SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Ortopedico Rizzoli di Bologna
Istituto di Ricovero e Cura a Carattere Scientifico

FRONTESPIZIO PROTOCOLLO GENERALE

AOO: DA

REGISTRO: Protocollo generale

NUMERO: 0014178

DATA: 28/09/2021

OGGETTO: Risposta a: Prot. 02/09/2021.0798317.U - "Mani App Emilia-Romagna" (MAppER): indicazioni operative. Adesione al Sistema MAppER della Regione Emilia-Romagna

SOTTOSCRITTO DIGITALMENTE DA:

Anselmo Campagna

CLASSIFICAZIONI:

- [06-04]
- [08-01]

DOCUMENTI:

File	Firmato digitalmente da	Hash
PG0014178_2021_Lettera_firmata.pdf:	Campagna Anselmo	A04F81C29DBADBD383023C1F748E227E AAE4D05A66D1A84B2FF3E0D39200D91F
PG0014178_2021_Allegato2.pdf:		8A9E694873E0CBB54AC15F6C658A91EB 3481C1377833EC275AE1DB30BDB4902A
PG0014178_2021_Allegato3.pdf:		2C127FD24F902416E54F3A85F092E4778 FBFE4361B9EEF0A9E3CC24116EC29E1
PG0014178_2021_Allegato4.pdf:		B1A53E4673E2CA26907118453780FF271 16E5B08CB10641CA3FC2BB3DAFF0FBF
PG0014178_2021_Allegato1.pdf:		18E953F445CE4A641AF7201D1EE8AB9E 0CEF77C33F44F011C4687E4A31A0486F

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Ortopedico Rizzoli di Bologna
Istituto di Ricovero e Cura a Carattere Scientifico

Direzione Generale

Alla Dr.ssa Maria Luisa Moro
Direttrice dell'Agenzia sanitaria e sociale regionale
asrdirgen@postacert.regione.emilia-romagna.it

OGGETTO: Risposta a: Prot. 02/09/2021.0798317.U - "Mani App Emilia-Romagna" (MAppER): indicazioni operative. Adesione al Sistema MAppER della Regione Emilia-Romagna

L'IRCCS Istituto Ortopedico Rizzoli (di seguito Istituto o IRCCS) con la presente aderisce al servizio MAppER, applicativo web per agevolare gli interventi di audit e feedback sull'adesione all'igiene delle mani da parte degli operatori sanitari.

A tale scopo, questo Istituto si impegna a rispettare quanto contenuto nell'" *Accordo per il trattamento di dati personali*", da voi inviato e qui allegato.

A seguito dell'adesione, l'Istituto si impegna a rendere disponibile e fruibile agli osservati l'informativa sul trattamento dei dati personali nonché le modalità e tempistiche di effettuazione dei controlli da parte degli osservatori attraverso un duplice canale informativo: per gli operatori sanitari interni agli Enti del SSR attraverso la piattaforma GRU, mentre per tutti gli operatori sanitari esterni agli Enti del SSR attraverso i canali ordinari di comunicazione ad oggi in uso.

Ai fini dell'art. 28 del Regolamento (UE) 2016/679 (c.d. GDPR), il Direttore Generale dell'IRCCS è Titolare del trattamento dei dati personali raccolti e/o generati dall'applicativo "MappER".

La policy dell'Istituto relativa e necessaria all'espletamento dell'attività esternalizzata è contenuta nelle seguenti Delibere, che si allegano alla presente:

- Delibera n. 320 del 21.12.2018, "Adeguamenti al Regolamento (UE) n. 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e al D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) come integrato e modificato dal D.lgs. n. 101/2018: DEFINIZIONE DELL' ORGANIGRAMMA DELLE RESPONSABILITÀ PRIVACY AZIENDALI E MODALITÀ DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI – provvedimenti conseguenti di individuazione dei soggetti autorizzati al compimento delle operazioni di trattamento e dei referenti privacy del trattamento dati";
- Delibera n. 402 del 23.12.2019, "ADOZIONE DEL DOCUMENTO 'LINEE GUIDA PER L' APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL D.LGS. 30.06.2003 N. 196'".

Sandra Montanari
Segreteria Direzione Generale

Istituto Ortopedico Rizzoli
Sede legale Via Di Barbiano, 1/10 - 40136 Bologna
Ospedale Via G. C. Pupilli, 1 - 40136 Bologna
Centro di Ricerca Via Di Barbiano, 1/10 - 40136 Bologna
Tel. 051/6366111 - Fax 051/580453 www.ior.it
Codice Fiscale e Partita IVA 00302030374

Conseguentemente codesta Regione e, nella specie, l'Agenzia sanitaria e sociale regionale sarà designata Responsabile del trattamento dei dati personali trattati, per le attività di competenza. Si allega, allo scopo, l' atto di designazione.

Distinti saluti

Firmato digitalmente da:
Anselmo Campagna

Responsabile procedimento:
Francesco Soncini

Sandra Montanari
Segreteria Direzione Generale

Istituto Ortopedico Rizzoli
Sede legale Via Di Barbiano, 1/10 - 40136 Bologna
Ospedale Via G. C. Pupilli, 1 - 40136 Bologna
Centro di Ricerca Via Di Barbiano, 1/10 - 40136 Bologna
Tel. 051/6366111 - Fax 051/580453 www.ior.it
Codice Fiscale e Partita IVA 00302030374

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Ortopedico Rizzoli di Bologna
Istituto di Ricovero e Cura a Carattere Scientifico

FRONTESPIZIO DELIBERAZIONE

AOO: DA

REGISTRO: Deliberazione

NUMERO: 0000320

DATA: 21/12/2018 18:04

OGGETTO: Adeguamenti al Regolamento (UE) n. 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e al D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) come integrato e modificato dal D.lgs. n. 101/2018: DEFINIZIONE DELL'ORGANIGRAMMA DELLE RESPONSABILITÀ PRIVACY AZIENDALI E MODALITÀ DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI - provvedimenti conseguenti di individuazione dei soggetti autorizzati al compimento delle operazioni di trattamento e dei referenti privacy del trattamento dati

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Cavalli Mario in qualità di Direttore Generale
Con il parere favorevole di Landini Maria Paola - Direttore Scientifico
Con il parere favorevole di Rolli Maurizia - Direttore Sanitario
Con il parere favorevole di Cilione Giampiero - Direttore Amministrativo

Su proposta di Laura Mandrioli - Affari Legali e Generali che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [06-04]

DESTINATARI:

- Collegio sindacale
- Servizio Unico Metropolitano Amministrazione del Personale (SUMAP)
- Affari Legali e Generali
- Accesso ai Servizi
- Amministrazione della Ricerca
- Programmazione, Controllo e Sistemi di Valutazione
- ICT
- Servizio Prevenzione e Protezione
- Dipartimento Patologie Complesse
- Dipartimento Patologie Specialistiche

- Struttura di Supporto Direzionale
- Patrimonio ed Attivita' Tecniche
- Direzione Servizio di Assistenza Infermieristica, Tecnica e della Riabilitazione (DAITER)
- Farmacia
- Servizio Unico Metropolitano Contabilita' e Finanza (SUMCF)
- Servizio Unico Metropolitano Economato (SUME)
- Servizio Bilancio e Coordinamento Processi Economici
- Dipartimento Rizzoli - Sicilia
- Direzione Scientifica
- Comunicazione e Relazione con i Media
- Marketing Sociale
- Clinical Trial Center
- Dip. Rizzoli - RIT Research, Innovation & Technology

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000320_2018_delibera_firmata.pdf		7950FF37D7FEC5799268D4E4135FC7818DDFFD8B22789D4553CAB3735226413A
DELI0000320_2018_Allegato1.docx:		98A77842EEDA1A3C8EF14E1DEE913AC80433EA4B5D72E7FDB330505D52FDBE3A
DELI0000320_2018_Allegato2.docx:		F680B62E491507AA59CCE4ACD9D8BE7BBCE0A75FB313454E4C17AED59C2DB397
DELI0000320_2018_Allegato3.docx:		91E576F2FB642629032CD94C0D2E972F91D7AAFF32656D1FBED32D1DC742324A

DELIBERAZIONE

OGGETTO: Adeguamenti al Regolamento (UE) n. 2016/679 (c.d. GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e al D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) come integrato e modificato dal D.lgs. n. 101/2018: DEFINIZIONE DELL'ORGANIGRAMMA DELLE RESPONSABILITÀ PRIVACY AZIENDALI E MODALITÀ DI DESIGNAZIONE DEI SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI - provvedimenti conseguenti di individuazione dei soggetti autorizzati al compimento delle operazioni di trattamento e dei referenti privacy del trattamento dati

IL DIRETTORE GENERALE

Premesso che

- Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito anche solo "Regolamento" o "GDPR"), detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni;
- Le disposizioni del D.lgs. n. 196/2003 " *Codice in materia di protezione dei dati personali*" continuano a trovare applicazione, così come integrate e modificate dal D.lgs. n. 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)*";
- Nelle more necessarie per il consolidamento della nuova normativa entrata in vigore i Provvedimenti di carattere generale emanati dal Garante per la protezione dei dati personali (di seguito anche solo "Garante") e i principi ivi sanciti continuano a trovare applicazione nella misura in cui non siano in contrasto con la normativa sopra citata;

Considerato che

- Nel percorso di attuazione ai suddetti obblighi ed adempimenti, occorre aggiornare i provvedimenti a suo tempo assunti da questa Amministrazione, ad iniziare dai provvedimenti concernenti l'individuazione di coloro che – per motivi di servizio – trattano dati personali di cui è titolare IOR;
- Il GDPR individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

a) *il Titolare del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali,

b) *il Responsabile (esterno) del trattamento*: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento,

c) *il Responsabile della protezione dei dati* (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del Regolamento, che ne disciplinano compiti, funzioni e responsabilità,

d) ***persone autorizzate* al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (esterno):** figura che si desume implicitamente dalla definizione di " *terzo*" di cui al n. 10 del comma 1 art. 4 del Regolamento e dall'articolo 29 del Regolamento, che pone l'obbligo di dare istruzioni a chi abbia accesso a dati personali e agisca per conto del titolare o del responsabile (esterno) e che trova conferma nell'art. 2 quaterdecies del D.lgs. 196/2003 come modificato dal d.lgs. 101/2018;

Richiamata

- La DGR Regione Emilia Romagna n. 919 del 10/4/2018 " *Linee di programmazione e di finanziamento delle Aziende e degli enti del Servizio Sanitario regionale per l'anno 2018"* che prevede fra gli obiettivi indicati al punto 4.6 dell'allegato B, oltre la nomina del DPO l'adozione del registro delle attività di trattamento, la ri-definizione ed articolazione delle specifiche responsabilità privacy aziendali;

Richiamate inoltre:

- la Delibera n. 188 del 12/06/2018 dell'Azienda USL di Bologna di nomina del Data Protection Officer (DPO), ai sensi degli artt. 37, 38 e 39 del GDPR;
- **le delibere IOR n. 704 del 17/11/2004 e n. 503 del 9/6/2006 con le quali i dipendenti e tutti i soggetti (legati da altro** rapporto formalizzato con l'Ente, di carattere contrattuale, convenzionale, di collaborazione, ecc…), **che compiono operazioni di trattamento per conto di questo Istituto sono stati individuati quali incaricati** (ai sensi dell'abrogato art. 30 D.Lgs.196/2003) di tutti i trattamenti dei dati facenti capo all'Unità Operativa alla quale sono formalmente assegnati, nell'ambito delle funzioni e dei compiti specificatamente attribuiti;
- le delibere IOR n. 178 del 23/3/2004, n. 300 del 09/7/2013 e n. 239 del 30/10/2015;

Ritenuto

- che sia necessario, pur confermando la sostanza dei provvedimenti citati, provvedere ad un loro aggiornamento, nei termini che seguono, stante l'intervenuta diretta applicabilità del Regolamento (UE) n. 2016/679 e l'entrata in vigore del D.Lgs n. 101/2018;

Ritenuto altresì:

- che talune **prerogative o obblighi inerenti gli aspetti applicativi della normativa** Privacy, senza incidere sulla titolarità, possono essere demandati a un numero ristretto di figure aziendali in ragione degli incarichi ricoperti e delle aree di autonomia correlate;

- **che** per effetto dell'incarico ricoperto e senza necessità di nomina *ad personam* **per tali prerogative o obblighi si ritiene di individuare, le seguenti figure professionali**, in quanto possiedono le competenze necessarie al fine di garantire l'adozione delle misure tecniche ed organizzative per assicurare un trattamento conforme alla normativa vigente:
  - per l'area clinica e della ricerca nonché dell'assistenza:
  i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali;
  - per l'area amministrativa:
  i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali;

- **di stabilire che tali figure assumano la denominazione di "Referenti privacy"**;

- che la nomina ai singoli Referenti privacy verrà comunicata mediante lettera del Direttore Generale;

- che la designazione quali Referenti Privacy potrà rendersi necessaria in capo ad **altri soggetti** – ulteriori e diversi da quelli indicati sopra – anche non titolari di incarico di Struttura Complessa e/o di Struttura Semplice Dipartimentale (a titolo esemplificativo il *Responsabile Scientifico* e/o il *Principal Investigator* dei progetti di ricerca / sperimentazione clinica), i quali verranno **individuati di volta in volta e formalmente nominati** con separati atti in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati;

Dato atto ulteriormente:

- che l'elenco dei Referenti privacy potrà essere integrato o modificato, in ragione delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati e che, in caso di vacanza del ruolo, i compiti sono svolti dalla figura che ne assume le funzioni;

- che tale individuazione quale Referente privacy si esplica in particolare nello svolgimento dei **compi ti - di cui all'allegato 1 -** la cui elencazione non può comunque ritenersi esaustiva rispetto a tutti i compiti e gli adempimenti connessi ad una compiuta e corretta attività di protezione dei dati;

Atteso inoltre che:

- coerentemente con quanto previsto dalla normativa citata, si ritiene ora di confermare l'autorizzazione al trattamento dei dati personali da parte di tutti i soggetti che operano sotto la diretta autorità del Titolare del trattamento;

- per " **soggetti autorizzati"** si intendono tutti i dipendenti/collaboratori dell'Istituto, ognuno per il proprio specifico ambito di competenza professionale, i quali sono tenuti alla osservanza delle istruzioni – contenute nell' **allegato 2** al presente atto - impartite dal Titolare per il corretto trattamento dei dati personali, oltre ad ulteriori istruzioni che il Titolare del trattamento, anche per il tramite dei Referenti privacy, impartirà loro con riferimento a particolari trattamenti di dati;

- il personale in servizio presso l'Istituto (quale dipendente e/o collaboratore) alla data di adozione del presente Atto – e come tale già designato "incaricato del trattamento" ai sensi dell'abrogato art. 30 d.lgs. 196/2003 – deve considerarsi personale "autorizzato" al trattamento ai sensi dell'art. 29 del GDPR;

- il personale che, invece, entrerà in servizio successivamente alla data di adozione del presente Atto dovrà considerarsi designato quale "autorizzato" al trattamento dei dati contestualmente alla sottoscrizione del contratto di lavoro e/o di collaborazione;

- l'autorizzazione di cui sopra deve intendersi circoscritta esclusivamente ai trattamenti che afferiscono all'unità operativa a cui è assegnato il dipendente / collaboratore, così come indicati, oltre che nel registro dei trattamenti, nell'atto aziendale e suo regolamento attuativo, nelle assegnazioni funzionali del dipendente / collaboratore, nonché negli ulteriori atti ricognitivi dei processi e dei procedimenti e nelle eventuali ulteriori e specifiche indicazioni fornite dal Referente privacy al quale le singole unità operative fanno capo;

Ritenuto

- di comunicare tale autorizzazione al trattamento a tutti i dipendenti/collaboratori dell'Istituto tramite il portale del personale e apposita news sulla intranet;

Valutato inoltre

- con riferimento alle persone che prenderanno servizio in data successiva alla adozione del presente Atto, che l'autorizzazione al trattamento dei dati personali debba operare:

- per i dipendenti, mediante inserimento di idoneo riferimento e richiamo nel contratto di lavoro;

- per i soggetti che – in virtu' di un rapporto comunque formalizzato con l'Ente – debbano accedere e trattare dati personali, mediante la previsione, laddove possibile, di idoneo riferimento e richiamo anche nelle altre forme di contratto e/o di conferimento incarico variamente denominati (a titolo non esaustivo: legali, borsisti, tirocinanti, stagisti ecc.);

- per tutti gli altri soggetti per i quali non è prevista la sottoscrizione di un contratto/accordo individuale o comunque per i quali non è possibile la forma di designazione indicata al punto che precede (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili, specializzandi ecc) sarà l'ufficio amministrativo che cura gli adempimenti finalizzati all'istaurazione del rapporto con l'Istituto a provvedere di volta in volta all'autorizzazione al trattamento dei dati attraverso l'atto di designazione **allegato sub 3)** alla presente delibera;

Atteso che

- con delibera n. 160 del 29.06.2018 l'Istituto ha provveduto a nominare il **Responsabile della protezione dei dati** (di seguito anche Data Protection Officer e/o DPO), nella persona della dott.ssa Federica Banorri (recapito mail: *dpo@ausl.bologna.it*), in condivisione con Azienda USL di Bologna, Azienda Ospedaliera Universitaria - Policlinico S. Orsola Malpighi, Azienda USL di Imola e Montecatone Rehabilitation Insitute S.p.A.;

- i compiti del nominato DPO, considerata la sua competenza riferita all'area metropolitana, sono i seguenti:
  - informare e fornire consulenza alle Aziende/Enti, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. Per il tramite dei referenti aziendali individuati dalle singole Aziende/Enti dovrà altresì assicurare attività di informazione/consulenza ai Responsabili del trattamento nonché ai dipendenti che, in qualità di incaricati al trattamento, eseguono operazioni di trattamento dati;
  - sorvegliare l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti aziendali individuati dalle singole Aziende/Enti;
  - fornire, se richiesti, pareri anche scritti in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;
  - cooperare con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa per questioni connesse al trattamento (tra cui la consultazione preventiva) ed effettuare eventuali consultazioni e curarne in generale i rapporti;
  - supportare le strutture aziendali deputate alla tenuta del Registro del trattamento delle singole Aziende/Enti al fine di uniformarne la predisposizione;
  - garantire il corretto livello di interlocuzione con gli altri DPO delle Aziende sanitarie regionali e/o con il DPO della Regione Emilia-Romagna in relazione a progetti ed iniziative di valenza regionale/metropolitana (ad es. FSE, ARA, GRU, GAAC);
  - promuovere iniziative congiunte tra le Aziende/Enti affinchè l'applicazione della normativa in materia di protezione dei dati personali nonché delle policy aziendali sia sviluppata secondo linee applicative omogenee e coerenti nelle singole Aziende/Enti;
  - favorire il coordinamento dei DPO delle altre aziende sanitarie regionali relativamente alle tematiche precedentemente presidiate dal Tavolo Privacy Regionale, come da richiesta della Regione Emilia-Romagna, nota PG/2018/0482475 del 5 luglio 2018.

Ritenuto infine

- di costituire un **Gruppo Aziendale Privacy** (di seguito anche solo Gruppo o GAP) di cui faranno parte i seguenti componenti:
  - Il Coordinatore Aziendale sulle tematiche privacy e coordinatore del Gruppo (già Referente Aziendale privacy);
  - Il Responsabile ICT anche quale responsabile della transizione digitale (nominato con delibera n. 79 del 28/3/2018) e in particolare relativamente alle prerogative di cui all'art. 17 comma 1 lett. C e G del CAD (indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica di dati, sistemi e alle infrastrutture);
  - Il Responsabile della SSD Accesso ai Servizi;
  nonché
  - per l'area Direzione Sanitaria/ Area Clinica:
    Un **componente individuato dalla Direzione Sanitaria,** anche proveniente dall'area Clinica;
  - per l'area Direzione Scientifica:
    Un **componente individuato dal Direttore Scientifico nell'ambito dei Laboratori di Ricerca**;
  - per l'Area dell'Assistenza:
    Un **componente individuato dalla direzione DATER;**

- che il GAP, in attuazione dei principi di informazione e sensibilizzazione richiamati dal GDPR, ha il compito di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali;

- che, pertanto, il GAP, coordinato dalla Dott.ssa Laura Mandrioli, ha i seguenti compiti specifici:
  - supportare i Referenti privacy nell'adozione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Istituto, a seguito degli approfondimenti e delle analisi effettuate dal coordinatore del GAP con il DPO nel Tavolo di area metropolitana,
  - supportare i Referenti privacy nell'aggiornamento del Registro dei trattamenti di dati personali effettuati dalle strutture di appartenenza e, con la collaborazione del DPO, nella eventuale valutazione di impatto,
  - fornire supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO,
  - coordinare le richieste di parere al DPO da parte dei singoli Referenti Privacy;

- **che con il presente provvedimento vengono superati** tutti i provvedimenti adottati precedentemente e cioè, oltre a quelli citati, anche le delibere n. 674 del 8 ottobre 2001 e n. 643 del 15 ottobre 2003 con cui erano stati nominati i cosiddetti " responsabili interni";

- che sul presente provvedimento è stato acquisito il parere favorevole del DPO;

Delibera

1. di individuare, quali " **Referenti privacy**" :
   - per l'area clinica e della ricerca nonché dell'assistenza:
   i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali,
   - per l'area amministrativa:
   i Direttori delle Strutture Complesse e i Responsabili delle Strutture Semplici Dipartimentali;

2. di stabilire che la designazione e nomina dei Referenti privacy è conseguente all'assunzione/conferma degli incarichi di responsabilità come sopra specificati o all'assegnazione della funzione "ad interim" e di "facente funzioni" e che, pertanto, tale atto reca in sè la nomina a Referente privacy, con specificazione circa i compiti/istruzioni assegnati (allegato 1);

3. di riservarsi di designare quali Referenti privacy del trattamento dati altri soggetti – ulteriori e diversi da quelli indicati ai punti che precedono – anche non titolari di incarico di Struttura Complessa e/o di Struttura Semplice Dipartimentale (a titolo esemplificativo, Responsabile di struttura semplice, Responsabile Scientifico e/o Principal Investigator di progetti e/o sperimentazioni), i quali verranno individuati e nominati di volta in volta in virtù delle particolarità organizzative e funzionali delle attività di competenza e/o della tipologia dei dati trattati;

4. di disporre che **chiunque compie operazioni di trattamento dei dati personali per conto dell' Istituto Ortopedico Rizzoli è individuato come "autorizzato" di trattamento al quale, come tale, sono consentite le operazioni di cui all'art. 4 del GDPR,** ciascuno nell'ambito delle funzioni e dei compiti specificatamente attribuiti;

5. di dare atto che tale individuazione si concretizza, di norma e senza l'adozione di ulteriori atti, all'atto dell'instaurazione di qualsivoglia rapporto - purché formalizzato - con l'Istituto Scientifico anche tramite il SUMAP;

6. di dare atto che per tutti i soggetti per i quali non è prevista la formalizzazione di un contratto/accordo individuale e, comunque, per i quali non è possibile la forma di designazione indicata al punto 5) che precede (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili, specializzandi ecc) sarà l'ufficio amministrativo che cura gli adempimenti finalizzati all'istaurazione del rapporto con l'Istituto a provvedere, di volta in volta, all'autorizzazione al trattamento dei dati attraverso l'atto di designazione di cui all'allegato 3) della presente delibera;

7. di dare atto che l'autorizzazione di cui sopra deve intendersi circoscritta esclusivamente ai trattamenti che afferiscono all'unità operativa a cui è assegnato il dipendente / collaboratore, così come indicati, oltre che nel registro dei trattamenti, nell'atto aziendale e suo regolamento attuativo,

nelle assegnazioni funzionali del dipendente / collaboratore, nonché negli ulteriori atti ricognitivi dei processi e dei procedimenti e nelle eventuali ulteriori e specifiche indicazioni fornite dal Referente privacy al quale le singole unità operative fanno capo;

8. di precisare che gli autorizzati al trattamento operano secondo le direttive dei Referenti privacy ai quali afferiscono attenendosi alle istruzioni operative impartite dagli stessi nonché a quelle di carattere generale ricevute dal titolare e contenute nella presente delibera e nel suo allegato 2);

9. di dare mandato al SUMAP di trasmettere la presente deliberazione ai Dirigenti attualmente titolari degli incarichi dirigenziali di cui al punto 1 e di procedere analogamente per il futuro, a seguito di ogni conferimento/rinnovo o comunque di variazioni soggettive nella titolarità degli incarichi come sopra individuati, integrando altresì il contratto individuale con apposita clausola;

10. di comunicare l'autorizzazione al trattamento a tutti i dipendenti e alle categoria di personale indicate al precedente punto 5 mediante messa a disposizione della presente deliberazione nel profilo personale del portale del dipendente (GRU), oltre che tramite pubblicazione nell'intranet aziendale e nel sito internet dell'Istituto all'indirizzo *http://www.ior.it/il-rizzoli/atti-amministrativi-generali*, dando mandato al SUMAP, secondo le rispettive competenze, di procedere analogamente nei confronti del personale di nuova "assunzione" integrando i (futuri) contratti di lavoro con apposita clausola;

11. di costituire il **Gruppo Aziendale Privacy** composto dai seguenti membri:
    - Il **Coordinatore Aziendale sulle tematiche privacy e coordinatore del Gruppo** (già Referente Aziendale privacy);
    - il Responsabile ICT anche quale responsabile della transizione digitale (nominato con delibera n. 79 del 28/3/2018) e in particolare relativamente alle prerogative di cui all'art. 17 comma 1 lett. C e G del CAD (indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica di dati, sistemi e alle infrastrutture);
    - Il Responsabile della SSD Accesso ai Servizi;
    nonché
    - per l'area Direzione Sanitaria/ Area Clinica:
      Un **componente individuato dalla Direzione Sanitaria,** anche proveniente dall'area Clinica;
    - per l'area Direzione Scientifica:
      Un **componente individuato dal Direttore Scientifico nell'ambito dei Laboratori di Ricerca**;
    - per l'Area dell'Assistenza:
      Un **componente individuato dalla direzione DATER;**

12. di allegare **(allegato 1) l'elenco dei compiti/obblighi dei Referenti privacy**;

13. di allegare **(allegato 2) le istruzioni operative per il trattamento dei dati da parte degli autorizzati** e, in generale, quale contenuto minimo dei compiti/obblighi applicabile alla generalità dei trattamenti a prescindere dai profili di incarico;

14. di allegare **(allegato 3) il fac simile dell'atto di designazione del soggetto autorizzato al trattamento dei dati personali** da utilizzare per le nomine previste al punto 6 della presente delibera;

15. di precisare che dall'adozione del presente provvedimento non derivano oneri economici a carico del Bilancio dell'Istituto Ortopedico Rizzoli;

16. di diffondere il presente atto attraverso la rete intranet aziendale e il portale del personale GRU.

Responsabile del procedimento ai sensi della L. 241/90:
Marina Cioni

Allegato 1

COMPITI FUNZIONI E POTERI DEI REFERENTI PRIVACY

- Trattare i dati personali solo su istruzione del Titolare del trattamento e garantire la corretta applicazione del Regolamento generale per la protezione dei dati (GDPR) e del D.Lgs. 196/2003, come modificato dal D.Lgs.101/2018, nonché la conformità alle indicazioni dell'Autorità Garante per la protezione dei dati personali;
- Osservare e fare osservare:
    a) le direttive aziendali in materia di protezione, di finalità, di modalità di trattamento dei dati, fornite dal Titolare del trattamento, anche per il tramite del Gruppo Aziendale Privacy e del Servizio ICT Aziendale (a titolo esemplificativo: regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli approvato con delibera n. 225/2017 e informativa per gli utenti sull'utilizzo dei servizi informatici IOR consultabili sulla rete intranet (all'indirizzo: *http://intranet.internal.ior.it/documentazione/manuali/regolamento-ict*); linee guida in tema di fascicolo sanitario elettronico (FSE) e di dossier sanitario consultabili sulla rete intranet (all'indirizzo *http://intranet.internal.ior.it/documentazione/normativa/linee-guida-del-garante-protezione-dei-dati-personali-tema-di-fascicolo-san*), indicazioni sulla acquisizione dei consensi al Dossier Sanitario Elettronico (DSE) e relativi adempimenti in tema di privacy assunte con il protocollo n. 6054 del 19.02.2015, linee guida in materia di Dossier Sanitario – provvedimento 04.06.2015 del Garante per la protezione dei dati personali pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n.164 del 17.07.2015 assunte con protocollo n. 26344 del 24.07.2015, procedura di *data breach* assunta con protocollo n. 5968 del 25.05.2018 e consultabile nella cartella di Fileserver2020 denominata *Condivisioni\RegolamentoUE.679.2016* ed ulteriori regolamenti e disposizioni consultabili sulla rete intranet aziendale)
    b) le istruzioni di carattere generale impartire dal Titolare a tutti i soggetti autorizzati al trattamento (di cui all'**allegato 2**);
    c) eventuali ulteriori specifiche istruzioni predisposte dallo stesso in relazione agli specifici ambiti di competenza, anche per gruppi omogenei di funzioni.

- Porre in atto all'interno della propria struttura organizzativa le procedure e le linee guida aziendali per la corretta gestione dei dati, assicurando che i soggetti interessati (es. pazienti, dipendenti, fornitori ecc.) ricevano le informazioni relative al trattamento dei dati personali di cui agli artt.13 e 14 del GDPR;
- Provvedere alla designazione dei soggetti autorizzati al trattamento dei dati personali per i singoli operatori per i quali tale autorizzazione non può essere rilasciata contestualmente alla sottoscrizione di un contratto di lavoro/incarico (a titolo non esaustivo: frequentatori volontari, lavoratori socialmente utili ecc.), attraverso la predisposizione dell'apposito modello di cui l'**allegato 3**;
- Vigilare sulla conformità dell'operato dei soggetti autorizzati ad essi afferenti alle istruzioni e alle direttive di cui sopra, verificando periodicamente lo stato di adeguamento alla normativa in oggetto;
- Verificare che i dati oggetto di trattamento siano esatti, aggiornati, indispensabili, pertinenti e non eccedenti rispetto alle finalità per cui vengono trattati;

- Attenersi alle indicazioni di sicurezza dettate dal Titolare del trattamento e compatibilmente con l'ambito di attività, adottare le misure di sicurezza tecniche e soprattutto organizzative adeguate, al fine di proteggere i dati da trattamenti non autorizzati o illeciti, dal rischio di perdita, di distruzione o di danno accidentale;
- Partecipare ai momenti formativi organizzati dall'Istituto ed assicurare la partecipazione dei propri autorizzati;
- Fornire le informazioni richieste dal Gruppo Aziendale Privacy e segnalare al medesimo ogni questione rilevante in materia e trasmettere tempestivamente istanze e reclami degli interessati, da far pervenire al DPO;
- Comunicare al Gruppo Aziendale Privacy i trattamenti in essere all'interno del proprio settore di competenza, l'inizio di ogni nuovo trattamento e la cessazione o modifica di quelli esistenti, ai fini della compilazione e del continuo aggiornamento del Registro dei trattamenti aziendale;
- Collaborare con il Gruppo Aziendale Privacy e il Servizio ICT Aziendale per la predisposizione del documento della valutazione di impatto sulla protezione dei dati qualora ne ricorrano i presupposti in base all'art. 35 del GDPR;
- Non porre in essere trattamenti di dati diversi e ulteriori senza la preventiva autorizzazione del Titolare del trattamento;
- Provvedere, qualora tra le attività istituzionali della Struttura vi sia la stipula di contratti/convenzioni con soggetti esterni alla organizzazione che comportino il trattamento di dati personali per conto del Titolare del trattamento, alla contestuale stipula o predisposizione del relativo atto di designazione di tali soggetti esterni quali "responsabili del trattamento" a norma dell'art. 28 del GDPR e delle condizioni ivi indicate e trasmettere copia dell'atto di designazione e dell'accettazione della nomina al Gruppo Aziendale Privacy, attraverso l'invio della predetta documentazione agli *Affari Legali e Generali* tramite BABEL, con nota a protocollo che indichi gli estremi cronologici della nomina stessa (decorrenza e periodo di validità), anche ai fini dell'aggiornamento del registro dei trattamenti;
- Comunicare tempestivamente al Gruppo Aziendale Privacy i potenziali casi di *data breach* all'interno della propria struttura e collaborare alla istruttoria del caso al fine di sottoporre al DPO ogni utile e opportuna determinazione in merito.

Allegato 2

ISTRUZIONI di CARATTERE GENERALE impartite dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari, con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente aziendale privacy garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;

- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Istituto che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento.
- email e uso della rete internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di file o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali per gli utenti sull'utilizzo dei servizi informatici IOR consultabili sulla rete intranet (all'indirizzo: *http://intranet.internal.ior.it/documentazione/manuali/regolamento-ict*);
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii.
- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerà porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.);

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Istituto.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. *Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli;*
2. *Informativa per gli utenti sull'utilizzo dei servizi informatici IOR;*
3. *Linee guida in tema di fascicolo sanitario elettronico (FSE) e di Dossier Sanitario;*
4. *Indicazioni sull'acquisizione dei consensi al Dossier Sanitario Elettronico (DSE) e relativi adempimenti in tema di privacy;*
5. *Procedura di data breach;*

a cui si rinvia, reperibili sempre sulle pagine intranet dedicate.

Allegato 3

ATTO DI DESIGNAZIONE
DEL SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 2-quaterdecies del D.Lgs. n. 196/2003, così come modificato dal D.Lgs. n. 101/2018

Il sottoscritto_____

(indicare il nome del Referente Privacy di afferenza)

in qualità di Referente Privacy dell' UO/UOC/……_____

DESIGNA

(indicare NOME e COGNOME)

in qualità di ……

(indicare funzione, ruolo,…)

SOGGETTO AUTORIZZATO AL TRATTAMENTO DEI DATI relativi

AMBITO DEL TRATTAMENTO (sede/i di assegnazione) DESCRIZIONE DEL TRATTAMENTO ARCHIVI BANCHE DATI

A seguito della suddetta designazione Lei è autorizzato a svolgere operazioni di trattamento, per il proprio ambito di competenza, secondo i principi generali di trattamento, le prescrizioni, le istruzioni operative generali impartite dal Titolare e le ulteriori eventuali istruzioni specifiche dal sottoscritto impartite.

Principi di carattere generale:

- ✓ trattare i dati di propria pertinenza in modo lecito, secondo correttezza e trasparenza;
- ✓ trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
- ✓ verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;
- ✓ conservarli nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare (**allegate alla presente**) e sempre consultabili nella sezione Privacy della rete intranet aziendale, dalle prescrizioni e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto in qualità di Referente Privacy di Sua afferenza.

Prescrizioni:

a. Rispettare l'obbligo di riservatezza e segretezza, mantenendo la segretezza delle informazioni di cui venga a conoscenza mediante accesso ai sistemi informativi aziendali, secondo il profilo di autorizzazione assegnato alle proprie credenziali di autenticazione (user e password), corrispondente alla classe di autorizzato di appartenenza;
b. trattare i dati di propria pertinenza in modo lecito, secondo correttezza e trasparenza;
c. trattare i soli dati necessari allo svolgimento delle operazioni da effettuare;
d. verificare che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti e successivamente trattati;

e. conservare i dati nel rispetto delle misure di sicurezza previste dal Regolamento (UE) n. 2016/679, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella sezione Privacy della rete intranet aziendale, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;
f. utilizzare le informazioni e i dati, con cui si entra in contatto per ragioni di lavoro, esclusivamente per lo svolgimento delle attività istituzionali, con la massima riservatezza, secondo quanto definito dalle regole aziendali, per tutta la durata dell'incarico ed anche successivamente al termine di esso, astenendosi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
g. per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su tutti dispositivi in dotazione ad altri operatori e/o di lasciare, in caso di allontanamento anche temporaneo dalla postazione di lavoro il sistema operativo avviato con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
h. conservare correttamente i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che gli stessi siano accessibili a persone non autorizzate mettendo in atto tutte le misure di sicurezza previste dal Regolamento Europeo in materia di protezione dei dati n. 2016/679, dalla normativa nazionale, dalle istruzioni di carattere generale impartite dal Titolare, consultabili nella sezione sopra indicata, e dalle ulteriori eventuali misure di sicurezza impartite dal sottoscritto;
i. astenersi dal comunicare a terzi dati e informazioni (salvo i casi previsti dalla legge);
j. segnalare al sottoscritto eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza, al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
k. informare senza ingiustificato ritardo il soggetto delegato al trattamento di qualunque fatto o circostanza, anche accidentale, che abbia causato perdita, distruzione dei dati, accesso non consentito o comunque non conforme ai principi sopradetti.

La S.V. prende atto di quanto previsto nella presente designazione ed assume la qualifica di soggetto autorizzato al trattamento dei dati personali impegnandosi a:

- ✓ rispettare i principi e le prescrizioni sopraripportate, le istruzioni di carattere generale impartite dal Titolare, allegate al presente atto di designazione e disponibili nella sezione Privacy della rete intranet aziendale, e le eventuali istruzioni che Le verranno eventualmente impartite per l'ambito di competenza e del profilo professionale di appartenenza.

E' fatto obbligo a ciascun professionista autorizzato al trattamento consultare gli aggiornamenti della documentazione aziendale in materia sul sito intranet aziendale nella sezione sopra citata.

Ciò premesso, il presente atto costituisce pertanto conferimento formale dell'autorizzazione al trattamento dei dati connessi allo svolgimento dell'attività lavorativa connessa all'ambito del trattamento sopra individuato, secondo le istruzioni allegate e secondo le prescrizioni sopra riportate. Tale DESIGNAZIONE:

- ha validità per l'intera durata del rapporto di lavoro con l'Istituto;
- viene a cessare al modificarsi del rapporto di lavoro o con esplicita revoca dello stesso.

DICHIARAZIONE DI RICEVIMENTO DELL'ATTO DI DESIGNAZIONE E DI IMPEGNO ALL'OSSERVANZA DELLE ISTRUZIONI ALLEGATE

Il sottoscritto _____

(indicare NOME e COGNOME)

DICHIARA

1. di aver ricevuto la designazione ad autorizzato al trattamento;
2. di aver attentamente letto e compreso il contenuto del presente atto e del suo allegato, e di impegnarsi ad osservare tutte e specifiche istruzioni impartite;
3. di obbligarsi ad osservare le ulteriori direttive/regolamentazioni aziendali reperibili alla sezione intranet dedicata.
4. di dare atto che l'obbligo di riservatezza correlato all'incarico va osservato anche successivamente alla conclusione dello stesso

Data_____

Firma_____

Allegato

ISTRUZIONI di CARATTERE GENERALE impartire dal Titolare a tutti i SOGGETTI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Principi Generali

1. Trattare i dati di propria competenza nel rispetto dei principi di liceità, correttezza e trasparenza.
2. In attuazione del:
    a. principio di minimizzazione dei dati: trattare i soli ed esclusivi dati personali che si rilevino necessari rispetto alle finalità per le quali sono trattati nell'attività a cui ciascun autorizzato è preposto;
    b. principio di limitazione delle finalità: trattare i dati conformemente alle finalità istituzionali del Titolare, limitando il trattamento esclusivamente a dette finalità;
    c. principio di esattezza: garantire l'esattezza, la disponibilità, l'integrità nonché il tempestivo aggiornamento dei dati personali oggetto di trattamento e verificare la pertinenza, completezza e non eccedenza rispetto alle finalità per le quali sono stati raccolti, e successivamente trattati.
3. Utilizzare le informazioni e i dati personali, in particolare i dati c.d. particolari con la massima riservatezza sia nei confronti dell'esterno che del personale interno, per tutta la durata dell'incarico ed anche successivamente al termine di esso.
4. Conservare i dati rispettando le misure di sicurezza, predisposte dal Titolare e/o dal Referente privacy di afferenza garantendone la massima protezione in ogni attività di trattamento.
5. Segnalare al Referente privacy di afferenza eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

6. Astenersi dal comunicare a terzi e/o a diffondere dati ed informazioni appresi in occasione dell'espletamento della propria attività.
7. Partecipare ai corsi formativi in materia di protezione dei dati personali e di sicurezza informatica con le modalità che verranno indicate dal Titolare del trattamento o suo delegato.

Istruzioni operative

ISTRUZIONI PER LO SVOLGIMENTO DELLE OPERAZIONI CARATTERIZZANTI IL PROCESSO DI TRATTAMENTO

- identificazione degli interessati: nell'ambito dell'accesso alle prestazioni, l'autorizzato al trattamento può avere necessità di dover identificare il richiedente un servizio o il soggetto che deve presentare una istanza o una dichiarazione. Si deve procedere a tale verifica con rispetto della volontà dell'interessato, che deve essere invitato con cortesia ad esibire un proprio documento di identità, secondo quanto previsto dall'art.45 del DPR 445/2000 e nel rispetto di eventuali indicazioni operative aziendali;
- raccolta dei dati: prima di procedere all'acquisizione dei dati personali deve essere fornita l'informativa all'interessato o alla persona presso cui si raccolgono i dati, secondo quanto stabilito dagli artt.13 e 14 del Regolamento (UE) 2016/679. Occorre procedere alla raccolta dei dati con la massima cura, verificando l'esattezza dei dati stessi;
- registrazione dei dati: non lasciare a disposizione di estranei supporti, fogli, cartelle e quant'altro;
- al momento della consegna di copie dei documenti ai destinatari è necessario adottare tutte le garanzie di sicurezza, quali l'utilizzo di buste sigillate e l'eventuale acquisizione della delega se presente. L'invio di comunicazioni o di documentazione sanitaria al domicilio del paziente deve essere sempre preceduto dall'autorizzazione di questi ed essere sempre contenuto in busta sigillata, evitando di riportare sulla busta esterna riferimenti a servizi/strutture specifici dell'Azienda che possano in qualche modo essere idonee a rivelare lo stato di salute dell'interessato o a creare una forma di associazione con una qualsivoglia patologia.

ISTRUZIONI PER IL CORRETTO UTILIZZO DEGLI STRUMENTI AZIENDALI PER IL TRATTAMENTO DEI DATI PERSONALI

- Per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali a disposizione altrui e/o di lasciare avviato, in caso di allontanamento anche temporaneo dalla postazione di lavoro, il sistema operativo con inserita la propria password, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
- email e uso della internet: la posta elettronica può essere utilizzata per scopi di ufficio. Occorre prestare particolare attenzione alla spedizione, a mezzo di posta elettronica, di files o di messaggi contenti dati riferiti alla salute. A tal specifico fine si rinvia alle disposizioni aziendali per gli utenti sull'utilizzo dei servizi informatici IOR consultabili sulla rete intranet (all'indirizzo: *http://intranet.internal.ior.it/documentazione/manuali/regolamento-ict*);
- uso di software: è vietato installare e usare qualunque software senza la previa autorizzazione del Titolare e/o Suo delegato. Si ricorda che l'uso di software contraffatto, ovvero senza licenza d'uso, costituisce un illecito di natura sia penale sia civile, secondo

quanto previsto dalla legge sul diritto d'autore (legge 633/1941), così come integrata dal d.lgs.518/1992 e ss.mm. ed ii..

- protezione degli strumenti di lavoro: in caso di assenza, anche momentanea, dalla propria postazione di lavoro, devono essere adottate misure idonee ad escludere che soggetti non autorizzati possano acquisire la conoscenza di informazioni o accedere alle banche dati. A tal proposito, a titolo meramente esemplificativo, si consiglia di adottare un sistema di oscuramento (c.d. screensaver) dotato di password, ovvero di uscire dal programma che si sta utilizzando o, in alternativa, occorrerò porre lo strumento elettronico in dotazione in posizione di stand-by o spegnere l'elaboratore che si sta utilizzando. In caso di abbandono, anche temporaneo, dell'ufficio, l'autorizzato deve porre la massima attenzione a non lasciare incustoditi i documenti cartacei contenenti dati riferiti alla salute e altri tipologie di dati c.d "particolari" (es. adesione ad un sindacato) sulla scrivania o su tavolini di reparto: è infatti necessario identificare un luogo sicuro di custodia che dia adeguate garanzie di protezione da accessi non autorizzati (un armadio o un cassetto chiusi a chiave, una cassaforte, ecc.);

ISTRUZIONI RIGUARDANTI RAPPORTI DI FRONT OFFICE

- Rispetto della distanza di sicurezza: per quanto riguarda gli operatori di sportello deve essere prestata attenzione al rispetto dello spazio di cortesia e se del caso devono essere invitati gli utenti a sostare dietro la linea tracciata sul pavimento ovvero dietro le barriere delimitanti lo spazio di riservatezza;
- obbligo di riservatezza e segretezza: mantenere l'assoluta segretezza sulle informazioni di cui venga a conoscenza nel corso delle operazioni di trattamento. La diffusione di dati idonei a rivelare lo stato di salute è tassativamente vietata;
- controllo dell'identità del richiedente nel caso di richieste di comunicazioni di dati (presentate per telefono): occorre verificare l'identità del soggetto richiedente, ad esempio formulando una serie di quesiti (accertamento sommario).

Gli obblighi sopra descritti fanno parte integrante della prestazione lavorativa e pertanto per il personale dipendente o assimilato sono dovuti in base al contratto di lavoro sottoscritto con l'Azienda/Istituto.

Le suddette istruzioni sono integrabili dai singoli Referenti Privacy di afferenza attraverso ulteriori istruzioni di carattere specifico, anche per gruppi omogenei di funzioni.

Le istruzioni di cui sopra sono altresì integrate dalle puntuali disposizioni aziendali in materia di protezione dei dati personali:

1. *Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli;*
2. *Informativa per gli utenti sull'utilizzo dei servizi informatici IOR;*
3. *Linee guida in tema di fascicolo sanitario elettronico (FSE) e di Dossier Sanitario;*
4. *Indicazioni sull'acquisizione dei consensi al Dossier Sanitario Elettronico (DSE) e relativi adempimenti in tema di privacy;*
5. *Procedura di data breach;*

a cui si rinvia, reperibili sempre sulle pagine intranet dedicate.

SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Istituto Ortopedico Rizzoli di Bologna
Istituto di Ricovero e Cura a Carattere Scientifico

FRONTESPIZIO DELIBERAZIONE

AOO: DA

REGISTRO: Deliberazione

NUMERO: 0000402

DATA: 23/12/2019 09:56

OGGETTO: ADOZIONE DEL DOCUMENTO “LINEE GUIDA PER L’APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL D.LGS. 30.06.2003 N. 196"

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Cavalli Mario in qualità di Direttore Generale
Con il parere favorevole di Landini Maria Paola - Direttore Scientifico
Con il parere favorevole di Rolli Maurizia - Direttore Sanitario
Con il parere favorevole di Cilione Giampiero - Direttore Amministrativo

Su proposta di Laura Mandrioli - Affari Legali e Generali che esprime parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità del presente atto

CLASSIFICAZIONI:

- [06-04]

DESTINATARI:

- Collegio sindacale
- Affari Legali e Generali
- Dipartimento Rizzoli - Sicilia
- Dipartimento Patologie Complesse
- Servizio Bilancio e Coordinamento Processi Economici
- Direzione Servizio di Assistenza Infermieristica, Tecnica e della Riabilitazione (DAITER)
- Staff Direzione Sanitaria (Qualita', Risk Management, Ingegneria Clinica)
- Ufficio Relazioni con il Pubblico
- Comunicazione e Relazione con i Media

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000402_2019_delibera_firmata.pdf	Cavalli Mario; Cilione Giampiero; Landini Maria Paola; Mandrioli Laura; Rolli Maurizia	443C0A34D3053D3367ACFA3FFD6E46D0FAD44475D4E94D5F24EA8F829F59E19C
DELI0000402_2019_Allegato1.pdf:		04E20449FDF9EB4AFB8993A0B1B39AC7C1DFF42759CDB141177B55922689C081

DELIBERAZIONE

OGGETTO: ADOZIONE DEL DOCUMENTO "LINEE GUIDA PER L'APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL D.LGS. 30.06.2003 N. 196"

IL DIRETTORE GENERALE

PREMESSO CHE:

- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (in seguito "GDPR"), applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018, nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato principalmente sulla valutazione dei rischi sui diritti e le libertà degli interessati, attribuisce ai Titolari del trattamento (nel caso, a questa Azienda USL) il compito di assicurare ed essere in grado di comprovare il rispetto dei principi applicabili al trattamento dei dati personali e di adottare le misure che ritiene a ciò più idonee ed opportune (c.d. principio di responsabilizzazione o *accountability*);
- il "sistema privacy" delineato dal GDPR implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza dei rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati personali quale parte integrante dell'intero assetto informativo di un'organizzazione, con particolare attenzione ai dati di salute (ivi compresi i dati genetici);

RITENUTO che la piena realizzazione del suddetto principio di *accountability* e del nuovo approccio che ne deriva all'interno della organizzazione aziendale, passino anche attraverso la emanazione di un nuovo **Reg olamento aziendale in materia di protezione dei dati personali**, che dia atto dell'adeguamento operato dalla Azienda alla nuova normativa di settore (Regolamento UE n. 679/2016 e D. Lgs. 196/2003 come modificato dal D. Lgs. 101/2018) e fornisca una linea guida per l'applicazione della materia nei vari ambiti in cui quotidianamente si esplica la attività istituzionale della Azienda;

RITENUTO inoltre che un nuovo Regolamento in materia di protezione dei dati personali possa costituire uno strumento di ausilio affinché il trattamento dei dati personali da parte degli operatori dell'Istituto avvenga nel rispetto dei diritti, delle libertà fondamentali, della dignità di tutti gli interessati (utenti, pazienti e dipendenti), con particolare riferimento alla loro riservatezza e alla loro identità personale;

CONSIDERATO inoltre che la adozione del suddetto Regolamento aziendale in materia di protezione dei dati personali consegue l'obiettivo di "Predisposizione di un documento aziendale (regolamento, procedura) di definizione della *policy* aziendale in tema di trattamento dei dati personali", di cui alla DGR N. 977/2019 recante "Linee di programmazione e di finanziamento delle Aziende e degli Enti del Servizio sanitario regionale per l'anno 2019";

VISTE le seguenti Delibere con le quali questo Istituto ha via via realizzato operazioni di adeguamento al GDPR e il cui contenuto si intende qui completamente confermato:

delibera n. 225 del 27/10/2017
delibera n. 320 del 21/12/2018
delibera n. 160 del 29/06/2018
delibera n. 62 del 25/02/2019
delibera n. 123 del 24/04/2019
delibera n. 218 del 24/07/2019
delibera n. 368 del 03/12/2019

Acquisito il parere favorevole, sul testo delle linee guida, da parte del DPO;

RITENUTO di formalizzare l'adozione del documento denominato " **LINEE GUIDA PER L'APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL D.LGS. 30.06.2003 N. 196 a**llegato parte integrante e sostanziale del presente provvedimento, che, unitamente alle delibere più sopra citate delinea il nuovo assetto della privacy policy aziendale, superando le precedenti disposizioni interne e contestualmente aggiorna e recepisce le modulistiche citate nel medesimo documento;

Delibera

1. di approvare il testo del documento denominato " **LINEE GUIDA PER L'APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL D.LGS. 30.06.2003 N. 196"**
2. **d**i allegare quale parte integrante del presente atto il documento di cui al punto 1.

Responsabile del procedimento ai sensi della L. 241/90:
Laura Mandrioli

LINEE GUIDA PER L'APPLICAZIONE DEL REGOLAMENTO UE 2016/679 E DEL D.LGS. 30.06.2003 N. 196

PARTE PRIMA
DISPOSIZIONI GENERALI

Art. 1

PRINCIPI GENERALI

1. Il trattamento dei dati personali nell'ambito di ogni articolazione delle strutture dell'Istituto Ortopedico Rizzoli (di seguito anche abbreviato in "IOR") viene svolto garantendo a chiunque il rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

2. Il trattamento dei dati personali viene disciplinato dall'Istituto Ortopedico Rizzoli assicurando un elevato livello di tutela dei diritti e delle libertà di cui sopra nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati e per l'adempimento degli obblighi da parte del titolare del trattamento.

3. Il presente regolamento si applica al trattamento dei dati personali, effettuato dall'Istituto Ortopedico Rizzoli.

Art. 2

TRATTAMENTO DI DATI PERSONALI

1. Ai fini del presente atto si intende per:

a. "Regolamento UE": il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
b. "Codice": il decreto legislativo 30 giugno 2003 n. 196 rubricato "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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.

2. Ai fini dell'individuazione del significato dei termini utilizzati nel presente atto si applicano le definizioni di cui all'art. 4 del Regolamento UE, di cui all'art. 2-ter e 22, comma 2, del Codice.

Art. 3

TITOLARE E RESPONSABILE DEL TRATTAMENTO

1. Le presenti linee guida rappresentano lo strumento con il quale l'Istituto Ortopedico Rizzoli specifica e fissa i compiti e le regole alle quali devono attenersi le strutture aziendali in materia di trattamento dei dati, fermo restando quanto

dispongono il Regolamento UE, il Codice e le altre norme in materia di protezione dei dati.

2. Il Titolare del trattamento dei dati è l'Istituto Ortopedico Rizzoli di Bologna , persona giuridica di diritto pubblico, che esercita i poteri propri del titolare per mezzo del Legale Rappresentante dell'Ente il quale può agire d'ufficio o su impulso e/o proposta del Responsabile della Protezione dei Dati.

3. L'Istituto Ortopedico Rizzoli, designa inoltre responsabili del trattamento le persone fisiche e giuridiche delle quali si avvale per il trattamento dei dati, ivi compresi i soggetti che procedono al trattamento dei dati nel contesto di un servizio concesso in appalto, contratto e/o convenzione, solo se presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento UE e garantisca la tutela dei diritti dell'interessato.

4. Il Direttore Generale può delegare ai dirigenti la nomina dei responsabili di trattamento con apposito atto.

Art. 4

REFERENTI PRIVACY

1. Fermi restando gli obblighi e le prerogative in capo al Titolare, all'interno dell'Ente sono stati individuate delle figure di riferimento per l'applicazione della normativa e per coadiuvare il Direttore Generale nella gestione della policy aziendale in tema di trattamento dei dati. Questi soggetti sono definiti " referenti" ed i loro compiti e responsabilità sono declinati nella delibera organizzativa n. 320 del 21/12/2018, cui si fa rinvio. In particolare, nei propri ambiti di competenza, provvedono a:

- **a)** garantire il pieno rispetto delle vigenti disposizioni legislative in materia di trattamento, compreso il profilo relativo alla sicurezza, e le connesse procedure aziendali da parte degli incaricati;
- **b)** fornire indicazioni e sorvegliare affinché nella struttura di PROPRIA competenza non vengano svolti trattamenti autonomi di dati e affinché non vengano trattati dati personali per finalità diverse da quelle per le quali sono stati raccolti e successivamente trattati.
- **c)** verificare la liceità e la correttezza dei trattamenti effettuati, anche attraverso controlli periodici e verificare la qualità e la quantità dei dati oggetto dei trattamenti di competenza con specifico riferimento ai requisiti di esattezza, aggiornamento, pertinenza, non eccedenza rispetto alle finalità del trattamento;
- **d)** a provvedere agli adempimenti per la nomina dei responsabili del trattamento di cui all'art. 28 del Regolamento UE 2016/679, eventualmente anche previa acquisizione del parere del Responsabile della Protezione dei Dati, qualora sia di competenza la stipula di contratti che comportino il trattamento di dati personali;
- **e)** fornire indicazioni e dare disposizioni, anche in accordo o su richiesta del Responsabile della Protezione dei dati, per l'adeguamento alle misure di sicurezza organizzative di cui all'art. 32 del Regolamento UE 2016/679

f) informare il Titolare, e/o il Responsabile della Protezione dei dati laddove sia previsto un nuovo trattamento, ai fini della valutazione della necessità e/o opportunità di provvedere alla valutazione di impatto ai sensi dell'art. 35 del Regolamento, alla consultazione preventiva ai sensi dell'art. 36 del Regolamento e alla predisposizione del registro dei trattamenti ai sensi dell'art. 30 del Regolamento, e collaborare con i medesimi alla sua predisposizione;

g) segnalare informare il Titolare, e/o il Responsabile della Protezione dei dati, dell'avvenuta violazione dei dati personali di cui all'articolo 33 del Regolamento UE, collaborando con i predetti laddove per la compilazione dell'atto di notifica al Garante per la protezione dei dati personali e per la comunicazione agli interessati;

h) collaborare con il Gruppo Privacy Aziendale, all'aggiornamento del Registro delle Attività di trattamento;

i) provvedere ad ogni altro atto o adempimento necessario per l'applicazione ai trattamenti di dati dell'Azienda del Regolamento UE 2016/679 e di ogni altra norma in materia, europea e nazionale, anche in relazione alle indicazioni del Titolare, o Responsabile della Protezione dei dati, collaborando a tal fine con quest'ultimo e, ai sensi dell'art. 31 del Regolamento, con il Garante per la protezione dei dati.

Art. 5

AUTORIZZATI AL TRATTAMENTO DEI DATI

1. Ai fini dell'autorizzazione al trattamento prevista dall'art. 2-quaterdecies del d.lgs. 196/03, con **delibera del Direttore Generale n. 320 del 21/12/2018** sono stati individuati i soggetti autorizzati al trattamento dei dati personali e le modalità di designazione.

2. Per "**soggetti autorizzati"** si intendono tutti i dipendenti/collaboratori dell'Istituto, ognuno per il proprio specifico ambito di competenza professionale, i quali sono tenuti alla osservanza delle istruzioni – contenute nell'**allegato 2** alla delibera - impartite dal Titolare per il corretto trattamento dei dati personali, oltre ad ulteriori istruzioni che il Titolare del trattamento, anche per il tramite dei Referenti privacy, impartirà loro con riferimento a particolari trattamenti di dati;

3. Per i dipendenti viene inserito uno specifico richiamo nel contratto di lavoro.
4. Laddove possibile, analogo richiamo viene inserito nelle altre forme di contratto e/o di conferimento incarico variamente denominati (a titolo non esaustivo: legali, borsisti, tirocinanti, stagisti ecc.);
5. Per i soggetti per i quali non è prevista la sottoscrizione di un contratto/accordo individuale (come per frequentatori volontari, lavoratori socialmente utili, specializzandi ecc) l'ufficio amministrativo che cura gli adempimenti finalizzati all'istaurazione del rapporto con l'Istituto, provvede di

volta in volta all'autorizzazione al trattamento dei dati attraverso l'atto di designazione allegato sub documento 3) alla delibera;

6. L'ambito dell'autorizzazione coincide con le attività del profilo e all'unità operativa di afferenza.

ART. 6

GRUPPO AZIENDALE PRIVACY

1. il **Gruppo Aziendale Privacy (GAP)** , istituito con la delibera citata n. 320 del 21/12/2018 ha il compito di assicurare un presidio aziendale per quel che concerne gli adempimenti organizzativi e procedurali derivanti dalle nuove disposizioni normative in materia di protezione dei dati personali.

Il Gruppo Aziendale Privacy svolge in particolare le seguenti attività:

- supporta i referenti privacy nell'adozione di misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Azienda a seguito degli approfondimenti e delle analisi effettuate dal Coordinatore del GAP con il DPO nel Tavolo di area metropolitana;
- supporta i referenti privacy nell'aggiornamento del Registro dei trattamenti di dati personali effettuati dalle strutture di appartenenza e nella eventuale valutazione di impatto, in collaborazione con il Servizio ICT;
- fornisce supporto alle verifiche di sicurezza svolte dal Servizio ICT e/o dal DPO;
- coordina le richieste di parere da sottoporre al DPO formulate dai singoli referenti privacy.

2. Il Coordinatore del GAP è l'interlocutore ufficiale del DPO. Il DPO rappresenta, pertanto, il riferimento principale per il Coordinatore del GAP.

3. Con Delibera 218 del 24/7/2019 sono stati definiti i rapporti fra il Gruppo Aziendale Privacy , il coordinatore e il DPO, di cui al successivo articolo

ART. 7

DATA PROTECTION OFFICER

1. Il Regolamento UE 2016/679 introduce la figura del Responsabile della protezione dei dati (di seguito, DPO) (artt. 37-39), e prescrive l'obbligo per il titolare o il responsabile del trattamento di designare il *DPO «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali»* (art. 37, paragrafo 1, lett a).

2. Con delibera 160 del 29/6/2018 questo Istituto ha designato il Data Protection Officer, DPO.

3. Il DPO, nominato congiuntamente dalle Aziende dell'Area Metropolitana di Bologna, svolge – fra le altre - le seguenti attività:

- informa e fornisce consulenza all'Ente, in ordine agli obblighi derivanti dal Regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati assicura attività di informazione/consulenza ai dipendenti che, in qualità di autorizzati al trattamento, eseguono operazioni di trattamento dati;
- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché delle policy aziendali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti, coordinando il gruppo dei referenti/responsabili privacy aziendali individuati dalle singole Aziende/Enti;
- fornisce, se richiesti, pareri anche scritti in merito alla valutazione di impatto sulla protezione dei dati e ne sorveglia lo svolgimento;
- coopera con l'Autorità Garante per la protezione dei dati personali, fungendo da punto di contatto per la stessa su questioni connesse al trattamento (tra cui la consultazione preventiva); effettua eventuali consultazioni e ne cura in generale i rapporti;
- supporta le strutture aziendali deputate alla tenuta del Registro del trattamento al fine di uniformarne la predisposizione;
- promuove iniziative congiunte tra le Aziende/Enti affinché l'applicazione della normativa in materia di protezione dei dati personali, nonché delle policy aziendali, sia sviluppata secondo linee applicative omogenee e coerenti nelle singole Aziende/Enti;

PARTE TERZA
TRATTAMENTO DEI DATI PERSONALI PER FINALITA' AMMINISTRATIVE

ART. 8

INFORMATIVA PER I TRATTAMENTI EFFETTUATI AI SOLI FINI AMMINISTRATIVI

1. L'Istituto Ortopedico Rizzoli può trattare i dati personali per fini amministrativi esclusivamente ai fini di cui all'articolo 6, par. 2, lettera e) del Regolamento UE, ovvero quanto è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investita l'Azienda, e ai fini dell'articolo 9, par. 2, lett g) del medesimo Regolamento, ovvero quando il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri.

2. I Referenti sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del Regolamento UE. Si comportano analogamente gli autorizzati al trattamento, qualora svolgano attività che comportino tale opportunità (ad es. operatori di front office).

3. Le informazioni sono rese note alla platea degli interessati mediante pubblicazione nel sito internet aziendale, e supportate eventualmente da modulistica cartacea.

ART. 9

INFORMATIVE VARIE

1. L'Istituto Ortopedico Rizzoli può inoltre trattare i dati per i fini di cui all'articolo 6, par. 2, lett. b) del Regolamento UE, ovvero quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso, nonché per i fini di cui all'art. 6, par. 2, lett. b) del medesimo Regolamento UE, ovvero quando il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale.

2. I Referenti sono tenuti a porre in essere ogni atto necessario per fornire agli interessati le informazioni di cui agli articoli 13 e 14 del Regolamento UE nel rispetto delle indicazioni fornite dal Titolare e/o dal Responsabile della Protezione dei Dati. In ogni caso le predette informazioni dovranno essere inserite nei relativi atti contrattuali e, laddove il rapporto sia soggetto a procedure concorsuali, le predette informazioni dovranno essere necessariamente contenute nei bandi di concorso, di gara, nelle lettere di invito e/o avvisi pubblici.

3.Referenti privacy, per i trattamenti di rispettiva competenza, anche su proposta del Responsabile della protezione dei dati, curano che le informazioni di cui al comma 1 siano rese note anche mediante pubblicazione nel sito internet aziendale o **piattaforme condivise (GRU)** (es. Informativa sito internet e cookies, informativa URP, informativa dipendenti) e supportate eventualmente da modulistica cartacea (punti di accesso). Altre specifiche informative vengono consegnate agli interessati (es. per foto e video) o allegate alle comunicazioni a riscontro delle istanze presentate (es. richiesta di risarcimento e comunicazione di apertura sinistro)

- **L'informativa privacy – policy** (destinata agli utenti che consultano il sito web dell'Istituto) è stata pubblicata, a far tempo dal 14.11.2018, sul sito dello IOR all'indirizzo web *http://www.ior.it/privacy*
- **L'informativa privacy per la gestione diretta dei sinistri** è stata pubblicata, a far tempo dal 15.03.2019, nella rete intranet dello IOR quale allegato alla procedura **PG 02 DG Percorso operativo di gestione diretta dei sinistri** all'indirizzo web *http://intranet.internal.ior.it/modulistica/mod-01-pg-02-dg-informativa-trattamento-dati*

- L'informativa privacy per segnalazioni / **reclami URP:** a far tempo dal 21.03.2019 sono stati pubblicati sul sito dello IOR – all'indirizzo *http://www.ior.it/curarsi-al-rizzoli/infourp* - l'informativa privacy per l'URP aggiornata secondo le disposizioni del GDPR e il modulo per le segnalazioni con riportato, in calce, la seguente dicitura (in sostituzione a quella in uso ante GDPR):
"Avvertenza: con riferimento alla normativa sul trattamento dei dati personali e tutela della privacy, si fa presente che i dati personali raccolti con il presente modulo saranno utilizzati dall'Ente allo scopo di migliorare la qualità delle proprie prestazioni. Restano fermi per l'interessato tutti i diritti riconosciuti dalla normativa sulla protezione dei dati personali vigente in Italia: D.lgs 196/2003 (Codice in materia di protezione dei dati personali) e successive modifiche e Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.
Il trattamento dei dati personali, pertanto, sarà effettuato nel rispetto dei principi di liceità, trasparenza e correttezza, indispensabilità, pertinenza e non eccedenza, mediante strumenti anche informatici idonei a garantirne sicurezza e riservatezza.

In merito alle specifiche modalità di trattamento dei dati, all'ambito di comunicazione degli stessi e ai diritti dell'interessato si rinvia alla lettura delle "Informazioni sul trattamento dei dati personali" reperibili sul sito internet dell'Istituto all'indirizzo: .....

L'Ufficio Relazioni con il pubblico è contattabile anche via telefono (.....) fax (.....) oppure e-mail (.....)"

ART.10

TRATTAMENTO DEI DATI NEGLI ATTI SOGGETTI A PUBBLICAZIONE

1. Gli atti dell'Azienda soggetti a pubblicazione contenenti dati particolari di cui agli articoli 9 e 10 del Regolamento UE, i provvedimenti disciplinari e gli atti concernenti i minori, non dovranno essere pubblicati in forma identificativa

2. Sarà cura dei referenti valutare le modalità per pseudoanonimizzarli, eventualmente previa consultazione con il Responsabile per la protezione dei dati, garantendo in ogni caso al diretto interessato la possibilità di identificarsi.

PARTE QUARTA
TRATTAMENTO DI DATI PERSONALI E PARTICOLARI PER FINALITA' DI DIAGNOSI, ASSISTENZA, TERAPIA SANITARIA

ART. 11

MODALITA' PER L'INFORMATIVA AL PAZIENTE

1. Con riferimento al trattamento dei dati per finalità di diagnosi, assistenza, terapia sanitaria IOR rende le informazioni previste dagli articoli 13 e 14 del Regolamento UE secondo le modalità concordate con il Responsabile della Protezione dei dati.

2. In ogni caso tali informazioni sono fornite, anche sinteticamente ma con rinvio al sito internet aziendale, al momento della richiesta di accesso alla presentazione sanitaria nonché attraverso specifica cartellonistica situata nelle zone di accesso e transito dei pazienti e modulistica cartacea a disposizione nei punti di accettazione visite o ricoveri.

L'informativa privacy generale per i pazienti / **assistiti** è stata pubblicata, a far tempo dal 19.03.2019, sul sito dello IOR all'indirizzo web *http://www.ior.it/il-rizzoli/informazioni-sul-trattamento-e-sulla-protezione-dei-dati-personali*

Quanto alla diffusione dell'informativa privacy "generale" è stata **inserita** negli SMS di conferma delle prenotazioni telefoniche di visite mediche la dicitura "informativa privacy all'indirizzo *http://www.ior.it/il-rizzoli/informazioni-sul-trattamento-e-sulla-protezione-dei-dati-personali* ;

ed inserita nei promemoria cartacei rilasciati al momento della prenotazione di visite agli sportelli la dicitura "informativa privacy all'indirizzo *http://www.ior.it/il-rizzoli/informazioni-sul-trattamento-e-sulla-protezione-dei-dati-personali"*

I cartelli sono stati posizionali nei punti di accettazione ambulatoriale e ricoveri, nonché in sala d'aspetto Pronto Soccorso.

ART. 12

TRATTAMENTO DATI GENETICI

1. Si richiama il Provvedimento del Garante per la protezione dei dati personali n. 146 del 05.06.2019 recante le prescrizioni relative al trattamento di categorie particolari di dati, con il quale sono state individuate, ex art. 21 comma 1 del d.lgs. 101/2018, le prescrizioni contenute nella Autorizzazione generale n. 9 del 15.12.2016 (afferente il trattamento dei dati personali per scopi di ricerca scientifica) che risultano compatibili con il Regolamento UE 2016/679 e con il d.lgs. 196/2003, come modificato e adeguato dal d.lgs. 101/2018.

2. Ai sensi del suddetto Provvedimento n. 146 del 05.06.2019 con il quale il Garante ha individuato, ex art. 21 comma 1 del d.lgs. 101/2018, le prescrizioni contenute nella Autorizzazione generale n. 8 del 15.12.2016 (relativa al trattamento dei dati genetici) che risultano compatibili con il Regolamento UE 2016/679 e con il d.lgs. 196/2003, come modificato e adeguato dal d.lgs. 101/2018, il trattamento dei dati personali e genetici forniti si svolge nel rispetto dei diritti, delle libertà fondamentali, della dignità

dell'Interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. In particolare vengono trattati soltanto nella misura in cui sono indispensabili, altri dati relativi all'origine, agli stili di vita e alla vita sessuale, ecc. Inoltre i dati ed i relativi campioni sono trattati esclusivamente da personale autorizzato e l'accesso ai sistemi informatici ed ai locali ove essi sono custoditi è controllato mediante idonee misure di sicurezza.

3. Il campione è identificato con un codice: i dati personali/sensibili raccolti, ad eccezione del nominativo, sono registrati, elaborati e conservati unitamente a tale codice.

4. Soltanto il titolare del trattamento dei dati e i soggetti da questi specificatamente delegati/autorizzati, potranno collegare questo codice al nominativo dell'interessato.

5. Per la custodia e la sicurezza dei dati genetici e dei campioni biologici sono adottate le seguenti cautele:

- la conservazione, l'utilizzo e il trasporto dei campioni biologici sono posti in essere con modalità volte a garantirne la qualità, l'integrità, la disponibilità e la tracciabilità;

- per la trasmissione dei dati genetici, si ricorre preferibilmente a canali di comunicazione protetti, anche di tipo web application, che garantiscano l'identità digitale del server che eroga il servizio e della postazione client da cui si effettua l'accesso ai dati, ricorrendo a certificati digitali emessi in conformità alla legge da un'autorità di certificazione; se necessario ricorrere all'invio di relazioni/referti genetici tramite messaggi di posta elettronica, la trasmissione dei dati deve avvenire in forma di allegato con cifratura dei dati o con trasmissione con mittente e destinatario di Pec;

- i dati genetici e i campioni biologici contenuti in elenchi, registri o banche di dati, sono trattati con tecniche di cifratura o di pseudonimizzazione o di altre soluzioni che, considerato il volume dei dati e dei campioni trattati, li rendono temporaneamente inintelligibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità, in modo da ridurre al minimo i rischi di conoscenza accidentale e di accesso abusivo o non autorizzato. Laddove gli elenchi, i registri o le banche di dati siano tenuti con strumenti elettronici e contengano anche dati riguardanti la genealogia o lo stato di salute degli interessati, le predette tecniche devono consentire, altresì, il trattamento disgiunto dei dati genetici e sanitari dagli altri dati personali che permettono di identificare direttamente le persone interessate.

6. Sono in uso presso l'Istituto le idonee informative per la raccolta dei consensi specifici sul trattamento dei dati genetici , anche ai fini del trattamento dati nell'ambito delle biobanche.

Art. 13
DOSSIER SANITARIO ELETTRONICO

1. Il trattamento dei dati mediante dossier sanitario è regolato secondo le seguenti disposizioni:

- Linee guida del Garante in materia di Dossier sanitario del 4 giugno 2015
- Provvedimento del Garante n. 273 "Dossier sanitario elettronico e trattamento di dati personali da parte di un'azienda ospedaliera - 22 giugno 2016
- Linee Guida Regione Emilia Romagna per la corretta gestione del Dossier Sanitario Elettronico,
- Nuovo Codice Privacy – D.lgs 196/2003 aggiornato con il D.lgs 101/2018 ed in particolare art. 110 bis comma 4 Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.

- Documento di sintesi allegato al Regolamento ICT (approvato con delibera n. 225 del 27/10/2017) , che individua i profili autorizzati al trattamento, le modalità, i termini, i tempi .

2. Il DSE può essere costituito esclusivamente con il consenso del paziente e le informazioni sanitarie in esso contenute o trattate sono accessibili ai professionisti sanitari autorizzati per finalità di cura e per il tempo in cui si articola la presa in carico del paziente. Stante la natura di Istituto di Ricovero e Cura a Carattere Scientifico di questo Ente, l'accesso al DSE è consentito anche ai professionisti autorizzati per finalità di ricerca. In questo caso la visualizzazione dei dati contenuti del DSE avverrà con la modalità dell'accesso giustificato.
3. Le informazioni contenute nel dossier consentono al personale sanitario aziendale di avere un quadro clinico il più completo possibile e permettono ai ricercatori di perseguire gli scopi di ricerca che caratterizzano la mission di questo Istituto.
4. E' prevista, per questo specifico trattamento, una informativa ad hoc ed una raccolta del consenso attraverso il sistema informativo ospedaliero.
   L'informativa è presente sul sito IOR all'indirizzo: http://www.ior.it/curarsi-al-rizzoli/informativa-e-consenso-il-dossier-sanitario-elettronico.

5. Il consenso è libero e revocabile in qualunque momento .
6. L'accesso al dossier è protetto ed è riservato ai soggetti autorizzati, mediante procedure di autentificazione, che permettono di identificare e tracciare

l'identità dell'operatore, che abbia accesso alle informazioni trattate tramite DSE.

ART. 14

GARANZIE E MISURE PER IL RISPETTO DEI DIRITTI DEI PAZIENTI

1. Al fine di garantire il rispetto dei diritti, delle libertà fondamentali, della dignità, della riservatezza e della protezione dei dati degli interessati, nonché del segreto professionale, all'interno di ogni struttura erogatrice di prestazioni sanitarie dell'Istituto Ortopedico Rizzoli sono adottate misure operative, atte a garantire la protezione dei dati, tra le quali:

a. soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;
b. l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;
c. soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;
d. cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;
e. il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;
f. la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, rispettando eventuali contrarie manifestazioni di volontà da parte degli interessati;
g. la sottoposizione del personale autorizzato, che sia tenuto per legge al segreto professionale, a regole di condotta analoghe al segreto professionale.

2. La copia della cartella clinica e di altra documentazione sanitaria deve essere consegnata all'interessato o a persona munita di apposita delega sottoscritta dell'interessato stesso e autenticata nelle forme di cui all'art. 38 del DPR 445/2000.

3. Eventuali richieste di presa visione o di rilascio di copia della cartella clinica o dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi

dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:

a. di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato e, quindi, consistente in un diritto della personalità o in un altro diritto o libertà fondamentale ed inviolabile;
b. di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato o consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

4. Le ricette contenenti prescrizioni relative a stupefacenti e sostanze psicotrope, di cui deve essere accertata l'identità dell'interessato, devono essere conservate separatamente da ogni altro documento che non ne richiede l'utilizzo.

ART.15

ALTRE MISURE OPERATIVE PER TRATTAMENTO DATI SU SUPPORTO CARTACEO

1. IL personale autorizzato che proceda alla eliminazione di stampe e fotocopie è tenuto a distruggere fisicamente i supporti in modo da impedire la ricostruzione o comunque da renderla non facilmente accessibile a terzi non autorizzati.
2. La trasmissione interna ed esterna di corrispondenza e di documentazione contenente dati particolari dovrà essere effettuata necessariamente in busta chiusa e sigillata che riporti il nominativo del destinatario.
3. Laddove necessario per finalità di diagnosi e terapia o per la corretta alimentazione del paziente, le domande relative alla convinzione religiosa dell'interessato devono essere formulate in modo generico tale da non arrecare pregiudizio e disagio allo stesso.

PARTE SESTA

ART.16
TRATTAMENTI DEI DATI RELATIVI ALLA SALUTE PER FINALITÀ DI RICERCA

1. Il trattamento ai fini di ricerca scientifica è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, così come richiamato all'articolo 89, paragrafo 1, del GDPR, volte a garantire il rispetto del principio della minimizzazione dei dati.

2. Nei trattamenti per finalità di ricerca scientifica l'Istituto applica le prescrizioni del Garante per la protezione dei dati personali e assicura la diffusione e il rispetto delle regole deontologiche di cui all'allegato A.4 del D. Lgs. n. 196/2003 fra tutti coloro che sono coinvolti nel trattamento dei dati personali realizzato nell'ambito delle attività di ricerca; segnala, inoltre, al Garante le violazioni delle regole deontologiche di cui viene a conoscenza.

3. Ai sensi di quanto previsto dall'art. 110 del D. Lgs. 196/2003, così come modificato dal D. Lgs. n. 101/2018, il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è necessario quando la ricerca è effettuata in base a disposizioni di legge o regolamento o al diritto dell'Unione Europea in conformità all'articolo 9, paragrafo 2, lettera j), del GDPR, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-bis del D.Lgs. 502/92, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del GDPR.

4. Il consenso non è inoltre necessario quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di ricerca. In tali casi il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato e il programma di ricerca è oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del GDPR.

5. In base al D.lgs 196/2003 aggiornato con il D.lgs 101/2018 ed in particolare art. 110 bis comma 4 non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento.

PARTE SETTIMA
MISURE TECNICHE E ORGANIZZATIVE

ART. 17
SICUREZZA INFORMATICA

1. In materia di trattamento dei dati personali con strumenti informatici, con delibera n. 225 del 27/10/2017 e' stato approvato il Regolamento IOR per l'utilizzo dei sistemi informatici aziendali

2. Il regolamento ha ad oggetto, in particolare, le norme per l'accesso e l'utilizzo dei seguenti servizi: posta elettronica, rete di telecomunicazione (dati, voce, immagini), Internet e sistemi informativi aziendali, postazioni di lavoro aziendali fisse e mobili, firma digitale e carta nazionale dei servizi, attrezzature informatiche personali.

3. Le politiche di sicurezza sono inoltre descritte nei documenti che riportano lo stato dell'arte e le azioni volte a garantire l'attività dell'Ente. Questi sono:

a) il piano di **Continuità Operativa**, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive.
b) il piano di **Disaster Recovery,** che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

4. Per tali aspetti si rinvia allo " Studio di fattibilità tecnica" e agli altri documenti allegati **alla delibera n 62 del 25/02/2019.**

ART. 18
DATA BREACH

1. Ogni responsabile o soggetto autorizzato al trattamento dei dati personali è tenuto ad informare senza ingiustificato ritardo del possibile caso di violazione dei dati personali (data breach) di cui agli art. 33 e 34 del GDPR. Ogni interessato può inoltre segnalare al titolare del trattamento dei dati un possibile caso di violazione dei dati personali. In tali casi IOR avvia le necessarie procedure e, avvalendosi della collaborazione dei Responsabili del trattamento e dei soggetti designati/autorizzati, accerta l'effettivo stato dell'arte.

2. Ove ricorrano i presupposti, IOR provvede a notificare la violazione all'Autorità Garante per la protezione dei dati personali 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 degli Interessati. Qualora la notifica non sia effettuata entro 72 ore, questa è corredata dei motivi del ritardo.

3. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati, a questi viene inoltrata, senza ingiustificato ritardo, apposita comunicazione dell'avvenuta violazione nei modi previsti dalla normativa vigente, salvo i casi di esclusione previsti dalla normativa. Indipendentemente dalla necessità di segnalazione all'Autorità di controllo ed all'interessato, IOR istituisce un registro di Data Breach in formato elettronico tenuto dal Responsabile Aziendale Privacy

4. IOR ha adottato la procedura interna per la segnalazione degli eventi di violazione dei dati personali con delibera n. 123 del 24/4/2019.

5. La procedura è stata diffusa e disponibile sul sito IOR ed Intranet

ART. 19
VIDEOSORVEGLIANZA

1. Dato atto che l'attivazione dei sistemi di videosorveglianza presso le strutture dell'Ente è strumentale allo svolgimento delle funzioni istituzionali dell' Istituto Ortopedico Rizzoli, il trattamento di dati personali (immagini) è finalizzato alla tutela delle persone e dei beni nell'eventualità di possibili reati (ad esempio: aggressioni, furti, danneggiamenti, atti di vandalismo), alla tempestiva reazione in caso di eventi avversi e improvvisi (ad esempio: incendi e allagamenti) e a supportare l'attività di sorveglianza sulla sicurezza ed agibilità delle strutture.
2. L'obiettivo che ci si prefigge è quello di garantire - mediante il controllo degli edifici o di alcune zone specifiche (entrate - cancelli - sbarre) - che l'attività all'interno dell'Istituto si svolga in condizioni di sicurezza per il lavoratore[1], per i pazienti e per chiunque si trovi all'interno dell'Istituto.

3. Nelle zone dove sono in funzione degli strumenti elettronici di rilevamento immagini, anche con videoregistrazione, finalizzati alla protezione dei dipendenti, degli utenti, dei visitatori e del patrimonio, viene affissa apposita informativa che avverte il pubblico della presenza degli impianti e delle finalità perseguite attraverso la videosorveglianza.

4. Le informative sono affisse in modo da essere visibili da chi accede all'area videosorvegliata.

5. Nel caso del reparto di rianimazione e terapia intensiva l'impianto di videosorveglianza è finalizzato al contatto fra paziente e parente ed è privo di funzioni di registrazione o sorveglianza. Occasionalmente può svolgere la funzione di supporto alle attività di assistenza

[1] Nel pieno rispetto della Legge 300/70 .

6. Le ragioni di installazione dei sistemi di videosorveglianza, in relazione ai diversi luoghi interessati, seguono i principi generali di liceità necessità proporzionalità finalità.

7. La mappatura degli impianti viene effettuata in autonomo documento.

8. In materia sono applicate le norme di cui all'art. 4 comma 1 della L. 300/1970 così come modificato dall'art. 23 del Dlgs 14 settembre 2015 n. 151, il quale prevede che: "*Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali…."*

PARTE OTTAVA
TUTELA DELL'INTERESSATO

ART. 20

ESERCIZIO DEI DIRITTI DELL'INTERESSATO NEI CONFRONTI DEL TITOLARE

1. Con Delibera 368 del 3/12/2019 è stata approvata la "PROCEDURA PER LAGESTIONE DELLE RICHIESTE INERENTI I "DIRITTI IN MATERIA DIPROTEZIONE DEI DATI PERSONALI DELL'INTERESSATO" AI SENSI DEGLIARTT. 12-22 DEL REGOLAMENTO UE 2016/679"

2. Tale documento descrive le modalità operative adottate dall'Istituto Ortopedico Rizzoli al fine di agevolare e garantire la gestione, in maniera standardizzata e nel rispetto di quanto previsto dal GDPR, delle richieste di esercizio dei diritti dell'interessato, relativamente al trattamento dei suoi dati personali.
3. Nello specifico, si individuano le misure procedurali disposte dal Titolare del trattamento per permettere all'utente interessato di ottenere in qualsiasi momento informazioni sull'utilizzo dei suoi dati ai sensi degli artt. 12-21 del GDPR, e precisamente il diritto:

- di informazione, comunicazione e trasparenza (artt. 12, 13 e 14);
- di accesso (art. 15); –
- di rettifica (art. 16);–
- alla cancellazione (art. 17);–
- di limitazione del trattamento (art. 18);

- alla portabilità dei dati (art. 20);
- di opposizione al trattamento (art. 21).

4. Si precisa che qualora l'interessato ottenga la rettifica, la cancellazione, ovvero la limitazione di trattamento dei propri dati personali, l'Istituto Ortopedico Rizzoli è tenuto a comunicare a ciascuno dei destinatari cui sono stati trasmessi i dati personali le rettifiche, le cancellazioni e le limitazioni di trattamento effettuato (art. 19). Tale obbligo di notifica viene meno solo qualora ciò si rilevi impossibile ossia – per qualsiasi ragione – non sia più possibile comunicare con il destinatario ovvero la comunicazione implichi uno sforzo sproporzionato.

5. Il Titolare del trattamento comunica all'interessato tali destinatari qualora l'interessato lo richieda. Inoltre, l'interessato ha il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che producano effetti giuridici che lo riguardano o incidano significativamente sulla sua persona (art. 22).

6. Esulano dal campo di applicazione della procedura adottata le richieste di accesso ai documenti amministrativi e sanitari prodotti o detenuti dall'Istituto Ortopedico Rizzoli per i quali si rinvia alle disposizioni di cui alla Legge 241/90 e s.m.i., al D.Lgs. n. 33/2013 e s.m.i. nonché ai relativi regolamenti aziendali in materia di accesso documentale, civico e generalizzato.

Art. 20 bis
Diritti riguardanti le persone decedute

1. Ai sensi di quanto previsto dall'art. 2-terdecies del D. Lgs. 196/2003, i diritti di cui agli articoli da 15 a 22 del GDPR, riferiti a dati personali concernenti persone decedute, 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.

ART. 21
RECLAMO ALL'AUTORITA' GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

1. Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il GDPR ha il diritto di proporre reclamo al Garante per la protezione dei dati personali ai sensi dell'articolo 77 del GDPR.

PARTE NONA
DISPOSIZIONI FINALI

ART. 22

FORMAZIONE

1. La formazione costituisce una importante misura di sicurezza ed in quanto tale viene considerata obbligatoria con programmazione degli interventi.

2. La formazione di base in materia di privacy si effettua anche con modalità FAD

3. Gli eventi formativi vengono promossi con ogni strumento e sono calibrati anche rispetto alle diverse figure aziendali che rivestono funzioni " privacy" come declinate nella delibera organizzativa 320/2018 più sopra citata .

4. Informazione sulle principali innovazioni/ adeguamenti organizzativi viene pubblicizzata anche tramite la Intranet aziendale ed il Mensile associato al cedolino dello stipendio

ART. 23

ATTIVITÀ DI AUDIT

1. Nell'ambito delle azioni di prevenzione e gestione del rischio, per venire a conoscenza di situazioni che necessitano di azioni correttive infrastrutturali, sul sistema applicativo oppure misure organizzative, il Gruppo di lavoro aziendale Audit Privacy coordinato dal DPO, a cui partecipano la Referente Privacy, il Direttore ICT, un referente medico della Direzione Sanitaria e un referente Saiter, è deputato alla definizione di un piano di verifiche sulla concreta applicazione del presente regolamento e in generale sulla applicazione della normativa sul trattamento dei dati personali. Il Gruppo Audit Privacy può essere integrato con un componente afferente all'area della Qualità.

ART. 24

DISPOSIZIONE FINALE

1. Ogniqualvolta sussistano dubbi sulla applicazione della normativa in materia di protezione dei dati personali e delle presente linee guida il personale autorizzato è tenuto ad attenersi al criterio della tutela e del massimo rispetto della riservatezza nei confronti dell'interessato, pur garantendo nel contempo il normale espletamento delle attività.

2. In ogni caso il personale autorizzato è tenuto, nei casi di cui al comma 1, a rivolgersi al referente del trattamento di competenza il quale, nel caso, può chiedere consulenza, per via telematica, al Responsabile della Protezione dei dati, per il tramite del Referente privacy Aziendale, secondo quanto previsto dalla delibera riguardante i rapporti con il DPO, n. 218 del 24/7/2019 .

3. Per tutto quanto non espressamente previsto dalle presenti linee guida si applicano le disposizioni del Regolamento UE e del Codice, nonché le pertinenti disposizioni amministrative.

INFORMATIVA per il trattamento dei dati personali
ai sensi dell'art 13 del Regolamento (UE) 2016/679

Premessa

Ai sensi dell'art. 13 del Regolamento (UE) 2016/679 – "Regolamento del Parlamento Europeo 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" (di seguito "Regolamento"), l'IRCCS Istituto Ortopedico Rizzoli in qualità di Titolare del trattamento è tenuto a fornirLe informazioni in merito all'utilizzo dei Suoi dati personali relativamente all'applicazione MAppER (Mani App Emilia-Romagna). L'applicazione ha lo scopo di monitorare la corretta igiene delle mani da parte del personale sanitario del Servizio Sanitario Regionale (SSR) al fine della prevenzione delle infezioni in ambiente ospedaliero.

1. **Identità e dati di contatto del Titolare del trattamento**

Il Titolare del trattamento dei dati personali di cui alla presente Informativa è l' Istituto Ortopedico Rizzoli, con sede in Bologna, via di Barbiano n. 1/10, CAP 40136 Bologna (BO)
PEC: direzione.generale@pec.ior.it

2. **Responsabile della protezione dei dati personali**

Il Responsabile della protezione dei dati (anche detto Data Protection Officer – DPO) designato dall'Ente è contattabile all'indirizzo mail dpo@aosp.bo.it - PEC: dpo@pec.aosp.bo.it o presso la sede dell'IRCCS Azienda Ospedaliero-Universitaria di Bologna Policlinico di S. Orsola, via Massarenti n. 9, CAP 40138 Bologna (BO).

3. **Responsabile del trattamento**

L'Ente si avvale dell'Agenzia sanitaria e sociale della Regione Emilia-Romagna, in qualità di Responsabile del trattamento, per l'espletamento di attività e relativi trattamenti di dati personali di cui l'Istituto mantiene la Titolarità. Conformemente a quanto stabilito dalla normativa, tale soggetto assicura livelli di esperienza, capacità e affidabilità tali da garantire il rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza dei dati.

L'Istituto formalizza istruzioni, compiti ed oneri in capo a tale soggetto con la designazione dello stesso a "Responsabile del trattamento". Sottopone tale soggetto a verifiche periodiche al fine di constatare il mantenimento dei livelli di garanzia registrati in occasione dell'affidamento dell'incarico iniziale.

4. **Soggetti autorizzati al trattamento**

I Suoi dati personali sono trattati da personale interno previamente autorizzato e designato quale incaricato del trattamento, a cui sono impartite idonee istruzioni in ordine a misure, accorgimenti, modus operandi, tutti volti alla concreta tutela dei Suoi dati personali.

5. Finalità e base giuridica del trattamento

Il trattamento dei Suoi dati personali viene effettuato, in qualità di Responsabile del trattamento, dall'Agenzia sanitaria e sociale regionale, per conto dell'Istituto Ortopedico Rizzoli, Titolare del trattamento, per lo svolgimento di funzioni istituzionali e, pertanto, ai sensi dell'art. 6 comma 1 lett. e) non necessita del suo consenso. I dati personali sono trattati per le seguenti finalità:

a) osservazione diretta del comportamento degli operatori sanitari, realizzata seguendo la metodologia promossa dall'OMS;
b) mettere a disposizione dei professionisti sanitari un metodo efficace di raccolta e gestione dei dati, il quale consenta, occasionalmente o periodicamente, l'elaborazione di reports, ottimizzando la raccolta delle informazioni rispetto al procedimento tradizionale attualmente in uso (compilazione di scheda cartacea e successivo inserimento e analisi con un software specifico);
c) velocizzare la raccolta e la trascrizione dei dati e permettere l'accesso immediato ad una reportistica dinamica a livello aziendale;
d) consentire di registrare i dati delle Aziende del Servizio Sanitario Regionale (SSR) in un archivio centrale.

6. Destinatari dei dati personali

I dati raccolti saranno utilizzati per la produzione di rapporti di sintesi che riportano il tasso di adesione, stratificato per categoria professionale e struttura, in un periodo di tempo definito, nel rispetto dei principi del trattamento dettati dall'articolo 5 del Regolamento (UE) 2016/679, rivolti esclusivamente agli utenti del sistema MAppER specificamente autorizzati a livello aziendale.

7. Trasferimento dei dati personali a Paesi extra UE

I Suoi dati personali non sono trasferiti al di fuori dell'Unione europea.

8. Periodo di conservazione dei dati

I Suoi dati personali sono conservati per un periodo non superiore a quello necessario per il perseguimento delle finalità sopra menzionate. A tal fine, anche mediante controlli periodici, viene verificata costantemente la stretta pertinenza, non eccedenza e indispensabilità dei dati rispetto al rapporto, alla prestazione o all'incarico in corso, da instaurare o cessati, anche con riferimento ai dati che Lei fornisce di propria iniziativa. I dati che, anche a seguito delle verifiche, risultano eccedenti o non pertinenti o non indispensabili non sono utilizzati, salvo che per l'eventuale conservazione, a norma di legge, dell'atto o del documento che li contiene.

9. I Suoi diritti

Nella Sua qualità di interessato, Lei ha diritto:

- di accesso ai dati personali;
- di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano;
- di opporsi al trattamento;
- di proporre reclamo al Garante per la protezione dei dati personali.

In qualità di interessato, Lei può inviare richieste formali di esercizio dei propri diritti oppure segnalazioni di presunte inottemperanze o violazioni all'attenzione del Direttore Generale dell'Istituto Ortopedico Rizzoli e del Data Protection Officer (DPO) del medesimo Istituto ai seguenti indirizzi:
direzione.generale@pec.ior.it
dpo@pec.aosp.bo.it

10. Conferimento dei dati

Il conferimento dei Suoi dati personali è necessario per le finalità sopra indicate. Il mancato conferimento comporterà l'impossibilità di procedere alla rilevazione.

Accordo per il trattamento di dati personali

Il presente accordo definisce i termini per il trattamento dei dati tra l'IRCCS Istituto Ortopedico Rizzoli, che fruisce del servizio "MAppER" (di seguito "Fruitore" o "Titolare"), e l'Agenzia sanitaria e sociale della Regione Emilia-Romagna quale Responsabile del trattamento di dati personali nominato ai sensi dell'art. 28 del Regolamento (UE) 2016/679 (di seguito anche solo "Responsabile"), accettati con l'adesione al servizio "MAppER".

1. Premesse

L'art. 28 del Regolamento (UE) 2016/679 (di seguito GDPR) dispone che qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a Responsabili del trattamento che garantiscano la adozione di misure tecniche ed organizzative adeguate, in modo tale che il trattamento sia conforme alla normativa in materia di protezione dati e garantisca la tutela dei diritti dell'interessato.

La sicurezza delle cure è un tema centrale per i servizi sanitari. Uno degli elementi fondamentali, per proteggere il paziente dalla trasmissione di una malattia infettiva da una persona a un'altra, è l'igiene delle mani. Pertanto, l'adesione elevata alla corretta igiene delle mani riduce il rischio di infezioni correlate all'assistenza. L'Organizzazione mondiale della sanità (OMS) ha promosso a livello mondiale la campagna "Clean Care is Safer Care", che in Italia è stata coordinata dall'Agenzia sanitaria e sociale. La campagna mirava a promuovere la corretta igiene delle mani nelle strutture sanitarie, attraverso l'adozione di linee guida basate su evidenze e la loro implementazione basata su una strategia multimodale. Per facilitare questo obiettivo nelle aziende sanitarie e ospedaliere dell'Emilia-Romagna è stato sviluppato e messo a disposizione degli operatori uno strumento informatizzato per agevolare gli interventi di audit e feedback sull'adesione all'igiene delle mani, il sistema MAppER.

2. Istruzioni per il trattamento dei dati

2.1 Il Responsabile del trattamento, relativamente a tutti i dati personali che tratta per conto del Titolare garantisce che:

2.1.1 tratta tali dati personali solo ai fini dell'esecuzione dell'oggetto del contratto e, successivamente, solo nel rispetto di quanto eventualmente concordato dalle Parti per iscritto, agendo pertanto, esclusivamente sulla base delle istruzioni documentate e fornite dall'Ente;

2.1.2 non trasferisce i dati personali a soggetti terzi, se non nel rispetto delle condizioni di liceità assolte dall'Ente e a fronte di quanto disciplinato nel presente accordo;

2.1.3 non tratta o utilizza i dati personali per finalità diverse da quelle per cui è conferito incarico dall'Ente, financo per trattamenti aventi finalità compatibili con quelle originarie;

2.1.4 prima di iniziare ogni trattamento e, ove occorra, in qualsiasi altro momento, informerà l'Ente se, a suo parere, una qualsiasi istruzione fornita dall'Ente si ponga in violazione della normativa applicabile.

2.2 Al fine di dare seguito alle eventuali richieste da parte di soggetti interessati, il Responsabile del trattamento si obbliga ad adottare:

2.2.1 procedure idonee a garantire il rispetto dei diritti e delle richieste formulate all'Ente dagli interessati relativamente ai loro dati personali e/o a conformarsi alle istruzioni fornite dall'Ente in materia;

2.2.2 procedure atte a garantire l'aggiornamento, la modifica e la correzione, su richiesta dell'Ente, dei dati personali di ogni interessato e/o a conformarsi alle istruzioni fornite dall'Ente in materia;

2.2.3 procedure atte a garantire la cancellazione o il blocco dell'accesso ai dati personali a richiesta del Titolare e/o a conformarsi alle istruzioni fornite dall'Ente in materia;

2.2.4 procedure atte a garantire il diritto degli interessati alla limitazione di trattamento, su richiesta dell'Ente e/o a conformarsi alle istruzioni fornite dall'Ente in materia.

2.3 Il Responsabile del trattamento fornisce al Titolare cooperazione, assistenza e le informazioni che potrebbero essere ragionevolmente

richieste dallo stesso, per consentirgli di adempiere ai propri obblighi ai sensi della

normativa applicabile, ivi compresi i provvedimenti e le specifiche decisioni del Garante per la protezione dei dati personali.

2.4 Il Responsabile del trattamento, anche nel rispetto di quanto previsto all'art. 30 del GDPR, deve mantenere e compilare e rendere disponibile a richiesta del Titolare un registro dei trattamenti di dati personali che riporti tutte le informazioni richieste dalla norma.

2.5 Il Responsabile del trattamento assicura la massima collaborazione al fine dell'esperimento delle valutazioni di impatto ex art. 35 del GDPR che l'Ente intenderà esperire sui trattamenti che rivelano, a suo insindacabile giudizio, un rischio elevato per i diritti e le libertà delle persone fisiche.

3. Misure di sicurezza

3.1 Il Responsabile del trattamento deve adottare e mantenere appropriate misure di sicurezza, sia tecniche che organizzative, per proteggere i dati personali da eventuali distruzioni o perdite di natura illecita o accidentale, danni, alterazioni, divulgazioni o accessi non autorizzati.

3.2 Nei casi in cui il Responsabile effettui trattamenti di conservazione dei dati personali del Titolare nel proprio sistema informativo, garantisce la separazione di tipo logico di tali dati da quelli trattati per conto proprio o di terze parti.

3.3 Il Responsabile del trattamento conserva, nel caso siano allo stesso affidati servizi di amministrazione di sistema, direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema.

3.4 Il Titolare del trattamento attribuisce al Responsabile del trattamento il compito di dare attuazione alla prescrizione di cui al punto 2 lettera e) "Verifica delle attività" del Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

3.5 Il Responsabile del trattamento deve adottare misure tecniche ed organizzative adeguate a salvaguardare la sicurezza di qualsiasi rete di

comunicazione elettronica o dei servizi forniti al Titolare, con specifico

riferimento alle misure intese a prevenire l'intercettazione di comunicazioni o l'accesso non autorizzato a qualsiasi computer o sistema.

3.6 Conformemente alla disposizione di cui all’art. 28 comma 1 del GDPR e alla valutazione delle garanzie che il Responsabile del trattamento deve presentare, lo stesso Responsabile attesta, a mezzo della sottoscrizione del presente accordo, la conformità della propria organizzazione almeno ai parametri di livello minimo di cui alle misure di sicurezza individuate da Agid nella circolare n. 2/2017.

3.7 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy dell’Ente in materia di privacy e sicurezza informatica.

4. Analisi dei rischi, privacy by design e privacy by default

4.1 Con riferimento agli esiti dell’analisi dei rischi effettuata dal Titolare sui trattamenti di dati personali cui concorre il Responsabile del trattamento, quest’ultimo assicura massima cooperazione e assistenza al fine di dare effettività alle azioni di mitigazione previste dal Titolare per affrontare eventuali rischi identificati.

4.2 Il Responsabile del trattamento collaborerà con il Titolare, tenuto conto dello stato della tecnica, dei costi, della natura, dell’ambito e della finalità del relativo trattamento, di adottare, sia nella fase iniziale di determinazione dei mezzi di trattamento, che durante il trattamento stesso, ogni misura tecnica ed organizzativa che si riterrà opportuna per garantire ed attuare i principi previsti in materia di protezione dati e a tutelare i diritti degli interessati.

4.3 In linea con i principi di privacy by default, dovranno essere trattati, per impostazione predefinita, esclusivamente quei dati personali necessari per ogni specifica finalità del trattamento, e dovrà essere garantito, in particolare, che non siano accessibili dati personali ad un numero indefinito di soggetti senza l’intervento di una persona fisica.

4.4 Il Responsabile del trattamento dà esecuzione al contratto in aderenza alle policy di privacy by design e by default adottate dal Titolare e specificatamente comunicate.

5. Soggetti autorizzati ad effettuare i trattamenti - Designazione

5.1 Il Responsabile del trattamento garantisce competenze ed affidabilità dei propri dipendenti e collaboratori autorizzati al trattamento dei dati personali (di seguito anche incaricati) effettuato per conto del Titolare.

5.2 Il Responsabile del trattamento garantisce che gli incaricati abbiano ricevuto adeguata formazione in materia di protezione dei dati personali e sicurezza informatica, consegnando al Titolare le evidenze di tale formazione.

5.3 Il Responsabile del trattamento, con riferimento alla protezione e gestione dei dati personali, impone ai propri incaricati obblighi di riservatezza non meno onerosi di quelli previsti nel contratto di cui il presente accordo costituisce parte integrante. In ogni caso il Responsabile del trattamento è direttamente ritenuto responsabile per qualsiasi divulgazione di dati personali dovesse realizzarsi ad opera di tali soggetti.

6. Sub-Responsabili del trattamento di dati personali

6.1 Nell'ambito dell'esecuzione del contratto, il Responsabile del trattamento è autorizzato sin d'ora, alla designazione di altri Responsabili del trattamento (d'ora in poi anche "Sub-Responsabili"), previa informazione dell'Ente ed imponendo agli stessi condizioni vincolanti in materia di trattamento dei dati personali non meno onerose di quelle contenute nel presente accordo.

6.2 Su specifica richiesta del Titolare, il Responsabile del trattamento dovrà provvedere a che ogni Sub-Responsabile sottoscriva direttamente con l'Ente un accordo di trattamento dei dati che, a meno di ulteriori e specifiche esigenze, preveda sostanzialmente gli stessi termini del presente accordo.

6.3 In tutti i casi, il Responsabile del trattamento si assume la responsabilità nei confronti del Titolare per qualsiasi violazione od omissione realizzati da un Sub- Responsabile o da altri terzi soggetti incaricati dallo stesso, indipendentemente dal fatto che il Responsabile del trattamento abbia o meno rispettato i propri obblighi contrattuali, ivi

comprese le conseguenze patrimoniali derivanti da tali violazioni od omissioni.

7. Trattamento dei dati personali fuori dall'Unione europea

7.1 Il Titolare non autorizza il trasferimento dei dati personali oggetto di trattamento al di fuori dell'Unione Europea.

8. Cancellazione dei dati personali

8.1 Il Responsabile del trattamento, a richiesta del Titolare, provvede alla restituzione o cancellazione dei dati personali trattati per l'esecuzione del presente contratto al termine dell'affidamento o del periodo di conservazione e in qualsiasi circostanza in cui sia richiesto dal Titolare, compresa l'ipotesi in cui la stessa debba avvenire per dare seguito a specifica richiesta da parte dei soggetti interessati.

9. Audit

9.1 Il Responsabile del trattamento si rende disponibile a specifici audit in tema di privacy e sicurezza informatica da parte del Titolare.

9.2 Il Responsabile del trattamento consente, pertanto, all'Ente l'accesso ai propri locali e ai locali di qualsiasi Sub-Responsabile, ai computer e altri sistemi informativi, ad atti, documenti e a quanto ragionevolmente richiesto per verificare che il Responsabile del trattamento, e/o i suoi Sub-Fornitori, rispettino gli obblighi derivanti dalla normativa in materia di protezione dei dati personali e, quindi, da questo accordo.

9.3 Il Titolare può esperire specifici audit anche richiedendo al Responsabile del trattamento di attestare la conformità della propria organizzazione agli oneri di cui alla normativa applicabile e al presente accordo.

9.4 L'esperimento di tali audit non deve avere ad oggetto dati di terze parti, né informazioni sottoposte ad obblighi di riservatezza degli interessi commerciali.

9.5 Il rifiuto del Responsabile del trattamento di consentire l'audit all'Ente comporta la risoluzione del contratto.

10. Indagini dell'Autorità e reclami

10.1 Nei limiti della normativa applicabile, il Responsabile del trattamento o qualsiasi Sub-Responsabile informa senza alcun indugio il Titolare di qualsiasi:

a) richiesta o comunicazione promanante dal Garante per la protezione dei dati personali o da forze dell’ordine;

b) istanza ricevuta da soggetti interessati.

Il Responsabile del trattamento fornisce, in esecuzione del contratto e, quindi, gratuitamente, tutta la dovuta assistenza al Titolare per garantire che quest'ultimo possa rispondere a tali istanze o comunicazioni nei termini temporali previsti dalla normativa e dai regolamentari applicabili.

11. Violazione dei dati personali e obblighi di notifica

11.1 Il Responsabile del trattamento, in virtù di quanto previsto dall'art. 33 del GDPR e nei limiti di cui al perimetro delle attività affidate, deve comunicare a mezzo di posta elettronica certificata all'Ente nel minor tempo possibile, e comunque non oltre 24 (ventiquattro) ore da quando ne abbia avuto notizia, qualsiasi violazione di sicurezza che abbia comportato accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, ivi incluse le violazioni che abbiano riguardato i propri Sub-Fornitori. Tale comunicazione deve contenere ogni informazione utile alla gestione del *data breach,* oltre a:

a) descrivere la natura della violazione dei dati personali;

b) indicare le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

c) indicare i recapiti del DPO nominato o del soggetto competente alla gestione del data breach;

d) descrivere le probabili conseguenze della violazione dei dati personali;

e) descrivere le misure adottate o che si intende adottare per affrontare la violazione, compreso, ove opportuno, le misure per mitigare i possibili effetti negativi della violazione stessa.

11.2 Il Responsabile del trattamento deve fornire tutto il supporto necessario al Titolare ai fini delle indagini e delle valutazioni in ordine alla violazione di dati, anche al fine di individuare, prevenire e limitare

gli effetti negativi della stessa, conformemente ai suoi obblighi ai sensi del presente articolo e, previo accordo

con il Titolare, per svolgere qualsiasi azione che si renda necessaria per porre rimedio alla violazione stessa. Il Responsabile del trattamento non deve rilasciare né pubblicare alcun comunicato stampa o relazione riguardante eventuali data breach o violazioni di trattamento senza aver ottenuto il previo consenso scritto del Titolare.

12. Responsabilità e manleve

12.1 Il Responsabile del trattamento tiene indenne e manleva il Titolare da ogni perdita, costo, sanzione, danno e da ogni responsabilità di qualsiasi natura derivante o in connessione con una qualsiasi violazione da parte del Responsabile del trattamento delle disposizioni contenute nel presente accordo.

12.2 Nel caso in cui il Responsabile del trattamento commetta violazioni alla normativa in materia di protezione dei dati personali e al presente accordo, quali ad esempio quelle indicate all'art. 83 commi 4 e 5 del GDPR, l'Ente può risolvere il contratto o chiedere una cospicua riduzione del prezzo.

12.3 A fronte della ricezione di un reclamo relativo alle attività oggetto del presente accordo, il Responsabile del trattamento:

- avverte, prontamente ed in forma scritta, il Titolare del reclamo;
- non fornisce dettagli al reclamante senza la preventiva interazione con il Titolare;
- non transige la controversia senza il previo consenso scritto del Titolare;
- fornisce al Titolare tutta l'assistenza che potrebbe ragionevolmente richiedere nella gestione del reclamo.

Allegato 1

GLOSSARIO

“Garante per la protezione dei dati personali”: è l’autorità di controllo responsabile per la protezione dei dati personali in Italia;

“**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;

“**GDPR” o “Regolamento”:** si intende il Regolamento (UE) 2016/679 sulla protezione delle persone fisiche relativamente al trattamento dei dati personali e alla loro libera circolazione (General Data Protection Regulation), direttamente applicabile dal 25 maggio 2018;

“**Normativa applicabile”:** si intende l’insieme delle norme rilevanti in materia di protezione dei dati personali, incluso il Regolamento (UE) 2016/679 ed ogni provvedimento del Garante per la protezione dei dati personali e del WP Art. 29.

“**Appendice Security”:** consiste nelle misure di sicurezza che il Titolare determina assicurando un livello minimo di sicurezza, e che possono essere aggiornate ed implementate dal Titolare, di volta in volta, in conformità alle previsioni del presente accordo;

“Reclamo”: si intende ogni azione o segnalazione presentata nei confronti del Titolare o di un suo Responsabile del trattamento;

“**Titolare del trattamento”:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il Titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

“**Trattamento”:** qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

“**Responsabile del trattamento”:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento;

“**Pseudonomizzazione”:** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.