Prot.. N° ……

REGOLAMENTO SUL TRATTAMENTO DEI DATI PERSONALI

DESTINATARI DEL DOCUMENTO
TUTTE LE ARTICOLAZIONI AZIENDALI

DATA REDAZIONE *17/12/2019* **DIREZIONE e STRUTTURA EMITTENTE** *Data Protection Officer (D.P.O.)*	**VERIFICA:** Acquisito Parere favorevole del **RESPONSABILE QUALITÀ AZIENDALE** *Dott.ssa Elisabetta Danielli*	**PARERI FAVOREVOLI:** **DIRETTORE AMMINISTRATIVO** *Dott.ssa Serena Sincovich* **DIRETTORE SANITARIO** *Dott.ssa Paola Toscani* **DIRETTORE SCIENTIFICO** *ad interim Prof. Paolo Gasperini*
PROCESS OWNER *D.P.O. Ing. Michele Bava*	**NORME E STANDARD APPLICABILI** *Regolamento UE 679/2006 (GDPR)* *d.lgs. 196/2003 come novellato dal d.lgs. 101/2018* *Requisiti norma ISO 9001/2015* *DGR 1436/2011* *D.lgs. 288/2003* *DGR 1083/2012* *DGR 3586/2004*	**APPROVAZIONE:** **DIRETTORE GENERALE** *Dott. Stefano Dorbolò*
GRUPPO DI LAVORO *Ing. Michele Bava* *Dott.ssa Marcella Paton* *Dott.ssa Rita Apollo* *Dott.ssa Valeria Mallozzi* *Dott.ssa Elisabetta Danielli*	**DA REVISIONARE ENTRO IL** *31.12.2022*	
PAROLE CHIAVE *Trattamento Dati Personali* *Privacy* *DPO*	**MODALITÀ DIFFUSIONE** *intranet aziendale* *pubblicazione sito internet nella sezione Amministrazione Trasparente*	

INDICE

1. SCOPO

Il presente Regolamento disciplina il trattamento dei dati personali da parte dell'Istituto di Ricerca e Cura a Carattere Scientifico "Burlo Garofolo" di Trieste (in seguito "Istituto").

2. DEFINIZIONI E ACRONIMI

GDPR: General Data Protection Regulation

DPO: Data Protection Officer

D.Lgs.: Decreto Legislativo

DPCM: Decreto del Presidente del Consiglio dei Ministri

D.G.R.: Delibera Giunta Regionale

D.D.G.: Decreto del Direttore Generale

Garante: Garante per la protezione dei dati personali

FSE.: Fascicolo Sanitario Elettronico

SSR: Servizio Sanitario Regionale

DPS: Documento programmatico della sicurezza

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

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, persona giuridica, ente od associazione, identificati o identificabili, 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»: c. d. dati sensibili, i dati personali che rivelino 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»: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) ad o) e da r) ad u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

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»: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

h) «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;

i) «interessato»: la persona fisica, la persona giuridica, l'ente o l'associazione 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) «Gruppo Multidisciplinare Privacy dell'Istituto»: il gruppo di lavoro interno nominato dal Direttore Generale dell'Istituto;

s) «Gruppo regionale privacy e sicurezza informatica» costituito da componenti di tutte le strutture sanitarie pubbliche del Servizio Sanitario della Regione Autonoma Friuli-Venezia Giulia;

t) «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;

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

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

z) «*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)

aa) «*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.

bb) «*chief information security officer*» (CISO): ruolo aziendale organizzativo per stabilire e mantenere una visione, una strategia e un programma aziendale per assicurare che i beni d'informazione e le tecnologie aziendali siano adeguatamente protette.

3. 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 in materia di Dossier Sanitario (4 giugno 2015)
- Linee guida 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 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 in tema di referti online (19 novembre 2009)
- Linee guida in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario (16 luglio 2009)
- Provvedimento 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)
- Provvedimento in tema di Autorizzazioni generali del garante per la protezione dei dati personali (19.07.2018)
- Autorizzazione generale al trattamento dei dati genetici n.8/2016 (15 dicembre 2016)
- Autorizzazione generale al trattamento dei personali effettuato per scopi di ricerca scientifica n.9/2016 (15 dicembre 2016)

- Autorizzazione generale n. 2/2016 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale(15 dicembre 2016)

4. CAMPO DI APPLICAZIONE

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.

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.

5. CONTENUTO

TITOLO I

PRINCIPI GENERALI

Art. 1

Oggetto e ambito di applicazione

1. 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.

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 e co-titolari;

- DPO;

- responsabile/i;

- 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, il Direttore Generale/Commissario Straordinario.

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, inoltre, 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 della violazione dei 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 DPO, attua iniziative di formazione dei Responsabili e Autorizzati per consentire loro di acquisire conoscenze sul corretto trattamento dei dati personali.

Art. 4

Responsabile della protezione dei dati (DPO)

1. Il DPO può essere un dipendente del Titolare del trattamento oppure può assolvere i suoi compiti in base a un contratto di servizi e deve essere designato in funzione delle qualità professionali (conoscenza

specialistica sia della normativa sia della prassi in materia di protezione dei dati e capacità di assolvere 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) 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;

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

d) 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, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

e) supportare il Titolare e ogni Responsabile nelle attività connesse al trattamento, 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 Regolamento UE.

Art. 5

Responsabili del trattamento

1. I Responsabili del trattamento dei dati vengono designati dal Titolare con un contratto o altro atto giuridico, preferibilmente utilizzando lo schema allegato al presente regolamento (Allegati 3 e 4), fra soggetti che per esperienza, capacità e affidabilità, forniscano idonee garanzie del pieno rispetto delle vigenti disposizioni in materia di trattamento e tutte le indicazioni che sono in grado di fornire agli amministratori di sistema che si occupano della protezione e sicurezza dei dati.

2. Nel caso di Responsabili “esterni” si fa riferimento al successivo art. 6 mentre all’art.7 sono disciplinati i responsabili “interni”.

3. Ai sensi dell’art. 28 del Reg. UE 679/2016, 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; in tal caso, il

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

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 Reg. UE 679/2016;

e) in presenza di autorizzazione scritta del titolare, ricorra ad altro responsabile (interno) 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 Reg. UE 679/2016;

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, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile;

i) cancelli o gli 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;

l) 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;

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

4. 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

Responsabili "esterni"

1. In tutti i contratti o convenzioni, con cui l'Istituto affida a terzi (ad es. enti e aziende pubbliche, 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, 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, devono utilizzare preferibilmente il modello allegato al presente regolamento (Allegato 3).

Art. 7

Responsabili "interni"

1. Per i Responsabili interni la riservatezza, l'integrità, la disponibilità e la resilienza dei dati è assicurata dal Sistema Informativo mentre sono responsabili per tutto ciò che concerne gli altri aspetti relativi al presente Regolamento (es. acquisizione consensi su dati e campioni, conservazione degli stessi, portabilità e scambio dati con altri enti pubblici e privati.
2. Per la nomina del responsabile interno deve essere utilizzato preferibilmente il modello allegato al presente regolamento (Allegato 4).

Art. 8

Autorizzati

1. Le persone fisiche che, nell'ambito di rispettiva competenza, effettuano materialmente operazioni di trattamento di dati personali, vengono individuate quali autorizzate e sottostanno all'autorità del Titolare o del Responsabile.
2. Hanno accesso esclusivamente ai dati la cui conoscenza sia strettamente necessaria per l'espletamento dell'attività cui sono preposti.
3. Tale individuazione può avvenire sia tramite specifica indicazione nel contratto individuale di lavoro o con dedicato e idoneo atto.
4. Sono tenuti a rispettare la riservatezza e a ricevere la necessaria formazione in materia di protezione dei dati personali.
5. Per la nomina degli autorizzati deve essere utilizzato preferibilmente il modello allegato al presente regolamento (Allegato 4).

TITOLO III

GRUPPI PRIVACY E SICUREZZA INFORMATICA

Art. 9

Gruppo Multidisciplinare Privacy dell'Istituto

1. Il Direttore Generale istituisce il Gruppo Multidisciplinare Privacy dell'Istituto e nomina all'interno dell'Istituto i componenti del Gruppo per ciascuna delle seguenti articolazioni aziendali:

- Direzione Sanitaria
- Direzione Scientifica
- S.C. Direzione delle Professioni Sanitarie
- S.C. Affari Generali e Legali
- S.S.D. Politiche del Personale
- Gestione e Valorizzazione della Qualità
- Gestione Rischio Clinico
- Ufficio Relazioni con il Pubblico e Comunicazione
- Ufficio Formazione
- S.C. Gestione Tecnica e Realizzazione del nuovo ospedale
- S.C. Ingegneria Clinica, Informatica e Approvvigionamenti

2. Il Gruppo potrà essere integrato con esperti secondo quanto reputato necessario dal DPO.

3. Il Gruppo Multidisciplinare privacy svolge i seguenti compiti:

- garantisce il supporto al DPO nei rapporti con il Garante e 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 il registro dei trattamenti partendo dai trattamenti già attivi e digitalizzati mappati nel Documento informatico della sicurezza;
- effettua la valutazione d'impatto per ciascun trattamento previsto sulla protezione dei dati personali di cui all'art. 35 del Regolamento UE attraverso, di norma, un software di ausilio metodologico messo a disposizione dal Garante della Privacy denominato PIA (*Privacy Impact Analysis*);
- detiene l'elenco annualmente aggiornato dei Responsabili del trattamento dati in ambito aziendale sulla scorta dei dati forniti dall'articolazione del personale.

4. Nell'esercizio delle competenze di cui ai commi precedenti deve essere garantito al Gruppo Multidisciplinare Privacy la collaborazione di tutte le articolazioni organizzative dell'Istituto, in particolare dalla Direzione Sanitaria, cui è demandato l'aggiornamento del censimento dei trattamenti dei dati personali.

Art. 10

Gruppo multidisciplinare Privacy e sicurezza informatica della Regione FVG

1. Il Gruppo privacy e sicurezza informatica della Regione FVG è costituito da due rappresentanti per ogni azienda del S.S.R. uno per la parte informatica ed uno con competenze giuridico - amministrative o sanitarie. È convocato da un referente incaricato dalla stessa Regione 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.

2. È costituito da due sottogruppi: uno per il settore informatico, uno per quello giuridico - amministrativo. 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. Soggetti preposti alla gestione e alla manutenzione di un impianto di elaborazione dati o di sue componenti. L'Amministratore di Sistema ricopre un ruolo estremamente delicato: progetta, sviluppa e gestisce l'infrastruttura di rete, i *server*, il *software* ed i servizi applicativi di base occupandosi spesso della

sicurezza e della protezione dei dati e delle risorse. Fornisce, inoltre, supporto tecnico (*help desk*) e informatico su *software e hardware*.

2. Relativamente al trattamento dei dati con strumenti elettronici, a livello aziendale sono individuate 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 sistemi operativi e software di base e d'ambiente.

- *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*, notificando al CISO (o al DPO) eventuali anomalie riscontrate su malfunzionamenti o rischi di sicurezza. Risponde delle attività svolte e delle conseguenze derivanti da un malfunzionamento della rete e supporta Responsabili del Trattamento e Incaricati per gli aspetti di tipo tecnico informatico nelle normali attività operative.

4. La nomina degli amministratori di sistema è effettuata con atto del Direttore generale.

Art. 12

Documento programmatico sulla sicurezza (DPS)

1. Il Titolare del trattamento dei dati è tenuto ad adottare le misure di sicurezza prescritte dalla normativa nazionale a tutela della privacy e aggiorna, entro l'anno solare - o entro la data comunque normativamente prevista- il Documento Programmatico sulla Sicurezza dei dati.

2. Il Titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del "documento programmatico sulla sicurezza". Il DPS riporta i sistemi e le procedure poste in essere al fine di garantire la riservatezza, l'integrità, la disponibilità e la resilienza di ogni singolo dato personale trattato.

3. Nel DPS si fa l'elenco delle risorse da proteggere e si mettono in atto delle misure di sicurezza per mitigare il rischio relativo alla sicurezza informatica delle stesse. In tal senso è riportata un'analisi del rischio che costantemente e in modo puntuale monitora le risorse, i sistemi, ecc., da proteggere seguendo un modello consono alle certificazioni ISO.

TITOLO IV

MODALITA' DI TRATTAMENTO

Art. 13

Criteri per il trattamento dei dati personali

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. Sono oggetto di trattamento i soli dati essenziali per svolgere attività istituzionali.

3. I Responsabili del trattamento 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 dati che risultano eccedenti o non pertinenti o non necessari, non possono essere utilizzati, salvo che per l'eventuale conservazione prevista ai sensi di legge.

5. I trattamenti di dati effettuati utilizzando le banche dati di diversi Titolari sono autorizzati nelle sole ipotesi previste da espressa disposizione di legge o previa specifica autorizzazione da parte dell'Autorità Garante.

TITOLO V

RAPPORTI CON L'UTENZA

Art. 14

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 collegata), previamente o al momento stesso della raccolta dei dati, anche tramite affissione di appositi manifesti nei locali di accesso dell'utenza, in relazione a:

a) estremi identificativi dell'IRCCS Burlo Garofolo di Trieste in quanto Titolare del trattamento.

b) dati di contatto del DPO;

c) finalità del trattamento dei dati, nonché la base giuridica del trattamento;

d) indicazione dei legittimi interessi perseguiti dal titolare del trattamento o da terzi;

e) eventuali destinatari o eventuali categorie di destinatari dei dati personali ai quali i dati possono essere comunicati;

f) la natura obbligatoria o facoltativa del conferimento dei dati;

g) le conseguenze di un eventuale rifiuto nel fornire i dati;

h) diritto di accesso ai dati personali ai sensi dell'art. 15 GDPR o diritto di accesso a documenti amministrativi contenenti dati personali a norma dell'art. 59 d.lgs. 196/2003;

i) periodo di conservazione dei dati personali, rettifica e cancellazione degli stessi (cd. «diritto all'oblio») o limitazione dei trattamenti, oltre al diritto alla portabilità dei dati;

l) diritto alla revoca o alla modifica del consenso in qualsiasi momento, senza pregiudicare la liceità del trattamento basata sul consenso dato prima della revoca o della modifica, salvo che il trattamento sia necessario per l'esecuzione di un compito di interesse pubblico;

m) diritto di effettuare segnalazioni o proporre reclamo.

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 2)

Art. 15

Diritti dell'interessato

1. Secondo quanto previsto dall'art. 7 del Codice, l'interessato può esercitare i seguenti diritti:

a) di avere informazioni sull'esistenza o meno di propri dati personali in possesso dell'Istituto;

b) di ottenere l'indicazione dell'origine dei dati personali, delle finalità e modalità del trattamento, della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici, degli estremi identificativi del titolare, dei responsabili, dei soggetti o delle categorie di soggetti ai quali i dati personali

possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati;

c) di ottenere l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati, la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;

d) di ottenere l'attestazione che le operazioni di cui alla lettera c) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si riveli impossibile o comporti per l'Istituto un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

2. L'interessato ha diritto di opporsi, in tutto o in parte:

e) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

3. Nell'esercizio dei diritti, l'interessato può conferire delega o procura scritta a persone fisiche, enti o associazioni od organismi. In tal caso copia dell'atto deve essere esibita o allegata all'istanza.

4. 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. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

Art. 16

Rapporti tra il diritto di accesso documentale e civico e il diritto alla privacy

1. L'accesso a documenti amministrativi, contenenti dati personali di terzi, formati o detenuti da questa amministrazione resta disciplinato ai sensi della Legge n. 241/1990 e s.m.i. e dal regolamento per la disciplina delle modalità di esercizio e dei casi di esclusione del diritto di accesso ai documenti amministrativi (DPR 184/2006).

2. Nel caso di dati idonei a rivelare lo stato di salute o l'orientamento sessuale, 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.

3. In ogni caso le strutture organizzative, che propongono l'adozione e/o adottano atti o provvedimenti, verificano, alla luce dei principi di pertinenza e non eccedenza sanciti dal Codice, che l'inclusione nel testo di dati personali sia realmente necessaria per le finalità proprie di ciascun atto o provvedimento.

4. Laddove gli allegati degli atti soggetti a pubblicazione contengano categorie particolari di dati personali tutelati dalla normativa sulla privacy, dovrà essere evidenziato nell'atto che l'allegato non viene pubblicato, rimanendo depositato agli atti per esigenze di tutela della riservatezza. Si applica comunque il Regolamento sull'Albo aziendale vigente.

5. I presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restano disciplinati dal d.lgs. 33/2013 e s.m.i.

TITOLO VI

DATI DELLA RICERCA

Art. 17

1. Si riportano di seguito le modalità di trattamento dei dati per scopi di ricerca presso l'Istituto che andranno seguite da tutti coloro che svolgono attività di ricerca, *critical review*, redazione di tesi di laurea, ecc.

2. Tutti i soggetti coinvolti in tali attività dovranno essere preventivamente nominati "autorizzati al trattamento" (allegato 5) dal Responsabile 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 professioni sanitarie. Ogni progetto di ricerca dell'Istituto, in termini di privacy e sicurezza dei dati, deve avere i seguenti requisiti:

    - il Responsabile del progetto, che diventa automaticamente il responsabile dei dati personali e particolari che vengono trattati.
    - le persone autorizzati a svolgere il progetto (ad esempio lo studente laureando) che devono essere autorizzate per iscritto dal Responsabile di riferimento relativamente allo specifico progetto.

- 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 dei dati stessi 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".*
- 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 art. 13 del Regolamento UE 679/2016, 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. Dovrà essere evidente che i dati che verranno trattati sono solo quelli 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 tali da garantire che l'interessato non sia 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 distrutti 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 a un ricercatore per altri scopi statistici chiaramente determinati per iscritto nella richiesta dei dati.

3. Inoltre, nel caso 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 deve porre specifica attenzione in modo da garantire il rispetto del Codice Privacy e la tutela dei diritti degli interessati.

4. Deve essere specificato che l'incaricato della raccolta dovrà in particolare:

- rendere nota la propria identità, la propria funzione e le finalità della raccolta, anche attraverso adeguata documentazione;
- fornire le informazioni 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 censimento dei trattamenti dell'IRCCS Burlo Garofolo (CE.TRA.)

Art. 18

Il Censimento dei trattamenti dell'IRCCS Burlo Garofolo (CE.TRA.)

1. L'Istituto effettua, tramite la Direzione Strategica, con la collaborazione dei Responsabili, con il supporto del DPO e, eventualmente, del Gruppo Multidisciplinare Privacy, il censimento dei trattamenti dei dati personali e particolari (CE.TRA.), valutando la conformità all'art. 30 del GDPR con particolare riguardo alle schede relative ai singoli trattamenti di competenza delle strutture sanitarie pubbliche del SSN. Tale censimento negli anni precedenti alla entrata in vigore del GDPR e ai sensi del Codice Privacy 196/03, veniva effettuato e riportato nel DPS (Documento Programmatico per la Sicurezza) aziendale sotto forma tabellare.

2. Il CE.TRA. viene comunque riportato nel DPS ed è tenuto a cura della Direzione Strategica che provvede ad aggiornarlo annualmente e, comunque, ogni volta che le vengano comunicati, da parte del Titolare o dei Responsabili del trattamento, casi di attivazione di un nuovo trattamento, variazione o cessazione di un trattamento in essere.

Art.19

Registro dei trattamenti

1. Il Titolare del trattamento o un suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità, che deve essere a messo a disposizione del Garante, su richiesta

2. Sul sito internet del Garante è messo a disposizione il fac-simile utilizzabile per l'implementazione

del registro dei trattamenti. Il registro deve venire aggiornato almeno annualmente, possibilmente in concomitanza alla redazione del DPS aziendale, pur rimanendo un documento a parte.

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) 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) 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, la documentazione delle garanzie adeguate;

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

g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

TITOLO VIII

Valutazione impatto privacy (DPIA)

Art. 20

Valutazione impatto del trattamento

1. La valutazione di impatto del trattamento (D.P.I.A.) è un onere posto direttamente a carico del titolare del trattamento ai sensi dell'art. 35 Reg. UE 679/2016, col quale si 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 dei trattamenti previsti 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 responsabile del trattamento che gli fornisce tutte le informazioni necessarie per lo svolgimento di tale compito, consultandosi con il DPO.

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 le misure specifiche richieste per attenuare o eliminare tali rischi.

TITOLO IX

DISPOSIZIONI FINALI

Art. 21

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. 22

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. 37 del 3 marzo 2011 del Direttore Generale.

2. Sono comunque abrogate tutte le disposizioni regolamentari dell'Istituto in contrasto con quelle previste dal presente regolamento.

° ° °

6. PRIVACY

Ai sensi del Reg. UE 679/2016 (GDPR) e del d.lgs. n. 196 /2003, come novellato dal d.lgs. 101/2018, le registrazioni a supporto dell'attività sono conservate per cinque anni presso archivi cartacei e supporti informatici dell'Istituto e, infine, archiviati presso l'archivio centrale. I documenti sono accessibili esclusivamente dal personale autorizzato a garanzia della tutela del trattamento dei dati personali.

7. ENTRATA IN VIGORE E TRASPARENZA

Il presente regolamento entra in vigore dal giorno della sua formalizzazione, con registrazione nel sistema informatico e assegnazione di un numero di protocollo generale.

Il presente Regolamento è soggetto alla pubblicazione nella sezione Amministrazione Trasparente *ex* D.lgs. 33/2013. È reperibile al seguente percorso. Disposizioni Generali - Atti Generali -regolamenti.

8. PREVENZIONE DELLA CORRUZIONE

Allo stato attuale le attività di cui al presente Regolamento non sono state inserite nel registro dei rischi allegato al vigente Piano Triennale di Prevenzione Corruzione e Trasparenza (PTPCT).

L'Istituto effettua costantemente processi per l'applicazione e l'eventuale revisione, ove necessaria, di procedure/protocolli/regolamenti che costituiscono strumenti ai fini del monitoraggio delle attività a rischio e della conseguente adozione di misure di intervento.

9. GESTIONE DELLE REGISTRAZIONI ARCHIVIAZIONE E ACCESSIBILITA'

Il presente Regolamento, dopo la sua approvazione, è registrato nel sistema informatico di Protocollo Generale dell'Istituto, archiviato e conservato agli atti e pubblicato come da punto 7.

10. DOCUMENTI COLLEGATI - MODALITA' DI APPLICAZIONE

- Regolamento Europeo n. 679/2016 in materia di trattamento dei dati personali (25.05.2018)
- Decreto del Direttore Generale n. 56 del 22.05.2018 di nomina del D.P.O. e di istituzione del Gruppo Multidisciplinare Privacy
- Informativa sul trattamento dei dati personali (generale per gli utenti)
- Modulo di espressione dell'avvenuta informazione e del consenso al trattamento dei dati personali con il dossier elettronico (DSE)

11. DOCUMENTI ABROGATI

Precedenti revisioni.

12. STORIA DEL DOCUMENTO

Di seguito è riportata la storia del documento con le modifiche apportate e lo stato di revisione corrispondente:

DESCRIZIONE	DATA:
PRIMA EMISSIONE: decreto del Commissario Straordinario n. 111/2000	18 /04/2000
REV. 1 decreto del Direttore Generale n. 37/2011	03/03/2011
REV. 2 Revisione format, normativa, contenuti	17/12/2019

13. 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 fornire le seguenti informazioni.

2. CONTITOLARI, RESPONSABILI 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 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 e/o convenzioni. I responsabili possono essere sia interni (Responsabili di Dipartimento, Struttura o Ufficio) sia esterni, quali le aziende con le quali l'IRCCS ha instaurato rapporti contrattuali.

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 (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. FINALITA' 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 le norme 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 sorveglianza sanitaria;

- adempimenti fiscali;

- adempimenti connessi al versamento di quote a istituti finanziari o ad altri soggetti creditori, a seguito di atti 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 fisica o 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 penali e 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 appropriate per 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. LICEITA' 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 ricerca scientifica 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 di procedimento 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 lavoratori su 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 a rendere conoscibile il proprio nominativo mediante l'uso dei cartellini identificativi appositamente predisposti.

8. MODALITA' 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 solo le informazioni connesse alla patologia denunciata.

10. PERIODO DI CONSERVAZIONE DEI DATI PERSONALI

I dati personali sono conservati, in conformità a quanto previsto dalla vigente normativa, 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.

Ai sensi dell'art. 20 Reg. UE 679/2016 l'interessato ha diritto alla portabilità dei dati, ossia di ricevere in un formato strutturato – se tecnicamente possibile-, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento cui li ha forniti.

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 alla cortese 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 al Garante per la protezione dei dati.

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 ESTERNI

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

Dove si parla di contratto, servizio andrebbe utilizzata una terminologia più generica del tipo: rapporto convenzionale, rapporto di collaborazione, collaborazione, etc.

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 provincia di 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. 14/08.
- 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 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 convenzionale DA PERSONALIZZARE

3. Tipologie di dati personali

I dati personali che vengono trattati sono dati DA PERSONALIZZARE in ragione del contenuto del rapporto 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 che il 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 4 dell'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 di sua competenza, della cessazione, per qualsiasi causa, del trattamento di dati e di ogni altra questione 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 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* -L imitazioni 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 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.

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 al più 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 resilienza dei sistemi e dei servizi di trattamento;
- ✓ la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- ✓ una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative 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 conservazione dei 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 ai sensi 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	DA PERSONALIZZARE
Il Direttore Generale	*firmato digitalmente*
firmato digitalmente	

ALLEGATO 3 NOMINA DEI RESPONSABILI INTERNI

ATTO DI NOMINA RESPONSABILE TRATTAMENTO

ex GDPR 679/2016 e Codice della Privacy (d.lgs. n. 196/2003 come novellato *ex* d.lgs. n. 101/2018)

IL DIRETTORE GENERALE

in qualità di legale rappresentante dell'Istituto, Titolare del trattamento dei dati personali, individua e nomina in base all'Atto aziendale adottato con Decreto n. 100 del 10.11.2016, il Direttore della seguente articolazione aziendale: _____ quale "Responsabile del Trattamento" considerato che, per preparazione ed esperienza, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di tutela del trattamento dei dati personali. Pertanto, con il presente atto

NOMINA IL/LA DOTT./SSA _____

RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

In relazione ai trattamenti effettuati, Lei ha il dovere di compiere tutto quanto necessario per il rispetto delle vigenti disposizioni contenute nel "Codice" con particolare riguardo alle banche dati utilizzate e a tutti i dati comunque trattati.

In particolare dovrà:

1. provvedere 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. **designare per iscritto gli autorizzati al trattamento come da *fac-simile* allegato al regolamento Privacy dell'Istituto scaricabile nella sezione *Intranet* del sito aziendale**, 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. Lei dovrà aver cura che ogni sub- responsabile abbia la propria *password.* Lei avrà cura di conservare l'originale dell'atto di

nomina degli autorizzati e di fornirne una copia all'ufficio giuridico del personale per l'inserimento nel relativo fascicolo se si tratta di personale dipendente.

5. adottare tutte le misure necessarie per garantire che gli autorizzati del trattamento di dati personali rispettino i requisiti di sicurezza, stabiliti dall'art. 32 del GDPR;

6. vigilare sulla puntuale osservanza delle istruzioni impartite agli autorizzati nominati e aggiornare sempre le nomine.

7. informare prontamente il Titolare di ogni eventuale trattamento da intraprendere nell'ambito di Sua competenza, della cessazione, per qualsiasi causa, del trattamento di dati e di ogni altra questione rilevante in materia;

8. verificare che, nell'ambito della propria articolazione organizzativa, sia divulgata adeguatamente l'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 sia raccolto il Consenso attraverso il sistema informatizzato vigente all'interno dell'Istituto, a cura di persone autorizzate, incaricate e munite di *password* personale;

9. rispondere alle richieste di accesso da parte degli utenti di cui all'art. 59 del d.lgs. 196/2003;

11. predisporre rapporto scritto al Titolare in merito agli adempimenti eventualmente eseguiti nell'ambito della propria attività istituzionale ai fini di legge con periodicità di norma annuale o nell'ambito degli incontri di *budget*;

12. adottare, in via preventiva, consultato il Responsabile/Referente dell'Ufficio Sistema Informativo dell'Istituto, tutte le misure tecniche e organizzative di sicurezza adeguate per il Trattamento dei dati personali, tra cui:

a) Nel caso di trattamento di dati senza l'ausilio di strumenti elettronici gli atti e i documenti devono essere conservati in classificatori o in armadi muniti di serratura o in stanze chiuse a chiave;

<u>Con riguardo al trattamento dei dati personali eventualmente effettuato mediante elaboratori NON collegati in rete nel rispetto del vigente regolamento informatico:</u>

a) prevedere per ogni postazione delle credenziali di accesso (username e password) nominando singolarmente gli autorizzati del trattamento;
b) custodire l'eventuale elenco aggiornato delle parole chiave di accesso a sistemi e servizi;
c) consentire, ove tecnicamente possibile, e favorire la autonoma sostituzione della parola chiave da parte di ciascun autorizzato;
d) individuare, qualora vi sia più di un autorizzato e siano in uso più parole chiave, i soggetti che hanno accesso alle informazioni relative alle parole chiave;
e) accertarsi, in collaborazione con l'Ufficio Sistema Informativo che ogni elaboratore sia dotato di aggiornati programmi (c.d. *antivirus e patch*) idonei a garantire un'efficace protezione dai rischi di intrusioni ad opera dei programmi indicati dall'art. 615 – *quinquies* del codice penale;
f) effettuare, in collaborazione con l'Ufficio Sistema Informativo, periodicamente copie di salvataggio delle basi informative e provvedere alla loro conservazione

<u>Con riferimento al trattamento di dati personali effettuato mediante sistemi collegati in rete, oltre a quanto sopra:</u>

a) osservare il Documento programmatico sulla sicurezza dell'Istituto (D.P.S.) depositato e disponibile presso l'Ufficio protocollo dell'Ente

13. eseguire controlli periodici con cadenza almeno annuale, sui trattamenti effettuati dai propri autorizzati con particolare riguardo agli accessi effettuati da questi presso le banche dati informatizzate allo scopo di verificare l'appropriatezza e la pertinenza degli accessi;

14. osservare, in particolare, il Regolamento Privacy dell'I.R.C.C.S. Burlo Garofolo, il Regolamento informatico dell'Istituto reperibili sul sito *intranet* dell'Istituto stesso e tutte le prescrizioni del Garante per la protezione dei dati personali reperibili presso il sito www.garanteprivacy.it in particolare le prescrizioni ai fini delle diverse Autorizzazioni specifiche (per es. al trattamento dei dati genetici, al trattamento a scopi di ricerca ecc.) e porre in essere tutte le relative cautele.

15. partecipare alle iniziative di formazione sull'argomento promosse dall'Istituto.

*** *** ***

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.

Trieste, _____

Per il Titolare

Il Direttore Generale

_____

Per presa visione

Il Responsabile (timbro e firma)

_____

ALLEGATO 4 NOMINA DEGLI AUTORIZZATI

ATTO DI AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

GDPR 679/2016 e Codice della Privacy 196/2003 come aggiornato *ex* D.lgs. 101/2018

Il/la sottoscritto/a dott./prof._____Responsabile del 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 _____[1] dallo/a stesso/a diretta, considerato che, per preparazione ed esperienza, fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di tutela del trattamento dei dati personali, con il presente atto

NOMINA IL/LA DOTT./SSA _____

AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI [2]

In relazione ai trattamenti effettuati presso la predetta Struttura/articolazione aziendale e di cui al Registro dei trattamenti ex art. 30 GDPR, Lei ha il dovere di compiere tutto quanto necessario per il rispetto delle vigenti disposizioni contenute nel "Codice" con particolare riguardo alle banche dati utilizzate e a tutti i dati comunque trattati.

In particolare dovrà:

1. provvedere 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;

---

[1] Il presente atto deve essere personalizzato, riguardando le attività svolte dall'autorizzato nell'ambito della Struttura/articolazione diretta dal Responsabile del Trattamento dati. L'art. 4, alinea 10, infatti, parla di "*persone autorizzate al trattamento dei dati personali sotto l'autorità diretta (…) del responsabile".*

[2] Figura deducibile dalla definizione di cui all'art. 4, alinea 10, del Regolamento UE (rif. previgente: "*incaricato del trattamento*" ex art. 30 del D.Lgs. n. 196/2003 e ss.mm.).

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

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

6. informare prontamente il Responsabile di ogni eventuale trattamento da intraprendere nell'ambito di Sua competenza, della cessazione, per qualsiasi causa, del trattamento di dati, e di ogni altra questione rilevante in materia;

8. agevolare, per quanto possibile e di Sua 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 la raccolta del Consenso attraverso il sistema informatizzato vigente all'interno dell'Istituto, utilizzando la propria *password* personale;

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

11. predisporre rapporto scritto al Responsabile in merito agli adempimenti eventualmente eseguiti nell'ambito delle proprie competenze istituzionali con periodicità _____ [3] e comunque a richiesta;

12. osservare tutte le misure tecniche e organizzative di sicurezza per il Trattamento dei dati personali e, almeno attenersi alle seguenti indicazioni:

a) Nel caso di trattamento di dati senza l'ausilio di strumenti elettronici gli atti e i documenti devono essere conservati in classificatori o in armadi muniti di serratura o in stanze chiuse a chiave;

<u>Con riguardo al trattamento dei dati personali eventualmente effettuato mediante elaboratori NON collegati in rete nel rispetto del vigente regolamento informatico:</u>

b) Utilizzare le proprie credenziali di accesso assegnate, dietro autorizzazione del Responsabile, dall'Ufficio Sistema Informativo, aggiornandole periodicamente secondo le modalità e i termini indicati per legge;
c) provvedere, ove tecnicamente possibile, alla autonoma sostituzione della parola chiave;
d) accertarsi che la propria stazione di lavoro sia dotata di aggiornati programmi (c.d. *antivirus e patch*) idonei a garantire un'efficace protezione dai rischi di intrusioni, segnalando al Responsabile eventuali criticità;
e) effettuare, in collaborazione con l'Ufficio Sistema Informativo, periodicamente copie di salvataggio delle basi informative e provvedere alla loro conservazione

<u>Con riferimento al trattamento di dati personali effettuato mediante sistemi collegati in rete, oltre a quanto sopra:</u>

f) osservare il Regolamento Informatico dell'Istituto e il Regolamento Privacy disponibili sulla rete intranet aziendale;

[3] La periodicità può essere definita a cura del Responsabile

g) concordare con l'Ufficio Sistema Informativo e previa autorizzazione da parte del proprio responsabile, il possibile utilizzo di sistemi BYOD (bring your own device) da collegare alla rete dell'Istituto;

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

15. partecipare alle iniziative di formazione sull'argomento promosse dall'Istituto.

Trieste, _____

Il Responsabile del Trattamento

(nome e cognome)

_____

Per accettazione

L'autorizzato

_____

Elenco firmatari

ATTO SOTTOSCRITTO DIGITALMENTE AI SENSI DEL D.P.R. 445/2000 E DEL D.LGS. 82/2005 E SUCCESSIVE MODIFICHE E INTEGRAZIONI

Questo documento è stato firmato da:

NOME: DARIO CARLEVARIS
CODICE FISCALE: CRLDRA62R28L424K
DATA FIRMA: 24/11/2020 12:22:07
IMPRONTA: 37B199A67A66B3ECF5FE656F9D9DD9A2E9F587E95BB193DF41EEFD0D791398DB
E9F587E95BB193DF41EEFD0D791398DBCDECB2F3E28F0324FFC734FBFA83A1DB
CDECB2F3E28F0324FFC734FBFA83A1DB70A4E407C42C5B9A61B72CEF59FC7B0E
70A4E407C42C5B9A61B72CEF59FC7B0EAC5D94B24AC7D290F06FE22F9307C34E