IRCCS Burlo
Istituto di ricovero e cura
a carattere scientifico
"Burlo Garofolo" di Trieste

REGIONE AUTONOMA FRIULI VENEZIA GIULIA

REGOLAMENTO
SUL TRATTAMENTO E LA PROTEZIONE
DEI DATI PERSONALI

INDICE

ACRONIMI

GDPR: General Data Protection Regulation Il Regolamento (UE) 2016/679 sulla tutela delle persone fisiche con riferimento ai dati personali

GPDP: Garante per la protezione dei dati personali

RPD | DPO: Responsabile della Protezione dei Dati | Data Protection Officer

UTPD: Ufficio che sovrintende al trattamento e alla protezione dei dati personali

DDG: Decreto del Direttore Generale

FSE: Fascicolo Sanitario Elettronico

SSR: Servizio Sanitario Regionale

D.P.I.A: *Data Protection Impact Assessment* o valutazione di impatto del trattamento

DEFINIZIONI

a) «trattamento»: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

b) «dato personale»: qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

c) «dati identificativi»: i dati personali che permettono l'identificazione diretta dell'interessato;

d) «dati particolari»: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (art. 9 del Reg. UE 679/2016);

e) «dati giudiziari»: dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1 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;

f) «titolare»: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

g) «responsabile»: soggetto esterno all'Istituto, preposto dal titolare al trattamento e/o allo svolgimento di operazioni di natura tecnica su dati personali relativi a trattamenti di titolarità dell'Istituto;

h) «delegato»: dirigente preposto, mediante apposita delega del titolare, a sovrintendere all'organizzazione del trattamento dei dati personali nell'ambito delle attività che gli sono affidate, nel rispetto della normativa vigente e dei regolamenti d'Istituto;

i) «autorizzato» o «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile; diretta del titolare o del responsabile;

j) «interessato»: la persona fisica cui si riferiscono i dati personali;

l) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51 del Reg. UE 679/2016;

m) «comunicazione»: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

n) «diffusione»: il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

o) «dato anonimo»: il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

p) «blocco»: la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento;

q) «banca di dati»: qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

r) «Ufficio Trattamento e Protezione dei Dati personali» dell'Istituto: organizzazione interna che funge da collegamento tra il Titolare del trattamento, le varie Strutture aziendali e il RPD e sovraintende e verifica il corretto trattamento dei dati personali;

s) «Referente aziendale per il Trattamento e la Protezione dei Dati personali» dell'Istituto: coordinatore dell'UTPD, che costituisce il collegamento interno tra la Direzione Strategica ed i referenti dei Dipartimenti/delle Strutture appositamente designati e il collegamento esterno tra l'Ente, il RPD, la Regione e i soggetti che, a vario titolo, interagiscono con l'Istituto nel trattamento di dati personali;

t) «Gruppo plenario multidisciplinare *Privacy* e sicurezza informatica» della Regione FVG: costituito da componenti di tutte le Aziende sanitarie pubbliche del Servizio Sanitario della Regione Autonoma Friuli-Venezia Giulia;

u) «misure adeguate»: il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello adeguato di protezione richiesto in relazione ai 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; fanno riferimento allo stato dell'arte e al principio di *accountability*;

v) «strumenti elettronici»: gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

w) «autenticazione informatica»: l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

x) «*data breach*»: violazione dei dati. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 del GDPR senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. (art. 33, art. 34 del Reg. UE 679/2016)

y) «*accountability*», principio di responsabilizzazione del Titolare, si traduce nel fatto che il Titolare è chiamato a dimostrare che i trattamenti sono coerenti con il disposto del Reg. UE 679/2016, a pianificare e mettere in atto misure tecniche e organizzative per poterne comprovare l'adeguatezza e ad attivare un modello di monitoraggio delle misure tecnico-organizzative implementate.

RIFERIMENTI NORMATIVI

- D.lgs. 101/2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"
- Reg. UE 679/2016 (GDPR) "Regolamento generale sulla protezione dei dati"
- D.lgs. 196/2003 "Codice in materia di protezione dei dati personali"
- D.lgs. 14 marzo 2013, n. 33 "Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni"
- D.P.R. 12 aprile 2006, n. 184. "Regolamento recante disciplina in materia di accesso ai documenti amministrativi"
- L. 7 agosto 1990, n. 241. "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"
- Decreto-Legge 69/2013 convertito con modificazioni dalla L. 9 agosto 2013, n. 98 (in materia di FSE)
- DPCM 08/08/2013 "Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali, nonché di effettuazione del pagamento online delle prestazioni erogate"
- DPCM 29/09/2015 "Regolamento in materia di Fascicolo Sanitario Elettronico"
- DPCM 14/11/2015 "Definizione delle modalità di attuazione del comma 2 dell'articolo 13 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modifiche, dalla legge 17 dicembre 2012, n. 221, in materia di prescrizioni farmaceutiche in formato digitale"
- Linee guida GPDP in materia di Dossier Sanitario (4 giugno 2015)
- Linee guida GPDP in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati (12 giugno 2014)
- Linee Guida GPDP in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute (25 gennaio 2012)
- Linee guida Ministero della salute 2010 (FSE)
- Linee guida GPDP in tema di referti online (19 novembre 2009)
- Linee guida GPDP in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario (16 luglio 2009)
- Provvedimento GPDP che individua le prescrizioni contenute nelle Autorizzazioni generali nn. 1/2016, 3/2016, 6/2016, 8/2016 e 9/2019 che risultano compatibili con il Regolamento UE e con il D.lgs. n. 101/2018 di adeguamento del codice (13.12.2018).

TITOLO I - PRINCIPI GENERALI

Art. 1 - Campo di applicazione e Oggetto

1. Il presente Regolamento si applica a tutto il personale della Dirigenza e del Comparto, Universitari convenzionati, personale della Ricerca, titolari di borsa di studio, medici in formazione specialistica, frequentanti volontari a diverso titolo, personale di aziende/enti esterni, soggetti di cui all'art. 7 D.lgs. 165/2001.
2. Non si applica al trattamento dei dati personali delle persone decedute, ma i diritti a essi riferiti possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario o per ragioni familiari meritevoli di protezione.
3. Il presente regolamento contiene disposizioni attuative in applicazione del Regolamento UE 679/2016 a cui si raccorda il D.lgs. n. 196/2003, così come novellato dal D.lgs. 101/2018, recante il "*Codice in materia di protezione dei dati personali*" (di seguito indicato come Codice) nell'ambito delle

articolazioni dell'Istituto, con lo scopo di garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone, con particolare riferimento alla riservatezza e all'identità personale degli utenti e di tutti coloro che hanno rapporti con l'Istituto.

4. L'Istituto rende note le modalità di trattamento dei dati personali dei propri dipendenti e collaboratori mediante una specifica informativa che viene redatta utilizzando preferibilmente il modello allegato al presente Regolamento, che viene sottoposto ad aggiornamento in caso di modifiche normative o variazioni delle prassi operative. (Allegato 1).

TITOLO II - SOGGETTI

Art. 2 - Soggetti ammessi al trattamento dei dati personali

1. Nel rispetto di quanto previsto dal Codice, il trattamento dei dati personali è consentito ai soggetti di seguito indicati:
   - titolare ed eventuali co-titolari;
   - RPD;
   - Responsabili;
   - Delegati;
   - Autorizzati.
2. L'Istituto non consente il trattamento dei dati personali da parte di persone non espressamente autorizzate.

Art. 3 - Titolare del trattamento

1. Il Titolare del trattamento dei dati è l'IRCCS Burlo Garofolo di Trieste nella persona del suo legale rappresentante *pro tempore*, il Direttore Generale.
2. Il Titolare adempie agli obblighi previsti dalla normativa europea e nazionale e dalle disposizioni regionali in materia di riservatezza, integrità e disponibilità dei dati personali e dal presente Regolamento.

   In particolare:
   a) mette in atto misure tecniche e organizzative adeguate, al fine di garantire ed essere in grado di dimostrare che il trattamento, conformemente al presente regolamento, è effettuato solo per i dati personali necessari per ogni specifica finalità del trattamento (principi di pertinenza e di non eccedenza);
   b) effettua la notifica delle eventuali violazioni di dati personali al Garante;
   c) richiede al Garante l'autorizzazione al trattamento di categorie particolari di dati personali, qualora sia necessario;
   d) assolve all'obbligo di nominare i Responsabili del trattamento dando le necessarie istruzioni per la corretta gestione e tutela dei dati personali.
3. Il Titolare, in sinergia con il RPD, attua iniziative di formazione dei Delegati e Autorizzati per consentire loro di acquisire conoscenze sul corretto trattamento dei dati personali.

Art. 4 - Responsabile della protezione dei dati (RPD, altresì DPO)

Il RPD, che viene designato dal legale rappresentante dell'Istituto ai sensi dell'art. 37 GDPR, può essere un dipendente del Titolare del trattamento oppure può assolvere i suoi compiti in base a un contratto di servizi e in assenza di conflitto di interessi e deve essere designato in funzione delle qualità professionali (conoscenza specialistica sia della normativa sia della prassi in materia di protezione dei dati, conoscenza

dettagliata dello specifico ambiente operativo, competenze manageriali e capacità di assolvere in autonomia i compiti individuati). Tra i compiti minimi si annoverano:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) collaborare al piano di formazione in materia dei dipendenti dell'Istituto;

c) sorvegliare l'osservanza del Regolamento UE, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 GDPR;

e) cooperare con il Garante e fungere da punto di contatto per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

f) supportare il Titolare e i Delegati nelle attività connesse al trattamento e prestare consulenza al bisogno, anche con riguardo alla tenuta del registro delle attività di trattamento dei dati personali svolte sotto la responsabilità del Titolare stesso e obbligatoria ex art. 30 del GDPR.

Art. 5 - Responsabili del trattamento

1. I Responsabili del trattamento dei dati sono soggetti esterni all'Istituto, ai quali vengono affidate attività di trattamento e/o operazioni di natura tecnica su dati personali relativi a trattamenti di titolarità dell'Istituto. Essi vengono designati dal Titolare con un contratto o altro atto giuridico, preferibilmente utilizzando lo schema allegato al presente Regolamento; sono individuati tra soggetti esterni all'Istituto che per esperienza, capacità e affidabilità, forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento e tutte le indicazioni necessarie agli amministratori di sistema che si occupano della protezione e sicurezza dei dati.
2. Ai sensi dell'art. 28 del GDPR, è previsto che il Responsabile:
   a) tratti 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; il personale preposto alla gestione del rapporto con il Responsabile deve verificare la conformità dei flussi di dati alla normativa vigente prima di iniziare del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
   b) informi immediatamente il Titolare del trattamento qualora ritenga che le istruzioni da lui impartite violino il presente Regolamento o altre disposizioni nazionali o dell'Unione - anche per fatti imprevisti (danneggiamenti, anomalia di funzionamento delle protezioni e controlli accesso, ecc.) – attuando, comunque, le possibili e ragionevoli misure di salvaguardia e concordando eventuali ulteriori misure di protezione;
   c) garantisca che le persone autorizzate al trattamento dei dati personali (di cui all'art.8 del presente Regolamento) si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
   d) adotti tutte le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio, ai sensi dell'art. 32 del GDPR;
   e) in presenza di autorizzazione scritta del Titolare, ricorra ad altro Responsabile del trattamento,

previa sottoscrizione di un contratto o altro atto giuridico, nel rispetto delle condizioni previste dai paragrafi 2 e 4 del citato art. 28;

f) tenendo conto della natura del trattamento, assista il Titolare del trattamento con misure organizzative adeguate, ove ciò sia possibile, e collabori con gli amministratori di sistema in relazione alle misure tecniche adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR;

g) tenga conto - utilizzando i materiali, i prodotti, le applicazioni od i servizi, - dei principi di protezione dei dati, a partire da quando questi vengono progettati e della protezione dei dati di default;

h) assista il Titolare nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a disposizione del Responsabile;

i) cancelli o restituisca tutti i dati personali, su indicazione del Titolare, dopo che è terminata la prestazione dei servizi relativi al trattamento e elimini le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

j) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e permetta le attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato;

k) coadiuvi l'Istituto nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria.

3. Il Responsabile del trattamento risponde al Titolare per ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di tutela dei dati personali relativamente al proprio settore di competenza.

Art. 6 - Nomina dei Responsabili

1. In tutti i contratti o convenzioni, con cui l'Istituto affida a terzi (ad es. enti e aziende, associazioni di volontariato, persone fisiche e società di persone o di capitali) attività che comportano il trattamento di dati personali o si impegna a svolgere studi osservazionali o sperimentazioni cliniche, qualora ritenuto necessario per la specificità dell'attività e tranne nei casi in cui il soggetto esterno sia considerabile un autonomo titolare del trattamento, deve essere sottoscritto idoneo atto con il quale il soggetto esterno si assume i seguenti obblighi, a integrazione di quanto previsto dal precedente articolo:

   a) trattare i dati personali nei limiti oggetto dell'accordo e per i fini ivi previsti;

   b) controllare che i dati trattati siano esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati e, se necessario, aggiornare quelli richiesti dall'interessato;

   c) conservare i dati in una forma che consenta l'identificazione dell'interessato, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

2. Le strutture organizzative dell'Istituto, che hanno l'onere di stipulare gli accordi di cui al comma 1, valutata la necessità, con l'eventuale consulenza dell'Ufficio trattamento dati nei casi maggiormente complessi, devono predisporre le nomine utilizzando preferibilmente il modello allegato al presente Regolamento, che viene sottoposto ad aggiornamento in caso di modifiche normative o variazioni delle prassi operative. (Allegato 2).

3. Resta inteso che i Responsabili sono soggetti agli obblighi di cui ai commi precedenti, secondo la normativa in vigore, relativa alla responsabilità disciplinare, civile, penale e amministrativa.

Art. 7 - Delegati al trattamento

1. I Delegati sono i dirigenti preposti, mediante apposita delega del Titolare, a sovrintendere

all'organizzazione del trattamento dei dati personali nell'ambito delle attività che sono loro affidate, nel rispetto della normativa vigente e dei regolamenti d'Istituto. Tali soggetti, identificati principalmente nei Direttori di Struttura, sono responsabili per tutto ciò che concerne gli aspetti relativi al presente Regolamento; in particolare, per la nomina e la formazione degli autorizzati a loro afferenti, per l'acquisizione e conservazione dei consensi degli interessati ove necessario. I Delegati si accertano che la riservatezza, l'integrità e la disponibilità dei dati informatizzati siano assicurate da un corretto uso del Sistema Informativo dell'Istituto e che i sistemi utilizzati siano da questo approvati.

2. Per la nomina a Delegato interno deve essere utilizzato preferibilmente il modello allegato al presente regolamento, che è sottoposto ad aggiornamento periodico in occasione di modifiche normative o variazioni delle prassi operative. (Allegato 3).
3. I Delegati operano nell'ambito delle competenze loro affidate con l'eventuale supporto dei referenti di cui all'art. 8, punto 7), che sono opportunamente formati riguardo alle competenze in materia di protezione dei dati e collaborano nello specifico ambito, in riferimento e a sostegno dell'Ufficio per il Trattamento e la Protezione dei Dati dell'Istituto (UTPD).

Art. 8 - Autorizzati al trattamento

1. Le persone fisiche che, nell'ambito di rispettiva competenza, effettuano materialmente operazioni di trattamento di dati personali sotto l'autorità del Titolare o del Delegato, devono essere da questi individuate per iscritto quali soggetti autorizzati al trattamento. L'autorizzazione costituisce un obbligo di legge in ragione dell'attività svolta e non è pertanto rinunciabile.
2. Hanno accesso esclusivamente ai dati la cui conoscenza sia strettamente necessaria per l'espletamento dell'attività cui sono preposti.
3. Tale individuazione deve avvenire con dedicato e idoneo atto, di norma da parte del Delegato cui sono afferenti.
4. Gli Autorizzati sono tenuti a rispettare la riservatezza e a ricevere la necessaria formazione e a mantenersi autonomamente aggiornati in materia di protezione dei dati personali.
5. Obbligo di formazione. Chiunque tratti dati personali è obbligato a seguire i corsi di formazione obbligatoria in servizio e di aggiornamento. Le comunicazioni, le indicazioni periodiche, comprese quelle pubblicate sulla pagina Intranet d'Istituto e le circolari in materia costituiscono a tutti gli effetti un importante momento di formazione.
6. Per la nomina ad Autorizzato deve essere utilizzato preferibilmente il modello allegato al presente regolamento, che viene sottoposto ad aggiornamento in caso di modifiche normative o variazioni delle prassi operative. (Allegato 4).
7. Ogni singolo Dipartimento/Struttura designa un autorizzato, quale referente di Dipartimento/Struttura, a supporto dell'Ufficio per il Trattamento e la Protezione dei Dati dell'Istituto (UTPD).
8. Soggetti esterni occasionalmente presenti in Istituto, quali tecnici od operatori di ditte, relatori a convegni, ospiti a qualsiasi titolo, ai quali non venga affidato uno specifico trattamento di dati personali, ma che per la loro attività e presenza possano avere inevitabilmente o occasionalmente conoscenza di dati personali di natura particolare riferiti a soggetti identificati o identificabili, dovranno preventivamente sottoscrivere un'impegnativa alla riservatezza utilizzando preferibilmente il modello allegato al presente regolamento (Allegato 5).

TITOLO III - ORGANIGRAMMA PRIVACY E SICUREZZA INFORMATICA

Art. 9- Ufficio per il Trattamento e la Protezione dei Dati personali

1. Il Direttore Generale istituisce l'Ufficio per il Trattamento e la Protezione dei Dati (UTPD), quale organizzazione interna che funge da collegamento tra il Titolare del trattamento, le varie Strutture aziendali e il RPD, per offrire il necessario e costante supporto operativo alle molteplici attività di gestione quotidiana degli adempimenti e dell'organizzazione per il trattamento e la protezione dei dati personali nel suo complesso.
2. Il Direttore Generale nomina, in qualità di Titolare del trattamento, mediante proprio atto di designazione e all'interno dell'Istituto, il Referente aziendale per il Trattamento e la Protezione dei Dati personali, che coordina l'UTPD e costituisce il collegamento interno tra la Direzione Strategica ed i referenti dei Dipartimenti/delle Strutture appositamente designati e il collegamento esterno tra l'Ente, il RPD, la Regione e i soggetti che, a vario titolo, interagiscono con l'Istituto nel trattamento di dati personali;
3. Il Direttore Generale individua, mediante proprio atto e all'interno dell'Istituto, i componenti dell'Ufficio per il trattamento e la protezione dei dati personali.
4. L'UTPD, nell'esercizio delle proprie competenze e con la collaborazione di tutte le articolazioni organizzative dell'Istituto, svolge i seguenti compiti:
   - garantisce il necessario supporto al RPD per l'espletamento delle sue funzioni, anche nei rapporti con altri soggetti pubblici o privati per quanto riguarda gli adempimenti derivanti dalla normativa in materia;
   - predispone la mappatura dei trattamenti dei dati;
   - implementa e mantiene aggiornato il registro dei trattamenti, partendo dai trattamenti digitalizzati già attivi, mappati nell'ultima versione del Documento informatico della sicurezza dell'Istituto;
   - accerta che sia effettuata, da parte dei professionisti coinvolti, ove ritenuto necessario, la valutazione d'impatto sulla protezione dei dati personali di cui all'art. 35 del Regolamento UE, ove possibile mediante un software di ausilio metodologico approvato dal Garante per la protezione dei dati personali;
   - detiene l'elenco annualmente aggiornato dei Responsabili del trattamento dati in ambito aziendale sulla scorta dei dati forniti dall'articolazione del personale;
   - presta consulenza interna;
   - collabora alla predisposizione del piano di formazione in materia;
   - supporta il RPD nella gestione dei *data breach* e tiene aggiornato il relativo registro;
   - collabora alla gestione del contenzioso in materia;
   - fornisce supporto all'analisi e all'interpretazione dell'evoluzione normativa e degli standard tecnici;
   - esegue gli audit periodici;
   - collabora all'aggiornamento di regolamenti e procedure;
   - gestisce i registri dei trattamenti e dei responsabili;
   - verifica le nomine dei responsabili (esterni) del trattamento.

Art. 10
Gruppo plenario multidisciplinare Privacy e sicurezza informatica della Direzione Centrale Salute, Politiche sociali e Disabilità della Regione FVG

1. L'IRCCS mette a disposizione del Gruppo plenario multidisciplinare Privacy e sicurezza informatica della Direzione Centrale Salute, Politiche sociali e Disabilità della Regione FVG, due rappresentanti aziendali a garanzia della loro partecipazione agli incontri della Conferenza dei Referenti Privacy. I due rappresentanti aziendali hanno competenze giuridico – amministrative e/o sanitarie l'uno e competenze informatiche e/o di ingegneria clinica l'altro.
2. Il referente privacy dell'IRCCS ne è membro di diritto. Il Gruppo è convocato da un referente individuato dalla stessa Direzione centrale Salute della Regione FVG con funzioni di coordinamento. Si riunisce di norma con cadenza mensile per affrontare e trovare soluzioni comuni ai problemi di applicazione della normativa privacy e ad essa correlata.
3. Sono previste sedute plenarie per argomenti riguardanti entrambi gli aspetti. Delle sedute è redatto un verbale, pubblicato sul sito della Regione FVG e denominato "*Comunità virtuale dei referenti dei sistemi informativi*".

Art. 11- Amministratori di sistema

1. L'Amministratore di sistema ricopre un ruolo estremamente delicato nella configurazione, gestione e manutenzione di un impianto di elaborazione dati e delle sue componenti: sulla base e nel rispetto delle indicazioni del Titolare, progetta, sviluppa e gestisce l'infrastruttura di rete, i *server*, il *software* ed i servizi applicativi di base occupandosi anche della sicurezza e della protezione dei dati e delle risorse informatiche. Fornisce, all'occorrenza, supporto tecnico (*help desk*) e informatico ai dipendenti dell'Istituto su *software e hardware*.
2. Relativamente al trattamento dei dati con strumenti elettronici, l'Istituto individua quattro distinte tipologie di Amministratori di sistema:

- *System Administrator*: Il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, salvataggi, protezioni, ecc. su software e sistemi operativi sia a livello client che server);
- *Network Administrator*: Il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, ecc.) sulle componenti di una rete telematica (apparati di rete di varia natura);
- *Database Administrator*: Il ruolo contempla lo svolgimento di attività di amministrazione (installazione, configurazione, risoluzione malfunzionamenti, ecc.) sui sistemi di gestione di basi di dati;
- *Software Administrator*: Il ruolo contempla lo svolgimento di attività di amministrazione (configurazione, manutenzione, attribuzione di privilegi, ecc.) specifiche nel contesto di un'applicazione adibita al trattamento dei dati personali e/o appartenenti a categorie particolari.

3. L'Amministratore di sistema, quando necessario, ricopre un ruolo proattivo nell'ambito delle notificazioni di violazioni di sicurezza e *data breach*, informando tempestivamente il Delegato da cui dipende funzionalmente e il RPD di eventuali anomalie riscontrate a seguito di malfunzionamenti e/o di rischi per la sicurezza che potrebbero determinare, anche potenzialmente, un evento di *data breach.*
4. L'Amministratore di sistema sovraintende allo svolgimento delle attività finalizzate ad eliminare o ridurre le conseguenze derivanti da un malfunzionamento della rete e supporta, in caso di necessità, Delegati, Autorizzati e responsabili di progetti di ricerca per gli aspetti di tipo tecnico informatico correlati all'espletamento delle mansioni.
5. La nomina degli Amministratori di sistema è effettuata con atto scritto del Titolare del Trattamento e

non è rinunciabile, in quanto costituisce un obbligo di legge in ragione dell'attività svolta.

TITOLO IV - MODALITA' DI TRATTAMENTO

Art. 12 - Criteri per il trattamento dei dati personali

L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di una copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato.

1. Le operazioni di trattamento dei dati personali devono essere effettuate con modalità atte ad assicurare il pieno rispetto della dignità personale e della riservatezza, dei principi di correttezza, liceità e trasparenza, con particolare riferimento ai diritti e alle libertà fondamentali dell'Interessato.
2. Dovranno essere oggetto di trattamento i soli dati essenziali per svolgere attività istituzionali.
3. I Responsabili del trattamento e i Delegati sono tenuti a verificare periodicamente l'esattezza e l'aggiornamento dei dati, nonché la loro pertinenza, completezza, non eccedenza e necessità rispetto alle finalità per le quali sono stati raccolti o successivamente trattati.
4. I trattamenti di dati effettuati utilizzando le banche dati di Titolari diversi sono autorizzati nelle sole ipotesi previste da espressa disposizione di legge, regolamento, adeguato accordo convenzionale o previa specifica autorizzazione esplicita del Titolare di riferimento.

TITOLO V - RAPPORTI CON L'UTENZA

Art. 13 - Informativa per l'utenza e i dipendenti

1. La persona fisica cui si riferiscono i dati (interessato) deve essere informata per iscritto (vedasi informativa generale allegata), previamente o al momento stesso della raccolta dei dati, anche tramite il sito Web d'Istituto. Le informative, redatte in conformità agli artt. 13 e 14 del GDPR dovranno contenere almeno:
   a) estremi identificativi dell'IRCCS Burlo Garofolo di Trieste quale Titolare del trattamento;
   b) dati di contatto del RPD;
   c) finalità e base giuridica del trattamento dei dati;
   d) modalità del trattamento;
   e) indicazione degli eventuali legittimi interessi perseguiti dal titolare del trattamento o da terzi;
   f) eventuali destinatari o eventuali categorie di destinatari dei dati personali ai quali i dati possono essere comunicati;
   g) natura obbligatoria o facoltativa del conferimento dei dati;
   h) conseguenze di un eventuale rifiuto nel fornire i dati;
   i) diritti dell'interessato ai sensi dell'art. 15 e successivi GDPR e modalità per esercitarli;
   j) periodo di conservazione dei dati personali;
   k) diritto alla revoca o alla modifica del consenso in qualsiasi momento, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico, senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca o della modifica;
   l) diritto di effettuare segnalazioni o proporre reclamo al Garante.
2. Ai dipendenti, al momento dell'instaurazione del rapporto di lavoro, o al personale che svolge

attività lavorativa, di studio e di ricerca con l'Istituto - a qualunque titolo -, viene consegnata apposita informativa (Allegato 1).

Art. 14 - Rapporto tra il diritto di accesso documentale e civico e il diritto alla riservatezza

1. Nel caso di dati particolari idonei a rivelare l'appartenenza etnica o razziale, il credo religioso e filosofico, l'appartenenza politica e sindacale, lo stato di salute e l'orientamento sessuale, dati genetici e dati biometrici, l'accesso è consentito solo se la situazione giuridicamente tutelata, che si intende salvaguardare con la richiesta di accesso ai documenti amministrativi, è di rango almeno pari ai diritti dell'interessato ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.
2. In ogni caso le strutture organizzative, che propongono l'adozione e/o adottano atti o provvedimenti, verificano, alla luce dei principi del GDPR che l'inclusione nel testo di dati personali sia realmente necessaria per le finalità proprie di ciascun atto o provvedimento.
3. Laddove gli allegati degli atti soggetti a pubblicazione contengano categorie particolari di dati personali tutelati dalla normativa sulla riservatezza, dovrà essere evidenziato nell'atto che l'allegato non viene pubblicato, rimanendo depositato agli atti per esigenze di tutela della riservatezza.

TITOLO VI - ATTIVITÀ DI RICERCA

Art. 15 - DATI DELLA RICERCA

1. Tutti i soggetti coinvolti nell'attività di ricerca dovranno essere, qualora già non lo siano, preventivamente nominati "Autorizzati al trattamento" (allegato 4) dal Delegato di riferimento e dovranno seguire le indicazioni dei Direttori/Responsabili dei reparti in cui svolgono le loro attività, i Regolamenti aziendali in materia e quanto dettagliato, conformarsi al rispetto della normativa in materia di protezione dei dati personali, ai regolamenti dell'Istituto e alle regole di riservatezza e di sicurezza cui sono tenuti gli esercenti le professionisanitarie. Ogni progetto di ricerca dell'Istituto deve avere i seguenti requisiti in termini di tutela e sicurezza dei dati personali:

- il Responsabile (generalmente corrispondente alla figura del *Principal Investigator*) del progetto è responsabile anche del corretto trattamento dei dati personali e particolari afferenti alla ricerca;
- le persone autorizzate a svolgere il progetto (ad esempio lo studente laureando) devono essere autorizzate per iscritto dal Delegato di riferimento per lo specifico progetto, qualora lo stesso ne ravvisi la necessità;
- l'evidenza delle misure di sicurezza da adottare nel trattamento dei dati personali, al fine di garantire il rispetto della normativa in materia di protezione dei dati personali. Tra queste: l'indicazione delle modalità di tenuta dei dati nominativi, considerato che non dovranno mai uscire dal reparto; l'anonimizzazione o pseudonimizzazione dei dati e la loro cifratura in caso di trasmissione e comunicazione a terzi (preventivamente autorizzati). È vietato copiare i dati su dispositivi mobili di memorizzazione (chiavette USB, HD rimovibili ecc.) e salvarli in servizi "Cloud", se non approvati dall'Istituto;
- la tipologia di ricerca ed i sui scopi, anche al fine di documentare che il trattamento sia effettuato per idonei ed effettivi scopi di ricerca (statistici o scientifici);
- l'eventuale informativa e consenso specifici relativa al progetto con tutti i dettagli relativi al trattamento dei dati personali come da artt. 13 e 14 del GDPR, con particolare evidenza dei diritti degli interessati;
- i criteri di selezione dei casi con chiara indicazione che comunque verranno utilizzati esclusivamente dati di pazienti che abbiano prestato il consenso per la ricerca;
- la tipologia, le fonti dei dati e le modalità con cui verranno estratti ovvero le modalità di raccolta.

Andranno trattati soltanto i dati strettamente necessari, senza eccedenza rispetto allo scopo della ricerca. Le modalità dovranno indicare nel dettaglio chi effettuerà effettivamente l'operazione. Si ricorda a tal fine che tutti gli accessi risultano tracciati;

- le modalità di anonimizzazione o pseudonimizzazione tali da garantire che l'interessato non sia ragionevolmente identificabile né direttamente né indirettamente, ossia non sia possibile ricondurre in modo significativamente probabile il dato ad un certo soggetto con l'impiego di mezzi ragionevoli;
- la modalità di pubblicazione e/o di diffusione dei risultati (per esempio, tesi di laurea) che deve chiaramente indicare che i dati devono essere presentati solo in forma aggregata ovvero secondo modalità che non rendano identificabili gli interessati neppure tramite dati identificativi indiretti;
- la dichiarazione che i nominativi, al termine della ricerca, verranno cancellati in modo non recuperabile e se i dati anonimizzati utilizzati per la ricerca verranno anch'essi distrutti o conservati per eventuale successiva comunicazione a un'università o istituto o ente di ricerca o ad un ricercatore per altri scopi, anche di natura statistica, chiaramente determinati per iscritto nella richiesta dei dati.

2. Inoltre, nel caso in cui la ricerca preveda anche il contatto diretto con il paziente, le regole di condotta (organizzazione e modalità) da tenere durante il contatto cui il Responsabile dovrà porre specifica attenzione in modo da garantire il rispetto della normativa e la tutela dei diritti degli interessati.
3. Deve essere specificato che l'incaricato alla raccolta dei dati dovrà in particolare:

- rendere nota la propria identità, la propria funzione e le finalità della raccolta, anche attraverso adeguata documentazione;
- accertarsi dell'identità dell'interessato;
- fornire le informazioni di cui all'informativa sul trattamento dei dati personali dell'Istituto, nonché ogni altro chiarimento che consenta all'interessato di rispondere in modo adeguato e consapevole, evitando comportamenti che possano configurarsi come artifici ed indebite pressioni;
- assicurare una particolare diligenza nella raccolta e provvedere tempestivamente alla correzione di eventuali errori e inesattezze.

TITOLO VII - Registro dei trattamenti e valutazione d'impatto

Art.16 - Registro dei trattamenti

1. Il Titolare realizza e mantiene aggiornato, per mezzo dell'Ufficio trattamento dati, il registro delle attività di trattamento svolte dall'Istituto, che deve essere a messo a disposizione del Garante, su richiesta. Il registro delle attività di trattamento è coordinato con il registro dei Responsabili.

   Il registro -che può essere implementato utilizzando un software apposito- deve contenere, ove applicabili, tutte le informazioni elencate all'art. 30 del GDPR e in particolare:

   a) il nome e i dati di contatto del Titolare del trattamento e, ove applicabile, del Contitolare del trattamento, del rappresentante del Titolare del trattamento e del Responsabile della protezione dei dati;
   b) la base giuridica e le finalità del trattamento;
   c) una descrizione delle categorie di interessati e delle categorie di dati personali;
   d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
   e) un'analisi preliminare del rischio associato al trattamento, prodromica alla valutazione dei rischi;
   f) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione

internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate;

g) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

h) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, comma 1 del GDPR.

Art. 17 - Valutazione d'impatto del trattamento

1. La valutazione di impatto del trattamento (D.P.I.A.) è un'attività posta direttamente in capo al Titolare del trattamento, ai sensi dell'art. 35 del GDPR, che assicura trasparenza e protezione nelle operazioni di trattamento dei dati personali.
2. Quando un tipo di trattamento prevede in particolare l'uso di nuove tecnologie e, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento deve effettuare, prima di procedere al trattamento, una valutazione dell'impatto dello specifico trattamento sulla protezione dei dati personali.
3. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
4. Il Titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, è affiancato dal Delegato responsabile del trattamento che gli fornisce tutte le informazioni necessarie per lo svolgimento di tale compito, consultandosi al bisogno con il RPD.
5. La valutazione del rischio dovrà portare il Titolare a decidere, in autonomia, se sussistono rischi elevati inerenti al trattamento, in assenza dei quali potrà procedere oltre. Qualora invece ritenesse sussistenti rischi per le libertà e i diritti degli interessati, dovrà individuare misure specifiche adeguate per attenuare o eliminare tali rischi. Nel caso in cui, nonostante l'applicazione delle misure aggiuntive, il rischio residuo fosse ancora elevato ma il trattamento sia ritenuto indispensabile, il Titolare può ricorrere, con l'ausilio del RPD, alla consultazione del Garante (art. 36 del GDPR).

TITOLO VIII - DISPOSIZIONI FINALI

Art. 18 - Norme di rinvio

1. Per quanto non previsto dal presente Regolamento trovano applicazione le disposizioni del Regolamento UE 679/2016 (GDPR) e del D.lgs. n. 196 /2003, come novellato dal D.lgs. 101/2018.

Art. 19 - Abrogazioni

1. È abrogato il "Regolamento per la protezione dei dati personali dell'I.R.C.C.S. Burlo Garofolo di Trieste", approvato con decreto n. 159/2020 del Direttore Generale.
2. Sono comunque abrogate tutte le disposizioni regolamentari dell'Istituto in contrasto con quelle previste dal presente regolamento.

Art. 20 - Revisioni

1. Gli allegati al presente regolamento sono soggetti a revisione e aggiornamento periodici in ragione dei mutamenti normativi e/o delle modifiche apportate alle modalità operative dell'Istituto.

DOCUMENTI ALLEGATI

ALLEGATO 1 INFORMATIVA AI DIPENDENTI E COLLABORATORI

INFORMAZIONE E ACCESSO AI DATI PERSONALI
ai sensi degli artt. 13 e 14 Reg. UE n. 679/2016 e dell'art. 2-ter del D.lgs. n. 196/2003 novellato dal D.lgs.n. 101/2018

Desideriamo informarLa che dal 25 maggio 2018 si applica in Italia il nuovo Regolamento Europeo sulla Protezione dei Dati Personali (Reg. UE n. 679/2016 o GDPR – *General Data Protection Regulation*), le cui disposizioni normative si aggiungono al vigente Decreto Legislativo n. 196/2003 (c.d. "Codice Privacy") novellato dal Decreto Legislativo n. 101/2018 di adeguamento dell'ordinamento nazionale al Reg. UE n. 679/2016, in vigore dal 19 settembre 2018.

1. ESTREMI IDENTIFICATIVI DEL TITOLARE DEL TRATTAMENTO

Titolare del trattamento è l'IRCCS Materno Infantile "Burlo Garofolo" di Trieste, con sede in Trieste (34137),Via dell'Istria n. 65/1, nella persona del legale rappresentante, il Direttore Generale *pro tempore*.
L'Istituto effettua il trattamento di dati personali per la gestione del rapporto di lavoro ed è tenuto a fornirele seguenti informazioni.

2. CONTITOLARI, RESPONSABILI, DELEGATI E AUTORIZZATI AL TRATTAMENTO

Contitolari del trattamento dei dati sono i soggetti che determinano congiuntamente le finalità e i mezzi del trattamento con l'Istituto.

Responsabili del trattamento sono le aziende o i soggetti esterni a cui l'IRCCS ricorre qualora il trattamento debba essere effettuato per conto del titolare del trattamento, nell'ambito delle attività di competenza, autorizzate e disciplinate in appositi accordi, convenzioni o rapporti contrattuali.

Sono delegati (interni) i direttori delle marco-articolazioni aziendali (Responsabili di Dipartimento, Struttura o Ufficio). Ai delegati è affidata la gestione pratica degli adempimenti relativi alla tutela dei dati personali, quali a. e. la nomina e l'istruzione dei soggetti autorizzati che operano alle loro dipendenze, la nomina dei Responsabili (esterni) che intervengono a vario titolo nei rapporti con l'IRCCS nell'ambito delle attività di competenza della struttura da loro diretta.

Autorizzati al trattamento sono le persone fisiche espressamente designate che operano sotto l'autorità del titolare o contitolare del trattamento o del responsabile del trattamento (a titolo esemplificativo: il personale dell'Istituto e il personale con contratto di collaborazione o titolare di borsa di studio, nonché il personale afferente alla SC Gestione del Personale presso l'ASUITS addetto alla complessiva gestione del personale, all'elaborazione dei dati e degli accertamenti sanitari, alla gestione del sistema informativo e degli strumenti informatici, nonché gli amministratori di sistema nominati dal Direttore Generale).

3. RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD/DPO)

L'IRCCS, con decreto del Direttore Generale n. 56 del 22.05.2018, ha provveduto alla designazione del DPO ("Data Protection Officer" o "Responsabile della Protezione dei Dati Personali"), anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie e ha istituito un apposito "Gruppo Multidisciplinare Privacy", di supporto al DPO, con la funzione di affrontare tutte le prerogative relative al nuovo Regolamento europeo n. 679/2016.

Il DPO è contattabile al seguente indirizzo di posta elettronica: dpo@burlo.trieste.it.

4. FINALITÀ DEL TRATTAMENTO

L'IRCCS tratta i dati personali nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro o del contratto di ricerca o formazione professionale (es. borsa di studio), avendo cura di applicare lenorme contenute in leggi, regolamenti, contratti e accordi collettivi, in modo da avvalersi di informazioni personali e modalità di trattamento proporzionate ai singoli scopi.

I dati personali che Le saranno richiesti sono necessari per le seguenti esplicite finalità:

- amministrazione e gestione del personale;
- controllo interno relativo all'idoneità lavorativa da parte del medico competente per la sorveglianzasanitaria;
- adempimenti fiscali;
- adempimenti connessi al versamento di quote a istituti finanziari o ad altri soggetti creditori, a seguito diatti dell'autorità giudiziaria o su richiesta dell'interessato;
- fini didattici, formativi o di aggiornamento;
- eventuali prerogative sindacali;
- ogni altro adempimento derivante dalla legge, contratto o regolamento.

5. DEFINIZIONI CATEGORIE DI DATI PERSONALI

DATI PERSONALI: 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.

DATI GENETICI: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.

DATI BIOMETRICI E RELATIVI ALLA SALUTE: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali e i dati personali attinenti alla salute fisicao mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria che rivelano informazioni relative al suo stato di salute, sono conservati in fascicoli separati.

DATI RELATIVI A CONDANNE PENALI E REATI: il trattamento dei dati personali relativi alle condanne penalie ai reati o a connesse misure di sicurezza deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriateper i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica

6. LICEITÀ DEL TRATTAMENTO

I dati personali devono essere esatti e aggiornati.

Il trattamento dei dati è indispensabile per l'instaurazione e gestione del rapporto di lavoro o ricercascientifica o formazione professionale, nonché per la prosecuzione o modifica del medesimo.

L'Istituto assicura che il trattamento dei dati personali avvenga rispettando i principi di

necessità,correttezza, liceità, imparzialità e trasparenza.

I dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati.

I dati sono raccolti e registrati unicamente per gli scopi sopra specificati e saranno tutelati dignità, riservatezza, identità personale e diritti del lavoratore.

Il rifiuto di fornire dette informazioni o il mancato consenso al trattamento dei dati personali necessari rende impossibile l'esecuzione delle operazioni di interesse del lavoratore (es. predisposizione busta-paga, versamenti a enti previdenziali, giustificazione di assenze).

7. DESTINATARI DEI DATI

I dati potranno essere comunicati a terzi nei casi previsti dalle L. n. 241/1990 ("*Nuove norme in materia diprocedimento amministrativo e di diritto di accesso ai documenti amministrativi*"), ove applicabile e, in caso di controlli sulla veridicità delle dichiarazioni ai sensi dell'art. 71 D.P.R. n. 445/2000 ("*Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*").

RAPPORTI CON LE ORGANIZZAZIONI SINDACALI: sulla base delle disposizioni dei CCNL del personale del Comparto e della Dirigenza, i criteri generali e le modalità inerenti a determinati profili di gestione del rapporto di lavoro sono oggetto di specifici diritti di informazione sindacale.

A esclusione dei casi in cui la normativa vigente e/o il contratto collettivo applicabile prevedano espressamente che l'informazione sindacale abbia per oggetto anche dati nominativi del personale per verificare la corretta attuazione di taluni atti organizzativi, l'Istituto può fornire alle organizzazioni sindacali dati numerici o aggregati e non anche quelli riferibili a uno o più lavoratori individuabili (es. informazioni inerenti ai sistemi di valutazione dell'attività, alla ripartizione delle ore di straordinario e alle relative prestazioni, nonché all'erogazione dei trattamenti accessori).

L'organizzazione sindacale può presentare istanze di accesso a dati personali attinenti a uno o più lavoratorisu delega o procura di questi oppure a documenti amministrativi in materia di gestione del personale, nel rispetto delle condizioni, dei limiti e delle modalità previsti dalle norme vigenti e per salvaguardare un interesse giuridicamente rilevante di cui sia portatore il medesimo sindacato.

L'IRCCS, per esempio, rende noto alle organizzazioni sindacali l'utilizzo delle prerogative sindacali da parte degli stessi, in conformità alle disposizioni normative e contrattuali vigenti.

SORVEGLIANZA SANITARIA: l'Istituto deve svolgere, attraverso, il medico competente, alcuni trattamenti di dati in applicazioni della disciplina in materia di igiene e sicurezza sul lavoro (D.lgs. n. 81/2008) al fine di tutelare l'integrità psico-fisica dei lavoratori.

In questo ambito il medico competente per la sorveglianza sanitaria:

-effettua accertamenti preventivi e periodici sui lavoratori e istituisce e aggiorna una cartella sanitaria e di rischio, custodita presso l'Istituto con salvaguardia del segreto professionale, trasmessa all'ente competente in caso di cessazione del rapporto di lavoro e consegnata in copia al lavoratore stesso al momento della risoluzione del rapporto di lavoro o quando lo stesso ne faccia richiesta per la tutela di situazioni giuridicamente rilevanti, direttamente o attraverso un procuratore o mediante l'assistenza del Sindacato di appartenenza;

-tratta dati sanitari dei lavoratori anche tramite annotazione nelle cartelle sanitarie e di rischio curando le opportune misure di sicurezza per salvaguardare la segretezza delle informazioni trattate in rapporto alle finalità e modalità del trattamento stabilite;

-può farsi assistere da personale sanitario, incaricato del trattamento dei dati personali e opportunamente istruito per la salvaguardia della segretezza delle informazioni trattate.

Alle predette cartelle il datore di lavoro non può accedere, dovendo soltanto concorrere ad assicurarne un'appropriata custodia nei locali aziendali, anche in vista di possibili accertamenti ispettivi da parte dei soggetti preposti alla vigilanza.

Ai fini dell'adozione delle misure preventive e protettive per i lavoratori interessati, il datore di

lavoro è informato dal medico competente in ordine alla valutazione finale sull'idoneità del dipendente allo svolgimento delle mansioni assegnategli.

CONCORSI E SELEZIONI: l'Istituto procede alla pubblicazione di graduatorie e di esiti di concorsi e selezioni pubbliche sia in forma cartacea sia in formato elettronico a mezzo del proprio sito internet.

AMMINISTRAZIONE TRASPARENTE: in virtù di quanto previsto dal D.lgs. n. 33/2013, l'Istituto provvede a pubblicare sul sito internet aziendale, all'apposita sezione «Amministrazione Trasparente», una serie di informazioni attinenti ai dati personali.

I dati personali pubblicati nella sezione «Amministrazione Trasparente» sono riutilizzabili alle condizioni previste dalla normativa vigente sul riutilizzo dei dati pubblici (Direttiva Comunitaria 2003/98/CE e D.lgs. n. 36/2006 di recepimento della stessa).

CARTELLINI IDENTIFICATIVI: i dipendenti, il personale della Ricerca e i titolari di borsa di studio sono tenuti arendere conoscibile il proprio nominativo mediante l'uso dei cartellini identificativi appositamente predisposti.

8. MODALITÀ DEL TRATTAMENTO

Il titolare del trattamento è tenuto ad adottare le misure minime volte ad assicurare un livello minimo di protezione dei dati personali.

Il trattamento dei dati avviene con o senza l'ausilio di strumenti elettronici o automatizzati, informatici e telematici, con logiche strettamente correlate alle finalità menzionate nei paragrafi precedenti e, comunque, finalizzati a consentire l'accesso e l'utilizzo ai soli operatori autorizzati e che ne abbiano necessità per garantire un'adeguata presa in carico.

In occasione del trattamento dei Suoi dati personali, l'Istituto può venire a conoscenza di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, che verranno trattati nel rispetto del principio di necessità e di indispensabilità.

9. COMUNICAZIONE MALATTIA E INFORTUNIO DEL DIPENDENTE

In caso di assenza per malattia il lavoratore dipendente a tempo indeterminato o determinato deve darne tempestiva comunicazione, salvo comprovato impedimento, alla struttura di appartenenza prima dell'inizio dell'orario di lavoro giornaliero e anche in caso di eventuale prosecuzione dell'assenza.

E' tenuto, altresì, a trasmettere alla casella di posta malattie.dipendenti@burlo.trieste.it il numero del certificato medico rilasciato.

Il datore di lavoro non accede alle cartelle sanitarie dei dipendenti sottoposti ad accertamenti dal medico competente per la sorveglianza sanitaria dei lavoratori.

Nel caso di denuncia di infortunio o malattia professionale all'INAIL, il medesimo si limita a comunicare solole informazioni connesse alla patologia denunciata.

10. PERIODO DI CONSERVAZIONE

I dati personali sono conservati, in conformità a quanto previsto dalla vigente normativa e dai regolamenti d'Istituto, per un periodo di tempo non superiore a quello necessario al conseguimento delle finalità per le quali essi sono raccolti e trattati.

L'art. 17, comma 1 lett. *a*, Reg. UE 679/2016 consente la cancellazione dei dati personali (cd. «diritto all'oblio») che non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti

trattati.

11. DIRITTI DELL'INTERESSATO

Come previsto dall'art. 15 e seguenti del Reg. UE 679/2016, l'interessato può in qualsiasi momento esercitare i diritti di accesso, di rettifica, nonché ha il diritto alla limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento.

In particolare, in virtù dell'art. 7 Reg. UE 679/2016, l'interessato ha il diritto di revocare il consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basata sul consenso dato prima della revoca, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico.

L'apposita istanza in carta libera per l'esercizio dei diritti di cui sopra può essere presentata all'attenzione del Direttore Generale dell'IRCCS Burlo Garofolo, via dell'Istria 65/1, 34137 Trieste oppure tramite PEC: **OIBurloTS.protgen@certsanita.fvg.it**

12. SEGNALAZIONI E RECLAMO

Chiunque può svolgere una segnalazione all'Autorità Garante per la protezione dei dati personali.

Ai sensi dell'art. 77 Regolamento UE 679/2016, l'interessato, ove ritenga che il trattamento che lo riguarda violi il sopracitato Regolamento, ha diritto di presentare reclamo all'autorità di controllo individuata nel Garante oppure al DPO.

13. LIMITAZIONI AI DIRITTI DELL'INTERESSATO

L'art. 2-undecies del D.lgs. 196/2003 elenca una serie di situazioni in cui il reclamo e i diritti di accesso, di rettifica, di cancellazione, di limitazione di trattamento, di portabilità dei dati e di opposizione non possono essere esercitati qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto agli interessi tutelati in base alle disposizioni in materia di riciclaggio, di sostegno alle vittime di richieste estorsive, allo svolgimento di investigazioni difensive o all'esercizio di un diritto in sede giudiziaria, alla riservatezza dell'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio, ai sensi della L. n. 179/2018 (cd. *whistleblowing*).

L'esercizio dei medesimi diritti può essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la limitazione possa compromettere la finalità della limitazione.

ALLEGATO 2 NOMINA RESPONSABILI ex art. 28 GDPR

NOTA BENE: Il testo va personalizzato (premesse e contenuti che richiamano il rapporto contrattuale, convenzionale o di collaborazione, d'interesse).

ATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO

TRA

IRCCS Burlo Garofolo di Trieste (C.F./P.IVA 00124430323) – di seguito IRCCS – con sede legale in via Dell'Istria n. 65/1, in Trieste, Titolare del trattamento dei dati personali, in persona del Direttore Generale e legale rappresentante *pro tempore*, di seguito "Istituto"

E

DA PERSONALIZZARE - in persona del legale rappresentante *pro tempore*, di seguito "Responsabile del trattamento"

PREMESSO CHE

- L'IRCCS Burlo Garofolo si caratterizza come ospedale di alta specializzazione e di rilievo nazionale nel settore pediatrico ed in quello della tutela della maternità e della salute della donna, persegue, secondo *standard* d'eccellenza, finalità di ricerca nel campo biomedico e in quello dell'organizzazione dei servizi sanitari, di innovazione nei modelli d'assistenza e di trasferimento delle conoscenze, unitamente a prestazioni di ricovero e cura di alta intensità. Lo stesso Istituto assicura l'erogazione di prestazioni diagnostiche, di cura e di riabilitazione a cittadini della provinciadi Trieste, della Regione Friuli Venezia Giulia ed extraregionali ed è sede di cliniche e di servizi diagnostici Universitari, la cui natura e funzionamento sono disciplinati da specifico Protocollo d'Intesa stipulato tra l'Università degli Studi di Trieste e la Regione FVG e fa parte del Servizio Sanitario Regionale (SSR) a mente della L.R. n. 14/06 s.m.i.
- Con determinazione dirigenziale n. DA PERSONALIZZARE

1. Oggetto

Con il presente atto viene affidato l'incarico di Responsabile del Trattamento dei Dati Personali connesso al rapporto contrattuale/convenzionale DA PERSONALIZZARE.

Il presente atto definisce le modalità con cui il Responsabile del trattamento si impegna ad effettuare per conto dell'IRCCS le operazioni di trattamento dei dati personali e fornisce le adeguate istruzioni.

Nel quadro delle loro relazioni negoziali, le parti si impegnano a rispettare la regolamentazione in vigore applicabile al trattamento dei dati personali e, in particolare, il GDPR 679/2016 e il "Codice in materia di protezione dei dati personali" di cui al D.lgs. n. 196/2003 così come novellato dal D.lgs. n. 101/2018 recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del citato GDPR.

2. Finalità del trattamento

A titolo meramente esemplificativo e non esaustivo, si stabilisce che il trattamento dei dati personali viene effettuato per l'esecuzione dell'atto di cui in premessa e conseguenti adempimenti fiscali, amministrativi.

In particolare, i dati sono trattati:

- da _____ limitatamente al rapporto contrattuale/convenzionale DA PERSONALIZZARE

3. Tipologie di dati personali

I dati personali che vengono trattati sono dati DA PERSONALIZZARE in ragione del contenuto del rapporto contrattuale/convenzionale.

4. Categorie interessati

I soggetti interessati al trattamento dei dati sono DA PERSONALIZZARE.

5. Obblighi del Responsabile del trattamento

Il Responsabile del trattamento si impegna a:

a) trattare i dati solo per la finalità o le finalità sopra specificate e per l'esecuzione delle prestazioni contrattuali;

b) controllare che i dati trattati siano esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati e, se necessario, aggiornare quelli richiesti dall'interessato;

c) conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;

d) cancellare o restituire, su scelta del titolare del trattamento, tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e a cancellare le copie esistenti, salvo cheil diritto del Unione o degli Stati membri preveda la conservazione dei dati;

e) trattare i dati conformemente alle istruzioni contenute nel presente contratto. Se il Responsabile del trattamento rilevi la sua impossibilità a rispettare le istruzioni impartite dall'IRCCS, anche per fatti imprevisti (danneggiamenti, anomalia di funzionamento delle protezioni e controlli accesso, ecc.) è suo dovere avvertirlo immediatamente ed attuare comunque le possibili e ragionevoli misure di salvaguardia concordando eventuali ulteriori misure di protezione;

f) se il Responsabile del trattamento è tenuto a procedere ad un trasferimento dei dati verso un paese terzo o un'organizzazione internazionale, in virtù delle leggi dell'Unione o delle leggi dello stato membro al quale è sottoposto, deve informare l'IRCCS del trattamento di quest'obbligo giuridico prima di procedere al trattamento, a meno che le leggi interessate proibiscano una tale informazione per motivi importanti di interesse pubblico;

g) garantire la riservatezza dei dati personali trattati nell'ambito del presente contratto;

h) adottare tutte le misure richieste ai sensi dell'art. 32; rispettare le condizioni di cui ai paragrafi 2 e 4dell'art. 28 per ricorrere a un altro responsabile del trattamento; assistere il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli dai paragrafi 32 a 36 del GDPR, tenendo conto della natura del trattamento e delle informazioni a

disposizione del responsabile del trattamento;

i) garantire che le persone autorizzate a trattare i dati a carattere personale in virtù del presente contratto:

- si impegnino a rispettare la riservatezza o siano sottoposti ad un obbligo legale appropriato di segretezza;
- ricevano la formazione necessaria in materia di protezione dei dati a carattere personale;

j) tenere conto, utilizzando i materiali, i prodotti, le applicazioni o i servizi, dei principi di protezione dei dati a partire da quando questi vengono progettati e della protezione dei dati di *default*;

k) assistere il titolare del trattamento, tenendo conto della natura dello stesso, con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del medesimo titolare di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del GDPR; mettere a disposizione del titolare tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da altro soggetto da questi incaricato;

l) coadiuvare l'IRCCS nella difesa in caso di procedimenti dinanzi all'autorità di controllo o all'autorità giudiziaria;

m) informare prontamente il Titolare di ogni eventuale trattamento da intraprendere nell'ambito disua competenza, della cessazione, per qualsiasi causa, del trattamento di dati e di ogni altraquestione rilevante ai fini di legge, in particolar modo, a titolo esemplificativo e non esaustivo, nei casi in cui abbia notizia, in qualsiasi modo, che risulti violata la normativa in materia di protezione dei dati personali, ovvero che il trattamento presenti rischi specifici per i diritti, le libertà fondamentali e/o la dignità dell'interessato, nonché qualora, a suo parere, un'istruzione violi la normativa, nazionale o comunitaria, relativa alla protezione dei dati.

6. Ulteriore Responsabile del trattamento

DA PERSONALIZZARE quale Responsabile è autorizzato espressamente a ricorrere a ulteriori responsabili, per l'esecuzione delle attività di trattamento (o parte delle stesse) oggetto del presente atto, imponendo agli stessi i medesimi obblighi in materia di protezione dei dati cui è soggetto il Responsabile stesso, in particolare in relazione alle misure di sicurezza.

A tal fine il Responsabile si impegna a darne preventiva comunicazione all'IRCCS per l'eventuale opposizione, ai sensi dell'art. 28, comma 2, del GDPR.

L'ulteriore Responsabile del trattamento deve rispettare gli obblighi del presente atto. Spetta al Responsabile del trattamento iniziale assicurare che l'ulteriore Responsabile del trattamento presenti le stesse garanzie sufficienti alla messa in opera di misure tecniche e organizzative appropriate in modo che il trattamento risponda alle esigenze del GDPR. Qualora l'ulteriore responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva, nei confronti dell'IRCCS, l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

7. Amministratori di sistema

Nell'effettuare il trattamento di dati per conto dell'IRCCS, sulla base del disposto dell'art. 2-quaterdecies - Attribuzione di funzioni e compiti a soggetti designati del D.lgs. n. 196/2003, il Responsabile è tenuto a tenere a disposizione su richiesta l'elenco dei dipendenti autorizzati ad

operare sui dati dell'IRCCS con le funzioni loro attribuite.

8. Esercizio dei diritti delle persone

Previa esplicita autorizzazione dell'IRCCS, il Responsabile del trattamento risponde direttamente, in nome e per conto dell'IRCCS e nei tempi previsti dal GDPR, alle domande delle persone interessate qualora queste esercitino i loro diritti di accesso, di rettifica, di cancellazione e di opposizione, diritto alla limitazione del trattamento, diritto a trasportare i dati, diritto di non essere oggetto di una decisione individuale automatizzata (compreso il profilo) per quanto riguarda i dati oggetto delle prestazioni previste dal presente atto.
Nella tutela dei diritti degli interessati il Responsabile è obbligato a rispettare l'art. 2-*undecies* -Limitazioni ai diritti dell'interessato del D.lgs. n. 196/2003 e di informare prontamente l'IRCCS delle limitazioni intervenute.

9. Notifica della violazione di dati a carattere personale

Previo esplicita autorizzazione dell'IRCCS, il Responsabile del trattamento, a seguito di classificazione dell'evento secondo la propria procedura di gestione delle violazioni, notifica all'autorità di controllo competente (il Garante per la protezione dei dati personali), in nome e per conto dell'IRCCS, le violazioni di dati a carattere personale senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio peri diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

La notifica deve almeno:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;
- descrivere le misure adottate o di cui si propone l'adozione da parte dell'IRCCS per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

10. Comunicazione della violazione di dati a carattere personale

Previa esplicita autorizzazione dell'IRCCS, il Responsabile del trattamento, a seguito di classificazione dell'evento secondo la propria procedura di gestione delle violazioni, comunica alla persona interessata e alpiù presto, in nome e per conto dell'IRCCS, la violazione dei dati a carattere personale qualora tale violazione sia suscettibile di generare un rischio elevato per i diritti e le libertà di una persona fisica.
La comunicazione alla persona interessata descrive, in termini chiari e semplici, la natura della violazione di dati a carattere personale e contiene almeno:

- descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie

e il numero approssimativo di interessati in questione, nonché le categorie e il numero approssimativo di registrazioni dei dati personali;
- comunicazione del nome e dei dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrizione delle probabili conseguenze della violazione dei dati personali;
- descrizione delle misure adottate o di cui si propone l'adozione da parte dell'IRCCS per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

11. Valutazione di impatto sulla protezione dei dati

Il Responsabile del trattamento assiste l'IRCCS e s'impegna fin da ora a fornirgli ogni elemento utile all'effettuazione della valutazione di impatto sulla protezione dei dati, qualora lo stesso sia tenuto ad effettuarla ai sensi dell'art. 35 del GDPR con riferimento al trattamento dei dati oggetto del presente contratto.

Il Responsabile, ove necessario ai sensi della normativa vigente o su richiesta dell'IRCCS, relativamente ai dati personali e alle procedure e tecnologie usate dal Responsabile nel trattamento degli stessi, si impegna ad effettuare analisi che esplicitino i rischi e le eventuali possibili misure di attenuazione degli stessi da proporre all'IRCCS, propedeutiche a valutazioni di impatto, informando quest'ultimo e fornendo copia degli elaborati finali.

Il Responsabile del trattamento assiste l'IRCCS nella consultazione preventiva dell'autorità di controllo, prevista dall'articolo 36 del GDPR.

12. Misure di sicurezza

Il Responsabile, in ottemperanza dell'articolo 32 del GDPR, 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, mette in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio che comprendono, se del caso:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienzadei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso diincidente fisico o tecnico;
- una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche eorganizzative al fine di garantire la sicurezza del trattamento.

13. Responsabile della protezione dei dati

L'IRCCS dichiara di avere un proprio responsabile della protezione dati personali che risponde all'indirizzo e-mail: dpo@burlo.trieste.it.

14. Registro delle categorie di attività di trattamento

Il Responsabile del trattamento dichiara di tenere in forma scritta il registro di tutte le categorie di attività relative al trattamento svolte per conto del Titolare nei termini di cui all'art. 30 del GDPR.

15. Documentazione

Il Responsabile del trattamento, presso la propria sede, mette a disposizione dell'IRCCS la

documentazione necessaria per dimostrare il rispetto di tutti gli obblighi e per permettere la realizzazione di revisioni, comprese le ispezioni, da parte dell'IRCCS o di un altro revisore da lui incaricato, e per contribuire a queste revisioni.
IRCCS potrà effettuare *audit* previo accordo con DA PERSONALIZZARE

16. Manleva

Il Responsabile si impegna a mantenere indenne l'IRCCS da ogni contestazione, azione o pretesa avanzate da parte degli interessati e/o di qualsiasi altro soggetto e/o Autorità a seguito di eventuali inosservanze da parte del Responsabile stesso e/o degli ulteriori Responsabili -se individuati- delle istruzioni impartite e/o delle norme di cui al presente contratto e/o delle disposizioni normative vigenti in materia.

17. Cessazione del trattamento

Il Responsabile, in caso di cessazione – per qualunque causa – dell'efficacia del presente atto, salvo la sussistenza di un obbligo di legge o di regolamento nazionale e/o comunitario che preveda la conservazionedei Dati Personali, dovrà interrompere ogni operazione di trattamento degli stessi e dovrà provvedere, a scelta dell'IRCCS, all'immediata restituzione allo stesso dei Dati Personali oppure alla loro integrale cancellazione, in entrambi i casi rilasciando contestualmente un'attestazione scritta che presso lo stesso Responsabile non ne esiste alcuna copia. In caso di richiesta scritta dell'IRCCS, il Responsabile è tenuto a indicare le modalità tecniche e le procedure utilizzate per la cancellazione/distruzione.
Rimangono in ogni caso valide le limitazioni alla cancellazione previste per il trattamento ai fini amministrativo-contabili del Responsabile del trattamento e, per le motivazioni in premessa indicate, per i trattamenti di tutela DA PERSONALIZZARE effettuati da____.

18. Durata del contratto

Il presente atto decorre dalla data in cui viene sottoscritto dalle Parti ed è valido fino alla cessazione per qualunque motivo del rapporto negoziale di cui alle premesse.
L'IRCCS dichiara di avere dato corretta informativa ai propri dipendenti coinvolti nel rapporto convenzionale.

19. Disposizioni finali

Resta inteso che il presente atto non comporta alcun diritto per il Responsabile ad uno specifico compenso o indennità o rimborso per l'attività svolta e, pertanto, sarà registrato solo in caso d'uso a tassa fissa aisensi del combinato disposto dell'art. 25 e della tariffa – parte II, art. 4 del D.P.R. 26.4.1986 n. 131.
Per quanto non espressamente ivi previsto, si rinvia alle disposizioni generali vigenti in materia di protezione di dati personali.
Il presente atto è regolato dalla legge italiana e controversie relative alla sua validità, efficacia e interpretazione sono devolute alla competenza esclusiva del Foro di Trieste.

Letto, confermato e sottoscritto.

IRCCS Burlo Garofolo
Il Direttore Generale
firmato digitalmente

DA PERSONALIZZARE
Il RESPONSABILE DESIGNATO
firmato digitalmente

ALLEGATO 3 NOMINA DEI DELEGATI

ATTO DI NOMINA A DELEGATO AL TRATTAMENTO DATI PERSONALI

ex GDPR 679/2016 e Codice della Privacy 196/2003 s.m.i.

L'IRCCS Burlo Garofolo di Trieste (C.F./P.IVA 00124430323) – di seguito IRCCS – con sede legale in via Dell'Istria n. 65/1, in Trieste, Titolare del trattamento dei dati personali, in persona del Direttore Generale e legale rappresentante pro tempore

PREMESSO CHE:

- l'IRCCS Burlo Garofolo, quale ospedale di alta specializzazione e di rilievo nazionale nel settore pediatrico ed in quello della tutela della maternità e della salute della donna con finalità di ricerca nel campo biomedico in quello dell'organizzazione dei servizi sanitari e di innovazione dei modelli d'assistenza e di trasferimento delle conoscenze, deve garantire che il trattamento dei dati personali avvenga nel rispetto dei diritti e delle libertà fondamentali e della dignità delle persone, con particolare riferimento alla riservatezza degli utenti e di tutti coloro che hanno rapporti con l'Istituto;

- i Responsabili apicali dell'organizzazione istituzionale forniscono, nell'ambito della rispettiva Struttura, idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di tutela del trattamento dei dati personali, in ragione del ruolo istituzionale rivestito e delle mansioni indicate nell'Atto aziendale Rep. n. 613 dd. 3.05.2023 adottato con Decreto n. 131 del 3.05.2023;

NOMINA

quale Delegato al trattamento dei dati personali, il Direttore della seguente articolazione aziendale:

_____

il quale, in relazione ai trattamenti dei dati personali effettuati nell'ambito della rispettiva Struttura, ha il dovere di svolgere le corrispondenti mansioni nel rispetto delle disposizioni vigenti in materia, ponendo particolare attenzione all'utilizzo delle banche dati e alle modalità di trattamento dei dati personali. In particolare, il Delegato dovrà:

1. provvedere ad adottare misure tecniche ed organizzative idonee a garantire che la raccolta e la registrazione dei dati avvenga per scopi determinati, espliciti e legittimi e le operazioni del

trattamento non siano incompatibili con tali scopi;

2. controllare che i dati trattati siano esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati e, se necessario, aggiornare quelli richiesti dall'interessato;
3. conservare i dati in modo tale da consentire l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;
4. designare per iscritto gli autorizzati al trattamento con atto formale sottoscritto per accettazione dagli interessati, contenuto in apposito modulo allegato al presente regolamento sul trattamento dei dati personali dell'Istituto scaricabile nella sezione *Intranet* del sito aziendale (all. 3), prescrivendo, in particolare, che gli stessi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati. Qualora sia necessaria una *password* da assegnare agli autorizzati, il Delegato avrà cura che ogni autorizzato abbia la propria *password* personale. Il Delegato, inoltre, avrà cura di conservare l'originale dell'atto di nomina degli autorizzati e di fornirne una copia all'Ufficio trattamento e protezione dati e all'Ufficio del personale per l'inserimento nel relativo fascicolo se si tratta di personale dipendente;
5. individuare un referente, comunicando il nominativo alla Direzione Generale, per tutte le problematiche relative ai trattamenti di dati personali di competenza diretta della struttura, che fungerà da punto di contatto e collegamento con l'Ufficio trattamento e protezione dati;
6. collaborare con l'Ufficio trattamento e protezione dati al fine di predisporre le designazioni a Responsabili del trattamento ex art. 28 GDPR dei i soggetti esterni che intervengono a vario titolo nei rapporti con l'IRCCS nell'ambito delle attività di competenza della struttura da loro diretta;
7. adottare tutte le misure necessarie a garantire che gli autorizzati al trattamento di dati personali rispettino i requisiti di sicurezza stabiliti dall'art. 32 del GDPR;
8. vigilare sulla puntuale osservanza delle istruzioni impartite agli autorizzati, aggiornando all'occorrenza le relative nomine e predisponendo *audit* di Struttura con cadenza almeno semestrale;
9. informare prontamente il Titolare di ogni eventuale nuovo trattamento da effettuare nell'ambito della rispettiva competenza e della cessazione, per qualsiasi causa, del trattamento di dati e di ogni altra operazione rilevante in materia;
10. verificare che, nell'ambito della propria articolazione organizzativa, sia divulgata adeguatamente l'informativa, di cui agli artt. 13 e 14 GDPR n. 679/2016 e all'art. 2-ter del D.lgs. n. 196/2003 novellato dal D.lgs. n. 101/2018 e che sia raccolto il consenso dell'interessato attraverso il sistema informatizzato vigente all'interno dell'Istituto, a cura di persone autorizzate, incaricate e munite di *password* personale;
11. rispondere alle richieste di accesso da parte degli utenti, di cui all'art. 59 del D.lgs. 196/2003;
12. predisporre relazione scritta da fornire al Titolare in merito agli adempimenti eventualmente eseguiti nell'ambito della propria attività istituzionale, con periodicità annuale o nell'ambito degli incontri di *budget*;
13. adottare le misure tecniche e organizzative idonee a garantire la sicurezza informatica dei trattamenti dei dati personali, sentito il parere del l'Ufficio trattamento e protezione dati nella persona del Responsabile/Referente dell'Ufficio del Sistema Informativo dell'Istituto;
14. garantire la conservazione di atti e i documenti in classificatori o in armadi muniti di serratura o in stanze chiuse a chiave, nel caso di trattamento di dati effettuato in forma cartacea;
15. eseguire controlli periodici, con cadenza almeno annuale, sui trattamenti effettuati dai propri autorizzati,con particolare riguardo agli accessi ai dati effettuati da questi mediante le banche

dati informatizzate allo scopo di verificare l'appropriatezza e la pertinenza dei profili loro assegnati;

16. osservare il presente Regolamento ed il Regolamento informatico dell'Istituto, reperibili sul sito *intranet* dell'Istituto stesso e le prescrizioni del Garante per la protezione dei dati personali reperibili sul sito www.garanteprivacy.it . In particolare, il Delegato dovrà osservare le prescrizioni relative alle specifiche Autorizzazioni (ad esempio, le Autorizzazioni al trattamento dei dati genetici, al trattamento a scopi di ricerca ecc.) e porre in essere le relative cautele.
17. partecipare alle iniziative di formazione promosse dall'Istituto e favorire la partecipazione degli autorizzati ai corsi di formazione con cadenza periodica, almeno annuale.

IL DIRETTORE GENERALE
TITOLARE DEL TRATTAMENTO
DEI DATI PERSONALI

IL DIRIGENTE
DELEGATO AL TRATTAMENTO
DEI DATI PERSONALI

Il presente atto deve essere personalizzato, riguardando le attività svolte dall'autorizzato nell'ambito della Struttura/articolazione diretta dal Delegato al Trattamento dati.

ALLEGATO 4 NOMINA DEGLI AUTORIZZATI

ATTO DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

ex GDPR 679/2016 e Codice della Privacy 196/2003 s.m.i.

Il/la sottoscritto/a dott./prof. _____Delegato al trattamento dei dati, ai sensi del GDPR 679/2016 e Codice della Privacy 196/2003 come novellato *ex* D.lgs. 101/2018, nell'ambito della struttura/articolazione aziendale dallo/a stesso/a diretta, in ossequio alle disposizioni vigenti in materia di tutela del trattamento dei dati personali ed in ragione del ruolo istituzionale rivestito e delle mansioni indicate nell'Atto aziendale Rep. n. 613 dd. 3.05.2023 adottato con Decreto n. 131 del 3.05.2023,

NOMINA

quale Autorizzato al trattamento dei dati personali:

_____

il quale, in relazione ai trattamenti effettuati presso questa Struttura/articolazione aziendale e indicati nel Registro dei trattamenti dell'Istituto di cui all'art. art. 30 GDPR, ha il dovere di svolgere le rispettive mansioni nel rispetto delle disposizioni vigenti in materia, ponendo particolare attenzione all'utilizzo delle banche dati e alle modalità di trattamento dei dati personali indicate dal Delegato. In particolare, l'Autorizzato dovrà:

1. osservare le istruzioni impartite dal Delegato affinché la raccolta e la registrazione dei dati avvenga per scopi determinati, espliciti e legittimi e affinché le operazioni del trattamento avvengano in termini non incompatibili con tali scopi;

2. controllare che i dati trattati siano esatti, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati e, se necessario, aggiornare quelli richiesti dall'interessato;

3. conservare i dati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati;

4. accedere ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;

5. rispettare i requisiti di sicurezza, stabiliti dall'art. 32 del GDPR;

6. informare prontamente il Delegato di ogni nuovo trattamento da effettuare nell'ambito della rispettiva competenza e della cessazione, per qualsiasi causa, del trattamento di dati e di ogni altra operazione rilevante in materia;

7. agevolare, per quanto possibile e di propria competenza, nell'ambito della predetta articolazione strutturale, la divulgazione dell'informativa ex art. 13 e 14 GDPR n. 679/2016 e dell'art. 2-ter del D.lgs. n. 196/2003, novellato dal D.lgs. n. 101/2018 e provvedere alla raccolta del consenso

dell'interessato attraverso il sistema informatizzato vigente all'interno dell'Istituto, utilizzando la propria *password* personale;

8. coadiuvare il sottoscritto Delegato nella predisposizione dei riscontri alle richieste di accesso da parte degli utenti di cui all'art. 59 del D. lgs. 196/2003;

9. predisporre breve nota scritta da fornire al Delegato in merito agli adempimenti eventualmente eseguiti nell'ambito delle proprie competenze istituzionali, con periodicità_____ e comunque a richiesta;

10. osservare tutte le misure tecniche e organizzative di sicurezza per il Trattamento dei dati personali previste dall'Istituto e attenersi alle seguenti indicazioni:
    a) provvedere alla conservazione di atti e i documenti in classificatori o in armadi muniti di serratura o in stanze chiuse a chiave, nel caso di trattamento di dati effettuato in forma cartacea;
    b) utilizzare le proprie credenziali di accesso assegnate, dietro autorizzazione del Delegato, dall'Ufficio Sistema Informativo, aggiornandole periodicamente secondo le modalità e i termini indicati dai Regolamenti d'Istituto;
    c) non condividere con nessuno e per nessun motivo le credenziali personali assegnate;
    d) uscire dall'applicativo o bloccare la postazione di lavoro in caso di allontanamento per qualsiasi motivo;
    e) effettuare periodicamente, in collaborazione con l'Ufficio Sistema Informativo, copie di salvataggio delle basi informative e provvedere alla loro conservazione;
    f) osservare i Regolamenti d'Istituto disponibili sulla rete intranet aziendale;

11. osservare le disposizioni, anche regolamentari, impartite in materia dall'Istituto e/o dal Delegato e tutte le prescrizioni del Garante per la protezione dei dati personali reperibili presso il sito www.gpdp.it.;

12. partecipare agli *audit* di Struttura e alle iniziative di formazione promosse in materia dall'Istituto.

IL DIRIGENTE DELEGATO AL TRATTAMENTO DEI DATI PERSONALI	IL DIPENDENTE IN FORZA ALLA STRUTTURA AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI
_____	_____

Il presente atto deve essere personalizzato, riguardando le attività svolte dall'autorizzato nell'ambito della Struttura/articolazione diretta dal Delegato al Trattamento dati.

ALLEGATO 5 IMEPEGNATIVA ALLA RISERVATEZZA

IMPEGNO ALLA RISERVATEZZA
PER L'ACCESO A SISTEMI INFORMATICI DELL'ISTITUTO

Io sottoscritto/a _____ nato/a a _____ il _____

Documento d'identità n. _____ rilasciato da _____ in data _____

Residente a _____ indirizzo _____

CAP/PO BOX_____ nazione _____ .

sono consapevole che per poter svolgere le attività di cui al *contratto/convenzione/progetto …… sottoscritto/avviato* dall'Istituto di ricovero e cura a carattere scientifico Burlo Garofolo di Trieste (Burlo) il ……. con ……., PROTGEN BURLO …… *oppure* di cui al Decreto n. …….. del ……, durante gli accessi ai sistemi informatici del Burlo a cui verrò autorizzato/a potrò venire a conoscenza, anche del tutto occasionalmente, di dati personali, anche di natura particolare, riferiti a soggetti che ricevono o hanno ricevuto prestazioni sanitarie presso il Burlo. Ciò potrebbe essere inevitabile anche se l'attività che dovrò svolgere non riguarda specificamente il trattamento di dati personali.

Un dato è considerato "personale" dalla legge europea e da quella italiana quando permette l'identificazione diretta o indiretta di una persona fisica ed è considerato "particolare" quando riguarda la sfera strettamente personale dell'individuo. Sono considerati dati particolari l'appartenenza etnica e razziale, il credo religioso e le convinzioni filosofiche, l'appartenenza politica e sindacale, le abitudini sessuali e i dati riguardanti la salute. In Europa la riservatezza di tali specifiche informazioni è soggetta a tutele particolari.

Il Burlo, in qualità di titolare del trattamento, è tenuto per legge a mantenere riservate le informazioni di tale natura riferite a soggetti identificati o in qualsiasi modo identificabili e le deve trattare nel rispetto del Regolamento (UE) 2016/679 (GDPR) e del Codice italiano in materia di protezione dei dati personali D.Lgs 196/2003, adeguato al Regolamento dal Dlgs 101/2018. Tali regole tutelano allo stesso modo il diritto alla riservatezza dei dati personali dei cittadini UE anche quando questi dati sono trattati da soggetti esterni all'Unione Europea.

Mi impegno pertanto a considerare le informazioni relative a tali tipologie di dati, quando riferite a soggetti identificati o in qualsiasi modo identificabili, strettamente confidenziali e riservate e ad adottare tutte le ragionevoli misure finalizzate a mantenerle tali. Qualora il mio compito comporti la conoscenza, anche temporanea e occasionale, di informazioni di questo tipo, per portarlo a termine utilizzerò soltanto i dati strettamente necessari, non li comunicherò a soggetti terzi non espressamente autorizzati dal Burlo, non ne tratterrò copia e non li esporterò al di fuori delle reti dell'Istituto, se non in forma aggregata o comunque non

riconducibile in alcun modo a soggetti identificati o identificabili, che stiano ricevendo o che abbiano ricevuto prestazioni presso il Burlo, a meno che il compito a me affidato non lo preveda espressamente.

Nel caso eventuale di partecipazione a collegamenti in teleconferenza, avrò cura di non consentirne la visualizzazione o l'ascolto a soggetti terzi non autorizzati, non registrerò le videochiamate né creerò *screenshot.* Al termine del collegamento eliminerò definitivamente tutti i file temporanei scaricati sul mio dispositivo.

Non userò dati personali relativi ad utenti, dipendenti o relativi a trattamenti di titolarità del Burlo dei quali venissi anche occasionalmente a conoscenza in modo da poter arrecare qualsivoglia tipo di danno ai soggetti interessati, né per scopi diversi da quelli strettamente necessari allo svolgimento dei miei compiti. Questo obbligo di non divulgazione e confidenzialità è a tempo indeterminato e rimane valido anche dopo la conclusione della mia attività. Sono consapevole che qualsiasi violazione degli obblighi di tutela dei dati personali imposti dal Regolamento Europeo e dalla legge italiana può causare danni a persone fisiche e comportare l'imposizione di rilevanti sanzioni, ai sensi dell'art. 83 del GDPR e degli artt. 167, 167 *bis*, 167 *ter*, 168 e 171 del Dlgs 196/03. Dichiaro pertanto di manlevare e tenere indenne l'Istituto Burlo da qualsiasi pretesa avanzata da terzi o sanzione imposta nei suoi confronti a causa di una mia inadempienza colposa all'obbligo di non divulgazione e confidenzialità.

Trieste, _____ _____

firma leggibile