SERVIZIO SANITARIO REGIONALE
EMILIA-ROMAGNA
Azienda Unità Sanitaria Locale di Piacenza

DELIBERAZIONE DEL DIRETTORE GENERALE

N° 122 DEL **23/05/2018**

Il DIRETTORE GENERALE acquisiti i pareri preventivi, favorevoli, del Direttore Amministrativo, del Direttore Sanitario e, ove previsto per competenza, del Direttore dell'attività Socio Sanitaria.

A D O T T A

la deliberazione avente per oggetto:

REGOLAMENTO UE N. 2016/679 IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (GDPR) - DETERMINAZIONI

DIRETTORE GENERALE	**Dott. Ing. Luca Baldino**	**FIRMATO**
DIRETTORE AMM.VO	Dott.ssa Maria Gamberini	**FIRMATO**
DIRETTORE SANITARIO	Dr. Guido Pedrazzini	**FIRMATO**
DIRETTORE ATTIVITA' SOCIO SANITARIA	Dott.ssa Costanza Ceda	

IL DIRETTORE GENERALE
Dott. Ing. Luca Baldino

OGGETTO: REGOLAMENTO UE N. 2016/679 IN MATERIA DI PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI (*GDPR*) - DETERMINAZIONI

IL DIRETTORE GENERALE

Su proposta del Dott. Alberto Merli – Responsabile dell'U.O. Gestione Flussi Documentali - che, contestualmente all'apposizione della firma in calce alla presente proposta, attesta la legittimità della medesima in ordine ai contenuti ed il rispetto dei requisiti formali e sostanziali del procedimento;

Premesso che:

- la disciplina introdotta dal Regolamento europeo per la protezione dei dati personali, Regolamento (UE) 2016/679 (c.d. *GDPR*), diventerà direttamente applicabile in tutti gli Stati membri dell'Unione Europea a partire dal 25 maggio 2018;
- la principale novità introdotta dal Regolamento consiste nell'affrontare il tema della tutela dei dati personali attraverso un approccio basato sulla valutazione del rischio, in luogo del precedente approccio basato su adempimenti, e consegna la protezione dei dati nelle mani del Titolare del trattamento il quale, grazie al principio di responsabilizzazione, ("*accountability*") potrà, nei limiti e dentro i parametri delineati dal Regolamento, adottare le misure che ritiene più opportune e comprovare il conseguimento degli obiettivi che ha raggiunto nel rispetto dei principi che presiedono il trattamento (lecito) dei dati personali;
- l'implementazione del "*sistema privacy*" delineato dal *GDPR* implica la necessità di generare nell'organizzazione la piena consapevolezza del rischi inerenti ai trattamenti dei dati e le responsabilità connesse, nonché l'affermazione di una cultura della protezione dei dati quale parte integrante dell'intero *asset* informativo di un'organizzazione, con particolare attenzione ai dati sanitari (ivi compresi i dati biometrici e genetici), nonché ai cosiddetti dati sensibili sotto il profilo dei diritti e delle libertà fondamentali dell'individuo;
- tra gli adempimenti di più ampio impatto, anche per le pubbliche amministrazioni, rientra certamente la designazione ed il ruolo del *Data Protection Officer* (DPO) o, nella versione italiana, *Responsabile della Protezione dei Dati* (RPD), figura prevista dall'art.37 del *GDPR*;

Atteso che:

- in tale contesto normativo e di sistema, questa Azienda USL, unitamente all'Azienda sanitaria di Parma e all'Azienda Ospedaliero-Universitaria di Parma, ha ritenuto opportuno procedere all'individuazione di un unico DPO esterno per tutte e tre le Aziende, considerando che alcune figure che all'interno delle singole organizzazioni avrebbero potuto ricoprire detto ruolo, anche e soprattutto in virtù dell'esperienza maturata sul tema specifico, sono considerate dallo stesso GDPR incompatibili con il ruolo di DPO (come ad esempio il Responsabile dei Sistemi Informativi, Responsabile della Trasparenza, Responsabile della Gestione delle Risorse Umane);
- al fine di individuare la figura più idonea a ricoprire il ruolo è stata indetto un avviso pubblico, gestito, per conto di tutte le tre aziende succitate, dall'Azienda Sanitaria di Parma;
- al termine della suddetta procedura mediante avviso pubblico, è risultata aggiudicataria la società *Compliance Officer e Data Protection* di Polito dott.ssa Filomena – via Modda 79, 56021 Cascina (PI);

Visto il provvedimento n. 585 del 18 maggio 2018 con la quale il Direttore del Servizio Logistica e Gestione Amministrativa Lavori Pubblici dell'Azienda USL di Parma ha approvato i verbali di gara e conseguente aggiudicazione definitiva del servizio di "*Data Protection Officer* (DPO) e consulenza in materia di protezione dati personali" di cui al Regolamento UE n. 679/2016 del

Parlamento Europeo e del Consiglio (GDPR), per l'Azienda USL di Parma (AUSL Parma), l'Azienda Ospedaliero Universitaria di Parma (AOU Parma) e l'Azienda USL di Piacenza (AUSL Piacenza), nell'ambito dell'Area Vasta Emilia Nord (AVEN), per il periodo 23/05/2018 – 31/12/2019;

Richiamata la determina n.121 del 21 maggio 2018 con la quale il Direttore dell'U.O. Acquisizione Beni e Servizi di questa Azienda USL ha recepito gli esiti della procedura negoziata esperita dall'AUSL di Parma;

Considerato che i compiti del DPO, previsti dall'art.39 del *GDPR,* sono:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento, nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati, nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;
d) cooperare con l'autorità di controllo;
e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione;

considerando debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo;

Ritenuto di pertanto, ai sensi dell'art. 37 del *GDPR*, di designare DPO di questa Azienda la società *Compliance Officer e Data Protection* di Polito dott.ssa Filomena con sede in Cascina (PI);

Ritenuto, in occasione dell'avvenuta nomina del DPO, di 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 attuativo del suddetto *GDPR*, testo peraltro attualmente all'esame delle competenti commissioni parlamentari per il parere di competenza e, pertanto, non ancora approvato in via definitiva;

Visto, in relazione alle attività già svolte in attuazione del predetto *GDPR*, il "*gruppo regionale privacy*" ha prodotto un modello di registro delle attività di trattamento previsto dall'art.30, comma 1 del *GDPR* medesimo, uniforme per tutte le aziende*;*

Rilevato che il documento regionale, in conformità a quanto previsto dal suddetto art.30, contiene:

- nome e dati di contatto del Titolare, del DPO e del Contitolare, ove presente;
- numero progressivo del trattamento;
- descrizione del trattamento;
- finalità del trattamento;
- presupposti normativi del trattamento;
- Responsabile esterno del trattamento;
- categoria di interessati;
- categoria dei dati personali trattati;
- categoria dei soggetti destinatari;

- trasferimento di dati personali *extr*a UE con l'indicazione del Paese Terzo e, per i trasferimenti di cui al secondo comma dell'art.49 del *GDPR*, la documentazione delle garanzie adeguate;
- descrizione generale delle misure di sicurezza tecniche ed organizzative ritenute adeguate;
- termine ultimo previsto per la cancellazione del dato;

Considerato che il suddetto registro è stato e sarà implementato da questa Azienda USL, secondo la propria *policy* in materia di privacy, la propria organizzazione e i documenti di protezione dati, nonché in relazione agli applicativi *software* destinati a gestire i singoli trattamenti, fermo restando che il registro medesimo è da considerarsi quale documento "dinamico" e, pertanto, soggetto a variazioni e/o integrazioni;

Fatto presente che il suddetto registro, integrato da questa Azienda USL secondo le proprie specificità, è depositato presso l'U.O. Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo (UOSIT) a disposizione sia dell'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy), sia di chiunque possa vantare un legittimo interesse alla sua consultazione;

Visto l'art.12 del *GDPR* ove è stabilito che il Titolare adotti misure appropriate per fornire all'interessato tutte le informazioni previste dagli artt.13 e 14 del *GDPR* stesso;

Dato atto che è stato attivato un tavolo di lavoro AVEN, coordinato dalle direzioni amministrative, ai fini di dare attuazione alle disposizioni del *GDPR* cui sono stati affidati i compiti di

- definire i modelli di informazione secondo quanto previsto dall'art. 13 del GDPR;
- predisporre una procedura condivisa per la gestione di Data Breach e del registro delle violazioni;

Atteso che nell'ambito delle attività svolte dal tavolo di lavoro AVEN è stato predisposto e condiviso un modello d'informazione (che corrisponde all'informativa prevista dal Codice Privacy), da fornire a tutti i cittadini utenti/pazienti al momento in cui i loro dati personali vengono acquisiti e che nel suddetto modello - costituito da un'informazione di carattere generale - sono previste tutte le informazioni di cui al già citato art.13 del *GDPR*, fermo restando che il modello medesimo è da considerarsi quale documento "dinamico" e, pertanto, soggetto a variazioni e/o integrazioni;

Fatto presente che il suddetto modello è depositato presso l'U.O. Gestione Flussi Documentali a disposizione dell'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy);

Atteso inoltre che il medesimo tavolo in sede AVEN ha altresì redatto una procedura relativa ai *data breach* ex art.32 del *GDPR*, procedura depositata presso l'U.O. Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo (UOSIT) a disposizione dell'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy), in cui sono state previste le modalità operative in ordine a:

- scopo della procedura e ambito di applicazione della medesima;
- gestione del *data breach* interno alla struttura;
- modalità e profili di notifica al Garante Privacy;
- gestione del *data breach* esterno alla struttura,
- modalità di comunicazione agli interessati;
- schema di valutazione dei possibili scenari;
- registro delle violazioni;

Ritenuto pertanto di approvare la suddetta procedura condivisa in sede AVEN;

Richiamata la deliberazione n. 260/2005 con la quale erano stati assunte le prime decisione in attuazione del cosiddetto "Codice Privacy" (decreto legislativo n.196/2003);
Atteso che, in particolare, erano stati individuati quali "*Responsabili interni del trattamento*", ai sensi e per gli effetti dell'art. 29 del D.lgs. n.196/2003, i Direttori pro-tempore delle Unità Operative Complesse e Semplici Dipartimentali, stabilendo nel contempo che dovessero intendersi quali "*incaricati*", ai sensi per gli effetti dell'art.30 del suddetto decreto legislativo, tutti gli altri dipendenti e collaboratori, a qualsiasi titolo, di questa Azienda USL;

Evidenziato come il *GDPR* preveda che il Titolare del trattamento (nel caso specifico di questa Azienda USL) possa nominare quelli che vengono ora denominati "*delegati al trattamento*" e che lo stesso Titolare, o i delegati, possano individuare le "*persone autorizzate al trattamento dei dati*";

Ritenuto di procedere all'individuazione dei "*delegati al trattamento*" e delle "*persone autorizzate*" in coerenza con l'assetto organizzativo dell'Azienda in ordine ai profili di responsabilità, ricorrendo allo stesso criterio di cui alla citata delibera n.260/2005, nominando quindi soggetti "*delegati al trattamento*" i Direttori pro-tempore delle Unità Operative Complesse e Semplici Dipartimentali e di stabilire che "*persone autorizzate al trattamento*" siano da intendersi tutti gli altri dipendenti e collaboratori, a qualsiasi titolo, di questa Azienda USL;

Dato atto che l'elenco dei Direttori pro-tempore delle UU.OO. complesse e semplici dipartimentali e, di conseguenza, dei delegati al trattamento, è pubblicato sul sito *web* di questa Azienda USL a beneficio di chiunque lo voglia consultare;

Considerato che:

- il GDPR dispone altresì, all'art.28, che qualora il trattamento dei dati debba essere effettuato da soggetto esterno all'organizzazione del Titolare, questi debba incaricare tale soggetto quale "*Responsabile del trattamento*", previa contrattualizzazione mediante contratto o altro atto giuridico a norma del diritto dell'UE o degli Stati membri;
- il contratto, che vincola il Responsabile al Titolare, deve definire la durata del trattamento, la natura e le finalità del medesimo, le tipologie dei dati trattati e le categorie di interessati, gli obblighi e i diritti del Titolare, a patto che il Responsabile sia autorizzato a trattare i dati solo previa istruzione documentata del Titolare e offra tutte le garanzie previste dal succitato art.28;
- il nuovo impianto normativo lambisce pertanto anche il ruolo del Responsabile del trattamento, il quale è insignito di nuovi compiti rispetto al passato, condivide in certa misura le responsabilità del Titolare in ordine al risarcimento del danno a terzi, ed è oggetto di autonome sanzioni amministrative, a differenza di quanto avveniva con il Codice Privacy, ove la sanzione amministrativa era sempre diretta contro il Titolare;
- l'individuazione del Responsabile non avviene più, quindi, a discrezione del Titolare, ma è un atto dovuto e in ogni caso la designazione del Responsabile emerge "ex se" dallo stato di fatto. Il Titolare e il Responsabile regolano, come visto, i loro rapporti contrattualmente, ma non sarà possibile forzare l'assetto contrattuale per definire i reciproci ruoli: l'assetto contrattuale rispecchierà, invece, il concreto "potere" che questi soggetti eserciteranno sul trattamento dei dati personali, prendendo o meno decisioni in ordine alle finalità e ai mezzi del trattamento stesso;
- le garanzie di affidabilità del Responsabile, ad esempio quando si esternalizzerà un servizio (outsourcing), dovranno pertanto essere valutate attentamente già in fase di affidamento dato che, come già avveniva con il Codice Privacy, il trattamento potrà essere affidato dal Titolare solo a chi presenti "*garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*";

Ritenuto, nelle more dell'emanazione, da parte del Garante Privacy, di un modello di contratto da adottare da parte di ciascun Titolare per il conferimento dell'incarico di Responsabile del trattamento, da intendersi quale Responsabile esterno all'organizzazione aziendale, di predisporre un modello di contratto per la nomina a Responsabile esterno di tutti quei soggetti giuridici (enti, società, associazioni, ecc.) che trattano dati sensibili per conto di questa Azienda USL nell'ambito di rapporti contrattuali in essere o di contratti/convenzioni che verranno stipulati, fermo restando che il modello medesimo dovrà essere adattato alle diverse tipologie di contratto, secondo le specificità delle singole attività affidate in outsourcing;

Ritenuto di procedere alla formalizzazione della nomina del "*referente aziendale privacy*", individuato, su proposta del Direttore Amministrativo, nel Dott. Alberto Merli – Responsabile dell'U.O. Gestione Flussi Documentali – che peraltro ricopre da tempo di fatto il ruolo in virtù dell'esperienza maturata, prima quale Dirigente dell'U.O. Affari generali e Legali e, successivamente, quale Responsabile della suddetta U.O. Gestione Flussi Documentali, cui compete, secondo l'organizzazione aziendale, la materia privacy per gli aspetti giuridico-amministrativi;

Atteso che con deliberazione n.491 del 24 dicembre 2009 era stato costituito un "gruppo di lavoro privacy" con il compito di:

- individuare le azioni e gli adempimenti necessari per la piena applicazione della normativa di cui al Codice Privacy,
- esaminare, per quanto di competenza, le istanze d'accesso qualora le stesse si ponessero in potenziale conflitto con la protezione dei dati personali di terzi;
- programmare, d'intesa con l'U.O. Qualità e Formazione, le iniziative formative in materia di privacy;
- svolgere funzioni di consulenza giuridica ed esprimere pareri a beneficio della Direzione Strategica e dei Responsabili privacy;
- curare i rapporti con l'Autorità Garante, nei limiti delle proprie competenze;

Atteso che per effetto della nuova normativa europea in materia di protezione dei dati personali, si ritiene doveroso rivedere la composizione del gruppo medesimo, da intendersi quale gruppo di lavoro multidisciplinare, anche a supporto delle attività del DPO;

Ritenuto pertanto di costituire il suddetto gruppo nella seguente composizione:

RUOLO	TITOLARE	SOSTITUTO/I
Referente aziendale privacy (coordinatore)	Alberto Merli	
Direttore UOSIT e del Dipartimento Interaziendale ICT	Flavio Bisotti	Marco Sverzellati Fabio Zazzera
Direttore Medico	Vincenzo Nardacchione	Flavio Santilli
Direttore Assistenziale	Mirella Gubbelini	Cristina Vedovelli

Stabilito che i compiti assegnati al suddetto gruppo, che potrà essere di volta in volta integrato con altre professionalità a seconda dei temi che dovrà trattare e delle decisioni che dovrà assumere nell'ambito delle proprie competenze, sono, oltre a quanto già definito con la citata deliberazione n. 491 del 24 dicembre 2009, essenzialmente i seguenti:

- attivarsi – su impulso del referente aziendale privacy che coordina il gruppo – ai fini di vagliare i potenziali casi di *data breach* dal punto di vista dell'impatto sulla protezione dei dati, attività propedeutica alle valutazioni e alle decisioni di competenza del referente medesimo, del DPO e del Titolare del trattamento, sino all'eventuale notifica al Garante Privacy prevista dall'art.33

del GDPR; tutto ciò nell'ambito dei compiti e delle responsabilità previsti, oltre che dalla normativa, anche dalla procedura relativa ai *data breach*;

- fornire supporto al DPO – che ha facoltà di intervenire agli incontri del gruppo - nello svolgimento delle attività proprie di tale figura;

Considerato che il presente atto deliberativo non comporta l'assunzione di alcun onere finanziario in capo a questa Azienda USL;

Per quanto esposto in premessa;

Atteso che i pareri favorevoli del Direttore Amministrativo e del Direttore Sanitario si intendono acquisiti tramite la firma digitale apposta dai medesimi in calce alla presente deliberazione;

D E L I B E R A

1. di designare *Data Protection Officer* (DPO) di questa Azienda, ai sensi dell'art. 37 del *GDPR*, la società "*Compliance Officer e Data Protection"* di Polito dott.ssa Filomena con sede in Cascina (PI);

2. di adottare il *registro delle attività di trattamento*, redatto dal gruppo dei responsabili della privacy della Regione Emilia Romagna, il cui testo, integrato da questa Azienda USL sulla base delle proprie specificità, è depositato presso l'U.O. Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo (UOSIT) a disposizione sia dell'Autorità Garante per la Protezione dei Dati Personali, sia di chiunque possa vantare un legittimo interesse alla sua consultazione;

3. di adottare un *modello d'informazione*, ai sensi dell'art.12 del *GDPR*, depositato presso la U.O. Gestione Flussi Documentali, a disposizione dell'Autorità Garante per la Protezione dei Dati Personali, fermo restando che il modello medesimo è da considerarsi quale documento "dinamico" e, pertanto, soggetto a variazioni e/o integrazioni;

4. di approvare la procedura relativa ai *data breach* depositata presso l'U.O. Sistemi Informativi, Telecomunicazioni e Reingegnerizzazione di Processo (UOSIT) a disposizione dell'Autorità Garante per la Protezione dei Dati Personali (Garante Privacy);

5. di individuare i soggetti "*delegati al trattamento*" nelle persone dei Direttori pro-tempore delle Unità Operative Complesse e Semplici Dipartimentali e di stabilire che "*persone autorizzate al trattamento*" siano da intendersi tutti gli altri dipendenti e collaboratori, a qualsiasi titolo, di questa Azienda USL;

6. di adottare il *modello di contratto* per la nomina a Responsabile esterno di tutti quei soggetti giuridici che trattano dati sensibili per conto di questa Azienda USL nell'ambito di rapporti contrattuali in essere o di contratti/convenzioni che verranno stipulati, fermo restando che il modello medesimo dovrà essere adattato alle diverse tipologie di contratto, secondo le specificità delle singole attività affidate in *outsourcing*;

7. di nominare del Dott. Alberto Merli – Responsabile dell'U.O. Gestione Flussi Documentali – quale *referente aziendale privacy*, per le motivazioni esposte in premessa;

8. di costituire il *gruppo multidisciplinare privacy*, per le motivazioni e con i compiti declinati in premessa, nella seguente composizione:

RUOLO	TITOLARE	SOSTITUTO/I
Referente aziendale privacy (coordinatore)	Alberto Merli	
Direttore UOSIT e del Dipartimento Interaziendale ICT	Flavio Bisotti	Marco Sverzellati Fabio Zazzera
Direttore Medico	Vincenzo Nardacchione	Flavio Santilli
Direttore Assistenziale	Mirella Gubbelini	Cristina Vedovelli

9. di dare atto che il presente atto deliberativo non comporta l'assunzione di alcun onere finanziario in capo a questa Azienda USL.

Il Dirigente proponente
Dott. Alberto Merli

Documento firmato digitalmente e conservato in conformita'
e nel rispetto della normativa vigente in materia.
Il presente documento e' una copia elettronica del documento originale
depositato presso gli archivi dell'A.U.S.L. di Piacenza.

7E-61-BD-4E-E2-9D-02-DC-DC-9D-A7-F0-46-13-12-A2-05-95-84-E9

CAdES 1 di 4 del 23/05/2018 13:20:44

Soggetto: ALBERTO MERLI MRLLRT59B17G535W

Validità certificato dal 03/11/2017 02:00:00 al 03/11/2020 01:59:59

Rilasciato da ArubaPEC S.p.A. NG CA 3, ArubaPEC S.p.A., IT

CAdES 2 di 4 del 23/05/2018 15:12:12

Soggetto: MARIA GAMBERINI GMBMRA69T48H294I

Validità certificato dal 09/10/2017 02:00:00 al 09/10/2020 01:59:59

Rilasciato da ArubaPEC S.p.A. NG CA 3, ArubaPEC S.p.A., IT

CAdES 3 di 4 del 23/05/2018 18:41:17

Soggetto: LUCA BALDINO BLDLCU67L19F205V

Validità certificato dal 06/02/2017 02:00:00 al 07/02/2020 01:59:59

Rilasciato da ArubaPEC S.p.A. NG CA 3, ArubaPEC S.p.A., IT

CAdES 4 di 4 del 23/05/2018 18:34:57

Soggetto: PEDRAZZINI GUIDO TINIT-PDRGDU56M19D150L

Validità certificato dal 06/02/2018 02:00:00 al 06/02/2021 01:59:59

Rilasciato da ArubaPEC S.p.A. NG CA 3, ArubaPEC S.p.A., IT
