INDIVIDUAZIONE E NOMINA DEL DESIGNATO PRIVACY
ai sensi del Regolamento Generale sulla protezione dei dati personali 2016/679
e del D. Lgs. 196/2003 (Codice Privacy) così come novellato dal D. Lgs. 101/2018.

La Fondazione IRCCS San Gerardo dei Tintori, Titolare del trattamento dei dati, in persona del Direttore generale (art. 16 dello Statuto), ha previsto, 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.

PREMESSO CHE

- il Regolamento UE 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "Regolamento"), fissa le modalità da adottare e individua i soggetti che, in relazione all'attività svolta, sono tenuti agli adempimenti previsti dal Regolamento;
- l'art. 29 del Regolamento prevede 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";
- l'art. 32 paragrafo 4 del Regolamento prevede che "il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o degli Stati membri";
- l'art. 2-*quaterdecies* del D.lgs. n.196/2003 (Codice Privacy) così come novellato dal D.lgs. n.101/2018, in virtù del principio di "*Accountability*", prevede che "Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

INDIVIDUA QUALE "DESIGNATO PRIVACY"

Il dr./dr.ssa
In qualità di Direttore/Dirigente Responsabile della Struttura
in considerazione della sua esperienza, capacità ed affidabilità.

Con la presente designazione il "Designato Privacy" è autorizzato a trattare i dati personali in qualità di "Persona Autorizzata" e, ove sussistano le condizioni, in qualità di "Amministratore di Sistema".

Il Designato Privacy, in ossequio alle proprie funzioni e responsabilità, ha l'onere e il dovere di:

- assicurare che i dati personali vengano trattati nel rispetto dei principi di liceità, correttezza e pertinenza seguendo le prescrizioni fornite nell'art. 5 del Regolamento;
- assicurare che i dati da pubblicare sul sito istituzionale siano conformi alla normativa in materia di protezione dei dati personali, nel rispetto degli obblighi di trasparenza e tracciabilità. Si rammenta che vige un divieto assoluto di pubblicazione/diffusione di dati sanitari anche in forma pseudonimizzata cioè anche con la pubblicazione delle sole iniziali o altri codici che potrebbero insieme ad altre informazioni permettere l'identificazione dell'interessato;
- Individuare, con il supporto del Responsabile della protezione dei dati (RPD) o DPO (Data Protection Officer), una corretta base di liceità in riferimento all'art. 6 del Regolamento (indicando una tra l'obbligo legale, il pubblico interesse, la salvaguardia degli interessi vitali dell'interessato, il contratto con l'interessato, il consenso libero dell'interessato) e art. 2-*ter* del D.Lgs. 196/2003 s.m.i. (indicando la norma di legge che prevede il trattamento). In caso di trattamento di dati particolari deve essere individuata una delle deroghe previste all'art. 9, par. 2 del Regolamento (indicando una tra finalità di medicina, prevenzione sanitaria, tutela dell'interesse vitale dell'interessato, ricerca scientifica, necessità per il diritto del lavoro e sicurezza sociale, il consenso dell'interessato) e, qualora sia effettuato per motivi di interesse pubblico rilevante, una delle previsioni di cui all'art. 2-*sexies* del D.Lgs. 196/2003 s.m.i. In caso di dati giudiziari deve essere applicato l'art. 2-

octies del D.Lgs. 196/2003 s.m.i. Costituisce base di liceità il rispetto dei Codici Deontologici per trattamenti per scopi statistici e scientifici, per quelli a fini statistici e di ricerca scientifica, per quelli a fini di archiviazione nel pubblico interesse o di ricerca storica e per quelli effettuati per svolgere investigazioni difensive o per far valere o difendere un diritto in sede giudiziaria;

- limitare il periodo di conservazione dei dati al tempo strettamente necessario per conseguire le finalità previste;
- formalizzare le finalità e la base di liceità dei trattamenti;
- il Designato deve attenersi alle procedure aziendali, mettendo in atto le soluzioni organizzative e procedurali più appropriare al fine di garantire e agevolare l'effettivo esercizio del diritto d'accesso e degli altri diritti dell'interessato, di cui al capo III del Regolamento Europeo;
- compilare e tenere aggiornato il Registro dei Trattamenti per la parte di competenza;
- redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati e l'elenco delle banche dati. Tali informazioni andranno inserite nel Registro dei Trattamenti;
- comunicare al RPD/DPO le modifiche relative alle attività di trattamento dei dati, nonché gli eventuali mutamenti organizzativi o tecnici (acquisizione di nuove banche dati e/o applicativi hardware, etc.) che possano incidere direttamente sui medesimi;
- assicurare l'osservanza delle istruzioni impartite da altro Titolare qualora l'Ente agisca in qualità di Responsabile del Trattamento;
- al fine di garantire l'applicazione dei principi di "privacy by design & by default" in ottemperanza all'art. 25 del Regolamento, il Designato Privacy, con il supporto del RPD/DPO, deve adoperarsi per effettuare una valutazione della Compliance al Regolamento dei sistemi e applicazioni sviluppati prima del 25 maggio 2018 e, se necessario, richiederne l'aggiornamento;
- individuare, in caso di esternalizzazione, le modalità di condivisione dei dati personali e assicurare la liceità della trasmissione dei dati personali o per espressa previsione normativa oppure riconducendo la comunicazione alle previsioni dell'art. 26 del Regolamento (Contitolarità) e art. 28 del Regolamento (Responsabile del Trattamento);
- individuare i "Responsabili/Sub Responsabili del trattamento" con apposito atto giuridico scritto così come previsto dall'art. 28 del Regolamento;
- nel caso in cui il designato rivesta il ruolo di RUP/DEC verificare anche con l'ausilio del RPD che i Responsabili del trattamento come previsto dall'art. 28 del Regolamento rispettino le istruzioni impartite provvedendo a proporre l'adozione di diverse/ulteriori misure di sicurezza in funzione dello stato dell'arte e di eventuali incidenti di sicurezza;
- individuare e autorizzare le risorse assegnate ai diversi trattamenti e richiedere, all'interno dei piani di formazione aziendali, interventi formativi al fine di assicurare che essi dispongano delle necessarie conoscenze per operare nel rispetto della normativa applicabile;
- individuare ed autorizzare gli Amministratori di Sistema, ai sensi del Provvedimento Generale del Garante per la protezione dei dati personali del 27 novembre 2008 *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* così come modificato dal Provvedimento del Garante del 25 giugno 2009 *"Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema e proroga dei termini per il loro adempimento" e s.m.i.* da parte dell'Autorità;
- vigilare sull'operato dei propri collaboratori, preventivamente autorizzati, affinché svolgano i compiti istituzionali assegnati in conformità alle disposizioni di legge, Policy e procedure aziendali vigenti;
- verificare, con periodicità almeno semestrale, le autorizzazioni rilasciate alle persone autorizzate e provvedere ad un aggiornamento, qualora risulti necessario (Es. modifiche organizzative, nuovi trattamenti, etc.);
- provvedere tempestivamente, in caso di cessazione del rapporto di lavoro di un Autorizzato o di revoca delle autorizzazioni al trattamento dei dati, a richiedere all'ufficio competente la disabilitazione delle credenziali di accesso ai sistemi aziendali;

- richiedere al competente ufficio per i propri collaboratori/autorizzati la username personale e password per il trattamento dei dati effettuato con sistemi automatizzati e vigilare sul loro corretto utilizzo;
- assicurare che i soggetti debitamente autorizzati ai sensi della normativa sul trattamento dei dati personali che risultano sottoposte al coordinamento del designato e che sono sotto la sua area di responsabilità supportino il RPD/DPO per la gestione dell'esercizio dei diritti degli interessati ai sensi degli artt. 15 e ss. del Regolamento (tra cui le richieste di opposizione al trattamento, di limitazione, di rettifica dei dati o di loro cancellazione) nei tempi e nei modi previsti dalla normativa. Qualora uno o più interessati denunci situazioni o fatti rilevanti di particolare gravità, il Designato Privacy dovrà informarne tempestivamente il RPD e adottare tutte le misure precauzionali e/o riparatorie necessarie;
- assicurare che vengano fornite le informazioni di cui agli articoli 13 e 14 del Regolamento ai soggetti interessati ogniqualvolta si raccolgano dati personali, provvedendo secondo l'organizzazione aziendale all'esposizione delle apposite informative in tutti i luoghi accessibili al pubblico e nella sezione Privacy del sito istituzionale;
- integrare le informazioni rese agli interessati e i moduli di consenso, qualora sia richiesto, con il supporto del RPD/DPO;
- partecipare direttamente alle iniziative formative organizzate dalla Fondazione sul tema della protezione e sicurezza dei dati;
- garantire la partecipazione del personale autorizzato agli eventi formativi e di sensibilizzazione organizzati dalla Fondazione IRCCS San Gerardo dei Tintori in materia di protezione dei dati;
- supportare le Strutture coinvolte nell'analisi del rischio fisico ed informatico;
- custodire e conservare adeguatamente i supporti utilizzati per le copie dei dati;
- verificare periodicamente le modalità di accesso e le misure adottate per la protezione delle aree e dei locali, rilevanti ai fini della custodia ed accessibilità ai dati;
- adottare le misure necessarie affinché i dati trattati siano custoditi in locali protetti. Per esempio, l'accesso ai locali e/o archivi sia protetto e limitato ai soli soggetti autorizzati;
- verificare che vengano applicate efficacemente le misure di sicurezza adottate in conformità alla normativa privacy e segnalare al Direttore f.f. della S.C. Servizi Informativi Aziendali e al RPD/DPO 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;
- avvisare il RPD/DPO se si notano atti o comportamenti che violano la normativa privacy o ogni evento che possa costituire un potenziale pericolo per i dati;
- in caso di incidente di sicurezza, di una violazione o sospetta violazione dei dati personali seguire scrupolosamente la vigente procedura aziendale notiziando tempestivamente il RPD/DPO;
- verificare che, sia per i trattamenti in essere sia per i nuovi trattamenti in fase di progettazione, ove necessario, venga richiesta una Valutazione d'Impatto e di rischio, conforme alle direttive stabilite nel Regolamento e ai Provvedimenti dell'Autorità di controllo. In particolare, le "*Guidelines on Data Protection Impact Assessment (DPIA)*" (wp248) e "*L'Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati*" ai sensi dell'art. 35, paragrafo 4, del Regolamento. Nel caso in cui la Fondazione agisca in qualità di Responsabile del Trattamento deve supportare il Titolare qualora sia necessario effettuare una Valutazione d'Impatto. In tali casi il Designato Privacy avvisa con tempestività il RPD/DPO;
- garantire l'osservanza delle indicazioni contenute in tutte le Procedure aziendali per la protezione dei dati;
- provvedere alle incombenze previste in caso di cessazione del trattamento di dati personali secondo le formalità di legge, informandone il RPD/DPO;
- collaborare con il RPD/DPO, anche durante le fasi di audit interno, e rispondere con tempestività alle richieste d'informazione di quest'ultimo;
- supportare il Titolare in caso di indagini giudiziarie, ispezioni o audit interni;
- accertarsi che non vi siano trasferimenti di dati personali al di fuori dello SEE (Spazio Economico Europeo) ove non esista una base di liceità secondo gli articoli da 44 a 49 del Regolamento;
- designare una persona di riferimento che avrà il compito di mantenere i contatti e collaborare con il RPD/DPO.

Si rammenta che l'inosservanza di quanto sopra può costituire violazione dei doveri di ufficio e determinare rilevanti conseguenze sul piano disciplinare. Nel caso in cui la Fondazione sia riconosciuta responsabile per illegittimo trattamento dei dati personali e vengano comminate alla medesima sanzioni amministrative o le siano addebitate somme a titolo di risarcimento danni da erogare in favore dei soggetti interessati, quest'ultima potrà rivalersi nei confronti del pubblico dipendente, responsabile degli atti compiti in violazione di diritti, sotto forma di responsabilità amministrativa e contabile tutte le volte che, a causa dell'inosservanza dolosa o gravemente colposa dei propri obblighi di servizio, abbia cagionato un pregiudizio alla P.A. (c.d. responsabilità per "danno erariale")
Ulteriori istruzioni sono previste nel documento "Privacy Policy", pubblicato in "Amministrazione Trasparente" - Altri contenuti - Dati ulteriori - Privacy del sito web istituzionale, nonché nel Modello Organizzativo Privacy (MOP) e relativi allegati e nella documentazione (Procedure/Istruzioni operative) pubblicata sul portale intranet aziendale "DOCUWARE". Il Designato Privacy s'impegna a controllare periodicamente il contenuto della intranet/internet, che si considera parte integrante della presente disposizione organizzativa.
Si ricorda inoltre, che gli obblighi relativi alla riservatezza dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro e che tale autorizzazione cesserà automaticamente con il venir meno del rapporto intercorrente tra la Fondazione e il Designato Privacy.
Della presente designazione si dà evidenza mediante pubblicazione dell'elenco nella specifica sezione "Privacy" in amministrazione trasparente del sito web istituzionale.
La presente designazione annulla e sostituisce le precedenti autorizzazioni Privacy.

Monza,

Il Titolare del trattamento dei dati
Il Direttore Generale

NOME E COGNOME

MATRICOLA

Firma per presa visione ed accettazione

_____