IL DIRETTORE GENERALE

Det. n. 57 del 13/3/2025

OGGETTO: ISTITUZIONE DEL SISTEMA DI GESTIONE AZIENDALE PER LA PROTEZIONE DEI DATI PERSONALI (SGA PDP) FPO - IRCCS

Il Direttore Generale,

Visto

- il Regolamento (UE) n. 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)" e, in particolare, gli articoli 4, 24, e da 29 a 39;

- il D. Lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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" e, in particolare, l'articolo 2-quaterdecies;

Premesso altresì che

- un "sistema" è inteso come l'insieme delle procedure e dei processi organizzativi funzionali al soddisfacimento di requisiti definiti ed è uno strumento di carattere organizzativo e gestionale utilizzato per rispettare, in modo visibile e dimostrabile, i criteri ed i requisiti previsti dalla norma di riferimento. Inoltre, un sistema presenta fisiologiche caratteristiche di dinamicità, flessibilità e capacità di miglioramento;

- nello specifico, il "sistema di gestione della protezione dei dati personali (SGA PDP)" è il modello di gestione, organizzazione e controllo che governa il trattamento in sicurezza dei dati personali ed il rispetto dei principi e delle regole delle normative di riferimento, sostanziale e strettamente interconnesso alle attività dell'Istituto;

- le norme in materia di protezione dei dati personali impongono modalità di trattamento trasparenti e codificate. Di conseguenza, l'utilizzo di un sistema di gestione della protezione dei dati personali costituisce un efficace strumento utile non solo per la messa in sicurezza dei dati stessi, ma anche per la loro valorizzazione e la tutela dell'intero patrimonio informativo dell'Istituto;

- è compito dell'Istituto dimostrare la propria diligenza perseguendo gli obiettivi di conformità normativa, responsabile e documentata attraverso l'implementazione di un complesso di misure di sicurezza, anche di carattere organizzativo, in grado di proteggere, nel tempo, i dati personali trattati all'interno dell'ente;

IL DIRETTORE GENERALE

DELIBERA

1. Di considerare le premesse parti integranti del seguente provvedimento;

2. Di approvare il sistema di gestione aziendale della protezione dei dati personali (SGA PDP), come illustrato nell'allegato documento, i quale rappresenta parte integrante della presente deliberazione;

3. Di incaricare il Responsabile risorse umane e libera professione all'organizzazione e attivazione di un adeguato percorso formativo in accordo con il proponente e il DPO aziendale;

4. Di incaricare il Responsabile ICT di pubblicare la presente deliberazione nell'area riservata dei dipendenti.

Salvatore NIEDDU

Fondazione del Piemonte per l'Oncologia IRCCS Candiolo

IL DIRETTORE GENERALE

SISTEMA DI GESTIONE AZIENDALE PROTEZIONE DATI PERSONALI (SGA PDP)

Sommario:

1. PREMESSA

Come noto un "sistema" è inteso come l'insieme delle procedure e dei processi organizzativi funzionali al soddisfacimento di requisiti definiti ed è uno strumento di carattere organizzativo e gestionale utilizzato per rispettare, in modo visibile e dimostrabile, i criteri ed i requisiti previsti dalla norma di riferimento. Inoltre, un sistema presenta fisiologiche caratteristiche di dinamicità, flessibilità e capacità di miglioramento.

Nello specifico, il "Sistema di Gestione Aziendale Protezione Dati Personali (SGA PDP)" è il modello di gestione, organizzazione e controllo che governa il trattamento in sicurezza dei dati personali ed il rispetto dei principi e delle regole delle normative di riferimento, sostanziale e strettamente interconnesso alle attività dell'azienda.

Le norme in materia di protezione dei dati personali impongono modalità operative concrete e verificabili. Di conseguenza, l'utilizzo di un sistema di gestione costituisce un efficace strumento utile non solo per la messa in sicurezza dei dati, ma anche per la loro valorizzazione e la tutela dell'intero patrimonio informativo aziendale.

Poiché è compito dell'Istituto dimostrare la propria diligenza perseguendo gli obiettivi di conformità normativa, responsabile e documentata attraverso l'implementazione di un complesso di misure di sicurezza in grado di proteggere, nel tempo, i dati personali, si rende necessaria la revisione dell'attuale sistema di gestione della privacy, adeguandolo ai continui cambiamenti organizzativi dell'azienda.

I principi del Regolamento UE 679/2016 (GDPR) devono tradursi in prassi operative, controlli e comportamenti efficaci, assumendosi la responsabilità delle scelte. Si tratta del principio di accountability: "Titolare e Responsabili devono saper progettare e implementare misure di sicurezza pertinenti alla propria realtà organizzativa, ai rischi connessi al trattamento, funzionali agli obiettivi di protezione dei dati e del rispetto del Regolamento".

2 SCOPO

Scopo del presente documento è quello di delineare il Sistema di Gestione Aziendale Protezione Dati Personali (SGA PDP) all'interno dell'Istituto di Candiolo FPO-IRCCS, individuando compiti e responsabilità dei vari attori dell'Istituto e dei soggetti esterni che collaborano con l'Istituto.

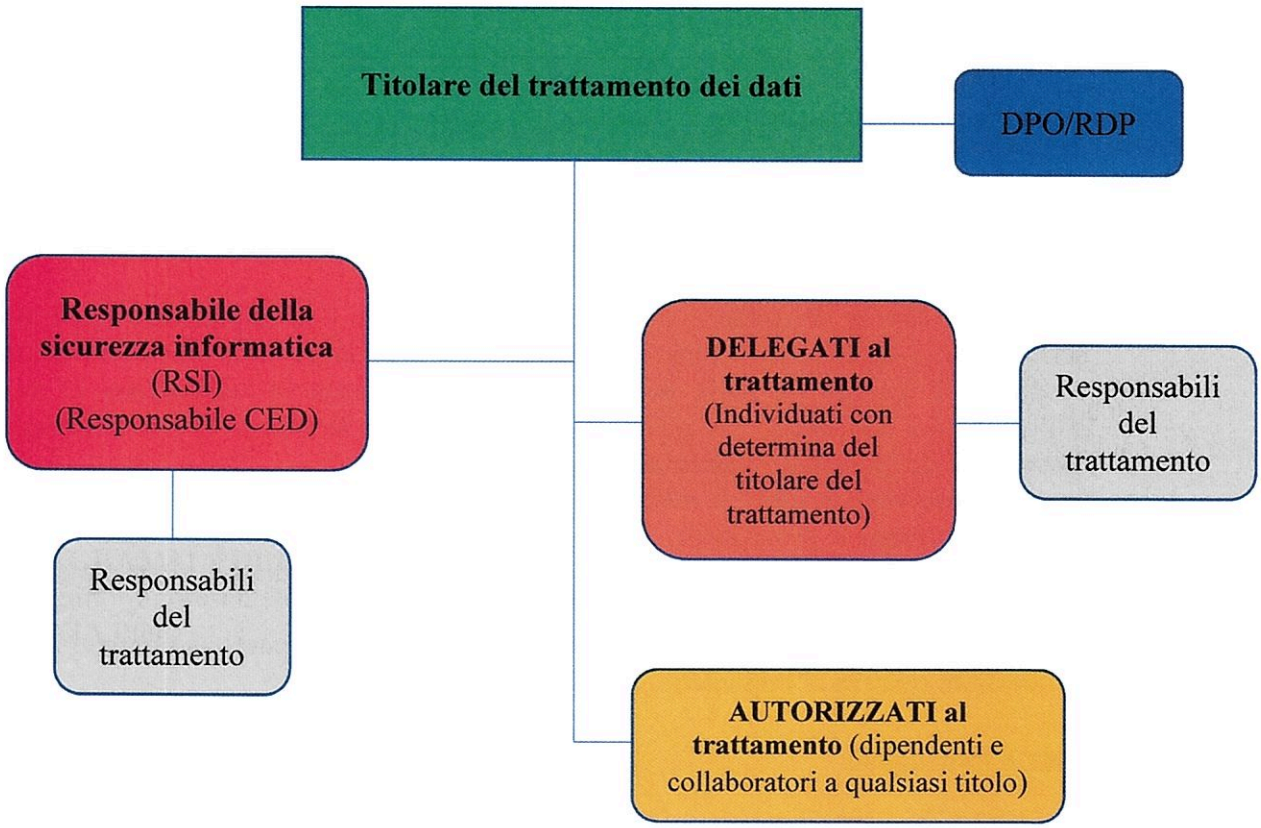
3. ACRONIMI

SGA PDP	Sistema Gestione Aziendale Protezione Dati Personali
GDPR	General Data Protection Regulation (Regolamento generale sulla protezione dei dati)
DPO/RPD	Data Protection Officer /Responsabile Protezione Dati

RSI	Responsabile Sicurezza Informatica
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.

4. ORGANIGRAMMA DEL SGA PDP

Viene di seguito rappresentato l'organigramma del Sistema di Gestione Aziendale Protezione Dati Personali (SGA PDP)



5. COMPITI E FUNZIONI DEI VARI ATTORI COINVOLTI NEL SGA PDP

5.1. Titolare del Trattamento

Il titolare del trattamento è colui che determina le finalità e i mezzi del trattamento dei dati personali.
Spetta al titolare del trattamento:

a) Rispettare i principi della protezione dei dati ai sensi dell'art. 5 GDPR;
b) Tutelare i diritti alla protezione dei dati delle persone fisiche;
c) Conservare la documentazione delle operazioni di trattamento;
d) Garantire la sicurezza del trattamento;
e) Scegliere un responsabile del trattamento dei dati idoneo;
f) Dettagliare, in un contratto vincolante, il rapporto titolare-responsabile;
g) Notificare le violazioni dei dati personali all'Autorità competente per la protezione dei dati dell'area SEE e alle persone fisiche, se previsto;
h) Vigilare le operazioni di trattamento, mettere in atto la protezione dei dati fin dalla progettazione e impostazione predefinita, effettuare valutazioni d'impatto sulla protezione dei dati, quando necessario;
i) Nominare il responsabile della protezione dei dati (RDP/DPO);
j) Individuare i soggetti "autorizzati" al trattamento;
k) Individuare i soggetti "delegati" al trattamento;
l) Rispettare gli obblighi in materia di protezione dei dati relativi ai trasferimenti internazionali di dati personali;
m) Cooperaree con le Autorità preposte alla protezione dei dati personali

5.2 DPO (Data Protection Officer) anche RPD–Responsabile Protezione Dati Personali

Il responsabile della protezione dei dati (DPO) assiste il titolare del trattamento o il responsabile del trattamento in tutte le questioni relative alla protezione dei dati personali. In particolare, il responsabile della protezione dei dati deve:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento, nonché ai loro dipendenti, sui loro obblighi ai sensi della legge sulla protezione dei dati;
b) verificare il rispetto da parte dell'organizzazione di tutta la legislazione in materia di protezione dei dati, anche per quanto riguarda gli audit, le attività di sensibilizzazione e la formazione del personale addetto al trattamento dei dati;
c) fornire consulenza in caso di esecuzione di una valutazione d'impatto sulla protezione dei dati e monitorarne le prestazioni;
d) fungere da punto di contatto per le richieste degli interessati relative al trattamento dei loro dati personali e all'esercizio dei loro diritti;
e) collaborare con le autorità di protezione dei dati e fungere da punto di contatto per le stesse su questioni relative al trattamento.

5.3 Delegati al trattamento

L'art. 2 – quaterdecies del Codice della Privacy (D.Lgs. 196/2003) – come modificato dal D.Lgs. 101/2018, stabilisce che il Titolare possa prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi con il trattamento dei dati personali siano attribuiti a persone fisiche espressamente designate.

I delegati al trattamento sono dunque chiamati a svolgere i compiti e le funzioni, secondo quanto previsto dalla norma sopraindicata, specificatamente indicate con atto di designazione da parte del titolare del trattamento.

5.4 Autorizzati al trattamento

Gli autorizzati al trattamento dei dati personali sono le persone fisiche appositamente istruite dal titolare del trattamento al fine di eseguire dei compiti materiali in nome e per conto del titolare stesso. Sono coloro che eseguono materialmente i trattamenti dei dati.
Sono nominati "Autorizzati al Trattamento", ai sensi dell'articolo 29 GDPR e dell'articolo 2-quaterdecies Codice Privacy, tutti i dipendenti e collaboratori a vario titolo dell'Istituto che svolgono attività di trattamento dei dati personali in ragione delle mansioni attribuite, nell'ambito di operatività dalla struttura organizzativa a cui sono assegnati,
Gli autorizzati sono tenuti a svolgere i loro compiti nei limiti dell'area di competenza assegnatagli, e si devono attenere scrupolosamente alle istruzioni del Titolare del trattamento, rispettando in particolare, il regolamento interno sul trattamento dei dati.

5.5. Responsabili del trattamento
Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che tratta dati personali per conto del titolare del trattamento.
L'esecuzione dei trattamenti da parte del titolare del trattamento è disciplinata da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri.
Il contratto deve prevedere, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste ai sensi dell'articolo 32 GDPR;
d) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
e) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR;
f) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento
g) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 del GDPR.

5.5. Responsabile della sicurezza informatica
Il Responsabile della Sicurezza Informatica (RSI) è la persona fisica che ha il compito di:
a) sviluppare e implementare policy e procedure di sicurezza informatica;
b) adottare un *security framework* che metta l'organizzazione al riparo da potenziali minacce;
c) coordinare, con la collaborazione del DPO, la risposta in caso di eventuali *data breach*;
d) supervisionare l'operatività quotidiana e la funzionalità dei sistemi di sicurezza infomatici;

e) redigere e aggiornare, anche con la collaborazione di soggetti interni ed esterni all'Istituto, il *Disaster Recovery Plan*.