AO Brotzu

Deliberazione 2312

Adottata dal DIRETTORE GENERALE in data 24 OTT. 2018

Oggetto: Applicazione Regolamento UE N. 2016/679 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 (GDPR regolamento generale sulla protezione dei dati) – D.Lgs n.101/2018 : individuazione Designati

Pubblicata all'Albo Pretorio dell'Azienda a partire dal 25 OTT. 2018 per 15 giorni consecutivi e posta a disposizione per la consultazione.

Il Direttore Amministrativo

Il Direttore Generale Dott.ssa Graziella Pintus

coadiuvato da

Direttore Amministrativo Dott.ssa Laura Balata
Direttore Sanitario Dott. *Vinicio Atzeni*

Su proposta della S.S.D. Affari Generali

VISTO

- il Regolamento UE N. 2016/679 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);

- il D.Lgs n. 101 del 10 agosto 2018 " disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati persoanli, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/C£E (regolamento generale sulla protezione dei dati).

PREMESSO

- che la principale novità introdotta da Regolamento UE N. 2016/679 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, consegnando quindi la protezione dei dati al Titolare del trattamento che, grazie al principio di responsabilizzazione *("accountability")* adotterà, secondo quanto previsto dal Regolamento, le misure che riterrà più opportune per garantire il trattamento dei dati personali;

- altresì che implementare il sistema privacy secondo quanto previsto dal GDPR significa generare nell'organizzazione la piena consapevolezza dei rischi relativi ai trattamenti dei dati e le responsabilità connesse, nonché la cultura della protezione dei dati quale parte integrante dell'intera struttura informativa dell'organizzazione, con particolare attenzione ai dati sanitari e ai dati sensibili, ora denominati "categorie particolari di dati", sotto il profilo dei diritti e delle libertà fondamentali dell'individuo.

CONSIDERATO

- che l'art.37 del GDPR prevede che venga nominato il *Data Protection Officer* (DPO) ovvero del Responsabile per la Protezione dei Dati;

- che l'art.24 del GDPR prevede che, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il Titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento effettuato è conforme a quanto stabilito nel GDPR.

- che il D.Lgs n. 101 del 10.08.2018 all'art.2-quaterdecies, c.1 prevede che " Il titolare o il responsabile del trattamento possono prevedere, sotto la loro responsabilità e nell'ambito del loro assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità" ;

- che il D.Lgs n. 101 del 10.08.2018 all'art.2-quaterdecies, c.2 prevede che " Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta".

- che le persone Designate, dovranno definire, con il supporto della struttura tecnica, i trattamenti da inserire nello specifico registro;

SENTITO il *Data Protection Officer* che ha espresso parere favorevole

RITENUTO pertanto di dover procedere alla designazione delle persone fisiche a cui sono attribuiti specifici compiti e funzioni connessi al trattamento dei dati personali.

CON il parere favorevole del Direttore Amministrativo nonché del Direttore Sanitario

DELIBERA

Per i motivi esposti in premessa:

1) Di individuare le persone fisiche designate, ai sensi dell'art. 2 2-quaterdecies c.1,2 del D.lgs n. 101 del 10 agosto 2018, nelle persone dei Direttori di Struttura Complessa e dei Direttori di Struttura Semplice Dipartimentali e di stabilire che Persone Autorizzate al trattamento siano da intendersi tutti i dipendenti e collaboratori, a qualsiasi titolo, di questa Azienda Ospedaliera.
2) Di approvare il modello di nomina delle persone designate, e degli autorizzati alle attività di trattamento allegati A e B alla presente deliberazione per farne parte integrante e sostanziale.
3) Di demandare alla S.S.D. Affari Generali la pubblicazione sul sito Aziendale della presente deliberazione nella sezione Amministrazione Trasparente.

Il Direttore Amministrativo
Dott.ssa Laura Balata

Il Direttore Sanitario
Dott. Vinicio Atzeni

Il Direttore Generale
Dott.ssa Graziella Pintus

Resp. S.S.D. AA_GG R. Manattal

Allegato A
(Pagg. 3)

AO Brotzu

LETTERA DI INCARICO E ISTRUZIONI PER DESIGNATI DI PRIMO LIVELLO EX ART. 29 DEL REGOLAMENTO UE 2016/679 (GDPR) ED ART. 2-QUATERDECIES DEL D.LGS. 196/2003

Con il presente atto, l'Azienda Ospedaliera G. Brotzu, con sede legale in Cagliari, Piazzale Sandro Ricchi n. 1, codice fiscale e partita IVA 02315520920, nella persona del Direttore Generale, dott.ssa Graziella Pintus, in qualità di legale rappresentante, da ora in avanti anche **Titolare o Azienda**, secondo la vigente disciplina,

incarica

Il sig. /sig.ra - Dott./Dott.ssa _____, nato/a a _____ il _____, quale **Designato di I livello** relativamente allo svolgimento della propria attività istituzionale e per le funzioni di specifica competenza del Direttore di Struttura Complessa e Semplice Dipartimentale e con riguardo ai trattamenti che vengono effettuati nel contesto dell'attività istituzionale della struttura:

_____

e alle seguenti categorie di dati:

_____

al cui trattamento è stato preventivamente autorizzato, presso la sede dell'Azienda.

Il Designato/a di I livello al trattamento dichiara di aver preso conoscenza dei compiti a lui affidati e di essere al corrente di quanto stabilito dal **Regolamento UE 2016/679** (di seguito anche **GDPR**), nonché dal D.Lgs. 101/2018, e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in essi contenute, oggi o in futuro, individuate dal Titolare del trattamento e, in particolare:

- nominare mediante individuazione per iscritto gli autorizzati al trattamento, stabilendone i compiti e fornendo loro idonee istruzioni, oltre che vigilarne;
- richiedere, ove l'attività da svolgere non sia espressamente disciplinata dal presente documento di nomina, l'intervento del DPO mediante richiesta di parere sulla corretta modalità di trattamento dei dati personali;
- in relazione al Direttore della Struttura Complessa Tecnologie Informatiche, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più Amministratori di Sistema individuando, per essi, ulteriori misure finalizzate alla memorizzazione in modalità non alterabile e successiva conservazione del "foglio delle attività" relativamente agli interventi svolti sui sistemi informatici dell'Azienda contenenti dati personali di cui l'Azienda sia Titolare o Responsabile del trattamento;
- in relazione al Direttore della Struttura Complessa Tecnologie Informatiche, con l'ausilio degli Amministratori di Sistema, ove nominati, attribuire ad ogni autorizzato un Codice identificativo personale (USER–ID) per l'utilizzazione dell'elaboratore o del dispositivo, che deve essere individuabile e non riutilizzabile e la Chiave d'accesso (PASSWORD);
- vigilare sulla corretta custodia delle credenziali e delle password fornite agli autorizzati al trattamento e sull'uso degli strumenti informatici;
- cooperare alla redazione e all'aggiornamento del registro dei trattamenti ai sensi dell'art. 30 del GDPR;
- adottare, nell'organizzazione dei servizi di propria competenza, misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al GDPR, e sia idoneo a garantire il rispetto dei diritti e delle libertà fondamentali e procedere se necessario, al loro riesame;
- sottoscrivere, ove rientri nella sua competenza, gli atti di nomina a responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR, autorizzare (ove necessario) le attività dei sub-responsabili, e vigilare sul loro operato;

- verificare che siano attuate tutte le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato, ai fini di ridurre i rischi di distruzione o perdita dei dati, accessi non autorizzati, trattamenti non consentiti o non conformi alle finalità della raccolta, segnalando eventuali mancanze o criticità;
- comunicare tempestivamente al Titolare e al DPO l'inizio di ogni nuovo trattamento di dati personali, la modifica o la cessazione dei trattamenti in atto;
- vigilare sulla corretta conservazione dei documenti e degli archivi, sia in formato cartaceo che digitale, contenenti dati personali di cui l'Azienda sia Titolare o Responsabile del trattamento;
- vigilare e verificare che gli autorizzati al trattamento seguano quanto disposto in materia di utilizzazione di dispositivi di memorizzazione e sul divieto d'uso di dispositivi personali, se non espressamente autorizzati;
- vigilare e verificare che gli autorizzati al trattamento rispettino quanto stabilito relativamente alla duplicazione dei documenti dell'Azienda;
- informare senza ritardo l'Azienda nella eventualità che si siano rilevati dei rischi incombenti sul corretto trattamento dei dati personali;
- assicurare che il trattamento dei dati personali sia preceduto da idonee informazioni sul trattamento dei dati personali, anche ai sensi e per gli effetti degli artt. 77 e ss. del D.lgs 196/2003, in relazione alle modalità particolari per informare l'interessato e per il trattamento dei dati personali in ambito sanitario e (ove necessario) dalla manifestazione del consenso da parte dell'interessato;
- prestare la massima collaborazione nei confronti dell'Azienda, per le ipotesi di esercizio dei diritti ai sensi degli art. 15-22 del GDPR da parte degli interessati (accesso, rettifica, cancellazione, limitazione, blocco, etc.), comunicando senza ritardo al Titolare (e al DPO) ogni richiesta di esercizio dei diritti;

- assicurare che, con riferimento ai dati personali concernenti persone decedute, i diritti di cui agli articoli da 15 a 22 siano esercitati da chi abbia un interesse proprio o agisca a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione;
- rispondere tempestivamente alle richieste (es. richieste di accesso al materiale videoregistrato mediante i sistemi di videosorveglianza), eventualmente concordando con il DPO modalità e tempi della richiesta, ed eventuali reclami degli interessati, nonché offrire la massima collaborazione ed interagire con soggetti che, per legge, compiano verifiche, controlli o ispezioni sugli adempimenti riguardanti la tutela dei dati personali;
- verificare che i trattamenti di dati genetici, biometrici e relativi alla salute, siano conformi anche alle misure di garanzia disposte dal Garante ai sensi dell'art. 2-septies del D.Lgs. 196/2003;
- rispettare in maniera rigorosa quanto prescritto dal Regolamento Aziendale sull'uso degli strumenti informatici e di tutti gli altri documenti rilevanti in materia di protezione dei dati personali;
- dare, nel caso in cui constati o sospetti un incidente di sicurezza e di violazione dei dati personali (data breach), immediata comunicazione (e comunque entro 24 ore) al Titolare, al Direttore della Struttura Complessa Tecnologie Informatiche, e al DPO, includendo, ove possibile, una breve descrizione dell'evento;

_____, lì _____

Firma

_____

Il Designato di Primo livello nominato si impegna a:

- restituire la presente designazione, debitamente sottoscritta, entro __ giorni, con l'elencazione dei trattamenti di dati che vengono effettuati nella propria struttura, al fine di permettere l'aggiornamento del registro dei trattamenti;
- far sottoscrivere e inviare gli atti di nomina degli autorizzati al trattamento presso la propria struttura.

Allegato B (Pagg. 3)

AO Brotzu

LETTERA DI INCARICO E ISTRUZIONI PER GLI AUTORIZZATI AL TRATTAMENTO EX ART. 29-32 DEL REGOLAMENTO UE 2016/679 (GDPR) ED ART. 2-QUATERDECIES DEL D.LGS. 196/2003

Con il presente atto, il sottoscritto Dr. _____, nella sua qualità di Designato di primo livello (d'ora in avanti anche "**Designato**") in forza di atto del ____, prot. _____ dell'Azienda Ospedaliera G. Brotzu da ora in avanti anche "**Titolare" o "Azienda"**

nomina

Il sig. /sig.ra - Dott./Dott.ssa _____, nato/a a _____ il _____, quale **Autorizzato al trattamento dei dati personali** (di seguito anche "**Autorizzato**"), ai sensi degli artt. 29-32 del GDPR e dell'art. 2-quaterdecies del D.Lgs. 196/2003, relativamente allo svolgimento della propria attività all'interno della struttura e nell'ambito delle mansioni di propria competenza, ed in particolare quelle relative a _____ [*indicare genericamente le mansioni che importino trattamenti di dati personali*].

I dati personali che possono essere trattati dall'Autorizzato sono tutti quelli strettamente necessari all'espletamento delle proprie mansioni lavorative, quelli il cui trattamento è necessario al fine dell'adempimento di ulteriori funzioni delegate, nonché i dati personali ulteriori di seguito indicati: _____ [*specificare per ogni singolo dipendente*].

L'Autorizzato dichiara di aver preso conoscenza dei compiti a lui affidati e di essere al corrente di quanto stabilito dal **Regolamento UE 2016/679** (di seguito anche **GDPR**), nonché dal Codice della Privacy (d.lgs 196/2003, come emendato dal D.Lgs. 101/2018), e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in essi contenute, oggi o in futuro individuate dal Titolare del trattamento e, in particolare:

- attenersi alle istruzioni impartite dal Titolare (anche per il tramite del Designato), il quale, anche mediante periodiche verifiche e audit interni ed esterni, vigila sulla corretta osservanza delle stesse;
- consultare e fornire collaborazione all'attività del Data Protection Officer, sia per le sue funzioni di consulenza, che di controllo, che di cooperazione e punto di contatto con l'Autorità di controllo;
- informare senza ritardo il Designato nella eventualità che si siano rilevati dei rischi incombenti sul corretto trattamento dei dati personali, o che vi sia una variazione del rischio;
- garantire che il trattamento dei dati si svolga nel rispetto delle misure di sicurezza, e delle connesse misure aziendali, per quanto di propria competenza;
- adottare ogni misura idonea a ridurre il rischio di distruzione dati, perdita o accesso non autorizzato;
- rispettare gli obblighi di segretezza e non divulgazione dei dati di cui è venuto a conoscenza;
- nel caso in cui l'Autorizzato abbia ricevuto credenziali di autenticazione per il trattamento dei dati personali, le stesse devono essere conservate con la massima segretezza così come le parole chiave e i dispositivi di autenticazione in suo possesso e uso esclusivo;
- la parola chiave, quando è prevista dal sistema di autenticazione, deve rispondere ai seguenti principali requisiti di complessità, salvo ove diversamente disposto dal Regolamento Aziendale: almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi, non contenere riferimenti agevolmente riconducibili all'autorizzato. La parola chiave sarà modificata dall'autorizzato al primo utilizzo e, successivamente, almeno ogni 90 giorni. Le ultime tre parole chiave non dovranno essere riutilizzate;
- non lasciare in nessun caso incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali;
- non indicare o annotare le parole chiave e le credenziali di accesso ad aree riservate in spazi comuni o agevolmente accessibili, ad esempio mediante l'uso di agende, post-it o altre modalità

che siano in grado, anche solo potenzialmente, di mettere a rischio l'integrità e la disponibilità degli strumenti informatici o telematici dell'Azienda;

- controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali. I documenti cartacei contenenti dati personali devono essere conservati in archivi provvisti di serratura, e i documenti cartacei contenenti categorie particolari di dati devono essere, per quanto possibile, conservati in separato archivio, sempre provvisto di serratura;
- quando gli atti e i documenti contenenti dati personali e particolari categorie di dati di cui agli articoli 9 e 10 del GDPR (ivi compresi i dati relativi allo stato di salute), sono affidati al/agli Autorizzato/i al trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dall'Autorizzato/a fino alla restituzione;
- garantire che, all'interno dei locali adibiti al trattamento delle informazioni, non accedano persone prive di autorizzazione o siano oggetto di danneggiamenti intenzionali o accidentali. Deve altresì identificare e registrare i soggetti ammessi dopo l'orario di chiusura degli uffici stessi;
- impedire il danneggiamento, la manomissione, la sottrazione, la distruzione, o la copia di dati nei locali che gli sono stati affidati in custodia;
- trattare i soli dati la cui conoscenza sia necessaria e sufficiente per lo svolgimento delle operazioni da effettuare. Non è consentito l'accesso ai sistemi informatici per finalità non attinenti all'attività lavorativa o, comunque, per finalità differenti da quelle per le quali sia stata concessa l'abilitazione all'uso degli strumenti o l'accesso alle informazioni attraverso essi o in essi memorizzate;
- con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, restituire gli stessi al termine delle operazioni affidate;
- effettuare le copie di dati personali, oggetto di trattamento, esclusivamente se necessario e soltanto previa autorizzazione, generale o specifica, del Designato;

- omettere di trattare, duplicare, portare all'esterno dell'ambito aziendale o dall'ufficio qualsiasi dispositivo di memorizzazione (di qualsiasi natura) contenente dati nella disponibilità dell'Azienda o relativi alle attività da quest'ultima poste in essere in assenza di preventiva ed espressa autorizzazione;
- all'Autorizzato è vietato l'uso di dispositivi personali non espressamente autorizzati anche al fine di memorizzare o di esportare all'esterno immagini, registrazioni audio/video o altre informazioni relativi a luoghi, macchinari, documenti contenenti dati personali appartenenti al Titolare del trattamento;
- assicurarsi che il trattamento dei dati personali sia preceduto da idonee informazioni sul trattamento dei dati personali, anche ai sensi e per gli effetti degli artt. 77 e ss. del D.lgs 196/2003, in relazione alle modalità particolari per informare l'interessato e per il trattamento dei dati personali in ambito sanitario e (ove necessario) dalla manifestazione del consenso da parte dell'interessato;
- prestare la massima collaborazione nei confronti dell'Azienda, per le ipotesi di esercizio dei diritti ai sensi degli art. 15-22 del GDPR da parte degli interessati, comunicando senza ritardo al Designato e, se del caso, al Titolare (e al DPO) ogni richiesta di esercizio dei diritti;
- cooperare con il Designato e il Titolare al fine di rispondere tempestivamente alle richieste, eventualmente concordando con il DPO modalità e tempi della richiesta, ed eventuali reclami degli interessati, nonché offrire la massima collaborazione ed interagire con soggetti che, per legge, compiano verifiche, controlli o ispezioni sugli adempimenti riguardanti la tutela dei dati personali;
- rispettare in maniera rigorosa quanto prescritto dal Regolamento Aziendale sull'uso degli strumenti informatici e di tutti gli altri documenti rilevanti in materia di protezione dei dati personali;

- dare, nel caso in cui constati o sospetti un incidente di sicurezza e di violazione dei dati personali, immediata comunicazione al Designato, includendo, ove possibile, una breve descrizione dell'evento.

_____, lì _____

Firma

_____