non necessarie devono essere rese illeggibili prima di essere eliminate.

• Fotocopiatrici, fax, stampanti di rete, devono essere sempre collocate in un luogo non accessibile a terzi non autorizzati.

• In caso di ricevimento via fax di documentazione contenente dati sensibili occorre provvedere all'immediato ritiro della stessa.

• Prima dell'eventuale invio via fax documenti contenenti dati relativi alla salute occorre assicurarsi preventivamente che l'effettivo destinatario sia sul posto o comunque che il fax sia in un luogo protetto e presidiato, non accessibile a pubblico, e che non vi siano pertanto rischi di conoscenza da parte di soggetti estranei o non autorizzati. A seguito dell'invio del fax, dovrà essere telefonicamente accertata la ricezione del soggetto destinatario da parte del soggetto inviante.

• In fase di invio del fax occorre prestare la massima attenzione alla corretta digitazione del numero del destinatario.

• Sulla copertina del fax si consiglia di apporre la seguente formula: "Qualora il destinatario del presente fax nonsia la persona indicata nella presente copertina, è pregato di dare immediata comunicazione al mittente, a mezzotelefono o per fax. Il destinatario della presente comunicazione deve distruggere immediatamente la documentazione ricevuta e in ogni caso potrà essere ritenuto responsabile dell'uso non autorizzato delle informazioni ivi contenute, erroneamente acquisite".

ALLEGATO J)

MODELLO NOMINA DEL RESPONSABILE DEL TRATTAMENTO AI SENSI DELL'ART.28 REG. (UE) 2016/679

TRA

AST ASCOLI PICENO (in seguito per brevità ASTAP), con sede legale in Ascoli Piceno (AP), Via degli Iris, n.1 , codice fiscale e partita IVA 02500670449 - Titolare del trattamento, nella persona del Direttore generale AST _____ giusta nomina ai sensi della Determina n. __ del _

E

_____-, con sede in_____, in persona del legale rappresentante P.T. (soggetto individuato quale Responsabile del trattamento)
definite congiuntamente "Parti".

Premesso che:

- l'art.28, par.3, del Regolamento (UE) n. 2016/679 (General Data Protection Regulation), di seguito anche GDPR, prevede che i trattamenti effettuati per conto del Titolare del trattamento da parte di un Responsabile del trattamento siano regolati da un contratto o da altro atto giuridico che determini la materia del trattamento, la durata, la natura e la finalità, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento;
- l'art. 28 del Regolamento (UE) n. 2016/679 riconosce, altresì, al Titolare del trattamento la facoltà di avvalersi di uno o più responsabili del trattamento dei dati, che abbiano esperienza, capacità, conoscenza per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del regolamento, anche relativamente al profilo della sicurezza;
- le Parti hanno sottoscritto in data _____un contratto/una convenzione per una durata di _____
- ai fini del rispetto della normativa europea Regolamento (UE) n. 2016/679 e della normativa interna di attuazione (D.Lgs. 196/2003 – D.Lgs. 101/2018), ciascuna persona che tratta dati personali deve essere autorizzata e istruita in merito agli obblighi normativi per la gestione dei suddetti dati durante lo svolgimento delle proprie attività;
- AST Ascoli Piceno ha affidato alla ditta __lo svolgimento delle attività e delle prestazioni così come definite nel contratto sopra citato, che si richiama espressamente, e della quale la presente forma parte integrante e sostanziale;
- tenuto conto delle attività di trattamento necessarie e/o opportune per dare esecuzione agli obblighi concordati tra le Parti, previa valutazione di quanto imposto dal Regolamento UE n. 2016/679, il Titolare ha ritenuto che il Responsabile presenti garanzie sufficienti per mettere in atto misure tecniche e organizzative;

- adeguate a soddisfare i requisiti del Regolamento UE n. 2016/679 ed a garantire la tutela dei diritti e le libertà degli interessati coinvolti nelle suddette attività di trattamento;
- tale nomina non comporta alcuna modifica della qualifica professionale del Responsabile e/o degli obblighi concordati tra le Parti.

Tutto quanto sopra premesso:

l'AST di Ascoli Piceno,

NOMINA

_____ ai sensi dell'art.28 del GDPR Responsabile esterno per il trattamento dei dati personali di cui è Titolare l'AST Ascoli Piceno e di cui il Responsabile può venire a conoscenza nell'esercizio delle attività espletate per conto della stessa relativamente all'adempimento degli obblighi dedotti nel citato contratto/convenzione, affidati dal Titolare al Responsabile.

Articolo 1 - Natura e finalità del trattamento

Il trattamento dei dati personali è effettuato esclusivamente per la corretta esecuzione delle attività concordate tra le Parti e di cui al citato contratto.

Articolo 2 - Categorie di dati personali trattati

Il Responsabile del trattamento per espletare le attività pattuite tra le Parti per conto del Titolare tratta direttamente o anche solo indirettamente le seguenti categorie di dati:

- dati personali, di cui all'art. 4 n. 1 del GDPR, tra i quali:
- dati comuni di cui all'art. 6 del GDPR;
- dati rientranti nelle categorie "particolari" di dati personali (p.e. dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, alla vita sessuale, all'orientamento sessuale della persona) di cui all'art. 9 del GDPR.

Categorie di interessati cui si riferiscono i dati trattati

Per effetto della presente nomina, le categorie di interessati i cui dati personali possono essere trattati, sono:

- pazienti/utenti;
- familiari dei pazienti/utenti.

Articolo 3 - Obbligo alla riservatezza

Trattandosi di dati personali anche particolari, il responsabile e i propri dipendenti e collaboratori sono tenuti alla assoluta riservatezza analogamente al segreto professionale e al segreto d'ufficio, e comunque a trattare i dati in materia confidenziale e riservata, evitando l'eventuale comunicazione e/o conoscenza da parte di soggetti non autorizzati.

Articolo 4 – Disponibilità e uso dei dati

Qualunque sia la finalità e la durata del trattamento effettuato da parte del Responsabile:

 i dati non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti e dovranno essere restituiti alla conclusione o revoca dell'incarico, o in qualsiasi momento il Titolare ne faccia richiesta;

 il Responsabile si impegna a non vantare alcun diritto sui dati e sui materiali presi in visione.

Coerentemente con quanto prescritto dal GDPR, è esplicitamente fatto divieto al Responsabile di inviare messaggio pubblicitari, commerciali e promozionali, e comunque di contattare gli "interessati" per finalità diverse da quelle nel presente atto.

Articolo 5 - Cessazione del trattamento

Una volta cessati i trattamenti oggetto del contratto/convenzione, salvo rinnovo, il Responsabile si impegna a restituire al Titolare i dati personali acquisiti, pervenuti a sua conoscenza o da questi elaborati in relazione all'esecuzione del servizio prestato e, solo successivamente, si impegna a cancellarli dai propri archivi oppure distruggerli, ad eccezione dei casi in cui i dati debbano essere conservati in virtù di obblighi di legge.

Resta inteso che la dimostrazione delle ragioni che giustificano il protrarsi degli obblighi di conservazione è a carico del Titolare e che le uniche finalità perseguibili con tali dati sono esclusivamente circoscritte a rispondere a tali adempimenti normativi.

Articolo 6 - Validità e Revoca della nomina

La presente nomina avrà validità per tutta la durata del rapporto giuridico intercorrente tra le Parti e potrà essere revocata a discrezione del Titolare.

La presente nomina non costituisce aggravio in capo al Responsabile, rientrando la medesima negli obblighi normativi che regolano i rapporti con il Titolare sotto il profilo della protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Articolo 7 - Sub-responsabili

Il Responsabile del trattamento non potrà ricorrere ad altri Responsabili senza la preventiva autorizzazione specifica del Titolare del trattamento. In tale ipotesi il Responsabile dovrà inviare, a mezzo pec, circostanziata e motivata richiesta al Titolare che avrà la facoltà di consentire o meno detta nomina.

Ai sensi dell'art. 28, par. 4 del GDPR, fermo restando quanto previsto al precedente paragrafo, quando un responsabile del trattamento ricorre a un altro responsabile del trattamento, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra Titolare del trattamento e il responsabile del trattamento prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Articolo 8 - Designazione e autorizzazione degli incaricati

Il Responsabile del trattamento garantisce la puntuale individuazione dei soggetti operanti a qualsiasi titolo nella propria organizzazione quali soggetti autorizzati al trattamento.

In particolare, il Responsabile del trattamento si impegna a consentire l'accesso e il trattamento dei dati personali solo a personale debitamente formato e specificamente designato anche ai sensi

dell'art.2-quaterdecies del D.Lgs 196/2003 e s.m.i.

Il Responsabile si impegna ad effettuare per iscritto le nomine e limitare l'accesso e il trattamento ai soli dati personali necessari per lo svolgimento delle attività oggetto del contratto/convenzione.

Il personale autorizzato dovrà ricevere idonea e specifica formazione in relazione al rispetto delle misure organizzative e tecniche, in particolare alle misure di sicurezza adottate, adeguate ad assicurare la tutela dei dati personali trattati nel rispetto delle previsioni normative e della prassi in materia.

Nello specifico il Responsabile:

- individua le persone autorizzate al trattamento dei dati impartendo loro, per iscritto, istruzioni dettagliate in merito alle operazioni consentite e alle misure di sicurezza da adottare in relazione alle criticità dei dati trattati;
- vigila regolarmente sulla puntuale applicazione da parte delle persone autorizzate di quanto prescritto, anche tramite verifiche periodiche;
- garantisce l'adozione dei diversi profili di autorizzazione delle persone autorizzate, in modo da limitare l'accesso ai soli dati necessari alle operazioni di trattamento consentite rispetto alle mansioni svolte;
- verifica periodicamente la sussistenza delle condizioni per la conservazione dei profili di autorizzazione di tutte le persone autorizzate, modificando tempestivamente detto profilo ove necessario (es. cambio di mansione);
- cura la formazione e l'aggiornamento professionale delle persone autorizzate che operano sotto la sua responsabilità circa le disposizioni di legge e regolamentari in materia di tutela dei dati personali.

Il Responsabile, su richiesta, invia al Titolare del trattamento a mezzo pec l'elenco nominativo con specifica evidenza delle relative mansioni dei soggetti autorizzati al trattamento dei dati personali svolti per suo conto e nell'ambito del Contratto.

Articolo 9 – Responsabile della protezione dei Dati

Il Responsabile - ove tale obbligo si applichi anche al Responsabile stesso in base alle disposizioni dell'art. 37 del GDPR - si impegna a nominare e comunicare al Titolare il nominativo e i dati di contatto del Responsabile della Protezione dei Dati.

Articolo 10 - Diritti degli interessati

Premesso che l'esercizio dei diritti riconosciuti all'interessato ai sensi degli artt. 15 e seguenti del GDPR sarà gestito direttamente dal Titolare, il Responsabile si rende disponibile a collaborare con il Titolare stesso fornendogli tutte le informazioni necessarie a soddisfare le eventuali richieste ricevute in tal senso.

Il Responsabile si impegna ad assistere il Titolare con misure tecniche e organizzative adeguate al fine di soddisfare l'obbligo del Titolare e di dare seguito alle richieste per l'esercizio dei diritti dell'interessato. In particolare, il Responsabile dovrà comunicare al Titolare, senza ritardo e comunque non oltre le 72 ore dalla ricezione, le istanze eventualmente ricevute e avanzate dagli interessati in virtù dei diritti previsti dalla vigente normativa (es. diritto di accesso, ecc.) e a fornire le informazioni necessarie al fine di consentire al Titolare di evadere le stesse entro i termini stabiliti dalla normativa.

Articolo 11 - Registro dei trattamenti

Il Responsabile mantiene un registro (in forma scritta e/o anche in formato elettronico) di tutte le categorie di attività relative al trattamento svolte per conto del Titolare, contenente:

- il nome e i dati di contatto del Responsabile e/o dei suoi Sub Responsabili;
- le categorie dei trattamenti effettuati per conto del Titolare;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate adottate;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'art.32, par. 1 del GDPR.

Il Responsabile garantisce, inoltre, di mettere a disposizione del Titolare e/o dell'Autorità di controllo che ne dovessero fare richiesta, il suddetto registro dei trattamenti.

Il Responsabile si impegna a coadiuvare il Titolare nella redazione del proprio Registro delle attività di trattamenti, segnalando anche, per quanto di propria competenza, eventuali modifiche da apportare al Registro.

Articolo 12 - Sicurezza dei dati personali

Il Responsabile è tenuto, ai sensi dell'art. 32 del GDPR, ad adottare le necessarie e adeguate misure di sicurezza (eventualmente anche ulteriori rispetto a quelle nel seguito indicate) in modo tale da ridurre al minimo i rischi di distruzione accidentale o illegale, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non consentito ai dati personali trasmessi, conservati o comunque trattati, o il trattamento non conforme alle finalità della raccolta. Il Responsabile fornisce al Titolare l'elenco delle adeguate misure di sicurezza adottate.

Articolo 13 - Sicurezza e Amministrazione del Sistema (ADS)

Il Responsabile fornirà al Titolare la lista nominativa degli ADS, con questi intendendo le persone fisiche che svolgono per conto del Responsabile ed in esecuzione dei compiti concordati ed affidati dal Titolare, attività di gestione e manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i software complessi che trattano dati, le reti locali e gli apparati di sicurezza di quest'ultimo, o comunque che possano intervenire sulle misure di sicurezza a presidio dei medesimi dati. Con riferimento ai soggetti individuati, il Responsabile deve comunicare rispetto ad ognuno i compiti e le operazioni svolte.

Articolo 14 - Compiti e istruzioni per il Responsabile

Il Responsabile ha il potere ed il dovere di trattare i dati personali indicati nel rispetto della normativa vigente, attenendosi sia alle istruzioni di seguito fornite, sia a quelle che verranno rese note dal Titolare mediante procedure e/o comunicazioni specifiche.

Il Responsabile dichiara espressamente di comprendere ed accettare le istruzioni di seguito rappresentate e si obbliga a porre in essere, nell'ambito dei compiti contrattualmente affidati, tutti gli adempimenti prescritti dalla normativa di riferimento in materia di tutela dei dati personali al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non

autorizzato è di trattamento non consentito o non conforme alla raccolta.

Articolo 15 - Modalità di trattamento e requisiti dei dati personali

Il Responsabile si impegna:

 a trattare direttamente, o per il tramite dei propri dipendenti, collaboratori esterni, consulenti, etc. specificamente designati incaricati del trattamento, i dati personali per le sole finalità connesse alo svolgimento delle attività previste dal contratto/convenzione, in modo lecito e secondo buona fede e correttezza, nonché nel pieno rispetto delle disposizioni previste dal GDPR, nonché, infine, dalle presenti istruzioni:

 non divulgare o rendere noti a terzi - per alcuna ragione ed in alcun momento, presente o futuro ed anche una volta cessati i trattamenti oggetto del contratto - i dati personali ricevuti dal Titolare e o pervenuti a sua conoscenza in relazione all'esecuzione del servizio prestato, se non previamente autorizzato per iscritto dal Titolare stesso, fatti salvi eventuali obblighi di legge o ordini dell'Autorità Giudiziaria e/o di competenti Autorità amministrative;

 collaborare con il Titolare per garantire la puntuale osservanza e conformità alla normativa in materia di protezione dei dati personali;

 dare immediato avviso al Titolare in caso di cessazione dei trattamenti concordati;

 non creare banche dati nuove senza espressa autorizzazione del Titolare, fatto salvo quando ciò risulti strettamente indispensabile ai fini dell'esecuzione degli obblighi assunti;

 in caso di ricezione di richieste specifiche avanzate dall'Autorità Garante per la protezione dei dati personali o altre autorità, a coadiuvare il Titolare per quanto di sua competenza;

 segnalare eventuali criticità al Titolare che possono mettere a repentaglio la sicurezza dei dati, al fine di consentire idonei interventi da parte dello stesso;

 coadiuvare, su richiesta, il Titolare ed i soggetti da questo indicati nella redazione della documentazione necessaria per adempiere alla normativa di settore, con riferimento ai trattamenti di dati effettuati dal Responsabile in esecuzione delle attività assegnate.

Articolo 16 - Istruzioni specifiche per il trattamento dati particolari

Il Responsabile deve:

 verificare la corretta osservanza delle misure previste dal Titolare in materia di archiviazione nel rispetto di quanto previsto dal precedente articolo 6, potendo derivare gravi conseguenze da accessi non autorizzati alle informazioni oggetto di trattamento;

 prestare particolare attenzione al trattamento dei dati personali rientranti nelle categorie particolari degli interessati conosciuti, anche incidentalmente, in esecuzione dell'incarico affidato, procedendo alla loro raccolta e archiviazione solo ove ciò si renda necessario per lo svolgimento delle attività di competenza e istruendo in tal senso le persone autorizzate che operano all'interno della propria struttura;

 conservare, nel rispetto di quanto previsto dal precedente articolo 6, la documentazione contenente dati particolari adottando misure idonee al fine di evitare accessi non autorizzati ai dati, distruzione, perdita e/o qualunque violazione di dati personali;

 vigilare affinché i dati personali degli interessati vengano comunicati solo a quei soggetti preventivamente autorizzati dal Titolare (ad esempio a propri fornitori e/o subfornitori) che presentino

garanzie sufficienti secondo le procedure di autorizzazione disposte e comunicate dal Titolare. Sono altresì consentite le comunicazioni richieste per legge nei confronti di soggetti pubblici;

 sottoporre preventivamente al Titolare, per una sua formale approvazione, le richieste di dati da parte di soggetti esterni;

 non diffondere i dati personali, comuni e particolari, degli interessati;

 segnalare eventuali criticità nella gestione della documentazione contenente dati personali particolari al fine di consentire idonei interventi da parte del Titolare.

Articolo 17 - Violazione dei dati

Il Responsabile si impegna a notificare al Titolare, senza ingiustificato ritardo dall'avvenuta conoscenza, e comunque entro 24 ore, con comunicazione da inviarsi all'indirizzo pec del Titolare, ogni violazione dei dati personali (data breach) fornendo, altresì:

- la descrizione della natura della violazione e l'indicazione delle categorie dei dati personali e il numero approssimativo di interessati coinvolti;
- comunicare il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro punto di contatto presso cui ottenere più informazioni;
- la descrizione delle probabili conseguenze;
- la descrizione delle misure adottate o di cui dispone per porre rimedio alla violazione o, quantomeno, per attenuarne i possibili effetti negativi.

Fermo quanto sopra previsto, il Responsabile si impegna a prestare ogni più ampia assistenza al Titolare al fine di consentirgli di assolvere agli obblighi di cui agli artt. 33 - 34 del GDPR.

Una volta definite le ragioni della violazione, il Responsabile di concerto con il Titolare e/o altro soggetto da quest'ultimo indicato, su richiesta, si attiverà per implementare nel minor tempo possibile tutte le misure di sicurezza fisiche e/o logiche e/o organizzative atte ad arginare il verificarsi di una nuova violazione della stessa specie di quella verificatasi, al riguardo anche avvalendosi dell'operato di subfornitori.

Articolo 18 - Valutazione di impatto e consultazione preventiva

Con riferimento agli artt. 35 e 36 del GDPR, il Responsabile si impegna, su richiesta, ad assistere il Titolare nelle attività necessarie all'assolvimento degli obblighi previsti dai succitati articoli, sulle base delle informazioni in proprio possesso, in ragione dei trattamenti svolti in qualità di Responsabile del trattamento, ivi incluse le informazioni relative agli eventuali trattamenti effettuati dai Sub - Responsabili.

Articolo 19 - Trasferimento dei dati personali

Il Responsabile del trattamento si impegna a circoscrivere gli ambiti di circolazione e trattamento dei dati personali (es. memorizzazione, archiviazione, conservazione dei dati sui propri server) ai Paesi facenti parte dell'Unione Europea, con espresso divieto di trasferirli in Paesi extra UE che non garantiscano (o in assenza di) un livello adeguato di tutela, ovvero, in assenza di strumenti di tutela previsti dal Regolamento UE 2016/679.

Articolo 20 - Attività di audit

Il Responsabile si impegna a mettere a disposizione del Titolare tutte le informazioni necessarie per

dimostrare il rispetto degli obblighi di sicurezza descritti nel presente documento e, in generale, il rispetto delle obbligazioni assunte in forza del presente atto e del GDPR, consentendo e, su richiesta, contribuendo alle attività di audit, comprese le ispezioni, realizzate dal Titolare o da altro soggetto da esso incaricato.

Qualora il Titolare rilevasse comportamenti difformi a quanto prescritto dalla normativa in materia nonché dalle disposizioni contenute nei provvedimenti del Garante per la protezione dei dati personali, provvederà a darne comunicazione al Responsabile, senza che ciò possa far venire meno l'autonomia dell'attività di impresa del Responsabile ovvero possa essere qualificato come ingerenza nella sua attività.

Articolo 21 - Ulteriori istruzioni

Il Responsabile comunica tempestivamente al Titolare qualsiasi modificazione di assetto organizzativo o di struttura proprietaria che dovesse intervenire successivamente all'affidamento dell'incarico, affinché il Titolare possano accertare l'eventuale sopravvenuta mancanza dei requisiti previsti dalla vigente normativa o il venir meno delle garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate per il corretto trattamento dei dati oggetto della presente nomina.

Il Responsabile informa prontamente il Titolare delle eventuali carenze, situazioni anomale o di emergenza rilevate nell'ambito del servizio erogato - in particolare ove ciò possa riguardare il trattamento dei dati personali e le misure di sicurezza adottate dal Responsabile - e di ogni altro episodio o fatto rilevante che intervenga e che riguardi comunque l'applicazione del GDPR (ad es. richieste del Garante, esito delle ispezioni svolte dalle Autorità, ecc.) o della normativa nazionale ancorché applicabile.

Articolo 22 – Norme finali e responsabilità

Il Titolare, poste le suddette istruzioni e fermi i compiti sopra individuati, si riserva, nell'ambito del proprio ruolo, di impartire per iscritto eventuali ulteriori istruzioni che dovessero risultare necessarie per il corretto e conforme svolgimento delle attività di trattamento dei dati collegate all'accordo vigente tra le Parti, anche a completamento ed integrazione di quanto sopra definito.

Il Responsabile dichiara sin d'ora di mantenere indenne e manlevato il Titolare da qualsiasi danno, onere, spesa e conseguenza che dovesse loro derivare a seguito della violazione, da parte del Responsabile o di suoi Sub – Responsabili, degli impegni relativi al rispetto della disciplina in materia di protezione dei dati personali o delle istruzioni contenute nei relativi atti di nomina anche in seguito a comportamenti addebitabili ai loro dipendenti, rappresentanti, collaboratori a qualsiasi titolo.

Il presente atto di nomina viene sottoscritto dalle parti digitalmente.

Per la AST Ascoli Piceno

Il Direttore generale

_____

Per _____

Il legale rappresentante

_____