

ATTO DI NOMINA
A RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI
(ai sensi dell'art. 28 del Regolamento UE 2016/679)

TRA

ASL di Rieti con sede legale in Via del Terminillo 42, 02100 Rieti, in persona del legale rappresentante *pro-tempore*, quale *Titolare del Trattamento*, (di seguito, per brevità "**Titolare**" o "**ASL**" o "**Azienda**");

E

L'Ospedale Pediatrico Bambino Gesù - IRCCS, con sede legale in Roma, Piazza S. Onofrio n. 4, zona extraterritoriale in base del Trattato del Laterano, quale *Responsabile Esterno del Trattamento* (di seguito, per brevità, "**Responsabile**"),

Di seguito, congiuntamente, le "**Parti**".

PREMESSO CHE

(Le premesse formano parte integrante e sostanziale del presente Atto)

- tra la ASL di Rieti e l'Ospedale Pediatrico Bambino Gesù - IRCCS è in atto una Convenzione finalizzata all'espletamento di attività di chirurgia in ambito urologico pediatrico e neonatale presso la U.O.S.D. Pediatria e Neonatologia dell'Ospedale di Rieti (di seguito, per brevità, "**Convenzione**");
- per l'esecuzione delle attività previste nella Convenzione, il Responsabile tratterà dati personali di cui l'Azienda è Titolare;
- l'ASL, in persona del legale rappresentante *p.t.*, Titolare del trattamento dei dati personali, di "categorie particolari di dati personali" (già "dati sensibili" ai sensi del Codice Privacy) ed in particolare di "dati relativi alla salute" ai sensi degli artt. 4 e 24 del Regolamento UE 2016/679, ha pertanto individuato, l'Ospedale Pediatrico Bambino Gesù - IRCCS, quale Responsabile Esterno del Trattamento medesimo sulla base delle evidenze documentali e delle dichiarazioni dallo stesso fornite al Titolare e della successiva verifica da parte di quest'ultimo, per quanto ragionevolmente possibile, della loro rispondenza al vero, circa le caratteristiche di esperienza, capacità e affidabilità che devono caratterizzare chi esercita tale funzione affinché il trattamento rispetti i requisiti della normativa vigente e garantisca la tutela degli interessati.

SI CONCORDA E SI STIPULA QUANTO SEGUE:

Art. 1

Definizioni

Ai fini del presente Atto di nomina valgono le seguenti definizioni:

- Per **“Legge Applicabile”** o **“Normativa Privacy”**, si intende il 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 (di seguito, per brevità, **“GDPR”**) nonché qualsiasi altra normativa sulla protezione dei dati personali applicabile in Italia ivi compresi il D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018 e i provvedimenti dell’Autorità Garante per la Protezione dei dati personali applicabili alla fattispecie oggetto della Convenzione;
- per **“Dati Personali”**: si intendono tutte le informazioni direttamente o indirettamente riconducibili ad una persona fisica così come definite ai sensi dell’art. 4 par. 1 del GDPR, che il Responsabile tratta per conto del Titolare allo scopo di fornire i Servizi di cui alla Convenzione stipulato con l’Azienda;
- per **“Categorie particolari di dati”**: si intendono i dati personali che rivelano l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché i dati genetici, biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona.
- per **“Dati relativi alla salute”**: si intendono i dati personali attinenti alla salute fisica e mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;
- per **“Interessato”**: si intende la persona fisica cui si riferiscono i Dati Personali;
- per **“Servizi”**: si intendono i Servizi resi dal Responsabile oggetto della Convenzione nonché il relativo trattamento dei dati personali, così come meglio descritto nel presente Atto di nomina;
- per **“Titolare”**: si intende, ai sensi dell’art. 4, par. 7 del GDPR, 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;
- per **“Responsabile del Trattamento”**: si intende, ai sensi dell’art. 4, par. 8 del GDPR, la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;
- per **“Ulteriore Responsabile”**: si intende la persona fisica o giuridica, l’autorità pubblica, il servizio o altro organismo, soggetto terzo (fornitore) rispetto alle Parti, a cui il Responsabile del trattamento, previa autorizzazione del Titolare, abbia, nei modi di cui al par. 4 dell’art. 28 del GDPR, eventualmente affidato parte dei Servizi e che quindi tratta dati personali;
- per **“Persona autorizzata al trattamento”** o **“Incaricato”**: si intendono le persone fisiche autorizzate a compiere operazioni di trattamento dal Titolare o dal Responsabile;
- per **“Amministratore di sistema”** o **“ADS”**: si intende la persona fisica 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 quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali;

- per **“Misure di Sicurezza”**: si intendono le misure di sicurezza di cui alla Normativa privacy;
- per **“Trattamento”**: si intende, ai sensi dell'art. 4, par. 2 del GDPR, 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.

Art. 2

Nomina e oggetto

In attuazione dell'art. 28 del GDPR, l'Asl di Rieti, in qualità di Titolare del trattamento dei dati personali, di “categorie particolari di dati personali” (già “dati sensibili” ai sensi del Codice Privacy) ed in particolare di “dati relativi alla salute”, nomina l'Ospedale Pediatrico Bambino Gesù - IRCCS quale Responsabile dello stesso trattamento come previsto nella Convenzione, da intendersi quale parte integrante e sostanziale del presente atto, reso necessario per l'espletamento dei Servizi.

Il Responsabile tratterà i Dati personali, così come specificati al precedente comma, di cui verrà in possesso/a conoscenza nello svolgimento dei Servizi oggetto della Convenzione solo in base a quanto ivi stabilito e a quanto previsto nel presente Atto.

Art. 3

Durata e finalità

Il presente Atto produce i suoi effetti a partire dalla data di sottoscrizione delle Parti e rimarrà in vigore fino alla cessazione delle attività svolte dal Responsabile a favore del Titolare, indipendentemente dalla causa di detta cessazione. Inoltre, fermo il diritto del Titolare di revocare, in qualsiasi momento e senza bisogno di motivazione, l'affidamento del Trattamento al Responsabile e/o la sua stessa nomina, il Trattamento, fatto salvo ogni eventuale obbligo di legge e/o contenzioso, avrà una durata non superiore a quella necessaria al raggiungimento delle finalità per le quali i dati sono stati raccolti.

Art. 4

Modalità e istruzioni

Le modalità e le istruzioni per il Trattamento dei Dati Personali impartite dal Titolare al Responsabile sono specificatamente indicate e declinate nella Convenzione e nella presente nomina. In particolare, ai sensi e per gli effetti della vigente Normativa Privacy, il Responsabile tratta i dati personali soltanto su istruzione documentata del Titolare del trattamento, anche in caso di trasferimento di dati personali verso un Paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il Responsabile del trattamento. In tal caso, il Responsabile del trattamento

informa il Titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico.

In ragione della presente nomina, il Responsabile ha l'obbligo di attenersi, tra l'altro, alle seguenti istruzioni:

- deve nominare formalmente tutte le persone autorizzate al trattamento dati (c.d. Incaricati), conferendo incarico scritto ai propri dipendenti e/o collaboratori che, sulla base delle relative competenze, effettuano i trattamenti di dati personali di competenza del Titolare e deve vigilare costantemente sull'operato degli stessi. Grava sul Responsabile la tenuta, la conservazione e l'archiviazione degli atti di nomina degli incaricati/persone autorizzate al trattamento dei dati. Tale documentazione è messa a disposizione del Titolare e/o dell'Autorità Garante per la protezione dei dati personali a semplice richiesta;
- deve garantire che le persone autorizzate al trattamento dei dati personali siano costantemente formate e informate in materia di tutela della riservatezza e dei dati personali e si siano impegnate alla riservatezza nello svolgimento dei propri compiti lavorativi o abbiano un adeguato obbligo legale di riservatezza;
- deve vigilare attentamente affinché il trattamento che gli viene demandato sia effettuato nei termini e nei modi stabiliti dalla normativa vigente in materia di protezione dei dati personali ivi compresi i provvedimenti e le linee guida emanate dalle Autorità di controllo, delle procedure adottate dal Titolare e nel rispetto delle presenti istruzioni, anche in caso di trasferimento di dati personali verso un Paese terzo o un'Organizzazione internazionale nei limiti sanciti dal Regolamento;
- deve verificare e monitorare costantemente che il trattamento dei dati avvenga effettivamente in modo lecito e secondo correttezza nonché nel rispetto del principio di minimizzazione, assicurando che, fatti salvi eventuali obblighi di legge e/o contenzioso, i dati non siano conservati per un periodo superiore a quello necessario per gli scopi del trattamento medesimo;
- 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, il Responsabile mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, anche al fine di soddisfare possibili richieste per l'esercizio dei diritti dell'interessato, nonché per garantire il rispetto degli obblighi di cui agli artt. da 32 a 35 compresi del Regolamento, relativi alla sicurezza del trattamento, alla notifica ed alla comunicazione di una violazione dei dati personali e alla valutazione di impatto sulla protezione dei dati. A questo fine, il Responsabile deve:
 - verificare costantemente l'efficacia delle misure di sicurezza adottate in conformità alla normativa vigente ed in linea con aggiornamenti e/o a eventuali perfezionamenti tecnici, che si rendano disponibili nel settore informatico;
 - relazionare, se richiesto, sulle misure di sicurezza adottate ed allertare immediatamente il Titolare in caso di situazioni anomale o di emergenza;

- accettare il diritto del Titolare alla verifica periodica dell'applicazione delle norme di sicurezza adottate (audit) ed assoggettarsi ad esso;
 - eseguire gli ordini del Garante o dell'Autorità Giudiziaria, salvo che il Titolare abbia tempestivamente comunicato la propria volontà di promuovere opposizione nelle forme di rito;
 - procedere all'immediata segnalazione al Titolare di eventuali casi, anche solo presunti, di violazione di dati personali (da intendersi come tale la violazione di sicurezza che comporti 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), in linea con le norme e le procedure aziendali vigenti;
- il Responsabile, per quanto di competenza, deve verificare periodicamente l'esattezza e l'aggiornamento dei dati che tratta per conto del Titolare, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
 - il Responsabile, quando richiesto, deve mettere immediatamente a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al Regolamento consentendo e collaborando alle periodiche attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato;
 - il Responsabile deve informare immediatamente il Titolare del trattamento qualora, a suo parere, un'istruzione da questi ricevuta violi il Regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati;
 - il Responsabile deve tenere il Registro delle attività di trattamento svolte per conto del Titolare del trattamento ai sensi del comma 2 dell'art. 30 del Regolamento mettendolo immediatamente a disposizione di quest'ultimo e/o del Garante a semplice richiesta;
 - il Responsabile assume con la sottoscrizione del presente Atto, specifico obbligo legale di riservatezza e confidenzialità nonché l'obbligo di concordare con il Titolare il corretto riscontro all'esercizio dei diritti degli interessati di cui agli artt. 15 e ss. del Regolamento;
 - il Responsabile deve garantire che nella propria organizzazione ogni accesso informatico ai dati trattati per conto del Titolare richieda l'assegnazione ad ogni incaricato di una specifica utenza individuale che abiliti al solo trattamento delle informazioni necessarie al singolo per lo svolgimento della propria attività lavorativa verificando almeno annualmente la permanenza in capo all'incaricato del relativo profilo di autorizzazione al trattamento;
 - nel processo di autenticazione, il Responsabile deve prevedere l'inserimento di un codice identificativo dell'incaricato associato a una parola chiave riservata (password) di adeguata complessità, comunicata all'incaricato in modalità riservata e modificata dallo stesso al primo utilizzo e successivamente con cadenza almeno trimestrale;
 - il Responsabile deve fornire istruzioni per non consentire che due o più incaricati al trattamento accedano ai sistemi, simultaneamente o in maniera differita, utilizzando il medesimo identificativo utente;

- il Responsabile deve fare in modo che ogni incaricato, al fine di proteggere la sessione di lavoro da utilizzi non autorizzati in sua assenza, non lasci mai incustodito e accessibile lo strumento elettronico;
- il Responsabile deve effettuare il salvataggio dei dati con finalità di backup e disaster recovery con cadenza almeno mensile e comunque prima di procedere al riutilizzo per altri scopi dei supporti di memorizzazione nel caso fosse necessario conservare le informazioni contenute negli stessi;
- il Responsabile deve proteggere i dati personali trattati per conto del Titolare contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di adeguati strumenti elettronici da aggiornare con cadenza almeno settimanale;
- il Responsabile deve aggiornare periodicamente e, comunque, almeno annualmente, i programmi per elaboratore con interventi volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti;
- il Responsabile deve adottare adeguate misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e, comunque, non superiori a sette giorni;
- nell'ambito del trattamento dei documenti cartacei, il Responsabile deve:
 - individuare e configurare i profili di autorizzazione, per ciascun incaricato e/o per classi omogenee di incaricati, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento;
 - periodicamente e comunque almeno annualmente, verificare la sussistenza in capo agli incaricati delle condizioni per la conservazione per i profili di autorizzazione;
 - identificare e comunicare agli incaricati gli archivi dove riporre i documenti contenenti i dati personali e/o categorie particolari di dati (armadi, stanze, caserforti, ecc.);
 - prevedere, ove possibile, la conservazione dei documenti contenenti dati personali di categorie particolari (i.e. sensibili e/o giudiziari) separata dai documenti contenenti dati personali comuni;
 - verificare la corretta esecuzione delle procedure di distruzione dei documenti, quando non più necessari o quando richiesto dall'interessato;
- il Responsabile, al pari dei propri incaricati, deve inoltre:
 - trattare i dati personali e/o le categorie particolari degli stessi secondo il principio di limitazione della finalità, ovvero unicamente per lo scopo per cui sono stati raccolti;
 - non diffondere o comunicare i dati personali e/o le categorie particolari degli stessi a soggetti non autorizzati al trattamento;
 - non lasciare incustoditi documenti contenenti i dati personali e/o le categorie particolari degli stessi durante e dopo l'orario di lavoro;
 - non lasciare in luoghi accessibili al pubblico i documenti contenenti i dati personali e/o le categorie particolari degli stessi;
 - riporre i documenti negli archivi quando non più operativamente necessari;

- limitare allo stretto necessario l'effettuazione di copie dei suddetti documenti.
- Laddove rilevante ai fini dei servizi e delle attività di cui alla Convenzione, in ottemperanza a quanto previsto dal Provvedimento del Garante Privacy del 27 novembre 2008, e sue successive modificazioni, riguardante "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema" e s.m.i., il Responsabile si impegna, altresì, ad adempiere a tutti gli obblighi prescritti dai predetti Provvedimenti, tra cui, in particolare:
 - individuare e designare quale "Amministratore di Sistema" la/e persona/e cui sono attribuiti compiti e/o funzioni di Amministratore di Sistema in riferimento ai sistemi impegnati per la fornitura dei servizi oggetto della Convenzione, previa valutazione dei requisiti di esperienza, capacità ed affidabilità di tali persone e con l'elencazione analitica nella designazione individuale degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
 - mantenere un documento interno aggiornato, contenente gli estremi identificativi delle persone preposte quali Amministratori di Sistema, con l'elenco delle funzioni ad esse attribuite, e renderlo disponibile in caso di accertamenti del Garante e, ove necessario, di verifica da parte del Titolare, su richiesta di quest'ultima;
 - adottare sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi ed archivi elettronici da parte degli Amministratori di Sistema designati, assicurando che le registrazioni abbiano le caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità prescritte dal citato Provvedimento e siano conservate per almeno 6 mesi;
 - adottare per tutti i sistemi Sw di base ed Hw che prevedano un'utenza di super user, che non possa essere identificata fisicamente con un Amministratore di Sistema, la creazione di un registro ove siano riportate i dati anagrafici dell'utente incaricato di svolgere tale attività; Qualora gli utenti incaricati per accedere al medesimo Sw di base ed Hw fossero più di uno, in tale registro dovrà essere previsto il controllo quotidiano delle presenze in servizio di tali incaricati al fine di poter ricondurre le attività svolte sui sistemi ai medesimi amministratori;
 - procedere, annualmente, alla verifica dell'operato dei suddetti Amministratori di Sistemi, in modo da controllare la loro rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti di dati connessi ai servizi forniti alla nostra Azienda;
 - produrre ed aggiornare annualmente, se richiesto, un documento attestante i servizi svolti che contenga anche la copia degli attestati della formazione del personale incaricato allo svolgimento delle attività e spieghi esaurientemente tutti i processi svolti al fine del mantenimento della sicurezza dei dati.

Art. 5

Obblighi e doveri del Responsabile del trattamento

Il Responsabile, al momento della sottoscrizione del presente Atto, dichiara e garantisce di possedere una struttura ed una organizzazione adeguata per l'esecuzione dei Servizi e si impegna ad adeguarla ovvero a mantenerla adeguata alla delicatezza della nomina, garantendo il pieno rispetto (per sé e per i propri dipendenti e collaboratori interni ed esterni) delle istruzioni sul trattamento dei dati personali specificatamente indicate e declinate nella Convenzione, nella presente nomina, oltre che della Normativa Privacy.

Art.6

Tipologie di dati, finalità e categorie di interessati

Il Responsabile svolge per conto del Titolare le attività di Trattamento dei Dati Personali relativamente alle tipologie, alle finalità ed alle categorie di soggetti esplicitate nella Convenzione, parte integrante e sostanziale del presente Atto di nomina.

Art.7

Nomina di ulteriori responsabili

In esecuzione e nell'ambito dei Servizi, il Responsabile, ai sensi dell'art. 28 comma 2 del GDPR, è autorizzato, salva diversa comunicazione scritta del Titolare, a ricorrere alla nomina di Ulteriori Responsabili ad esso subordinati, previo esperimento delle necessarie procedure di selezione dei fornitori applicabili di volta in volta.

Il Responsabile è tenuto, in sede di individuazione degli eventuali Ulteriori Responsabili e/o della loro sostituzione, ad informare preventivamente il Titolare, al fine di consentire a quest'ultimo, in attuazione dell'art. 28 comma 2 summenzionato, di poter manifestare eventuale formale opposizione alla nomina entro e non oltre il congruo termine di 20 (venti) giorni dalla ricezione della comunicazione. Decorso detto termine, il Responsabile potrà procedere all'effettuazione delle nomine, normativamente previste, nei confronti degli Ulteriori Responsabili individuati.

La nomina di un Ulteriore Responsabile da parte del Responsabile sarà possibile a condizione che sull'Ulteriore Responsabile siano imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel presente Atto, incluse garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il Trattamento soddisfi i requisiti richiesti dalla Normativa Privacy.

Qualora l'Ulteriore Responsabile ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare l'intera responsabilità dell'adempimento degli obblighi dell'Ulteriore Responsabile.

Il Responsabile, infine, si obbliga a comunicare al Titolare, con cadenza annuale, eventuali modifiche ed aggiornamenti dei trattamenti di competenza dei propri Ulteriori Responsabili.

Art.8

Vigilanza, sanzioni e responsabilità

Ai sensi e per gli effetti dell'art. 28, comma 3 del GDPR, al fine di vigilare sulla puntuale osservanza della Legge Applicabile e delle istruzioni impartite al Responsabile, il Titolare,

anche tramite il proprio Responsabile della Protezione Dati e/o altro soggetto allo scopo individuato, potrà effettuare periodiche azioni di verifica. Tali verifiche, potranno aver luogo a seguito di comunicazione da parte del Titolare, da inviare con un preavviso di almeno cinque giorni lavorativi. Nell'ambito di tali verifiche, il Responsabile fornirà l'assistenza ed il supporto necessario, rispondendo alle richieste del Titolare, in relazione ai dati e ai trattamenti rispetto ai quali ha valore il presente atto di nomina.

Le Parti del presente Atto sono soggette, da parte dell'Autorità di controllo, alle sanzioni pecuniarie ai sensi dell'art. 83 del GDPR. Ferma restando l'applicazione di tale norma e, in generale, della Normativa Privacy, il mancato rispetto delle funzioni delegate e delle istruzioni impartite al Responsabile ovvero la violazione delle condizioni prescritte, darà luogo - anche in relazione a quanto previsto dalla Convenzione, alla risoluzione della Convenzione.

Il Responsabile assume piena responsabilità diretta verso gli Interessati per i danni subiti derivanti da inadempimento o da violazione delle istruzioni legittime del titolare.

Art. 9

Disposizioni Finali

Il presente Atto di nomina, in uno con la Convenzione, deve intendersi quale contratto formale che lega il Responsabile al Titolare del trattamento e che contiene espressamente le Istruzioni documentate del Titolare, le modalità di gestione dei dati, la durata, la natura, la finalità del trattamento, il tipo di dati personali e le categorie di interessati, nonché gli obblighi e i diritti del Titolare del trattamento, così come le responsabilità in ambito privacy.

Con la sottoscrizione, il Responsabile accetta la nomina e si dichiara disponibile e competente alla piena attuazione di quanto nella stessa previsto.

La presente nomina ha carattere gratuito e ha durata pari alla durata della Convenzione a cui accede o, comunque, dell'atto giuridicamente vincolante che ne forma presupposto indefettibile e, fermo quanto indicato al precedente art. 3, si intenderà, pertanto, revocata al venir meno dello stesso, indipendentemente dalla causa, ovvero, in qualsiasi momento, per insindacabile decisione del Titolare.

LETTO CONFERMATO E SOTTOSCRITTO

Il Titolare del trattamento
ASL Rieti



Il Responsabile Esterno
Ospedale Pediatrico Bambino Gesù - IRCCS



AZIENDA SANITARIA LOCALE RIETI

Via del Terminillo, 42 – 02100 RIETI - Tel. 0746.2781 – PEC: asl.rieti@pec.it
www.asl.rieti.it C.F. e P.I. 00821180577

Egregio Dottore / Gentile Dottoressa

Oggetto: Atto di nomina a persona autorizzata al trattamento (già incaricato del trattamento) ai sensi dell'art. 29 del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del D.Lgs. 196/2003 come modificato dal D.Lgs.101/2018

Nell'organizzazione aziendale, ciascun dipendente (fisso o itinerante) o assimilabile (stagista, collaboratore, interinale, ecc.) è assegnato ad una Unità, stabilmente ovvero in via temporanea, presso cui sono trattati dati personali.

In relazione a ciò l'Asl di Rieti, in qualità di Titolare del trattamento dei dati (di seguito anche il "Titolare") **conferisce a tutti tali soggetti, nei termini e con le modalità previste in riferimento a quanto disposto dall'art. 29 e al principio di accountability di cui al nuovo Regolamento (UE) 2016/679 (infra detto "Regolamento") e dall'art. 2-quaterdecies del D.Lgs. 196/2003 come modificato dal D.Lgs.101/2018, nonché come raccomandato dall'Autorità Garante per la protezione dei dati personali (infra detta "Garante"), la nomina a persona autorizzata del trattamento (già "incaricato") dei dati personali ivi compresi quelli appartenenti a categorie particolari (i.e. "sensibili") e giudiziari di cui agli articoli 9 e 10 del Regolamento, laddove ciò sia richiesto in ragione delle mansioni loro affidate.**

Nella specie, si ricorda come a mente di tale Regolamento la "*persona autorizzata opera sotto l'autorità diretta del titolare o del responsabile*".

Ciò premesso, secondo il Garante, le disposizioni del D.Lgs. 196/2003 (antecedenti al Regolamento europeo e alle modifiche introdotte dal D.Lgs. 101/2018) in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del Regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del Regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4 del Regolamento, in tema di misure tecniche e organizzative di sicurezza, si ritiene che titolari e responsabili del trattamento possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento, così come delineatesi negli anni anche attraverso gli interventi del Garante, in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al Regolamento (si veda art. 24, paragrafo 1, del Regolamento).

Considerato che, ai sensi dell'art. 30 del D.Lgs. 196/2003, "*La designazione (ad incaricato) è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad una unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima*" e ai sensi dell'art. 2 – quaterdecies del D. Lgs. 196/2003, come modificato dal D.Lgs.101/2018, "*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 dei 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", il presente documento, congiuntamente con l'organigramma interno, i profili professionali e le competenze previste a livello contrattuale, costituisce puntuale individuazione dell'ambito di trattamento consentito alle persone autorizzate (già incaricati) degli uffici medesimi.

Per ciò che attiene, inoltre, alle persone autorizzate al trattamento dei dati sensibili e giudiziari di cui agli articoli 9 e 10 del Regolamento, la presente nomina potrà essere integrata con le istruzioni aggiuntive che il Referente interno eventualmente riterrà di conferire all'atto della loro applicazione alla Unità dove se ne prevede il trattamento.

Il Titolare ritiene la presente nomina condizione indispensabile per l'esecuzione di qualsivoglia attività lavorativa che contempra, anche saltuariamente, il trattamento di dati personali di propria competenza.

Tutto ciò premesso, le operazioni che ogni persona autorizzata effettuerà nello svolgimento della sua attività lavorativa riguarderanno, in particolare, l'accesso ad applicazioni informatiche tramite dispositivo informatico collegato alla rete aziendale o *stand alone* e/o l'uso di appositi archivi cartacei.

Rispetto a tutto quanto precede, si segnala quanto segue:

- 1) Titolare del trattamento è l'Asl di Rieti, con sede in Via del Terminillo n. 42 - Rieti coadiuvato dai Referenti Privacy.
- 2) Responsabile della Protezione Dati è l'Avv. Franco Angelo Ferraro domiciliato per la funzione presso i medesimi Uffici e sempre contattabile all'indirizzo e-mail dpo@asl.rieti.it ovvero ai numeri 06.37351632 o 06.3722608.
- 3) Per trattamento di dati personali si intende "*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*".
- 4) Sono considerati dati personali, ai sensi dell'art. 4 num. 1) del Regolamento, "*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*"; sono considerati "dati biometrici", ai sensi dell'art. 4 num. 14) del Regolamento, "*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*"; sono considerati "dati relativi alla salute", ai sensi dell'art. 4 num. 15) del Regolamento, "*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*".
- 5) Sono considerati appartenenti a "*categorie particolari di dati personali*" ovvero "*dati sensibili*", ai sensi dell'art. 9 del Regolamento, tutti quei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- 6) Sono considerati "*dati giudiziari*", ai sensi dell'art. 10 del Regolamento, tutti quei dati personali relativi "*alle condanne penali e ai reati o a connesse misure di sicurezza*" ovvero, secondo l'ordinamento italiano, idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi

pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

7) Ai sensi del comma 4 dell'art. 32 del Regolamento *"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 dal titolare del trattamento"*. Per tale ragione, ogni persona autorizzata è tenuta a fruire, con cadenza almeno annuale, delle occasioni formative, in presenza o a distanza e sempre documentate, predisposte dal Titolare del trattamento, dal Responsabile Protezione Dati e/o dal Referente interno.

8) È espressamente vietato alla persona autorizzata di trattare in Azienda dati personali di terzi non attinenti alle attività istituzionali nonché divulgare sia all'interno che fuori dell'Azienda, ovvero utilizzare in qualsiasi altro modo, dati personali di terzi soggetti dei quali sia venuta a conoscenza nello svolgimento delle proprie mansioni al di fuori delle indicazioni espressamente riportate nel presente incarico.

9) È espressamente vietato conferire dati, banche dati o la loro fruizione a soggetti terzi esterni senza aver preventivamente verificato con il Titolare, con il Responsabile Protezione Dati o, quantomeno, con un Referente interno, la necessità di provvedere alla loro nomina a Responsabile esterno del trattamento ex art. 28 del Regolamento da parte del Titolare del trattamento.

10) Le operazioni di trattamento oggetto del presente incarico dovranno essere svolte in conformità alle norme di legge e regolamenti vigenti in materia, ai provvedimenti e alle linee guida applicabili dell'Autorità Garante per la protezione dei dati personali, nonché alle espresse istruzioni impartite dal Titolare, dal Responsabile Protezione Dati o dal Referente interno di competenza con riferimento anche a quanto descritto nelle procedure eventualmente pubblicate sul Portale del Dipendente. In ogni caso, per qualsiasi chiarimento le persone autorizzate dovranno fare esclusivo riferimento al Responsabile Protezione Dati, al Referente o al Titolare.

11) Ai sensi dell'art. 5 del Regolamento, i dati personali devono sempre essere trattati in modo lecito, corretto e trasparente ed in conformità alle finalità del trattamento, nonché aggiornati di volta in volta al momento di eventuali loro variazioni portate a conoscenza del Titolare durante tutta l'attività di trattamento secondo la definizione che di questo fornisce l'art. 4 num. 2) del Regolamento.

12) Nell'ambito di quanto previsto dal Regolamento, ogni persona autorizzata al trattamento, nei limiti del proprio incarico e per quanto ragionevolmente possibile considerato lo stato dell'arte, ha l'obbligo di custodia, controllo e conservazione dei dati, con l'adozione, tenendo conto 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, di ogni cautela adeguata a evitare ogni rischio di violazione di sicurezza che comporti 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. A puro titolo esemplificativo, ciascuna persona autorizzata dovrà curare, al momento di allontanarsi dalla propria stanza, di non lasciare acceso il computer, o, in alternativa, di attivare uno screen-saver dotato di password di blocco/sblocco; di non lasciare incustoditi dispositivi informatici portatili e di proteggerne l'accesso con password adeguata, di cambiare la propria password almeno ogni tre mesi; di non abbandonare elenchi o schede contenenti dati personali, e in particolare quelli sensibili, sulla scrivania, curandone piuttosto la conservazione in cassetti o contenitori chiusi a chiave; di segnalare prontamente al proprio superiore diretto eventuali anomalie o inesattezze dei dati trattati.

13) Si considera obbligo di ogni persona autorizzata al trattamento segnalare immediatamente e senza ingiustificato ritardo al Responsabile Protezione Dati e al Titolare per il tramite del proprio Referente Privacy (o direttamente in caso di assenza di quest'ultimo) qualsiasi ipotesi di violazione di sicurezza, anche potenziale, che possa comportare, 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, attivarsi per limitarne gli effetti e offrire piena collaborazione alla verifica degli elementi richiesti dall'art. 33 del Regolamento.

14) Le rammentiamo che il Regolamento riconosce agli interessati, oltre alla possibilità di proporre reclamo al Garante, il diritto, ai sensi degli artt. 15 e seguenti, di essere informati circa i dati identificativi del Titolare e del Responsabile Protezione Dati e le finalità e modalità del trattamento dei propri dati; di chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che li riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati nei casi previsti dal Regolamento. Ogni comunicazione o richiesta in tal senso che dovesse pervenirle in Azienda dovrà essere prontamente e comunque non oltre 1 (uno) giorno sottoposta all'attenzione del Responsabile Protezione Dati per le opportune istruzioni.

15) L'Asl di Rieti è tenuta, in forza del presente atto di nomina e del principio di responsabilizzazione previsto dal Regolamento, a vigilare sull'operato delle persone autorizzate del trattamento e pertanto, si riserva il diritto di effettuare verifiche periodiche sulle attività dalle medesime svolte.

16) In forza del presente atto di nomina, Lei è autorizzato a trattare tutti i dati personali, sensibili e giudiziari dei quali potrà venire a conoscenza nell'ambito delle competenze e delle funzioni proprie della Unità di appartenenza, nonché in altre Unità in cui dovesse essere chiamato, anche temporaneamente o saltuariamente, a svolgere le proprie funzioni, in virtù delle specifiche competenze e dei relativi compiti assegnati nell'ambito delle attività trasversali finalizzate a garantire la continuità dei servizi (ad es. consulenze, turni di guardia, reperibilità, ecc.).

17) Il presente incarico è gratuito ed ha durata pari a quella del rapporto della persona autorizzata al trattamento con il Titolare e si intenderà revocata per insindacabile decisione del Titolare ovvero all'atto dello scioglimento di detto rapporto, per qualsiasi causa ciò avvenga e al termine del quale Lei dovrà cessare ogni trattamento di dati acquisiti in costanza di rapporto e restituire tutti i supporti su cui gli stessi venivano custoditi impegnandosi sin d'ora al rispetto delle prescrizioni e dei divieti di cui al Regolamento anche per il tempo successivo alla scadenza o cessazione della presente nomina.

18) Si ricorda, infine, che il mancato rispetto della normativa stabilita dal Regolamento a protezione dei dati personali e/o il mancato rispetto delle procedure aziendali poste a tutela degli stessi può essere fonte di responsabilità civili, penali ed amministrative e comportare, nei casi previsti, l'apertura di procedimenti disciplinari anche in ambito lavorativo.

Distinti saluti.

Per il Titolare

Per presa visione, la persona autorizzata al trattamento

[cognome e nome]

[firma leggibile]

