ALLEGATO A
INDIVIDUAZIONE E NOMINA DEI DESIGNATI AL TRATTAMENTO

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.

L'Azienda Sanitaria Locale ASM Matera, nella persona del suo legale rappresentante, 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, che operano sotto la sua autorità.

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, comma 1, del D.lgs. n.196/2003 (Codice Privacy), 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

INDIVIDUA E NOMINA QUALI "DESIGNATI AL TRATTAMENTO"

I DirettorI di Dipartimento, i Direttori di Distretto,i DirettorI di UOC, I Responsabili di UOSD

in considerazione della loro esperienza, capacità ed affidabilità.

Con la presente designazione il "Designato al Trattamento" 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 al Trattamento, 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 e correttezza 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 ricorda 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 dell'RPD, (che a sua volta potrà avvalersi se ritenuto opportuno, avvalendosi, di altre figure presenti in Azienda come ad esempio: Ufficio Privacy, Direzione Sanitaria, Innovazione Tecnologiche tra cui ingegneria clinica/servizi informatici o informativi, Medicina Legale e Gestione del Rischio Clinico, RSPP, ecc...) una corretta base di liceità in riferimento all'art. 6 del Regolamento Europeo (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 allo stretto indispensabile 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, previsto dall'art. 30 del Regolamento Europeo, con il supporto dell'RPD e dell'Ufficio Privacy e, ad ogni variazione o introduzione di nuovi trattamenti, darne comunicazione scritta al Ufficio Privacy privacy@asmbasilicata.it;
- Redigere, aggiornare e comunicare, 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 all'RPD e all' Ufficio Privacy 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'Azienda agisca in qualità di Responsabile del Trattamento;
- Al fine di garantire l'applicazione dei principi di "privacy by design" (protezione dei dati fin dalla progettazione) & "by default" (protezione dei dati per impostazione predefinita) in ottemperanza all'art. 25 del Regolamento, il Designato al Trattamento, con il supporto dell'RPD, deve adoperarsi per effettuare una valutazione della corrispondenza al Regolamento dei sistemi e applicazioni sviluppati prima del 25 maggio 2018 e, se necessario, richiederne l'aggiornamento;
- Individuare, le modalità di condivisione dei dati personali e assicurare la liceità della trasmissione dei dati personali o per norma oppure riconducendo la comunicazione alle previsioni dell'art. 26 del Regolamento (Contitolarità) e art. 28 del Regolamento (Responsabile del Trattamento);
- Accertarsi che i "Responsabili/Sub Responsabili del trattamento" siano stati individuati, ovvero individuarli, con apposito atto giuridico scritto così come previsto dall'art. 28 del Regolamento, qualora non sussistano altre fattispecie di liceità;
- Nel caso 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;
- Collaborare con l'UOC "Innovazioni Tecnologiche" per l'individuazione e autorizzazione degli 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", così come eventualmente modificato o sostituito dallo stesso Garante, e ad ogni altro pertinente provvedimento dell'Autorità;

- Vigilare sull'operato dei propri collaboratori, preventivamente autorizzati, affinché operino in conformità alle disposizioni di legge, Politiche e procedure aziendali;
- Provvedere tempestivamente, in caso di dimissioni di un Autorizzato o di revoca delle autorizzazioni al trattamento dei dati, a richiedere al competente amministratore di procedura la disabilitazione delle credenziali di accesso ai sistemi aziendali per il soggetto in questione;
- Richiedere username personale e password per il trattamento dei dati effettuato con sistemi automatizzati dagli Autorizzati e vigilare sul loro corretto utilizzo;
- Assicurare che le persone debitamente autorizzate ai sensi della normativa sul trattamento dei dati personali che risultano sottoposte al suo coordinamento e che sono sotto la sua area di responsabilità supportino il RPD 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 al Trattamento dovrà informarne tempestivamente il Titolare del Trattamento, l'RPD e l'Ufficio Privacy 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 dell'RPD e dell'Ufficio Privacy;
- Partecipare direttamente alle iniziative formative organizzate dalla ASL sul tema della protezione e sicurezza dei dati;
- Garantire la partecipazione del personale autorizzato agli eventi formativi e di sensibilizzazione organizzati dall'Azienda in materia di protezione dei dati;
- Supportare le Strutture coinvolte nell'analisi del rischio fisico e 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 RPD, al Responsabile IT e all' Ufficio Privacy* 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;
- Individuare le eventuali misure necessarie, tra cui i Provvedimenti Generali dell'Autorità di Controllo, applicabili ai trattamenti in essere con il supporto dell'RPD (che a sua volta potrà avvalersi se ritenuto opportuno, avvalendosi, di altre figure presenti in Azienda come ad esempio: Ufficio Privacy, Direzione Sanitaria, Innovazione Tecnologiche tra cui ingegneria clinica/servizi informatici o informativi, Medicina Legale e Gestione del Rischio Clinico, RSPP, ecc... ;
- Avvisare il RPD e l'Ufficio Privacy 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 le relative procedure, compilare l'apposito allegato e inviarlo al DPO e al Titolare del Trattamento (Legale Rappresentante dell'ASM);
- Verificare che, sia per i trattamenti in essere sia per i nuovi trattamenti in fase di progettazione, ove necessaria, 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 l'Ente agisca in qualità di Responsabile del Trattamento deve

supportare il Titolare qualora sia necessario effettuare una Valutazione d'Impatto. In tali casi il Designato al Trattamento deve avvisare il RPD e l' Ufficio Privacy* ;

- Garantire l'osservanza delle indicazioni contenute nelle 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 e l'Ufficio Privacy;
- Fornire al RPD il supporto necessario, anche nelle fasi di audit interno e rispondere prontamente a tutte le sue richieste d'informazione;
- 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 e l'Ufficio Privacy aziendale.

Si ricorda che l'inosservanza di quanto sopra può costituire violazione dei doveri di ufficio e comportare sanzioni disciplinari sulla base del vigente contratto di lavoro. In caso di sanzioni amministrative e di pagamento di danni agli interessati, l'Azienda potrebbe rivalersi sui singoli per danno erariale.

Ulteriori istruzioni sono previste nel "Regolamento aziendale per l'utilizzo delle risorse informatiche, della rete internet e della telefonia" (Deliberazione n. 1157/2018) che sarà aggiornato in conformità con le modifiche della normativa vigente.

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 l'Ente e il Designato al Trattamento.