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

L'originale del presente documento, redatto in formato elettronico e firmato digitalmente e' conservato a cura dell'ente produttore secondo normativa vigente.
Ai sensi dell'art. 3bis c4-bis Dlgs 82/2005 e s.m.i., in assenza del domicilio digitale le amministrazioni possono predisporre le comunicazioni ai cittadini come documenti informatici sottoscritti con firma digitale o firma elettronica avanzata ed inviare ai cittadini stessi copia analogica di tali documenti sottoscritti con firma autografa sostituita a mezzo stampa predisposta secondo le disposizioni di cui all'articolo 3 del Dlgs 39/1993.

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.