SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Reggio Emilia
IRCCS Istituto in tecnologie avanzate e modelli assistenziali in oncologia

OECI CLINICAL Cancer Centre

DELIBERA DEL DIRETTORE GENERALE

2018/0202 DEL 24/05/2018

OGGETTO:

Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - ricognizione delle prime attività di adeguamento

ATTESTAZIONE DI PUBBLICAZIONE

ALL'ALBO PRETORIO ON LINE

Il sottoscritto attesta che la presente deliberazione viene inserita nell'Albo on-line di questa Azienda Unità Sanitaria Locale in data odierna e vi rimarrà per la durata di 15 giorni consecutivi.

☒ DELIBERA NON SOGGETTA A CONTROLLO. Esecutiva dalla data di pubblicazione, a sensi della L.R. 50/94 art. 37 e successive modificazioni.

☐ DELIBERA SOGGETTA A CONTROLLO. Esecutiva a seguito di approvazione da parte della Regione Emilia Romagna.

Reggio Emilia, Data inserimento: 24/05/2018

La presente deliberazione è automaticamente ritirata dall'Albo on-line, con procedura informatizzata, nei termini di legge.

Per copia conforme all'originale ad uso amministrativo.
Il Funzionario
_____

OGGETTO: Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali - ricognizione delle prime attività di adeguamento.

IL DIRETTORE GENERALE

Su proposta del Direttore Amministrativo, e con contestuale ed espresso parere favorevole in ordine ai contenuti sostanziali, formali e di legittimità;

Premesso che**:**

- il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (*General Data Protection Regulation*, o 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 potere di adottare le misure che ritiene più idonee ed opportune per garantire la protezione dati personali;

- il "*sistema privacy*" delineato dal GDPR implica la necessità di infondere nell'organizzazione aziendale la piena consapevolezza del rischi inerenti ai trattamenti, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero *asset* organizzativo, con particolare attenzione alle categorie particolari di dati, tra i quali quelli relativi alla salute;

Ritenuto opportuno procedere ad una ricognizione delle decisioni prese e delle attività svolte in applicazione della nuova normativa europea, tenendo altresì conto di quanto previsto dallo schema di decreto legislativo di adeguamento del quadro normativo nazionale alle disposizioni del suddetto *GDPR*, testo peraltro attualmente all'esame delle competenti commissioni parlamentari per il relativo parere e, pertanto, non ancora approvato in via definitiva;

Considerato che tra le attività prioritarie di più ampio impatto da porre in essere entro la data di applicazione del Regolamento (tenendo conto, nei limiti del possibile, di quanto previsto dallo schema di decreto citato sopra), figurano:

1. la revisione delle informative in uso presso l'Azienda, al fine di renderla conforme alle disposizioni di cui agli artt. 12, 13 e 14 del Regolamento;

2. l'adozione di una procedura per la gestione delle violazioni dei dati personali (cd. *data breach*), ai sensi e per gli effetti di cui all'art. 33 del Regolamento;

3. la tenuta di un Registro delle attività di trattamento contenente le informazioni indicate dall'art. 30, par. 1, del Regolamento;

4. la designazione di un *Data Protection Officer* (DPO), ex art. 37 del Regolamento;

Atteso che in tale contesto normativo e di sistema, questa Azienda USL, in qualità di Titolare del trattamento:

1. ha proceduto ad una revisione dell'informativa generale sul trattamento dei dati personali, recependo le indicazioni ed osservazioni avanzate in seno al "gruppo di lavoro privacy AVEN", gruppo coordinato dalle direzioni amministrative e costituito dai referenti aziendali privacy di ciascuna Azienda aderente all'Area Vasta Emilia Nord, il cui testo è depositato agli atti del Comitato Privacy;

2. ha recepito una bozza di procedura per la gestione delle violazioni dei dati personali, come elaborata nell'ambito del suddetto gruppo di lavoro allargato a tecnici informatici di ciascuna Azienda, il cui testo è depositato agli atti del Comitato Privacy;

3. ha recepito una bozza di Registro delle attività di trattamento così come elaborato dal "gruppo regionale privacy", da implementare secondo le specificità dei trattamenti eseguiti e da eseguire, il cui testo è depositato agli atti del Comitato Privacy;

4. nel ritenere opportuno avvalersi della possibilità prevista dall'art. 37, par. 3, del Regolamento, stante il contesto normativo e di sistema l'Azienda Usl di Reggio Emilia, l'Azienda USL di Modena, e l'Azienda Ospedaliero - Universitaria di Modena, sentito il parere favorevole della Regione Emilia Romagna, hanno proceduto all'individuazione di un unico DPO, nella persona della Dr.ssa Erica Molinari, formalmente nominata, rispettivamente, con le Deliberazioni numero: -166/2018 - 110/2018 - 90/2018;

5. ha proceduto contestualmente ad aggiornare, anche alla luce dello sviluppo tecnologico intervenuto, il regolamento recante le linee guida sull'uso dei sistemi ICT, (adottato inizialmente con deliberazione n.189/2009, rispetto al quale sono fatte salve le disposizioni relative alle modalità dei controlli e verifiche di sicurezza), il cui testo è depositato agli atti del Comitato Privacy, e viene adottato nella sua versione aggiornata, per fornire rapidamente ai professionisti le indicazioni operative necessarie a garantire una maggiore sicurezza nelle modalità di trattamento dei dati personali;

Richiamata inoltre la delibera del Direttore Generale n.16/2018 avente ad oggetto "Costituzione del Comitato Aziendale per la gestione degli aspetti applicativi connessi a quanto previsto dal D.Lgs. 196/2003 - e per quanto innovato - dal Regolamento (UE) Generale sulla Protezione dei dati o GDPR n. 2016/679.", con la quale, alla luce della fusione dell'Azienda Usl di Reggio Emilia e dell'Azienda Ospedaliera Santa Maria Nuova, ai sensi della Legge Regionale E.R. n.9/2017, si determinava l'istituzione di un gruppo di lavoro multidisciplinare vocato ad aggiornare ed uniformare tutte le attività che fin dal secondo semestre 2003 erano state poste in essere in ottemperanza al dettato normativo allora vigente e concernente la protezione dei dati personali;

Preso atto della delibera del Direttore Generale n.145/2018, all'oggetto "Determinazioni in merito alla protezione dei dati personali all'interno della Azienda Usl di Reggio Emilia, alla luce del D.Lgs.196/2003 e del Regolamento (UE) generale sulla protezione dei dati n. 2016/679", con la quale si provvedeva a perfezionare e unificare l'esistente schema di regolamento per il trattamento e la tutela dei dati personali all'interno dell'Azienda Usl di Reggio Emilia-IRCCS, ai sensi della Legge Regionale E.R. n.9/2017, avendo tuttavia presente i nuovi principi già inseriti nel regolamento europeo;

Richiamato inoltre il verbale della seduta del Comitato Privacy del 18/05/2018, nel quale, tra i diversi adempimenti inerenti il mandato ricevuto, è definito di proporre al Titolare l'istituzione di un ufficio privacy, il cui responsabile costituisca principale interfaccia per il DPO, per il Comitato Privacy nonché per i referenti dipartimentali che verranno nominati, con compiti, tra gli altri, di creare un raccordo tra le varie strutture aziendali affrontando le tematiche privacy specifiche e trasversali;

L'ufficio viene individuato, per la rilevanza aziendale e la valenza trasversale, quale articolazione del Dipartimento Amministrativo;

Rilevato che detto ufficio, in via generale e non esaustiva sarà chiamato a garantire:

- funzione di studio e approfondimento continuo della normativa in materia di protezione dei dati personali e di accesso agli atti, per la sua corretta applicazione in ogni ambito aziendale;
- impostazione le procedure aziendali per l'applicazione pratica di detta normativa, ne cura i relativi adempimenti e predispone la necessaria documentazione (pareri, informative, modulistica, atti di nomina ...);
- attività di consulenza, sia per la direzione strategica aziendale, che nei confronti delle varie articolazioni organizzative;
- predisposizione e divulgazione della "policy" aziendale sulla protezione dei dati, attraverso il programma di formazione e la diffusione delle informazioni attraverso la Intranet e il sito Internet aziendali;
- attività in sinergia con il Servizio ICT, in particolare nella applicazione dei principi della privacy by design e della privacy by default, oltre che nel controllo sul corretto funzionamento degli applicativi aziendali, in termini di abilitazioni/autorizzazioni all'accesso agli stessi;

- con l'entrata in vigore del Regolamento Europeo nel maggio 2018, svolgerà ulteriori e nuove attività propedeutiche all'adeguamento della Azienda alle nuove norme: valutazione di impatto delle attività istituzionali sulla privacy, redazione del registro dei trattamenti, valutazione dei rischi, attività di audit, ridefinizione dei ruoli e delle responsabilità all'interno della Azienda, con il supporto del Comitato Privacy;
- collaborazione con il Responsabile Gestione Documentale e con ICT per la corretta applicazione del Codice dell'Amministrazione Digitale, con l'obiettivo di favorire la dematerializzazione nei rapporti con i dipendenti e gli utenti, tenendo conto delle inevitabili connessioni con la normativa privacy e dei relativi limiti;
- cura di una corrente e corretta archiviazione, anche digitale, dei documenti aziendali inerenti la materia complessiva, con riferimento specifico all'implementazione della sezione web dedicata;

Vista la nota del Direttore Generale del 21/05/2018, giacente in atti, nella quale si conferma l'istituzione dell'ufficio privacy, specificando che, trattandosi di funzione strategica in ambito aziendale, la stessa viene individuata quale articolazione del Dipartimento Amministrativo; il Responsabile, per la funzione ricoperta e la rilevanza strategica, è invitato permanente alle riunioni del Board di Direzione Strategica, per gli aspetti rilevanti di programmazione, in analogia alle funzioni afferenti allo staff del Direttore Generale;

Precisato che l'individuazione del Responsabile dell'ufficio privacy avverrà con successivo apposito provvedimento;

Ritenuto altresì opportuno:

- avvalersi del citato Comitato Privacy, che oltre alle funzioni sopra elencate, svolga il ruolo di supporto ai fini della valutazione dei potenziali casi di *data breach* in termini di probabilità e gravità dei rischi per i diritti e le libertà degli interessati;

- di mantenere, per quanto possibile, l'assetto organizzativo della Azienda in ordine ai profili delle responsabilità in tema di protezione dei dati, procedendo mediante un successivo atto deliberativo ad hoc, alla individuazione dei "delegati al trattamento" in luogo dei "responsabili interni del trattamento dei dati", figura non più prevista dal DGPR;

Acquisito il parere favorevole del Direttore Amministrativo e del Direttore Sanitario, espresso ai sensi dell'art. 3 del D. Lgs. n. 502/92 e successive modificazioni ed integrazioni;

DELIBERA

1) Di dare atto con la presente deliberazione delle misure e degli adempimenti preliminari alla definitiva applicazione del GDPR fino ad ora adottati da questa Azienda, in linea con le priorità suggerite dalla Autorità Garante alle amministrazioni pubbliche, ai fini di un primo adeguamento della Azienda stessa alla nuova normativa europea sulla protezione dei dati personali; in particolare;

2) Di provvedere alla comunicazione dei dati di contatto del DPO al Garante per la protezione dei dati personali;

3) Di adottare il Registro delle attività di trattamento redatto dal "gruppo privacy regionale", tenuto anche presso il Comitato Privacy ed eventualmente integrarlo nel tempo sulla base delle specificità proprie dei trattamenti eseguiti e/o da eseguire;

4) Di adottare l'informativa generale sul trattamento dei dati personali redatta dal "gruppo di lavoro privacy AVEN" il cui testo è depositato agli atti del Comitato Privacy;

5) Di provvedere a darne ampia pubblicità mediante pubblicazione sul sito istituzionale dell'ente ed affissione nei luoghi aperti al pubblico;

6) Di adottare la procedura per la gestione delle violazioni dei dati personali, come elaborata nell'ambito del suddetto gruppo di lavoro, il cui testo è depositato agli atti del Comitato

Privacy e di provvedere a darne ampia pubblicità mediante pubblicazione sulla rete intranet dell'ente;

7) Di adottare l'aggiornato regolamento recante le linee guida sull'uso dei sistemi ICT, anche per fornire rapidamente ai professionisti le indicazioni operative necessarie a garantire una maggiore sicurezza nelle modalità di trattamento dei dati personali, il cui testo è depositato agli atti del Comitato Privacy;

8) Di istituire apposito ufficio privacy, le cui attività sono dettagliate in parte espositiva ed il cui responsabile costituirà principale interfaccia per il DPO, per il Comitato Privacy nonché per i referenti dipartimentali che verranno nominati, con compiti, tra gli altri, di creare un raccordo tra le varie strutture aziendali affrontando le tematiche privacy specifiche e trasversali;

9) Di dare atto che trattandosi di funzione strategica in ambito aziendale, la stessa viene individuata quale articolazione del Dipartimento Amministrativo, ed il Responsabile, per la funzione ricoperta e la rilevanza strategica, è invitato permanente alle riunioni del Board di Direzione Strategica, per gli aspetti rilevanti di programmazione, in analogia alle funzioni afferenti allo staff del Direttore Generale;

10) Di mantenere, per quanto possibile, l'assetto organizzativo della Azienda in ordine ai profili delle responsabilità in tema di protezione dei dati, procedendo mediante un successivo atto deliberativo ad hoc, alla individuazione dei "delegati al trattamento" in luogo dei "responsabili interni del trattamento dei dati", figure non più previste dal DGPR;

11) Di individuare quale responsabile del procedimento ai sensi della legge n. 241/90 la dr.ssa Marina Ferrari, Coordinatore del Comitato Privacy, Direttore del Servizio Gestione Affari Assicurativi;

12) Di trasmettere copia della presente deliberazione al Collegio Sindacale, al Direttore Amministrativo, al Direttore Sanitario, al Direttore delle Attività Socio Sanitarie, ai Distretti Aziendali, al Presidio Ospedaliero, ai Dipartimenti di Sanità Pubblica/Salute Mentale e Dipendenze Patologiche/Farmaceutico/Cure Primarie Aziendale, alle Funzioni di Staff, ai Programmi Aziendali, ai Servizi Amministrativi, ai Servizi Tecnici, al Direttore Scientifico IRCCS, alla Direzione delle Professioni Sanitarie.

Letto, approvato e sottoscritto

Firma apposta digitalmente da:
Il Direttore Generale
Dott. Fausto Nicolini

Sulla presente delibera hanno espresso il parere favorevole:

Firma apposta digitalmente da:
Il Direttore Sanitario
Dott.ssa Cristina Marchesi

Firma apposta digitalmente da:
Il Direttore Amministrativo
Dott.ssa Eva Chiericati

Documento firmato digitalmente e archiviato nel rispetto della normativa vigente.
Il presente documento e' una copia elettronica del documento originale depositato presso gli archivi dell'A.U.S.L. di Reggio Emilia.

B3-04-8F-09-92-D2-C4-C2-32-D7-B5-57-55-54-24-9A-9C-E8-E9-E1

CAdES 1 di 3 del 24/05/2018 14:25:08

Soggetto: EVA CHIERICATI

S.N. Certificato: 04AE 0129 CC77 D95A

Validità certificato dal 21/12/2017 13:03:05 al 20/12/2023 13:03:05

Rilasciato da Actalis EU Qualified Certificates CA G1, Actalis S.p.A., IT

CAdES 2 di 3 del 24/05/2018 14:27:02

Soggetto: CRISTINA MARCHESI

S.N. Certificato: 6D1F B691 906E ABA9

Validità certificato dal 21/12/2017 13:31:57 al 20/12/2023 13:31:57

Rilasciato da Actalis EU Qualified Certificates CA G1, Actalis S.p.A., IT

CAdES 3 di 3 del 24/05/2018 16:50:28

Soggetto: FAUSTO NICOLINI

S.N. Certificato: 423B F4C0 1188 3F70

Validità certificato dal 21/12/2017 13:40:38 al 20/12/2023 13:40:38

Rilasciato da Actalis EU Qualified Certificates CA G1, Actalis S.p.A., IT
