MODELLO ORGANIZZATIVO PRIVACY (MOP)
PER L'IMPLEMENTAZIONE ED ATTUAZIONE
DI POLITICHE ADEGUATE ED EFFICACI
IN MATERIA DI PROTEZIONE DEI DATI

Regolamento UE 2016/679 (GDPR) e D. Lgs n. 196 del 30/06/2003, modificato dal D. Lgs n. 101 del 10/08/2018

SOMMARIO

1. OBIETTIVI

Premessa

Il presente documento costituisce l'evoluzione del *"Regolamento inerente le azioni di carattere organizzativo, gestionale e documentale volte ad ottemperare agli obblighi del Regolamento Europeo 679/2016 sulla protezione dei dati personali"* adottato dalla ex Azienda Socio Sanitaria Territoriale (ASST) di Monza con provvedimento n. 564 del 16.12.2021 in attuazione del Regolamento europeo UE 679/2016 e del vigente D.Lgs. 30 giugno 2003, n. 196 (c.d. "Codice privacy") come novellato dal D. Lgs. 10 agosto 2018, n. 101.

Prima di entrare nel merito degli obiettivi del presente documento, è doveroso fare una premessa di sistema, tenuto conto che la predetta organizzazione sanitaria, a far data dal 1°gennaio 2023 "ha cambiato pelle" a seguito del riconoscimento del carattere scientifico e della sua correlata trasformazione, ai sensi dell'articolo 13, comma 2, del decreto legislativo n.288/2003 e s.m.i., in Fondazione IRCCS di diritto pubblico denominata "Fondazione IRCCS San Gerardo dei Tintori" (di seguito FSGT).

Ed infatti, la costituzione della FSGT è il risultato di un complesso iter giuridico-amministrativo, avviato con la DGR n. XI/5725 del 15.12.2021 e terminato con Decreto del Ministro della Salute del 12.10.2022, e relativa integrazione con DM del 25.10.2023.

Peraltro, giova precisare che, a far data dal 3 aprile 2023, per effetto del decreto n. 4765 del 30.03.2023 della Direzione Welfare di Regione Lombardia, in relazione al completamento dell'evoluzione in IRCCS dell'Ospedale San Gerardo, sono state trasferite ad ASST Brianza alcune delle più rilevanti funzioni territoriali.

La nuova FSGT è in particolare impegnata nell'attività di assistenza sanitaria e di ricerca, con la finalità di rafforzare le sinergie presenti ed implementarne di nuove, al fine di valorizzare al massimo gli asset strategici in termini di know how, di progetti di ricerca e di personale. Peraltro, la FSGT può vantare al suo interno una forte integrazione clinica e dei processi operativi, nonché importanti partnership di tipo clinico, assistenziale e scientifico.

La trasformazione della ex ASST Monza in Fondazione IRCCS di diritto pubblico ha comportato, pertanto, il potenziamento di alcune aree (area materno-infantile -oggi Dipartimento area della Donna e materno-infantile- , ricerca) e l'introduzione della Struttura "Direzione Scientifica", con necessaria focalizzazione di tali ambiti, così determinando la necessità di una revisione complessiva dei processi, e di tutte le componenti agli stessi correlate, delle procedure, nonché della documentazione aziendale al fine di implementare o consolidare percorsi gestionali virtuosi in termini di miglioramento della qualità dell'assistenza, razionalizzazione dei costi ed ottimizzazione dei risultati.

Obiettivi specifici

Per la FSGT, nella sua qualità di Titolare del trattamento, esiste un vero e proprio obbligo di porre in essere comportamenti proattivi, tali da assicurare la concreta individuazione ed adozione di misure tese a garantire l'applicazione del predetto Regolament UE 679/2016 (GDPR). Pertanto, in conformità a quanto previsto dall'articolo 24 del GDPR, FSGT ha inteso definire politiche adeguate ed efficaci in tema di protezione dei dati con l'obiettivo primario di attuare una gestione responsabile del trattamento dei dati, nonché di documentare e dimostrare in ogni momento la conformità dei trattamenti alle disposizioni normative vigenti, l'efficacia delle misure di sicurezza selezionate ed adottate nelle attività di trattamento, la continuità nel tempo del percorso di adeguamento intrapreso - anche a fronte delle recenti variazioni dell'assetto organizzativo aziendale - ed il pieno rispetto dei principi generali dettati dal legislatore europeo.

Posto che il Legislatore ha conferito alle Amministrazioni ampio margine e discrezionalità nella scelta del modello organizzativo e gestionale ritenuto maggiormente aderente alle rispettive realtà organizzative, la Fondazione SGT, in ossequio al principio di *accountability,* che rinvia letteralmente al concetto di responsabilizzazione (*rectius*: del "comprovare"), ha optato per un modello organizzativo corrispondente alla propria *mission* istituzionale e, quindi, adeguato ed efficace rispetto agli obiettivi da conseguire. Peraltro, anche il processo di individuazione delle misure di sicurezza ha tenuto necessariamente conto della natura delle attività della Fondazione e della peculiarità dei dati oggetto di trattamento tra cui si annoverano anche quelli sanitari.

Il presente documento – che si caratterizza per dinamicità ed evoluzione continua dei suoi contenuti, prestandosi pertanto ad un aggiornamento costante – intende rappresentare un punto di riferimento per tutti coloro che, a diverso titolo, livello e funzione, contribuiscono alla gestione di trattamenti dei dati ed al nuovo orientamento che guarda alle politiche di protezione dei dati personali non alla stregua di un mero adempimento burocratico che onera ulteriormente le amministrazioni, bensì ad uno degli asset strategici da attuare per il miglioramento dell'organizzazione nella sua interezza, a maggior ragione quando si tratti di un'organizzazione complessa come quella sanitaria. Ed infatti, il presente documento è strettamente correlato agli altri strumenti (e documenti) di programmazione aziendale a valenza strategica e concorre con i predetti ad assicurare elevati standard di qualità e di *performance* organizzativa ed individuale. Nell'ambito di questo percorso virtuoso di revisione ed ottimizzazione dei processi, la Fondazione ha ritenuto di intervenire in maniera ancora più incisiva attraverso interventi strutturali, trasversali e di sistema.

In questo percorso, in aggiunta alla progettazione ed alla erogazione di percorsi di formazione per il personale la FSGT, ha inteso promuovere anche una specifica azione di sensibilizzazione e di coinvolgimento che, a partire dai Responsabili delle Strutture, raggiunga a cascata tutti i collaboratori alle stesse afferenti. Ciò al fine di attuare il processo di cambiamento culturale degli operatori sanitari e degli utenti e migliorare le performance organizzative aziendali.

Peraltro, al fine di accompagnare e rendere ancora più efficace la riorganizzazione in atto che impegna a tutti i livelli, soprattutto coloro che sono chiamati ad attuare gli obiettivi strategici definiti dall'Organo di indirizzo politico, si è ritenuto opportuno sviluppare, in un'ottica di promozione dell'eccellenza, un nuovo modello di *governance* attraverso l'individuazione di un sistema integrato di gestione della privacy fortemente interconnesso con l'organizzazione aziendale finalizzato a stabilire politiche, obiettivi e processi e di affidarne la definizione al Responsabile per la protezione dei dati in stretto raccordo con la Direzione strategica.

Per le suddette finalità, con decreto del direttore generale n. 73 del 18 gennaio 2024 è stato altresì istituito un Comitato "Privacy" che, in raccordo con il DPO, si pone l'obiettivo di contribuire a migliorare il processo di implementazione e di adeguamento della FSGT alle previsioni di cui al Regolamento (UE) 679/2016, e di realizzare un orientamento omogeneo, nell'ottica dell'accrescimento qualitativo delle attività individuali e della performance organizzativa della FSGT. A ciò si aggiunga che l'istituzione del Comitato "Privacy" intende contribuire alla definizione di un modello istituzionale di *governance* del sistema finalizzato all'analisi, alla verifica, al monitoraggio ed al controllo degli adempimenti di cui al predetto Regolamento Europeo, consentendo, altresì, alla FSGT di intervenire in via preventiva, mediante appositi meccanismi di allerta, nell'individuazione di eventuali e significativi scostamenti che possano comprometterne l'attuazione, nonché nell'identificazione dei correlati rimedi e misure di sicurezza.

Il modello organizzativo proposto nel presente documento si pone, pertanto, l'obiettivo di individuare strategie, linee guida generali e disposizioni operative interne volte a disciplinare il trattamento dei dati personali effettuato dalla FSGT. In essa sono quindi disciplinati i ruoli e le responsabilità, nonché gli adempimenti da seguire in materia di protezione dei dati personali, facendo rinvio per gli aspetti più specifici a regolamenti, procedure, indirizzi e indicazioni aziendali emanati nel tempo ed opportunamente allegati in quanto parti integranti e sostanziali del MOP.

2. METODOLOGIA ADOTTATA

L'approccio metodologico utilizzato nella sequenza delle attività finalizzate a porre in essere le condizioni necessarie alla corretta implementazione di quanto prescritto dal Regolamento europeo, ha previsto anzitutto una valutazione di tipo preventivo ed evolutivo – peraltro molto simile a quella già utilizzata per l'implementazione delle politiche in tema di anticorruzione e trasparenza e per la predisposizione del Piano triennale della prevenzione della corruzione - secondo lo schema P.P.D.A. (*plan, prevent, do, act*) che si basa sulla valutazione dei rischi secondo il seguente flusso: a) accertamento ed analisi quantitativa e qualitativa del rischio; b) esame relativo alla natura, all'oggetto, al contesto ed alla finalità del trattamento; c) computazione dei costi di attuazione e manutenzione delle misure; d) specificazione/esecuzione delle misure tecniche ed organizzative ritenute adeguate.

Pertanto, attraverso iniziali e specifiche sessioni di *assessment*, si è provveduto a:

a) analizzare lo stato dell'arte;

b) comparare lo stato dell'arte con lo standard normativo;

c) programmare le azioni oggetto di nuova individuazione e quelle di aggiornamento dello stato dell'arte;

d) programmare un sistema di sicurezza nella protezione dei dati, mediante l'analisi ed eventuale revisione di procedure e infrastrutture organizzative con particolare riguardo alla sicurezza informatica e di quella degli edifici (es. video-sorveglianza);

e) aggiornare la modulistica e gli schemi negoziali;

f) pianificare la formazione del personale;

g) individuare un sistema di analisi, valutazione e monitoraggio della correttezza/efficacia/efficienza delle azioni realizzate.

Ciò premesso, si ritiene opportuno ribadire che la realizzazione delle azioni e delle misure, anche di aggiornamento, oggetto di pianificazione e programmazione aziendale, sottendono un lavoro che è in continuo divenire. Pertanto, il presente documento - lungi dal rappresentare una fotografia statica di quanto implementato sino ad oggi in materia di protezione dei dati personali - si caratterizza per la sua attitudine all'aggiornamento continuo e per la capacità del medesimo di stare al passo con le strategie aziendali sullo specifico tema.

3. DEFINIZIONI

Ai fini del presente Modello Organizzativo Privacy si applicano le seguenti definizioni, coerenti con quanto previsto dalla normativa di settore:

- Normativa: D. Lgs. 196/2003 (come modificato dal D. Lgs. 101/2018) e Regolamento (UE) 2016/679, nonché ulteriori provvedimenti in materia di fonte normativa secondaria in vigore al momento dell'approvazione del presente Modello Organizzativo Privacy.
- Codice Privacy: Decreto legislativo 30 giugno 2003, n. 196 "*Codice in materia di protezione dei dati personali*", come modificato dal Decreto Legislativo 10 agosto 2018, n. 101;
- Regolamento: 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, che abroga la direttiva 95/46/CE (GDPR - Regolamento Generale sulla Protezione dei Dati);
- FSGT: Fondazione IRCCS San Gerardo dei Tintori

- SGP: Sistema di Gestione della Privacy;
- 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 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;

  A proposito delle tipologie di "dati" sopra indicate, si fa rinvio, per la disciplina di dettaglio, alle disposizioni di cui al D.lgs. 101 del 2018 che ha novellato il D. Lgs. 196/2003 (vedasi, in particolare, il Titolo 1° della Parte 1^, rubricato "Disposizioni generali").
- Interessato: la persona fisica cui si riferiscono i dati personali;
- 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;
- 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;
- Comitato "Privacy": la struttura aziendale preposta alla sorveglianza e al supporto in merito all'applicazione e il rispetto delle disposizioni in materia di trattamento di dati impartite dal Titolare del trattamento e, per quanto di sua competenza se nominato da quest'ultimo, dal DPO;
- Designato (o Referente privacy): la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile con compiti di coordinamento di più o soggetti autorizzati al trattamento;
- Autorizzato: la persona fisica autorizzata a compiere operazioni di trattamento dal Titolare del trattamento o dal Responsabile 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 del trattamento o del responsabile del trattamento;

- 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 del 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;

- 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;

- 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;

- Autorità di controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Regolamento UE;
- 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 inciderebbe in modo sostanziale sugli interessati in più di uno Stato membro.
- Paesi terzi: paesi non appartenenti all'UE o allo spazio Economico Europeo (Norvegia, Islanda, Liechtenstein);

4. AMBITO DI APPLICAZIONE

La politica della protezione dei dati che discende dal presente Modello Organizzativo Privacy (MOP) si applica alla FSGT nella sua interezza, nonché a tutti coloro che stabiliscono rapporti con la medesima.

Infatti, l'attuazione del MOP è obbligatoria per tutto il personale e deve essere considerata parte integrante di qualsivoglia rapporto giuridico instaurato dalla FSGT.

A questo riguardo, si rappresenta che è stata svolta una preliminare analisi del contesto interno ed esterno in cui opera la FSGT: sistema delle responsabilità e livello di complessità dell'amministrazione, organi di indirizzo, struttura organizzativa, ruoli e responsabilità; politiche, obiettivi, e strategie; risorse, conoscenze, sistemi e tecnologie; qualità e quantità del personale; cultura organizzativa; sistemi e flussi informativi, tipologia di dati oggetto di trattamento; relazioni interne ed esterne che la medesima intrattiene con i diversi interlocutori istituzionali e non e che concorrono al raggiungimento degli obiettivi strategici di politica sanitaria e delle finalità proprie della FSGT.

Ciò ha consentito di contestualizzare e configurare il trattamento, analizzare i potenziali rischi per i diritti e le libertà delle persone fisiche ed individuare le misure di sicurezza, così prevedendo le garanzie indispensabili finalizzate a soddisfare i requisiti richiesti dal Regolamento europeo e tutelare i diritti degli interessati.

Proprio in ragione della *mission* istituzionale della FSGT e della particolare categoria dei dati oggetto di trattamento, la medesima si impegna a garantire che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel pieno rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato.

Peraltro, si deve tener conto che i diritti alla riservatezza dei dati, in particolar modo di quelli sanitari, devono sempre più misurarsi con la diffusione degli strumenti informatici e telematici che consentono una raccolta di informazioni ampia, organizzata in modo più sistematico e più difficilmente controllabile. E' il caso dell'accesso ai **referti *on line.*** A questo riguardo sono state predisposte specifiche misure (accesso dell'interessato con utilizzo di password dedicate sia attraverso collegamento al sito, che ricevendo il referto per posta elettronica).

Altro tema rilevante è quello della **cartella clinica**. In particolare, all'atto del ricovero è prevista la compilazione del consenso generico alle cure e del consenso al trattamento dei dati personali/tutela della privacy, che vengono conservati nella cartella clinica, di cui costituiscono parte integrante (vedasi pag. 18 del documento ASST-DA-014). Alcuni dei processi di cura di questa FSGT dispongono di strumenti informatizzati per la gestione, archiviazione e consultazione di dati clinico/sanitari. Attualmente non è disponibile una Cartella Clinica Elettronica aziendale, tuttavia sono in corso di avvio specifiche progettualità a valere sui fondi del PNRR che, tra gli altri, ne prevedono l'introduzione ed attuazione entro il 30.6.2025. Sono presenti alcune soluzioni definibili come "verticali" ovvero specialistiche che possono essere definite come cartelle. A livello aziendale si possono individuare due macro settori di gestione dei sistemi informativi clinici.

La totalità dei sistemi concorre a comporre le informazioni dei pazienti gestite in formato elettronico. In generale l'accesso ai sistemi avviene tramite l'uso di utenze personali dotate di password. L'accesso a un sistema tramite utenza personale consente l'accesso ai dati presenti solo al sistema per cui si è autorizzati. Ad un livello inferiore è possibile definire ulteriori criteri di accesso a seconda dei profili degli utilizzatori autorizzati. Per quanto concerne le informazioni sanitarie ricomprese tra quelle "a maggior tutela dell'anonimato", come per esempio: Test HIV, Interruzioni Volontarie di Gravidanza, utilizzo di sostanze stupefacenti, parto anonimo, atti di violenza sessuale o di pedofilia, i sistemi integrati con il SISS prevedono di acquisire in associazione al referto prodotto il c.d. DAO. La generazione del documento oscurante è determinato automaticamente dalla codifica delle prestazioni associate all'erogazione. In altri casi è compito del refertatore oscurare il documento prima della firma digitale del documento. I documenti che vengono firmati per l'invio al SISS e corredati di DAO non vengono notificati al Fascicolo Sanitario Elettronico.

Ulteriore tema di grande attualità è il **fascicolo sanitario elettronico,** ovvero di quell'atto informatico che raccoglie l'insieme dei dati sanitari di un determinato soggetto a esito di trattamenti effettuati da diversi operatori sanitari nel corso del tempo. Esso raccoglie la storia sanitaria di un soggetto indipendentemente dalle strutture e dal personale medico che hanno contribuito a definirla. La L. R. 31 luglio 2007, n. 18, ne ha previsto l'implementazione e la FSGT, partecipa al progetto regionale SISS, mettendo a disposizione i propri documenti clinici, prodotti e firmati digitalmente, al fine di comporre il Fascicolo Sanitario Elettronico (FSE).

Per quel che concerne il tema della **telemedicina,** si rappresenta che nel 2023 la FSGT ha avviato un servizio di Televisita, svolto in modo sperimentale presso il servizio di

Reumatologia. Lo strumento attualmente in uso è il *C4C Meetings* della società Dedalus spa, in attesa dalla nuova Infrastruttura Regionale di Telemedicina che Regione Lombardia metterà a disposizione degli ES nell'ambito dei servizi del SGDT (Sistema di Gestione Digitale del Territorio) e che permetterà la diffusione dei servizi di Telemedicina su tutto il territorio regionale in modalità sicura, strutturata e integrata.

La Fondazione, mediante un team di lavoro multidisciplinare, ha definito una procedura aziendale per la gestione del processo di telemedicina che prevede, tra le altre, l'acquisizione di un consenso informato ad hoc per l'erogazione di servizi di telemedicina, che prevede di limitare solo a casi eccezionali l'uso della mail quale strumento per lo scambio di informazioni sanitarie, in quanto non completamente sicuro.

Con le Regole di Sistema 2024, Regione Lombardia ha avviato un percorso di diffusione dei servizi di Telemedicina a tutti gli enti del servizio sanitario. Al fine di ottemperare alle indicazioni regionali, anche FSGT ha chiesto alle discipline individuate da Regione Lombardia, unitamente ai servizi che già erogano prestazioni in modalità telematica di predisporre dei percorsi strutturati di Televisita, Teleconsulto, Teleassistenza e Telemonitoraggio che saranno poi implementati nel secondo semestre 2024. A tal fine quindi, si prevede un'attività di adeguamento della procedura aziendale che risponda alle esigenze di tutti i servizi di telemedicina.

Inoltre, l'attività ha la duplice funzionalità di far emergere attività che già si svolgono all'interno dell'ospedale ma al di fuori del perimetro dettato dalla procedura aziendale. L'obiettivo è quindi di far confluire le varie progettualità all'interno delle finalità aziendali e di portare le Unità Operative ad utilizzare strumenti informatici in dotazione all'azienda e più sicuri di altri strumenti commerciali in uso, che possono incorrere in rischi di perdita delle informazioni o di erogare le prestazioni senza previo consenso informato da parte del paziente.

In aggiunta, sono previste delle attività da parte di ARIA spa di VA/PT (Vulnerability Assessment e Penetration Test) finalizzati a testare la capacità dell'applicativo in uso di resistere ad eventuali attacchi esterni. In funzione delle risultanze, FSGT procederà con la definizione di adeguate misure di mitigazione se necessarie.

Ciò premesso, la FSGT si impegna a dimostrare che il trattamento dei dati personali avvenga in maniera conforme a quanto previsto dalla normativa e, secondo i principi di applicabili al trattamento dei dati personali, ai sensi dell'art 5 GDPR.

In particolare i dati devono essere:

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

- esatti e, se necessario, aggiornati. A tal proposito, si segnala l'impegno all'adozione di misure atte a cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- 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;
- 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.

Le presenti indicazioni sono valide, oltre che per i trattamenti dei dati personali di cui la FSGT è Titolare, anche per tutti quei trattamenti per cui quest'ultima è nominata in qualità di Responsabile del trattamento.

5. SICUREZZA DELLE INFORMAZIONI

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni trattate nell'espletamento delle procedure aziendali, rispetto alle quali la FSGT si impegna ad assicurare integrità e protezione, consentendo l'accesso esclusivamente ai ruoli e alle funzioni necessarie, preventivamente autorizzate.

La mancanza di adeguati livelli di sicurezza può, infatti, comportare un danno di immagine, nonchè il rischio di incorrere in sanzioni correlate alla violazione delle leggi vigenti, nonché altri danni di natura economica e finanziaria.

Per conseguire l'allineamento normativo e aumentare la capacità di controllo, la FSGT ha istituito un Registro delle attività di trattamento, ai sensi dell'art. 30 GDPR, rispetto al quale è in corso un'attività di revisione e di aggiornamento con il nuovo DPO/RPD.

La FSGT ha avviato, inoltre, specifiche azioni finalizzate ad identificare le ulteriori esigenze di sicurezza tramite la valutazione di impatto sulla protezione dei dati (DPIA), ai sensi dell'art. 35 GDPR che consente di acquisire un livello aggiuntivo di sicurezza e consapevolezza con riguardo al grado di esposizione a minacce esterne che possano compromettere i sistemi di gestione dei dati, nonché presentare un rischio elevato per i diritti e le libertà delle persone fisiche. La valutazione del rischio, che dovrà essere eseguita su tutti i trattamenti in essere o previsti, permette, infatti, di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione delle misure di sicurezza, oltre ad indicare quale sia la probabilità che le minacce identificate trovino reale attuazione. I risultati di questa valutazione determinano le azioni necessarie per individuare le corrette e adeguate misure di sicurezza e i meccanismi per garantire la protezione dei dati personali.

La gestione della sicurezza delle informazioni è fondata su alcuni imprescindibili principi

generali, di seguito enunciati:

a) classificazione delle informazioni in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza, integrità e disponibilità coerenti e appropriati;

b) presenza di una procedura di identificazione e autenticazione degli accessi ai sistemi informativi;

c) definizione di procedure per l'utilizzo sicuro dei beni e del patrimonio informativo della FSGT;

d) sensibilizzazione del personale sulle problematiche relative alla sicurezza delle informazioni, anche al fine di prevenire e gestire in modo tempestivo eventuali incidenti occorsi, attraverso tempestiva notifica di criticità occorse relative alla sicurezza di cui si venga a conoscenza nell'esercizio delle funzioni istituzionali;

e) individuazione di misure di sicurezza atte a prevenire l'accesso non autorizzato ai locali e alle apparecchiature dove sono gestite le informazioni;

f) individuazione di misure volte a garantire il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente alla sicurezza delle informazioni.

Il Titolare del Trattamento, con il supporto del RPD/DPO e della S.C. Sistemi Informativi Aziendali sostiene attivamente le attività inerenti alla gestione della protezione dei dati tramite indirizzi precisi, incarichi espliciti ed il riconoscimento delle rispettive responsabilità con riguardo alla sicurezza delle informazioni.

In particolare:

a) individua gli obiettivi relativi alla sicurezza delle informazioni;

b) approva e sostiene tutte le iniziative volte al miglioramento della sicurezza delle informazioni;

c) attiva programmi per la diffusione della consapevolezza e della cultura della sicurezza delle informazioni.

Per la protezione dei dati personali degli utenti, la FSGT si avvale di specifiche tecnologie e procedure aziendali di protezione.

6. RISERVATEZZA DELLE INFORMAZIONI

La FSGT si impegna a garantire la riservatezza e la confidenzialità delle informazioni e dei dati degli interessati acquisiti nel corso della propria attività istituzionale in conformità alle procedure interne, nonché al presente MOP.

Il trattamento dei dati può essere effettuato attraverso strumenti manuali e informatici atti a

memorizzare, elaborare, gestire e trasmettere i dati stessi nel rispetto delle misure di sicurezza previste. Tutti i soggetti a qualsiasi titolo e livello, coinvolti nel trattamento dei dati personali, indipendentemente dal rispetto degli obblighi derivanti dal codice deontologico relativo alla professione regolamentata eventualmente esercitata nell'espletamento delle proprie mansioni, sono tenuti al segreto previsto dall'art. 2407 del codice civile.

La FSGT garantisce adeguati livelli minimi di sicurezza delle informazioni rese disponibili da terzi con la medesima diligenza e livello di protezione utilizzati per la sicurezza e la riservatezza dei propri dati.

7. ATTUAZIONE DEL MODELLO ORGANIZZATIVO PRIVACY (MOP)

L'osservanza e l'attuazione delle previsioni di cui al presente MOP, da valorizzare anche ai fini della valutazione della *performance* organizzativa ed individuale, è una specifica responsabilità posta in capo a:

a) tutto il personale che, a qualsiasi titolo e livello, collabora con la FSGT ed è in qualche modo coinvolto nel trattamento di dati e informazioni. Il personale è infatti responsabile, ciascuno per quanto di propria competenza, della segnalazione di tutte le anomalie e violazioni di cui dovesse venire a conoscenza nell'espletamento delle funzioni assegnate;

b) tutti i soggetti esterni che intrattengono rapporti e collaborano con l'azienda e che devono garantire il rispetto dei requisiti contenuti nel presente MOP;

c) Comitato "Privacy", con specifico riferimento ai compiti allo stesso assegnati e descritti puntualmente nel paragrafo dedicato.

8. ATTIVITA' DI ANALISI, MONITORAGGIO E CONTROLLO DEL SISTEMA PRIVACY

Il Titolare del trattamento, per il tramite delle Strutture della FSGT e con il supporto del RPD/DPO, vigila sulla corretta implementazione e sull'efficacia delle misure di sicurezza, al fine di favorire l'attivazione di un processo di aggiornamento e miglioramento continuo in materia di protezione dei dati personali.

L'attività di revisione è finalizzata a verificare lo stato di attuazione delle azioni preventive e correttive e l'aderenza alla politica di cui al presente MOP delle procedure in atto.

La predetta attività di revisione e di aggiornamento deve inoltre tenere conto di tutti i cambiamenti che possono influenzare l'approccio alla gestione della sicurezza delle informazioni, includendo i cambiamenti organizzativi, l'ambiente tecnico, la disponibilità di risorse, le condizioni legali, regolamentari o contrattuali e dei risultati dei precedenti riesami.

9. INFORMAZIONE E FORMAZIONE

La FSGT sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

A tal riguardo, uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è rappresentato dall'attività formativa del personale aziendale e dall'attività informativa diretta a tutti coloro che hanno rapporti con la FSGT.

Pertanto, l'obiettivo di garantire un corretto trattamento dei dati, conforme ai requisiti previsti dalla normativa, viene raggiunto dalla FSGT anche e soprattutto grazie alla particolare attenzione riposta nei confronti della formazione del proprio personale.

Per le suddette finalità la FSGT provvede a:

a) adottare un piano formativo con l'obiettivo di alfabetizzazione iniziale in materia di protezione dei dati personali destinato a tutto il personale in servizio;

b) prevedere l'erogazione di moduli specifici all'interno dei corsi di formazione per il ruolo ricoperto;

c) prevedere un piano di formazione programmato con cadenza annuale sulla formazione erogata in ambito privacy a tutto il personale in servizio;

d) conservare la documentazione distribuita e la modulistica attestante la partecipazione agli interventi formativi.

La formazione dei soggetti autorizzati al trattamento e, ove ritenuto necessario, delle altre figure chiave, riguarda in particolare:

a) gli aspetti generali della disciplina di protezione dei dati personali;

b) le minacce, le vulnerabilità, la probabilità di accadimento e di conseguenza i rischi che minacciano i dati trattati;

c) le conseguenze derivanti dalla violazione dei dati personali (Data Breach);

d) le procedure da seguire in caso di violazione dei dati personali;

e) le misure di prevenzione per evitare o almeno ridurre la probabilità di accadimento delle violazioni e le misure di mitigazione del danno in caso si verifichino;

f) gli aspetti specifici della disciplina di protezione dei dati personali nel settore sanitario;

g) l'addestramento specifico per aggiornare il personale sulle misure di sicurezza e protezione dei dati personali ritenute adeguate e adottate dal Titolare del trattamento.

La formazione è pianificata affinché la medesima sia

- adeguata al sistema di trattamento dei dati personali;

- efficace nella trasmissione delle informazioni in materia di protezione dei dati personali;
- efficiente nel fornire strumenti per l'esecuzione delle procedure;
- documentabile, in quanto parte integrante della policy della FSGT

10. ORGANIGRAMMA, SISTEMA DI NOMINE E RESPONSABILITÀ

Al fine di garantire la tutela dei diritti delle persone fisiche relativamente al trattamento dei dati personali, la FSGT provvede alla puntuale individuazione dei soggetti che ricoprono ruoli attivi nel trattamento.

Ciò ai fini di una immediata comprensione della catena delle responsabilità parametrate alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento, nonché ai rischi per i diritti e le libertà delle persone fisiche.

In conformità con la normativa di riferimento e con la policy che discende dal presente MOP, costituiscono figure imprescindibili quelle di seguito descritte.

10.1 Titolare del Trattamento

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

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti della normativa vigente è la Fondazione IRCCS San Gerardo dei Tintori, in persona del Direttore Generale, così come previsto dall'art. 16 del vigente Statuo della FSGT, con sede in MONZA Via Pergolesi, 33, allorquando la medesima non sia individuata quale Responsabile del trattamento.

Conformemente a quanto previsto dalla normativa il Titolare del trattamento si impegna a:

a) richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;

b) nominare il Responsabile per la protezione dei dati (RPD) o Data Protection Officer, (DPO), come stabilito dall'articolo 37 del Regolamento UE 679/2016;

c) adeguare il proprio assetto organizzativo per rendere il governo della privacy allineato ai dettami normativi;

d) adottare le modalità operative necessarie alla corretta gestione degli adempimenti ai fini della protezione dei dati personali trattati;

e) assumere le decisioni in ordine alle finalità, alle modalità del trattamento dei dati e agli strumenti utilizzati, ivi compreso il profilo della sicurezza, sia per i trattamenti svolti all'interno che all'esterno della propria struttura;

f) individuare e designare i Responsabili del trattamento dei dati, impartendo loro le relative direttive e, se necessario, istruzioni specifiche;

g) vigilare sulla puntuale osservanza delle disposizioni e istruzioni impartite a tutti i soggetti che hanno un ruolo attivo nel trattamento dei dati personali;

h) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

i) garantire sempre il pieno controllo sulla piramide organizzativa di cui è al vertice, concedendo autorizzazioni generali o specifiche ai responsabili del trattamento secondo criteri di opportunità nelle diverse situazioni ed esprimendo o negando il gradimento nei confronti di sub-responsabili eventualmente proposti dai responsabili assumendo così un ruolo di effettivo controllo e indirizzo.

Inoltre, il Titolare del trattamento si impegna a garantire l'esercizio dei diritti degli interessati e a tal scopo individua e mette in pratica apposite procedure al fine di informare gli interessati e garantire a ciascuno di essi il:

a) diritto all'accesso, ovvero di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e di averne accesso. In particolare l'interessato ha diritto di conoscere l'origine dei dati personali; le finalità e modalità del trattamento; la logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici; gli estremi identificativi del titolare, dei responsabili e degli eventuali rappresentanti designati; l'elenco dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza a qualsiasi titolo in linea con la normativa e quello dei soggetti autorizzati al trattamento;

b) diritto alla rettifica, ovvero di ottenere l'aggiornamento, la correzione e, allorchè sussista l'interesse, l'integrazione dei dati;

c) diritto alla cancellazione, ovvero di ottenere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) diritto di limitazione del trattamento, ovvero il diritto di limitare il trattamento dei dati personali;

e) diritto all'opposizione, ovvero il diritto di limitare il trattamento od opporsi al trattamento.

10.2 Contitolari del trattamento

Come stabilito dall'art. 26 del Regolamento UE 679/2016, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE 679/2016, con particolare riguardo all'esercizio dei diritti dell'interessato, l'eventuale notifica di una violazione dei dati personali all'Autorità Garante e le rispettive funzioni di comunicazione delle informazioni.

All'interno del Registro dei Trattamenti sono previsti eventuali casi di contitolarità.

10.3 Il Responsabile della Protezione dei Dati (RPD o DPO - Data Protection Officer)

Il Regolamento Europeo ha previsto l'obbligo di nomina del Responsabile della protezione dei dati (RPD) o *Data Protection Officer* (DPO) che deve essere in possesso di specifiche conoscenze competenze e capacità, nonché di particolari caratteristiche di indipendenza ed autorevolezza, oltre che adeguate competenze manageriali.

Il RPD/DPO svolge i seguenti compiti:

a) sorveglia sull'osservanza del Regolamento, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;

b) fornisce consulenza, anche attraverso l'emissione di pareri, al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;

c) collabora con il Titolare, laddove necessario, nel condurre una valutazione di impatto sulla protezione dei dati (DPIA);

d) informa e sensibilizza il Titolare o il Responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;

e) coopera e fungere da punto di contatto con l'Autorità Garante su ogni questione connessa al trattamento;

f) supporta il Titolare o il Responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta e all'aggiornamento del registro delle attività di trattamento.

I dati di contatto del RDP/DPO, in conformità al Regolamento, sono pubblicati sul sito web istituzionale ed inseriti nell'informativa aziendale sul trattamento dei dati; ciò al fine di

agevolarne la contattabilità da parte dei cittadini-utenti, nonché dall'Autorità Garante per la protezione dei dati personali.

Il RPD/DPO della FSGT partecipa di diritto ai lavori del Comitato "Privacy" di cui al successivo paragrafo.

10.4 Il Comitato "Privacy"

Come sopra anticipato, la FSGT ha ritenuto necessario sviluppare, in un'ottica di promozione e valorizzazione dell'eccellenza, un nuovo modello di governance in tema di protezione dei dati. Tra gli interventi finalizzati all'individuazione di un sistema di gestione integrato fortemente interconnesso con l'organizzazione aziendale, si annovera l'istituzione di un Comitato "Privacy" che, in raccordo con il RPD/DPO, contribuisca a migliorare il processo di implementazione e di adeguamento da parte della FSGT delle previsioni di cui al Regolamento europeo e a realizzare un orientamento omogeneo, nell'ottica dell'accrescimento qualitativo delle attività individuali e della *performance* complessiva della Fondazione SGT.

Il Comitato svolge le proprie funzioni con l'obiettivo di creare una sinergia diffusa tra tutti i soggetti del sistema privacy della FSGT, di prevenire o evitare possibili conflitti organizzativi e favorire in tal modo l'adeguamento continuo alla normativa sulla protezione dei dati personali.

Nell'esercizio delle proprie funzioni il Comitato si raccorda, in modo particolare, sistematico e trasparente, con il Responsabile per la Protezione dei Dati (RPD) o Data Protection Officer (DPO). Il Comitato, inoltre, supporta il Titolare del trattamento dei dati nel raggiungimento degli obiettivi finalizzati all'adeguamento continuo della Fondazione al Regolamento Europeo n. 679/2016.

I compiti del Comitato "Privacy" sono i seguenti:

a) supportare le politiche del Titolare del trattamento e le attività del Responsabile della Protezione dei Dati (Data Protection Officer - DPO) circa l'osservanza della normativa in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale con ruoli attivi nel trattamento e promuovere la cultura della protezione dei dati all'interno della FSGT;

b) definire le priorità e validare le proposte di sviluppo per la corretta implementazione delle politiche aziendali in tema di protezione dei dati, anche attraverso la lettura integrata con dati e informazioni derivanti dagli altri sistemi di monitoraggio aziendali e dall'ulteriore documentazione strategica della FSGT;

c) aggiornare il modello organizzativo privacy MOP ogni qualvolta se ne ravvisi l'esigenza;

d) esaminare e validare i programmi formativi da sviluppare e da inserire nel piano

annuale della formazione;

e) validare, sotto un profilo tecnico, la documentazione strategica predisposta con il supporto del DPO in materia di protezione dei dati personali ed assicurarne la capillare e tempestiva diffusione ed adozione da parte delle singole strutture della FSGT;

f) predisporre e attuare adeguati flussi di comunicazione da e verso il Responsabile della Protezione dei Dati (DPO), ivi inclusi gli allarmi (*alert)* e le violazioni (*data breach)* di sistema;

g) fornire al Responsabile della Protezione dei Dati (DPO) accesso alle informazioni necessarie per lo svolgimento dei compiti a quest'ultimo attribuiti;

h) vigilare sul tempestivo aggiornamento del Registro dei trattamenti ex art. 30 GDPR;

i) coinvolgere il Responsabile della Protezione dei Dati (DPO) in questioni di particolare complessità.

10.5 Designato alla gestione delle attività di trattamento dei dati

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

La FSGT in qualità di Titolare del trattamento dei dati, tenuto conto del grado di complessità che caratterizza la FSGT, ha reputato opportuno individuare i soggetti da "designare" quali Referenti privacy, ai sensi del D. Lgs. 101/2018 nelle seguenti, specifiche figure:

a) i Direttori delle Strutture complesse;

b) i Responsabili delle Strutture Semplici Dipartimentali;

c) i Responsabili delle Strutture Semplici;

d) i Responsabili delle S.S. (non incardinate in una S.C.) delle Strutture collocate direttamente "in staff" alla Direzione Aziendale;

e) ulteriori figure individuate specificamente.

La FSGT provvede con apposito atto di nomina ad individuare i "Designati al trattamento dei dati". La suddetta nomina viene sottoscritta dal Designato per presa visione ed accettazione **(*All. n. 1*).**

I compiti del soggetto Designato sono previsti in maniera puntuale nel suddetto atto di nomina che, allegato al presente documento, ne costituisce parte integrante e sostanziale.

Di seguito se ne riporta una breve sintesi:

a) individuare le persone da autorizzare al trattamento dei dati e promuoverne l'autorizzazione per area di competenza;

b) segnalare eventuali casi di violazioni dei dati personali;

c) segnalare eventuali richieste ricevute da parte dell'interessato sull'esercizio dei relativi diritti, nonché attenersi alla procedura interna sull'esercizio dei diritti;

d) cooperare in caso di attività di controllo nell'ambito della protezione dei dati personali da parte di strutture interne o esterne, fornendo eventuale documentazione richiesta e garantendo l'accesso ai locali;

e) informare il DPO dell'esistenza di un nuovo trattamento per cui risulta necessario aggiornare il registro o modificarlo, in applicazione del principio di privacy by design e by default;

f) informare il DPO della presenza di una nuova risorsa che tratta dati personali al fine di valutare necessità di formazione in ambito privacy;

g) monitorare che le persone autorizzate al trattamento rispettino le indicazioni impartite dall'Ente;

h) segnalare i casi di mancato rispetto delle disposizioni in tema di protezione dei dati al Titolare del trattamento.

10.6 Autorizzato alle attività di trattamento dei dati

Il D.lgs. 196/2003, come novellato dal D.lgs. 101/2018 di armonizzazione del Codice italiano della privacy alle novità del Regolamento europeo, all'art. 2-quaterdecies, co. 2, stabilisce che il Titolare "*individui le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta";* l'art. 29 GDPR stabilisce che "*Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".*

Per tale motivo, il Titolare del trattamento, in relazione all'ambito lavorativo assegnato, attraverso specifico atto **(*All. n. 2*)** nomina la "Persona Autorizzata al trattamento dei dati personali". L'autorizzazione è effettuata in relazione a tutte le operazioni di trattamento dei dati, censite nel Registro dei trattamenti, che siano strettamente correlate e necessarie al corretto adempimento dei compiti assegnati in relazione alle attività svolte nell'ambito della

Struttura di appartenenza e per le finalità strettamente pertinenti all'esecuzione della prestazione lavorativa.

Nei limiti delle mansioni affidate, le persone autorizzate, siano essi lavoratori dipendenti con rapporto di lavoro subordinato o rapporto di lavoro di altra natura e tipologia, devono eseguire le previste operazioni di trattamento, attenendosi scrupolosamente alle istruzioni impartite dal Titolare o dal Designato.

Il soggetto autorizzato effettua tutte le operazioni di trattamento dei dati personali attinenti all'attività lavorativa di competenza dell'area di appartenenza e si impegna a:

a) trattare i dati personali oggetto di comunicazione in modo lecito e corretto, mantenendo assoluto riserbo sugli stessi;

b) utilizzare le sole banche dati ed i soli strumenti oggetto di specifica autorizzazione preventiva;

c) trattare esclusivamente i dati necessari allo svolgimento della mansione lavorativa e solo contestualmente alla stessa;

d) non lasciare incustoditi o accessibili a terzi non autorizzati gli strumenti elettronici mentre è in corso una sessione di lavoro;

e) custodire e non divulgare né cedere a terzi le proprie credenziali di autenticazione;

f) procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti magnetici una volta terminate le ragioni della consultazione;

g) osservare scrupolosamente tutte le misure di sicurezza già predisposte, o che saranno successivamente comunicate dal Titolare e/o dal Designato;

h) rispettare tutte le misure di sicurezza previste per poter garantire la confidenzialità, disponibilità, integrità dei dati trattati;

i) informare il Titolare e/o il Designato nel caso si verifichino incidenti relativi alla sicurezza delle informazioni trattate;

j) rispettare pedissequamente le indicazioni contenute nella complessiva documentazione adottata dalla FSGT in tema di protezione dei dati personali

10.7 Responsabile del trattamento ex art. 28 GDPR

Cosi come previsto dall'art. 28 GDPR, qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo provvede a nominare un Responsabile del trattamento che presenti garanzie sufficienti, nonché misure tecniche ed organizzative adeguate atte a soddisfare i requisiti richiesti dal predetto Regolamento.

Pertanto, il Responsabile del trattamento dei dati è il soggetto che ha il compito di garantire

nelle operazioni di trattamento l'attuazione delle misure di sicurezza previste dalla normativa e dal presente MOP.

Il soggetto preposto allo svolgimento della funzione viene individuato tra quelli in possesso dei necessari requisiti e con adeguate garanzie. Tra le sue funzioni sono comprese quelle di:

a) osservare le procedure in materia di protezione dei dati personali adottate dal Titolare;

b) organizzare, gestire e supervisionare tutte le operazioni di trattamento dei dati personali affinché esse vengano effettuate nel rispetto delle disposizioni di legge e predisporre tutti i documenti nonché le misure tecniche organizzative richiesti dal Codice e dal Regolamento;

c) adottare e verificare il rispetto delle misure di sicurezza indicate dal Codice Privacy e dal Regolamento europeo e la conformità nel tempo dei sistemi e delle misure di sicurezza;

d) redigere e aggiornare il registro delle attività di trattamento, qualora si renda necessario;

e) informare il Titolare del trattamento di tutte le misure adottate e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato al compito specifico;

f) nominare i soggetti autorizzati che svolgono tali funzioni per suo conto, conservando i relativi estremi identificativi, definendo gli ambiti di operatività consentiti e verificando almeno annualmente il relativo operato per controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti il trattamento dei dati personali;

g) nominare i soggetti autorizzati al trattamento dei dati nelle altre funzioni ritenute necessarie conferendo loro apposite istruzioni sulle norme e le procedure da osservare e provvedendo alla relativa formazione;

h) vigilare e controllare le operazioni di trattamento svolte dai soggetti autorizzati sottoposti alla propria responsabilità e la conformità all'ambito di trattamento consentito;

i) redigere e aggiornare la lista dei nominativi dei soggetti autorizzati sottoposti alla propria responsabilità e verificarne almeno annualmente l'ambito di trattamento consentito;

j) proporre al Titolare del trattamento dei dati la nomina di soggetti per il ruolo di sub-Responsabile del trattamento dei dati in relazione all'affidamento agli stessi di determinate attività;

k) attuare gli obblighi di informazione ed acquisizione del consenso, quando richiesto, nei confronti degli interessati;

l) garantire all'interessato che ne faccia richiesta l'effettivo esercizio dei diritti previsti dalla normativa di settore inoltrando al Titolare del trattamento le richieste pervenute nel caso non possano essere evase autonomamente;

m) distruggere i dati personali alla fine del trattamento nei casi previsti dal Regolamento, secondo le procedure atte a garantire la sicurezza degli stessi e provvedere alle formalità di legge e agli adempimenti necessari;

n) comunicare immediatamente al Titolare, non oltre le 24 ore successive al loro ricevimento, ogni richiesta, ordine o attività di controllo da parte del Garante o dell'Autorità Giudiziaria;

o) osservare le procedure in materia di protezione dei dati personali adottate dal Titolare del trattamento;

p) notificare al Titolare del trattamento l'eventuale violazione dei dati personali senza ingiustificato ritardo e, comunque, entro 36 ore dal momento in cui ne sia venuto a conoscenza, attraverso la puntuale descrizione della natura della violazione e delle probabili conseguenze.

In ottemperanza all'articolo 28, paragrafo 7 del Regolamento Europeo 679/2016, la FSGT si è dotata di apposito documento, titolato *"Contratto per la nomina a Responsabile del trattamento dei dati personali"*, da utilizzare tutte le volte che la Fondazione intende stipulare contratti di lavori, servizi e forniture, nonché accordi e convenzioni, anche di ricerca, per la disciplina delle modalità con le quali il Responsabile del trattamento si impegna ad effettuare per conto della FSGT (Titolare) le operazioni di trattamento dei dati **(*All. n. 3*).**

Gli elenchi delle nomine dei responsabili del trattamento dei dati sono inseriti nella cartella di rete "Nomine responsabili art. 28" condivisa con le Strutture interessate (S.C. Convenzioni, libera professione e marketing, S.C. Gestione e Sviluppo delle Risorse Umane, S.C. Gestione Acquisti Provveditorato-Economato, S.C. Gestione Tecnico-Patrimoniale, S.C. Ingegneria Clinica, tenute all'aggiornamento dei dati. In futuro, con il supporto del DPO, si prevede la creazione di un archivio di informazioni strutturato.

10.8 Amministratore di Sistema

Come anticipato nelle premesse del presente documento, la FSGT ha subito di recente una trasformazione giuridica di grande rilevanza che ha determinato l'esigenza di rivedere processi, procedure e tutta la documentazione agli stessi afferente, nonché di mappare i rapporti in essere, anche con soggetti esterni, al fine di verificare la necessità di apportare eventuali modifiche/integrazioni. Si tratta di una attività, come sopra accennato, in continuo divenire, anche tenuto conto del fatto che l'organizzazione aziendale, come scaturita all'esito del percorso di riconoscimento quale IRCCS di diritto pubblico, è da poco entrata in

pieno regime. Questo *leit motive* che, lo si rammenta, costituisce il filo conduttore del presente documento, vale anche per quel che concerne, nello specifico, gli Amministratori di sistema. La FSGT ha provveduto di recente ad aggiornare l'atto per la nomina ad Amministratore di sistema ovvero quella figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi, le reti locali e gli apparati di sicurezza, nella misura in cui tali attività di gestione e manutenzione consentano di intervenire sui dati personali (Provvedimento del Garante per la 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). **(*All. n. 4*).**

L'attribuzione delle funzioni di Amministratore di Sistema avviene previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia, ivi compreso il profilo relativo alla sicurezza.

L'Amministratore di sistema, in linea generale e come da indicazioni dell'Autorità garante, ha le seguenti responsabilità che, nel caso della Fondazione, saranno oggetto, di volta in volta, negli atti di nomina di specifica contestualizzazione:

- sovraintendere alle risorse dei sistemi computerizzati al fine di consentirne un corretto ed efficiente utilizzo;
- fornire guida e supporto ai Soggetti Designati ed ai Soggetti Autorizzati in merito al trattamento dei dati personali;
- amministrare e gestire la sicurezza informatica operando anche come gestore e custode delle password;
- effettuare, nell'ambito delle responsabilità assegnate, periodici controlli e verifiche tecniche, in merito a quanto previsto dal Regolamento sull'utilizzo degli strumenti aziendali informatici;
- individuare i soggetti a cui affidare l'incarico di manutentore del sistema.

Per consentire all'Amministratore di Sistema di svolgere adeguatamente le proprie funzioni, il Titolare del trattamento concede al medesimo le "Autorità di sistema", ovvero l'assegnazione di attributi, privilegi, o accessi che consentono la gestione delle "risorse critiche del sistema operativo", ovvero degli oggetti informatici necessari al funzionamento dei sistemi e del servizio di elaborazione dati.

Si rappresenta che l'elenco dei soggetti nominati Amministratori di Sistema in corso di aggiornamento è conservato adeguatamente.

****

Con deliberazione n. 254 del 28.10.2021 la FSGT ha provveduto a designare il

Responsabile della sicurezza delle informazioni, con il compito di coordinare tutte le attività di definizione, attuazione e verifica delle regole per la sicurezza delle informazioni della Fondazione e il **Responsabile della transizione digitale** per lo svolgimento dei compiti di cui all'art. 17, comma 1, D. L.gs. 82/2005 e da quelli previsti da fonti normative secondarie o atti amministrativi di portata generale emanati successivamente.

11. MISURE DI SICUREZZA GENERALI

L'art. 25 del Regolamento Europeo n.679/2016 introduce il principio sintetizzato dall'espressione inglese *"data protection by default and by design",* ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti richiesti e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà delle persone fisiche. La responsabilità delle attività di impostazione e coordinamento dei sistemi che garantiscono la sicurezza e la tutela di tutti i dati oggetto di trattamento sono in carico ai relativi ruoli come da organigramma della FSGT.

Per le modalità organizzative con le quali questa FSGT ottempera a tale adempimento, si fa rinvio alle specifiche competenze che sono poste in capo alla S.C. Sistemi Informativi Aziendali (SIA), che provvede a monitorare costantemente tutto l'apparato hardware e software della Fondazione, anche mediante una serie di contratti con aziende specializzate del settore e contratti di responsabilità affidati all'esterno. Peraltro, la materia è stata oggetto di una ricognizione in collaborazione con ARIA Spa volta ad individuare una serie di interventi al fine di recepire la Direttiva NIS. Questa survey ha prodotto *un assessment* condiviso tra ARIA Spa e la S.C. Sistemi Informativi Aziendali, nel quale viene evidenziato come la S.C. Ingegneria Clinica adotti le polizze di sicurezza dettate dalla S.C. Sistemi Informativi Aziendali.

11.1 MISURE PER GARANTIRE LA PROTEZIONE DEI DATI

Come stabilito dal Regolamento, le misure di sicurezza devono *"garantire un livello di sicurezza adeguato al rischio*" del trattamento ai sensi dell'art. 32, par. 1, GDPR e sono volte a minimizzare i rischi che le informazioni siano rivelate o modificate senza autorizzazione, ovvero perse o alterate accidentalmente o intenzionalmente.

Queste comprendono un sistema di autenticazione per assicurare che la persona che accede al sistema nelle sue diverse articolazioni sia identificata con certezza, basato su codice identificativo e password individuale segreta, nonché un sistema di autorizzazione che prevede che a ciascun soggetto che accede al sistema sia assegnato un profilo di accesso che definisca i dati ai quali l'utente è autorizzato ad accedere e, ove applicabile, le operazioni che per ciascun dato o gruppo di dati è autorizzato ad eseguire (consultazione,

inserimento, modifica, cancellazione).

Ad eccezione degli Amministratori di Sistema definiti e nominati secondo le disposizioni del Modello Organizzativo Privacy, nessun dipendente della FSGT è Amministratore di Sistema della propria macchina e tutti gli utenti che dispongono di una postazione informatica sono puntualmente censiti.

Per ridurre i rischi di indisponibilità (parziale o totale) nell'accesso al sistema informatico della FSGT, sono state previste una serie di attività, in particolare al momento dell'assunzione o della dimissione del personale, con la procedura di attivazione o dismissione dell'utenza personale. Sempre al fine di controllo, si procede a verificare con cadenza semestrale che la lista dei dipendenti cessati sia coerente con le utenze disabilitate.

I dispositivi della FSGT concessi in dotazione al personale in servizio vengono formattati a seguito della cessazione del rapporto di lavoro, al fine di rimuovere tutti i dati personali contenuti al loro interno. Pertanto, detto personale è tenuto ad assicurarsi che venga correttamente eseguito il passaggio di consegne affinché venga assicurata la continuità dei servizi erogati e la conservazione dei documenti di lavoro.

La FSGT ha poi fatto propria la politica della scrivania sgombra *(Clean Desk Policy)* e dello schermo inattivo *(Clear Screen Policy)*, una delle migliori strategie da attuare per ridurre il rischio di violazioni della sicurezza della postazione di lavoro. Lo scopo di tale politica è stabilire requisiti minimi per prevenire violazioni accidentali o dolose dei dati personali *(Data Breach)*. A questo riguardo si rinvia al documento aziendale "Privacy Policy" A1106-P22_D01 **(*All. n. 5*)** concernente le strategie e le correlate misure di sicurezza da attuare da parte del personale per ridurre il rischio di eventuali violazioni in tema di protezione dei dati.

Per quel che concerne invece la tempestiva notifica all'Autorità di controllo nell'ipotesi di **violazione dei dati personali *(Data Breach*),** da cui possano derivare rischi per i diritti e le libertà delle persone fisiche, si fa espresso rinvio alla normativa vigente e alle correlate indicazioni e procedure aziendali vigenti in materia: Procedura aziendale "Gestione delle violazioni di dati personali (*Data Breach*) **(*All. n. 6)*** e Modulo segnalazione *Data Breach*) **(*All. n. 7)***.

Infine, si rappresenta che con riferimento ai possibili rischi correlati al trattamento e al potenziale impatto negativo sulle libertà e i diritti degli interessati, la FSGT ha avviato uno specifico processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) già adottate o adottabili ai fini della mitigazione di tali rischi.

12. DISPOSIZIONI FINALI

12.1 Norma di rinvio

Per quanto non espressamente previsto dal presente Modello organizzativo Privacy (MOP), si fa rinvio alle disposizioni normative di cui al Regolamento europeo 679/2016 ed al D. L.gs. n. 196/2003 e s.m.i., nonché alle linee guida e ai provvedimenti dell'Autorità Garante per la protezione dei dati personali.

12.2 Pubblicazione

La FSGT provvede a dare pubblicità al presente Modello Organizzativo privacy tramite pubblicazione sul proprio sito internet istituzionale nella sezione "*Amministrazione Trasparente*".

12.3 Allegati

Si allega al presente Modello Organizzativo Privacy la seguente documentazione operativa:

1. Atto di nomina "Designato al trattamento dei dati" (A1106_P22_D03_M01);
2. Atto di nomina "Autorizzato al trattamento dei dati" (A1106_P22_D03_M02;
3. Contratto per il trattamento dei dati personali con il Responsabile ai sensi dell'art. 28, paragrafo 7 del Regolamento (UE) 2016/679 (A1106_P22_D03_M03;)
4. Atto di nomina "Amministratore di Sistema" (A1106_P22_D03_M04);
5. Documento aziendale "Privacy Policy" (A1106-P22_D01);
6. Procedura aziendale "Gestione delle violazioni di dati personali (*Data Breach*)" (A1106_P22_P02);
7. Modulo segnalazione Data Breach . (A1106_P22_P02_M01