Prot. n. 514 del 22/02/2019

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto di Montecatone
Ospedale di riabilitazione

MONTECATONE
REHABILITATION INSTITUTE S.p.A.

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(GDPR 2016/679 - Decreto Legislativo 30 giugno 2003 n. 196)

Indice

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI PERSONALI

1. PARTE GENERALE

1.1 Premessa

Il Regolamento Europeo 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "GDPR"), detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi e adempimenti a carico dei soggetti che trattano dati personali.

Le disposizioni del D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali", nonché i Provvedimenti di carattere generale adottati dal Garante per la protezione dei dati personali (di seguito "Garante"), continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa succitata. E' previsto, in ogni caso, l'adeguamento della normativa nazionale alle disposizioni del Regolamento.

Il GDPR affronta il tema della tutela dei dati personali attraverso un **approccio** nuovo, **basato principalmente sulla valutazione dei rischi** riguardanti i diritti e le libertà degli interessati, e attribuisce ai Titolari del trattamento il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali adottando le misure che ritiene a ciò più idonee ed opportune (**c.d. principio di responsabilizzazione** o **accountability**).

Per dare attuazione ai suddetti obblighi e adempimenti, occorre coinvolgere tutti i soggetti chiamati a trattare i dati personali e definire un preciso assetto di responsabilità tenuto conto della specifica organizzazione di Montecatone R.I. S.p.A. (di seguito MRI).

Con il presente documento MRI, nella persona del Direttore Generale, definisce il proprio ambito di titolarità, garantisce l'attuazione degli adempimenti previsti dalla normativa, indica i compiti assegnati al Responsabile della Protezione dei Dati personali (RDP) o Data Protection Officer (DPO) designato e definisce i criteri generali da rispettare nell'individuazioni dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito di responsabilità.

Il GDPR, all'art. 4, definisce **trattamento** "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate ai 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".

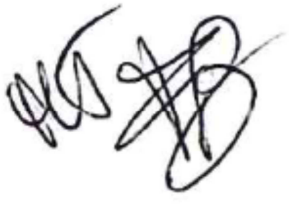
1.2 Riferimenti normativi e Documenti Aziendali

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 Europeo".

DGR Regione Emilia Romagna n. 919 del 10.04.2018 "Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l'anno 2018" che prevede, fra gli obiettivi indicati al punto 4.6 dell'allegato B, la nomina del DPO, l'adozione del registro delle attività di trattamento e l'articolazione delle specifiche responsabilità aziendali in tema di privacy.

Delibera di nomina del DPO prot. n. 1826 del 3 luglio 2018. Protocollo Garante n. 20180048565.

Delega di funzioni al Direttore Generale.
Struttura Sistema informativo Aziendale e Sistema Informatico Aziendale (DOC 23 e suoi allegati).
Disciplinare Aziendale Strumenti Elettronici (DOC 07-I)



2. STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI

2.1 Titolare del trattamento

Il Titolare del trattamento dei dati personali, ai sensi degli artt. 4, n.7 e 24 del Regolamento, è Montecatone R.I. S.p.A. Il Presidente del C.d.A., nonché legale rappresentante di MRI, cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento, delega il Direttore Generale a compiere ogni atto utile in tal senso, che comporti anche oneri economici a carico dell'Istituto.

2.2 Direttore Generale

Il Direttore Generale ha, sostanzialmente, il compito di definire gli obiettivi strategici per la protezione dei dati personali in ordine al trattamento degli stessi, individuare la politica di gestione, le misure di sicurezza da adottare e gli ulteriori profili di rilievo relativi alla gestione dei dati all'interno dell'Istituto. In particolare la delega conferita dal Titolare del trattamento al Direttore Generale è finalizzata a:

- designare il DPO di cui agli artt. 37- 39 del Regolamento UE 2016/679 specificando i compiti allo stesso assegnati;
- designare i Responsabili del trattamento di cui all'art. 28 del Regolamento UE 2016/679 stipulando il contratto o l'atto giuridico di cui al medesimo art. 28, par. 3 e 4;
- attribuire funzioni e compiti, connessi al trattamento dei dati personali, a persone fisiche espressamente designate che operano sotto la responsabilità del Titolare attraverso l'adozione di uno specifico **organigramma** (**Allegato n. 1**) e di un modello organizzativo aziendale che dettagli ambiti di responsabilità, funzioni e compiti per dare compiuta attuazione alle disposizione del Regolamento e del Codice Privacy;
- approvare le *policy* aziendali e mettere in atto le misure tecniche e organizzative necessarie a garantire il livello di sicurezza adeguato al rischio di cui all'art. 32 del Regolamento UE 2016/679;
- approvare documenti organizzativi finalizzati a fornire le informazioni di cui agli artt. 13 e ss. del Regolamento, alla raccolta del consenso eventualmente necessario e a garantire i diritti di cui al Capo III del medesimo Regolamento (Diritti dell'interessato);
- garantire la predisposizione e l'aggiornamento del Registro delle attività ai sensi degli artt. 30 e ss. del Regolamento;
- provvedere, se necessario, alla valutazione d'impatto ai sensi dell'art. 35 del Regolamento e alla eventuale successiva consultazione preventiva ai sensi dell'art. 36 del medesimo;
- allocare adeguate risorse per la formazione dei dipendenti, dei collaboratori e in generale di tutto il personale autorizzato al trattamento, in materia di protezione dei dati e sicurezza informatica;
- disporre periodiche verifiche sul rispetto delle funzioni impartite con riguardo agli aspetti relativi alla sicurezza dei dati e alla formazione;
- provvedere alle notifiche e alle comunicazioni di cui agli artt. 33 e 34 del medesimo Regolamento;
- sottoscrivere, se ritenuto necessario, l'atto interno di cui all'art. 26 del Regolamento UE 2016/679;
- favorire l'adesione a Codici di condotta ai sensi dell'art. 40 del Regolamento e a meccanismi di certificazione ai sensi dell'art. 42 del Regolamento;
- assolvere agli obblighi nei confronti del Garante per la protezione dei dati personali nei casi previsti dalla normativa.

2.3 Soggetti designati

Ai sensi dell'art. 32 del GDPR, al Titolare del trattamento competono le decisioni atte a garantire il profilo di sicurezza del trattamento dei dati personali, «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, […] e mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio».

Inoltre, ai sensi degli artt. 29 e 32 del GDPR **chiunque agisca sotto l'autorità del Titolare del trattamento e abbia accesso a dati personali può trattare tali dati solo se adeguatamente istruito.**

Alla luce di tali premesse, delle novità introdotte dal GDPR, dal D. Lgs. n.101/2018 e delle raccomandazioni del Garante per la protezione dei dati personali sopra richiamati, è necessario:

- **garantire,** nel rispetto degli adempimenti previsti dalla normativa vigente, **continuità** in merito alle scelte organizzative in precedenza assunte dall'Istituto, in ordine ai livelli delle responsabilità e alla individuazione dei soggetti designati ad eseguire operazioni di trattamento;
- modificare parzialmente l'attuale organigramma delle responsabilità privacy aziendali, sia in termini di professionisti coinvolti, che di attribuzioni di compiti e funzioni;
- infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati, quale parte integrante dell'intero asset informativo di un'organizzazione, con particolare attenzione ai dati di salute;
- che il nuovo approccio comporti il coinvolgimento di tutti i soggetti chiamati a trattare i dati personali all'interno della organizzazione aziendale, con assunzione delle relative responsabilità, distinguendo tra **Soggetti Referenti** (ex responsabili interni di trattamento) e **Soggetti autorizzati** (ex incaricati).

2.3.1. Referenti privacy

In considerazione della natura gestionale e della complessità delle strutture organizzative in termini di attività di trattamento dati e di personale assegnato, sono designati Referenti privacy aziendali:

- i Direttori di Struttura Complessa,
- i Coordinatori Infermieristici e Riabilitativi di Unità Operativa,
- i Coordinatori del Dipartimento Tecnico/Amministrativo,
- i Responsabili di Struttura o di Programma.

A tali Referenti si attribuiscono le funzioni dettagliate nel documento che si allega (A**llegato n. 2** – Compiti Funzioni e Poteri dei Referenti privacy) e di seguito riportate.

Nello specifico il Referente privacy ha il compito di:

- trattare i dati personali solo su istruzione del Titolare del trattamento o Suo delegato e garantire la corretta applicazione del Regolamento generale per la protezione dei dati (GDPR) e del D.Lgs. 196/2003, come modificato dal D. Lgs. 101/2018, nonché la conformità alle indicazioni dell'Autorità Garante per la protezione dei dati personali.
- Osservare e fare osservare:
  - le direttive aziendali in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento o Suo delegato, anche per il tramite del Gruppo Aziendale Privacy e del Servizio Sistemi Informativi Aziendale (es. regolamento sull'utilizzo delle risorse informatiche, regolamento sul DSE, procedura data breach, etc.);

- le istruzioni di carattere generale impartire dal Titolare o Suo delegato a tutti i soggetti autorizzati al trattamento;
- eventuali ulteriori specifiche istruzioni predisposte dallo stesso in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.

- Porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati, assicurando che i soggetti interessati (es. pazienti, dipendenti, fornitori etc.) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt.13 e 14 del GDPR.
- Provvedere alla designazione di soggetto autorizzato al trattamento dei dati personali dei singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili, stagisti etc.), attraverso la predisposizione dell'apposito modello.
- Vigilare sulla conformità dell'operato dei soggetti autorizzati, ad essi afferenti, alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto.
- Verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati.
- Attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento o Suo delegato e, compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e soprattutto organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale.
- Partecipare ai momenti formativi organizzati dall'Istituto ed assicurare la partecipazione dei propri autorizzati.
- Fornire le informazioni richieste dal Gruppo Aziendale Privacy (GAP) e segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO.
- Comunicare al Gruppo Aziendale Privacy (GAP) i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale.
- Collaborare con il Gruppo Aziendale Privacy (GAP) per la predisposizione del documento della valutazione di impatto sulla protezione dei dati (DPIA) qualora ne ricorrano i presupposti in base all'art. 35 del GDPR.
- Non porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento o Suo delegato.
- Provvedere, qualora tra le attività istituzionali dell'Istituto vi sia la stipula di contratti/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni quali "responsabili del trattamento" a norma dell'art. 28 del GDPR e delle condizioni ivi indicate e trasmettere copia dell'atto di designazione e dell'accettazione della nomina al Gruppo Aziendale Privacy (GAP) anche ai fini dell'aggiornamento del registro aziendale delle attività di trattamento dei dati.
- Comunicare tempestivamente al Gruppo Aziendale Privacy (GAP) i potenziali casi di data breach all'interno della propria struttura e collaborare all'istruttoria del caso al fine di sottoporre al DPO ogni utile e opportuna determinazione in merito, secondo le indicazioni contenute nell'apposita procedura aziendale di riferimento.

Il presente documento, unitamente ai suoi allegati, sarà trasmesso al singolo Soggetto Referente a cura del Servizio Risorse Umane, e analogamente si farà in futuro, a seguito di ogni conferimento/rinnovo di incarico, integrando altresì il contratto individuale con apposita clausola.

2.3.2 Soggetti autorizzati

Si riconoscono soggetti autorizzati al trattamento dei dati personali di titolarità aziendale tutti i soggetti che operano sotto la diretta autorità del Titolare o Suo delegato e quindi tutti i dipendenti della Società e i titolari di lavoro autonomo se ed in quanto operanti stabilmente nell'ambito delle strutture aziendali. Nello specifico:

- dipendenti a tempo indeterminato e determinato
- borsisti
- liberi professionisti che operano stabilmente nell'Istituto
- specializzandi
- interinali.

A loro si attribuisce automaticamente la qualifica di "**soggetti autorizzati**" al trattamento dei dati con riferimento ai trattamenti di cui sono addetti secondo quanto risulta dal registro dei trattamenti di titolarità aziendale e livelli di funzione aziendale, fatta salva la facoltà del Referente privacy di riferimento di circoscrivere l'autorizzazione generale se in relazione alla natura dei dati e al rapporto tra natura e finalità detta autorizzazione generale, per singoli lavoratori, non risulta giustificata.

Detta autorizzazione deve essere comunicata a tutti gli operatori sopra descritti mediante pubblicazione del presente documento e relativi allegati, comprese le Istruzioni di carattere generale impartite dal Titolare, o Suo delegato, a tutti i soggetti autorizzati al trattamento dei dati personali (**Allegato n. 3 – Istruzioni di carattere generale impartite a tutti i soggetti autorizzati al trattamento dei dati personali**) nel profilo personale del portale del dipendente oppure nella mail di Servizio, oltre che nella intranet aziendale. **Si prevede altresì di procedere analogamente con il personale di nuova assunzione integrando i futuri contratti di lavoro con apposita clausola.**

Per il personale non operante stabilmente nelle strutture aziendali (es. tirocinanti, studenti, stagisti frequentatori volontari, servizio civilisti etc.) la nomina di autorizzato deve essere conferita dal Referente privacy di riferimento *ad personam* utilizzando la modulistica allegata al presente documento (**Allegato n. 4 – Atto di designazione del soggetto autorizzato al trattamento dei dati personali**).

Si riportano di seguito le Istruzioni di carattere generale impartite dal Titolare o Suo delegato (**Allegato n. 3**).

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza, in attuazione del:
    a. **principio di minimizzazione dei dati**: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. **principio di limitazione delle finalità**: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. **principio di esattezza**: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
2. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari, con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
3. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare o Suo delegato e/o dal Referente privacy di afferenza garantendone la massima protezione in ogni attività di trattamento.
4. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario o opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione

o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

5. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
6. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o Suo delegato.

Istruzioni operative:

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- Identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare un'istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art. 45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;
- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Istituto che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento.
- E-mail e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute.
- Uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal D. Lgs. 518/1992 e ss. mm. ed ii.
- Protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire

la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerà porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d. "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, etc).

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e, se del caso, devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza.
- Obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata.
- Controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. Struttura Sistema Informativo Aziendale e Sistema Informatico Aziendale (DOC 23 e suoi allegati);
2. Disciplinare Aziendale Strumenti Elettronici (DOC 07 – I);
3. Codice Etico e Comportamentale

a cui si rinvia, reperibili sempre sulla intranet aziendale.

Il personale autorizzato è tenuto a seguire i corsi di formazione in materia di protezione dei dati personali e di sicurezza informatica con le modalità e le tempistiche indicate dal Titolare del trattamento o Suo delegato.

Gli obblighi sopra richiamati sono da considerare parte integrante della prestazione lavorativa, con efficacia fino alla risoluzione del rapporto di lavoro oppure revoca/modifica da parte del Titolare o Suo delegato, e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto. In caso di inadempimento saranno applicate le sanzioni previste dal relativo contratto di lavoro.

Le istruzioni generali qui richiamate possono essere integrate da disposizioni particolari da parte del Referente privacy di afferenza.

2.4 Gruppo Aziendale Privacy (GAP)

Il Gruppo Aziendale Privacy (da ora GAP), in attuazione dei principi di informazione e sensibilizzazione richiamati dal GDPR, ha il compito di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali.

Il GAP, coordinato dal Coordinatore del Servizio Programmazione RD – Privacy – Contenzioso, ha i seguenti compiti:

- supportare la Direzione aziendale attraverso la redazione di atti, regolamenti e istruzioni operative finalizzati al corretto trattamento dei dati, attraverso il monitoraggio sulla loro corretta applicazione e, più in generale, sulla corretta interpretazione e applicazione delle disposizioni normative vigenti;
- supportare i Referenti privacy nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo, anche a seguito degli approfondimenti e delle analisi effettuate dal coordinatore del GAP con il DPO nel Tavolo di area metropolitana;
- supportare i Referenti privacy nell'aggiornamento del Registro dei trattamenti di dati personali effettuati negli ambiti di competenza e nella eventuale valutazione di impatto;
- conservare e garantire l'aggiornamento del Registro dei trattamenti aziendale;
- fornire supporto alle verifiche di sicurezza svolte dal Servizio Sistemi Informativi e/o dal DPO;
- coordinare le richieste di parere al DPO da parte dei singoli Referenti privacy;
- coordinare le notifiche di violazione dei dati personali.

Si prevede che il GAP di MRI sia composto da:

Coordinatore: Coordinatore SPRD o Suo delegato.

Componenti:

Coordinatore SIA e CdG,

Amministratore di Sistema,

Direttore Dipartimento Clinico e dell'Integrazione o Suo rappresentante designato,

Responsabile di Area infermieristica e Riabilitativa o Suo rappresentante designato,

Direttore di Area Amministrativa o Suo rappresentante designato.

Al GAP viene riconosciuto altresì il compito di assicurare, all'interno della società, un adeguato livello di formazione/informazione e di predisporre e aggiornare i documenti aziendali in tema di privacy e sicurezza informativa e le informative aziendali.

2.5 Amministratore di Sistema

Al fine di adempiere agli obblighi di maggiore controllo e responsabilizzazione imposti dal GDPR, secondo un'ottica di prevenzione del rischio in relazione ai dati personali trattati con strumenti informatici, il Titolare o Suo delegato individua tra i dipendenti dell'Istituto l'Amministratore di Sistema nominandolo con apposito atto e fornendogli le necessarie istruzioni operative.

L'Amministratore di Sistema viene dunque preposto alla sicurezza, gestione e manutenzione di banche dati, sistemi e infrastrutture informatiche.

2.6 Amministratore per la videosorveglianza

Il Provvedimento in materia di videosorveglianza - 8 aprile 2010 - ha introdotto nuove regole alle quali conformarsi per installare telecamere e altri sistemi integrati di videosorveglianza. Sono dunque richieste misure tecniche ed organizzative che consentano al Titolare o Suo delegato di verificare l´attività espletata da parte di chi accede alle immagini o controlla i sistemi di ripresa. A tale proposito il Titolare o Suo delegato nomina un Responsabile del trattamento dei dati effettuato attraverso il sistema aziendale di video sorveglianza/videocontrollo.

2.7 Responsabile del trattamento

IL GDPR, con riferimento ai soggetti, disciplina espressamente la figura del **"Responsabile del trattamento"** intendendosi con questa espressione i soggetti esterni alla organizzazione che trattano dati personali per conto del Titolare del trattamento.

Per questi il GDPR richiede che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

Al tal fine i trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico che vincoli il Responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento (art. 28).

Si ribadisce che è compito del Referente privacy provvedere, qualora tra le attività istituzionali dell'Istituto vi sia la stipula di contratti/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni quali "Responsabili del trattamento" a norma dell'art. 28 del GDPR e delle condizioni ivi indicate e trasmettere copia dell'atto di designazione e dell'accettazione della nomina al Gruppo Aziendale Privacy (GAP) anche ai fini dell'aggiornamento del registro aziendale delle attività di trattamento dei dati.
Si allega fac-simile di nomina a Responsabile del trattamento ex art. 28 GDPR (**Allegato n. 5** – Atto di designazione a Responsabile del trattamento dei dati personali).

3. RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

3.1 RPD/DPO

Il GDPR prevede l'obbligo di designare il Responsabile della protezione dei dati (RPD) o Data Protection Officer (DPO).

3.2 Compiti

Il DPO, in attuazione dell'art. 39 del GDPR ("Compiti del responsabile della protezione dei dati"), i cui contenuti si intendono, fino al 30 giugno 2021, riferiti alle Strutture Sanitarie presso cui il DPO stesso svolge la propria attività:

- Azienda USL di Bologna,
- AOU S.Orsola-Malpighi,
- Istituto Ortopedico Rizzoli,
- Società Montecatone Rehabilitation Institute,
- Azienda USL di Imola,

ha il compito di:

✓ **informare e fornire consulenza in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.** Per il tramite del Direttore Generale e del Gruppo Aziendale Privacy dovrà altresì assicurare attività di informazione/consulenza ai Referenti privacy e Soggetti autorizzati che eseguono operazioni di trattamento dati;

✓ **sorvegliare l'osservanza della normativa in materia di protezione dei dati personali** nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo aziendale dei referenti individuati da Montecatone R.I. S.p.A;

✓ **fornire, se richiesti, pareri** anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

✓ **cooperare con l'Autorità Garante per la protezione dei dati personali**, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;

✓ **supportare la struttura deputata alla tenuta del Registro del trattamento**;

✓ **garantire il corretto livello di interlocuzione con gli altri DPO** delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE…)

✓ **promuovere iniziative congiunte** tra Montecatone R.I. S.p.A e altre Aziende sanitarie affinché l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti nelle singole Aziende;

✓ **favorire il coordinamento dei DPO delle altre aziende sanitarie regionali** relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna, nota PG/2018/0482475 del 5 luglio 2018.

Il DPO nello svolgimento dei compiti di cui sopra si avvale del Coordinatore del Servizio Programmazione RD – Privacy – Contenzioso, quale primario interlocutore dell'Istituto.

4. ALLEGATI

1. Organigramma Privacy
2. Compiti Funzioni e Poteri dei Referenti privacy
3. Istruzioni di carattere generale impartite a tutti i soggetti autorizzati al trattamento dei dati personali
4. Atto di designazione del soggetto autorizzato al trattamento dei dati personali
5. Atto di designazione a Responsabile del trattamento dei dati personali (M322)

Imola, 15/01/2019

Il Direttore Generale
Dott. Ing. Mario Tubertini

Il DPO
Dr.ssa Federica Banorri