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: 0000162

DATA: 07/06/2024 15:55

OGGETTO: Provvedimenti in merito alla designazione degli Amministratori di sistema in attuazione delle indicazioni dell'Autorità Garante per la Protezione dei Dati Personali

SOTTOSCRITTO DIGITALMENTE DA:

Il presente atto è stato firmato digitalmente da Campagna Anselmo in qualità di Direttore Generale
Con il parere favorevole di Fini Milena - Direttore Scientifico
Con il parere favorevole di Damen Viola - 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
- ICT
- Radiologia Diagnostica ed Interventistica
- Direzione Amministrativa
- Direzione Sanitaria
- Direzione Scientifica
- Direzione Generale

DOCUMENTI:

File	Firmato digitalmente da	Hash
DELI0000162_2024_delibera_firmata.pdf	Campagna Anselmo; Cilione Giampiero; Damen Viola; Fini Milena; Mandrioli Laura	2220A0C86297F56A1ADC08635EE98398F916B64F097A7541CAEBC9342D7B2C4B
DELI0000162_2024_Allegato1.pdf:		AE67597187D5CEE21FEB8C904FF0358B84E7F40E21B41EEDBB9EE5D06E60ED4C

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

DELIBERAZIONE

OGGETTO: Provvedimenti in merito alla designazione degli Amministratori di sistema in attuazione delle indicazioni dell'Autorità Garante per la Protezione dei Dati Personali

IL DIRETTORE GENERALE

Richiamati:
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), "GDPR";

il Decreto Legislativo n. 196 del 30 giugno 2003 recante il "Codice in materia di protezione dei dati personali", così come modificato e integrato dal Decreto Legislativo n. 101 del 10 agosto 2018, recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.

Richiamati altresì:
la Deliberazione IOR n. 685 del 15 dicembre 2009, "Adeguamento alle disposizioni previste dal Decreto Legislativo 30 Giugno 2003 n. 196 riguardanti la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Provvedimenti conseguenti: nomina degli amministratori di sistema.";

la Deliberazione IOR n. 264 del 17 ottobre 2022, "Approvazione del documento 'Regolamento aziendale sull'utilizzo della posta elettronica e di internet' dell'Istituto Ortopedico Rizzoli";

il "Regolamento per l'utilizzo dei sistemi informatici dell'Istituto Ortopedico Rizzoli", approvato con Deliberazione IOR n. 225 del 27 ottobre 2017, nel testo coordinato con il Regolamento metropolitano di cui al punto che precede.

Visti:
il Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 27 novembre 2008 recante " *Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*";

il Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali del 25 giugno 2009 recante "Modifiche del provvedimento del 27 novembre 2008 recante prescrizioni ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni di amministratore di sistema e proroga dei termini per il loro adempimento";

la disposizione transitoria e finale del D.lgs. 101/2018, art. 22, comma 4, per la quale “a decorrere dal 25 maggio 2018, i provvedimenti del Garante per la protezione dei dati personali continuano ad applicarsi, in quanto compatibili con il suddetto regolamento e con le disposizioni del presente decreto”.

Atteso che:
l’Autorità Garante per la Protezione dei Dati Personali definisce quali Amministratori di sistema "Le figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti (quali ad esempio gli amministratori di dominio e di server), nonché le altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi" prescrivendo in particolare:

1. che l'attribuzione delle funzioni di Amministratore di sistema debba avvenire previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza;
2. che la designazione quale Amministratore di sistema debba essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
3. che il tracciamento dei log degli accessi degli amministratori di sistema sia da conservare per sei mesi per la vigilanza dell'operato degli amministratori di sistema da parte del titolare o di un responsabile, ove delegata;
4. che, nel caso di servizi di Amministratore di sistema affidati in outsourcing, il Titolare o il Responsabile del trattamento debba conservare direttamente e specificatamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali Amministratori di sistema.

Considerata la necessità per l’IRCCS Istituto Ortopedico Rizzoli di definire e adottare gli indirizzi per assicurare la conformità dell’operato degli Amministratori di sistema alle prescrizioni dei sopra richiamati Provvedimenti dell’Autorità Garante per la Protezione dei Dati Personali e, in particolare, porre in essere adempimenti per la designazione individuale degli stessi con elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Dato atto che il Responsabile della Protezione dei Dati (DPO) ha attivato apposito gruppo di lavoro per definire in ambito metropolitano modalità omogenee di designazione degli Amministratori di sistema e che, a conclusione dei lavori, ha trasmesso il fac simile di atto di designazione, allegato quale parte integrante al presente provvedimento.

Ritenuto pertanto di recepire l’allegato fac-simile di atto di designazione individuale degli Amministratori di sistema interni all’IRCCS Istituto Ortopedico Rizzoli, dando mandato alla competente SC ICT per la tenuta dell’elenco aggiornato degli Amministratori di sistema;

Delibera

1. di prendere atto dello schema tipo di atto di designazione alle funzioni di Amministratore di sistema elaborato dall'apposito gruppo di lavoro coordinato dal DPO e da quest'ultimo trasmesso alle Aziende Sanitarie dell'area metropolitana per la conseguente adozione;
2. di dare atto che alla designazione individuale degli Amministratori di sistema interni all'IRCCS Istituto Ortopedico Rizzoli si provvederà con nota a firma del Legale Rappresentante dell'Ente su proposta del Referente privacy della struttura in cui l'Amministratore esplica la propria attività, che, se diverso dal Direttore della SC ICT, acquisirà il parere preventivo di quest'ultimo;
3. di dare atto altresì che l'Istituto provvederà a effettuare, tramite il Referente privacy di cui al punto che precede, verifica almeno annuale delle attività svolte dall'Amministratore di sistema, in modo da controllare la rispondenza di tali attività alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti, come prescritto dal Provvedimento dell' Autorità Garante per la Protezione dei Dati Personali del 27 novembre 2008;
4. di demandare alla SC ICT la tenuta dell'elenco aggiornato degli Amministratori di sistema in ottemperanza alle disposizioni dell'Autorità Garante per la Protezione dei Dati Personali.

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

Oggetto: Designazione ad "Amministratore di sistema"

Al/Alla Sig. /Sig.ra _____ nato/a a _____ il _____,

matricola _____ qualifica _____

UO _____ sede _____

Premesso che,

- nell'ambito della propria attività l'IRCCS Istituto Ortopedico Rizzoli, in qualità di Titolare del trattamento, tratta dati personali, compreso dati personali di natura particolare, avvalendosi anche di strumenti elettronici;
- tali trattamenti sono soggetti alle disposizioni del Regolamento (UE) 2016/679 (GDPR), della normativa italiana di armonizzazione (D.lgs. 30 giugno 2003, n.196 s.m.i. recante il "Codice in materia di protezione dei dati personali"), nonché ai Provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali;
- in forza del Provvedimento a carattere generale 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", così come modificato dal Provvedimento del 25 giugno 2009, l'Autorità Garante ha prescritto per i soggetti pubblici e privati l'adeguamento delle misure di sicurezza già in uso con l'adozione di altre e ulteriori finalizzate al corretto svolgimento delle funzioni degli Amministratori di sistema;
- l'attribuzione delle funzioni di Amministratore di sistema deve avvenire, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, secondo le prescrizioni dell'Autorità Garante per la Protezione dei Dati Personali.

Preso atto che, così come definito dai richiamati provvedimenti dell'Autorità, l'Amministratore di Sistema è:

- *"una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP (Enterprise resource planning) utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali";*
- *"...anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.".*

Preso atto, inoltre, che non rientrano nelle definizioni su elencate quei soggetti che solo occasionalmente intervengono (p.es., per scopi di manutenzione a seguito di guasti o malfunzionamenti) sui sistemi di

elaborazione e sui sistemi software, così come chiarito nella FAQ n. 1 al Provvedimento del 27 novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali sopra richiamato[1].

CON LA PRESENTE

ad integrazione della nomina quale "Persona autorizzata al trattamento dei dati personali", avendo valutato che le prestazioni da Lei effettuate in via ordinaria forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati personali, ivi compreso il profilo relativo alla sicurezza, la S.V. è designata quale "Amministratore di sistema".

Per effetto di tale designazione e delle funzioni conseguentemente attribuite, Lei si impegna a:

- accedere ai sistemi ICT nei limiti strettamente richiesti dall'espletamento delle Sue mansioni;
- eseguire gli accessi nel rispetto delle procedure di autenticazione a Lei già note, e di detenzione, custodia, segretezza e sicurezza delle relative credenziali di accesso;
- eseguire gli accessi nel rispetto delle misure di sicurezza organizzative, logiche e fisiche adottate dal Titolare del trattamento;
- attenersi alle istruzioni operative impartite dal Referente privacy (Direttore/Responsabile della UO di appartenenza);
- segnalare qualunque elemento che possa pregiudicare il corretto svolgimento delle Sue funzioni di Amministratore di sistema e/o rendere necessarie ulteriori istruzioni;
- cooperare con il Referente privacy per ogni verifica della rispondenza del Suo operato alle misure organizzative, tecniche e di sicurezza previste con riferimento ai dati personali trattati per conto e nell'interesse dell'Ente;
- collaborare per l'attuazione delle eventuali ulteriori prescrizioni che saranno emanate dall'Autorità Garante per la Protezione dei Dati Personali in tema di Amministratori di sistema;
- consentire il trattamento dei Suoi dati personali nei limiti e per le finalità previste dal citato Provvedimento del 27 novembre 2008 dell'Autorità Garante per la Protezione dei Dati Personali, incluse la registrazione e comunicazione di ogni dato di log relativo all'attività di Amministratore di sistema.

Nello specifico l'incarico disciplina la gestione dei seguenti servizi:

- gestione e manutenzione dell'infrastruttura di rete
- gestione e manutenzione dell'infrastruttura server
- gestione e manutenzione delle basi dati
- gestione e manutenzione delle postazioni di lavoro
- gestione e manutenzione dei sistemi applicativi
- affiancamento e assistenza agli utenti nell'utilizzo dei sistemi applicativi
- gestione e manutenzione della posta elettronica e dei servizi Internet

Resta inteso e convenuto che:

- la presente designazione non configura alcuna variazione della Sua qualifica e delle Sue mansioni e del relativo trattamento economico e normativo del rapporto di lavoro con Lei in essere;

[1] https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1577499#FAQ

- la registrazione e comunicazione dei dati di log sarà eseguita al solo fine di ottemperare a quanto specificatamente prescritto al riguardo dal su citato Provvedimento dell'Autorità Garante per la Protezione dei Dati Personali e non costituisce alcuna forma di controllo a distanza, neanche indiretto, della Sua attività lavorativa;
- ogni eventuale variazione dell'ambito di operatività consentito dalle Sue mansioni e dal Suo profilo di autorizzazione all'accesso ai sistemi ICT non comporterà il venir meno degli effetti della presente designazione.

Si rammenta, inoltre, che il Provvedimento del Garante già citato, obbliga il Titolare del trattamento alla verifica almeno annuale delle attività svolte dall'Amministratore di sistema, in modo da controllare la rispondenza di tali attività alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Il Direttore Generale

_____

Letto firmato e sottoscritto per accettazione

L'Amministratore di sistema

_____

Data

_____