REGIONE AUTONOMA DELLA SARDEGNA

AZIENDA OSPEDALIERO-UNIVERSITARIA DI SASSARI

Viale S. Pietro, 10 - 07100 SASSARI – C.F. - P. IVA 02268260904

A.D. MDLXII

DELIBERAZIONE N. 299 **DEL** 18.04.2018

Oggetto: **Adempimenti GDPR - Regolamento UE 679/2016 – Nomina Responsabile Protezione Dati (RPD/DPO) ex articolo 37 paragrafo 1 e deleghe ai Responsabili delle SC Affari Generali, Convenzioni e Rapporti con l'Università e ICT- Tecnologie della Comunicazione e dell'Informazione.**	
Struttura Proponente SC Affari Generali, Convenzioni e Rapporti con l'Università	**Conto di Costo** ----
Direttore della Struttura Proponente Dott. Antonio Solinas	**Responsabile del Procedimento** Dott. Antonio Solinas
Estensore: Dott. Giovanni Carlo Nicolino Manzoni	

Il Direttore della SC propone l'adozione del presente provvedimento, attestandone conformità alla norma, la corrispondenza del formato cartaceo al file inserito sul SISAR atti nonché l'utilità e l'opportunità per gli obiettivi aziendali e per l'interesse pubblico.

Il Direttore della SC: Dott. Antonio Solinas Firma_____

Il Responsabile della Struttura e il Responsabile del procedimento, con la sottoscrizione del presente atto, attestano che l'atto è legittimo nella forma e nella sostanza.

Il presente provvedimento contiene dati sensibili Si □ No ☒

Il Responsabile del procedimento: Dott. Antonio Solinas

Data 18 / 4 /2018 ***Firma***_____

Il Direttore della SC: Dott. Antonio Solinas

Data 18/4/2018 ***Firma***_____

Il Responsabile addetto al controllo di budget con la sottoscrizione del presente atto attesta che lo stesso

□ È □ NON È (le motivazioni sono allegate alla presente)

coerente con le proiezioni economiche comunicate alla Direzione Strategica.

Spesa prevista: ---------- C.E. n. _____

Il Direttore della SC Programmazione e Controllo di Gestione: Dott.ssa Sara Sanna

Data_____ ***Firma***_____

Il Responsabile del Bilancio con la sottoscrizione del presente atto attesta la copertura economico/finanziaria della spesa di cui al presente provvedimento.

Il Direttore della SC Bilancio e Contabilità : Dott.ssa Rosa Maria Bellu

Data_____ ***Firma***_____

Il Responsabile del Bilancio attesta altresì che la spesa non contrasta gli obiettivi Regionali di contenimento della spesa sanitaria e di rientro dal disavanzo (nota RAS Prot. 4801 del 29.12.2016).

Il Direttore della SC Bilancio e Contabilità: Dott.ssa Rosa Maria Bellu

Data_____ ***Firma***_____

Parere del Direttore Amministrativo: Dott. Lorenzo Pescini (Delibera del Direttore Generale. n. 378 del 02.11.2016)

Favorevole ☒ Non Favorevole □ (con motivazioni allegate al presente atto)

Data 18/4/18 ***Firma***_____

Parere del Direttore Sanitario: Dott. Nicolò Orrù (Delibera del Direttore Generale. n. 393 del 14.11.2016)

Favorevole ☒ Non Favorevole □ (con motivazioni allegate al presente atto)

Data 18/04/2018 ***Firma***_____

La presente Deliberazione si compone di n.10 pagine, di cui n.0 pagine di allegati, che ne formano parte integrante e sostanziale

IL DIRETTORE DELLA SC AFFARI GENERALI, CONVENZIONI E RAPPORTI CON L'UNIVERSITA'

Dott. Antonio Solinas

VISTO	il Decreto Legislativo n. 502 del 30.12.1992: "*Riordino della disciplina in materia sanitaria*" e s.m.i;
VISTO	il Decreto Legislativo n. 517 del 21.12.1999: "*Disciplina dei rapporti fra Servizio Sanitario Nazionale ed Università, a norma dell'art. 6 della legge 30 novembre 1998, n. 419*";
VISTO	il Protocollo d'Intesa sottoscritto in data 11.08.2017 dalla Regione Sardegna e dalle Università degli Studi di Cagliari e di Sassari;
VISTA	la Legge Regionale n. 23 del 17.11.2014: "*Norme urgenti per la riforma del Sistema Sanitario Regionale. Modifiche alle Leggi Regionali n. 23 del 2005, n. 10 del 2006 e n. 21 del 2012*" e s.m.i.;
VISTA	il Decreto del Presidente della Regione Sardegna n. 57 del 03.10.2016 con il quale veniva nominato il Direttore Generale dell'Azienda Ospedaliero – Universitaria di Sassari, Dott. Antonio D'Urso;
DATO ATTO	che il soggetto che propone il presente atto non incorre in alcuna delle cause di incompatibilità previste dalla normativa vigente, con particolare riferimento al Codice di Comportamento dei Pubblici Dipendenti e alla Normativa Anticorruzione e che non sussistono, in capo allo stesso, situazioni di conflitto di interesse in relazione all'oggetto dell'atto, ai sensi della L. 190 del 06/11/2012 e norme collegate;
VISTA	la Nota Prot. PG/2018/8531 del 18/04/2018 "*Adempimenti GDPR - Regolamento UE 679/2016 – Relazione sulle criticità, sullo stato di avanzamento attività e azioni richieste*", del Direttore della SC *ICT - Tecnologie dell'Informazione e della Comunicazione* in merito alle azioni necessarie per assicurare la conformità Aziendale rispetto alle disposizioni del nuovo GDPR;
CONSIDERATO	che la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale dell'individuo sancito a livello europeo dall'art. 8 della Carta dei Diritti Fondamentali dell'Unione;
PRESO ATTO	che in applicazione di tale diritto, il 27 aprile 2016 è stato adottato il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio *«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)»* (di seguito GDPR), in vigore in via immediata e diretta in tutti gli stati membri dal 24 maggio 2016 e applicabile a partire dal 25 maggio 2018;
CONSIDERATO	che - con l'entrata in vigore del Regolamento UE 2016/279 - non potranno più essere applicate le norme dell'attuale Codice Privacy (D.lgs. 196/2003) contrastanti con il primo, in quanto entrambe fonti primarie dove per il criterio cronologico la fonte successiva prevale sulla precedente;
PRESO ATTO	che tutti i trattamenti di dati personali dovranno essere resi conformi al GDPR entro la data del 25 maggio 2018 e che è ineludibile il dovere - da parte del Titolare – di allineare i sistemi, le procedure e le prassi interne delle Strutture aziendali al nuovo ordinamento;
PRESO ATTO	che la nuova normativa si limita ad indicare i principi e le finalità cui si deve attenere il Titolare, lasciandogli l'onere di trovare ed applicare le misure che ritenga migliori per la gestione sicura dei dati trattati e di dimostrare che le stesse siano adeguate ed efficaci *(c.d. accountability);*

PRESO ATTO che - dall'esame del Regolamento nel suo complesso - emerge con forza che il futuro della privacy non può più essere assicurato dal mero processo di conformità con il sistema normativo, ma piuttosto la garanzia della privacy deve costituire idealmente e fattivamente un modo di operare di default di un'organizzazione nella fase di progettazione e definizione dei processi *(privacy by design e by default);*

PRESO ATTO che - nell'incontro con le PP.AA. del 12 giugno 2016 - il Presidente dell'Autorità Garante ha auspicato un processo di riorganizzazione dei processi interni aziendali, che tenga in considerazione tre priorità operative:

- la designazione in tempi stretti del Responsabile della protezione dei dati (RPD, l'italianizzazione dell'acronimo DPO, Data Protection Officer, artt. 37-39);
- l'istituzione del Registro delle attività di trattamento (art. 30 e considerando 171);
- la notifica delle violazioni dei dati personali, i cosiddetti "*data breach*" (artt. 33 e 34).

PRESO ATTO che il predetto Regolamento introduce la figura del Responsabile della Protezione dei Dati (RPD o DPO), prevedendo l'obbligo per il Titolare del trattamento di designare la predetta figura *«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) e/o quando le principali attività del Titolare *"consistono nel trattamento, su larga scala, di categorie particolari di dati personali"* (art. 37, paragrafo 1, lett c);

CONSIDERATO che l'AOU Sassari è tenuta alla designazione obbligatoria del RPD/DPO nei termini previsti, rientrando nelle fattispecie previste dall'art. 37, par. 1, lett. a) e c) del GPDR;

VISTE le *"Linee Guida sui Responsabili della Protezione Dati – WP243"*, adottate il 13.12.2016 dal Gruppo di Lavoro istituito ex art. 29 Direttiva 95/46/CE in qualità di organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata;

CONSIDERATO che le predette disposizioni prevedono che il RPD/DPO, *"può essere un dipendente del titolare del trattamento o del responsabile del trattamento"* (art. 37, par. 6) e deve essere individuato *"in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'art. 39"* (art. 37, par. 5) e che *"il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal Titolare del trattamento o dal Responsabile del trattamento"* (considerando n. 97 del GDPR);

CONSIDERATO che i compiti del Responsabile della Protezione dei Dati attengono all'insieme dei trattamenti di dati effettuati dall'Ente;

PRESO ATTO che, ai sensi dall'art. 39, par. 1 del GDPR, il RPD/DPO debba essere incaricato di svolgere, in piena autonomia ed indipendenza, i seguenti compiti e funzioni:

- informare e fornire consulenza al Titolare o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR, nonché da altre disposizioni nazionali o dell'Unione relative alla protezione dei dati;
- sorvegliare l'osservanza del GDPR, di altre disposizioni nazionali o dell'Unione 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;

- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'art. 35 del GDPR;
- cooperare con il Garante nazionale per la protezione dei dati personali;
- fungere da punto di contatto con 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;

RILEVATO che l'autonomia nello svolgimento delle predette funzioni implica:

- che il RPD/DPO non sia soggetto ad istruzioni ed indicazioni circa le modalità di esplicazione dei compiti connessi alla figura, mentre può continuare ad esercitare, sotto le direttive di un responsabile, altri compiti non incompatibili con i primi;
- che il RPD/DPO non possa essere contemporaneamente controllante e controllato e pertanto non debba essere designato come tale un responsabile di struttura;

CONSIDERATO che la SC *ICT - Tecnologie dell'Informazione e della Comunicazione* è il luogo naturale dove il sistema informativo aziendale viene sviluppato, coerentemente con la missione aziendale; dove tutti i processi dematerializzati vengono supportati, controllati ed amministrati; dove le esigenze di sicurezza dei dati e delle informazioni sono conosciute e comprese e all'interno del quale vengono adottate le soluzioni adeguate al mantenimento di idonei livelli di sicurezza;

CONSIDERATO che attualmente tutti i principali work flow di raccolta, trattamento e conservazione dei dati sono informatizzati e che i residui processi cartacei sono destinati a ridursi progressivamente fino a scomparire;

DATO ATTO che la SC *ICT - Tecnologie dell'Informazione e della Comunicazione* - che ha tra le sue attribuzioni la protezione e la sicurezza del sistema informativo elettronico, delle reti, dei dispositivi informatici e dei dati negli stessi contenuti - ha da tempo intrapreso un percorso di adeguamento alle nuove disposizioni, quali, da ultimo, l'acquisizione di sistemi per la gestione del registro dei trattamenti, per il salvataggio di copie di sicurezza dei dati aziendali, la predisposizione di misure volte ad assicurare il *disaster recovery* e l'acquisizione di sistemi di monitoraggio di accesso ai documenti elettronici;

DATO ATTO che con nota prot. PG/2018/8531 del 18/04/2018 il dr. Luigi Spanu Direttore della SC *ICT - Tecnologie dell'Informazione e della Comunicazione* ha comunicato il nominativo della dott.ssa Ivette Podda - Collaboratore Professionale Amministrativo cat. D, la quale, sino ad ora, ha contribuito fattivamente ad accompagnare l'Azienda nel percorso di adeguamento al GDPR, e che la stessa, coniuga un'adeguata conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati con una esperienza pluriennale maturata nell'ambito del Servizio Sistemi Informativi; condizioni che le hanno permesso di sviluppare le conoscenze specialistiche connesse ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dall'Azienda;

che tali qualità professionali rendono la predetta collaboratrice idonea a ricoprire l'incarico RPD/DPO, conformemente a quanto previsto nelle *"Linee Guida sui Responsabili della Protezione Dati – WP243"* che richiedono:

- conoscenza dello specifico settore di attività e della struttura organizzativa del Titolare del trattamento; conoscenza dei trattamenti di dati effettuati dal Titolare e dai Responsabili del trattamento e della protezione richiesta;
- buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal Titolare;

- conoscenza approfondita delle norme e delle procedure amministrative applicabili;
- qualità personali ed elevati standard deontologici.

CONSIDERATO altresì che la figura del RPD/DPO possa trovare utile collocazione organica in seno alla predetta struttura, assicurando che esistano le condizioni di autonomia, indipendenza e terzietà della figura previste nelle predette Linee Guida e con l'attribuzione di ulteriori compiti compatibili - in quanto non concorrono a determinare le modalità o le finalità dei trattamenti – che siano suscettibili di promuovere un utilizzo appropriato dei sistemi informativi aziendali e di accrescere i livelli complessivi di conformità al GDPR dell'Azienda; in particolare:

- definizione delle Linee Guida sull'uso dei sistemi informativi aziendali e sul rispetto delle norme di sicurezza informatica, sotto la responsabilità del responsabile ed attenendosi alle istruzioni impartite;
- supporto alla definizione delle procedure informatiche e accesso alle risorse ICT, sotto la responsabilità del responsabile ed attenendosi alle istruzioni impartite;
- organizzazione di cicli formativi ai responsabili di trattamento in tema di GDPR, protezione dati, per accrescere la consapevolezza dei perimetri di responsabilità e dei profili di rischio; cicli formativi sulle procedure informatiche e sui servizi ICT, connesse ai progetti di sviluppo o ai processi di cambiamento;
- azioni di sensibilizzazione e formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

RITENUTO per i motivi sopra esposti, di dover allocare la funzione del RPD/DPO all'interno della SC *ICT - Tecnologie dell'Informazione e della Comunicazione* e di individuarlo nella persona della Dott.ssa Ivette Podda, Collaboratore Professionale Amministrativo cat.D;

PRESO ATTO che individuato il RPD/DPO occorra:

- comunicarne il nominativo al Garante per la Protezione dei Dati Personali per agevolare i contatti con l'Autorità;
- indicare nominativo e recapiti nell'informativa privacy fornita agli interessati;
- pubblicarne il nominativo e i contatti sul sito web nella sezione "*amministrazione trasparente*";
- comunicare il nominativo agli interessati in caso di violazione dei dati personali (art. 33, par. 3, lett. b del GDPR).

CONSIDERATO che l'art. 38 del GDPR prevede che il Titolare:

- si assicuri che il RPD/DPO sia tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati (par. 1);
- sostenga il RPD/DPO nell'esecuzione dei compiti allo stesso assegnati, fornendogli le risorse necessarie per assolvere tali compiti ed accedere ai dati personali ed ai trattamenti e per mantenere la propria conoscenza specialistica (par. 2).

RITENUTO di dover investire il RPD/DPO aziendale anche del compito di tenere il registro delle attività di trattamento, di cui all'art. 30 del Regolamento UE, sotto la responsabilità del titolare o del responsabile ed attenendosi alle istruzioni impartite;

DATO ATTO che - a seguito dell'entrata in vigore del GDPR - il Titolare adempie alle seguenti attività, delegate ad altre figure, come di seguito specificato:

- ***Adempimenti propri del Titolare:*** nomina del RPD/DPO; adozione di tutte le misure tecniche ed organizzative adeguate per la tutela dei dati personali, tramite delega ai Direttori delle SC/SS/SSD/Dipartimenti;
- ***Direttore della SC Affari Generali, Convenzioni e Rapporti con L'Università***: adempimenti inerenti la gestione delle deleghe verso i responsabili del trattamento interni ed esterni; redazione delle informative privacy e dei moduli di raccolta dei relativi consensi; redazione dei codici di condotta; DPIA – valutazione di impatto sui diritti e libertà degli interessati dei trattamenti "*analogici*" effettuati in azienda; predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza delle informazioni su supporto cartaceo su delega del Titolare; predisposizione del regolamento generale sulla privacy.
- ***Direttore della SC ICT – Tecnologie dell'Informazione e Comunicazione***: definizione delle procedure per la gestione dei c.d. "*data breach*"; predisposizione e tenuta del registro delle violazioni; DPIA – valutazione di impatto sui diritti e libertà degli interessati dei trattamenti "*informatici*" effettuati in azienda; predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza informatica su delega del Titolare;
- ***Responsabili del trattamento (Direttori SC/SS/SSD/Dipartimento):*** attuazione delle misure tecniche ed organizzative adeguate per la tutela dei dati personali negli ambiti di relativa competenza e in tutti i settori delegati dal Titolare; individuazione e nomina dei soggetti autorizzati al trattamento dati.
- ***RPD/DPO:*** notificazione all'Autorità Garante in caso di avvenuta violazione a seguito di Data Breach; verifica della regolare tenuta del registro delle violazioni; verifica di conformità al GDPR dell'informativa privacy e dei moduli di raccolta del consenso; tenuta del registro dei trattamenti; verifica di conformità al GDPR della DPIA e dei Codici di condotta; consulenza preventiva e verifica di conformità al GDPR su tutte le misure tecniche ed organizzative predisposte dal Titolare o dai Responsabili del trattamento (interni ed esterni); consulenza al Titolare ed ai Responsabili del trattamento in ogni ambito che possa coinvolgere la protezione dei dati personali; consulenza in fase di redazione agli AA.GG. del regolamento generale sulla privacy e controllo successivo di conformità.

DATO ATTO che il conferimento della funzione di RPD/DPO non comporta nuovi oneri a carico dell'Azienda;

RITENUTO che l'assetto sopra descritto concorra ad affermare efficacemente il ruolo del RPD/DPO non solo come supervisore interno per dimostrare la conformità, ma anche come facilitatore che promuove la cultura della protezione dei dati all'interno dell'azienda e contribuisce a dare attuazione concreta agli elementi essenziali del Regolamento, quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali;

PROPONE

Per i motivi espressi in premessa, che qui si richiamano integralmente:

1) **DI PROCEDERE** alla nomina del Responsabile della Protezione dati (RPD/DPO), obbligatoria ai sensi dell'art. 37, par. 1 del Reg. UE 679/2016;
2) **DI NOMINARE,** come RPD/DPO, la Dott.ssa Ivette Podda, Collaboratore Amministrativo Professionale cat. D, organicamente in forza alla SC *ICT - Tecnologie dell'Informazione e della Comunicazione*, dotata di adeguate qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere i compiti - conformemente a quanto previsto nelle "*Linee Guida sui Responsabili della Protezione Dati – WP243*";

3) **DI PREVEDERE** che il Titolare si assicuri che il RPD/DPO sia tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati e che questo venga costantemente sostenuto nell'esecuzione dei compiti allo stesso assegnati, fornendogli le risorse necessarie per assolvere tali compiti e per mantenere la propria conoscenza specialistica;

4) **DI STABILIRE** che il RPD/DPO, nell'esercizio delle sue funzioni tipiche, debba occuparsi delle seguenti attività:

   - notificazione all'Autorità Garante in caso di avvenuta violazione a seguito di Data Breach;
   - verifica della regolare tenuta del registro delle violazioni;
   - verifica di conformità al GDPR dell'informativa privacy e dei moduli di raccolta del consenso;
   - tenuta del registro dei trattamenti, sotto la responsabilità del titolare o del responsabile;
   - verifica di conformità al GDPR della DPIA e dei Codici di condotta;
   - consulenza preventiva e verifica di conformità al GDPR su tutte le misure tecniche ed organizzative predisposte dal Titolare o dai Responsabili del trattamento (interni ed esterni);
   - consulenza al Titolare ed al Responsabile del trattamento in ogni ambito che possa coinvolgere la protezione dei dati personali;

5) **DI STABILIRE** che il RPD/DPO possa svolgere all'interno della SC *ICT - Tecnologie dell'Informazione e della Comunicazione* anche altre attività compatibili con la predetta nomina, purché le stesse siano neutre rispetto ai compiti tipici del RPD/DPO, in quanto non concorrono a determinare le finalità o le modalità dei trattamenti;

6) **DI DARE ATTO** che il conferimento della funzione di RPD/DPO non comporta nuovi oneri a carico dell'Azienda;

7) **DI STABILIRE** che gli adempimenti a carico del Titolare vengano dallo stesso ripartiti secondo la seguente modalità, salvo quanto verrà stabilito e delegato con successivi atti formali:

   - **adempimenti propri del *Titolare***: nomina del RPD/DPO; adozione di tutte le misure tecniche ed organizzative adeguate per la tutela dei dati personali, tramite delega ai Direttori delle SC/SS/SSD/Dipartimenti;
   - **adempimenti del Direttore della *SC Affari Generali, Convenzioni e Rapporti con l'Università*:** adempimenti inerenti la gestione delle deleghe verso i responsabili del trattamento interni ed esterni; redazione delle informative privacy e dei moduli di raccolta dei relativi consensi; redazione dei codici di condotta; DPIA – valutazione di impatto sui diritti e libertà degli interessati dei trattamenti analogici effettuati in azienda; predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza delle informazioni su supporto cartaceo su delega del Titolare; predisposizione del regolamento generale sulla privacy.
   - **adempimenti del Direttore della SC *ICT – Tecnologie dell'Informazione e Comunicazione*:** definizione delle procedure per la gestione dei c.d. *data breach*; predisposizione e tenuta del registro delle violazioni; DPIA – valutazione di impatto sui diritti e libertà degli interessati dei trattamenti informatici effettuati in azienda; predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza informatica su delega del Titolare;
   - **adempimenti dei *Responsabili del Trattamento (Direttori SC/SS/SSD/Dipartimento)*** : attuazione delle misure tecniche ed organizzative adeguate per la tutela dei dati personali negli ambiti di relativa competenza e in tutti i settori delegati dal Titolare; individuazione e nomina dei soggetti autorizzati al trattamento dati.

8) **DI DELEGARE**, pertanto, il Direttore della *SC Affari Generali, Convenzioni e Rapporti con L'Università*, dott. Antonio Solinas, della redazione delle informative privacy e dei moduli di raccolta dei relativi consensi; della redazione dei codici di condotta; della Valutazione di impatto sui diritti e libertà degli interessati - DPIA - dei trattamenti analogici effettuati in azienda; della predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza delle informazioni su supporto cartaceo su delega del Titolare; della predisposizione del regolamento generale sulla privacy;

9) **DI DELEGARE**, parimenti, il Direttore della SC *ICT – Tecnologie dell'Informazione e Comunicazione,* Dott. Luigi Spanu, della definizione delle procedure per la gestione dei c.d. *data breach*; della predisposizione e tenuta del registro delle violazioni; della Valutazione di impatto sui diritti e libertà degli interessati - DPIA - dei trattamenti digitale effettuati in azienda; della

predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza informatica su delega del Titolare;

10) **DI PREVEDERE** che il nominativo del RPD/DPO:

- venga comunicato al Garante per la Protezione dei Dati Personali per agevolare i contatti con l'Autorità;
- venga indicato, assieme ai recapiti, nell'informativa privacy fornita agli interessati;
- venga pubblicato, unitamente ai contatti, sul sito web nella sezione "*amministrazione trasparente*";
- venga comunicato agli interessati in caso di violazione dei dati personali.

IL RESPONSABILE DELLA SC AFFARI GENERALI, CONVENZIONI E RAPPORTI CON L'UNIVERSITA'
(Dott. Antonio Solinas)

IL DIRETTORE GENERALE
Dott. Antonio D'Urso
Nominato con Decreto del Presidente della Regione Sardegna n. 57 del 03.10.2016

L'anno duemila diciotto, il giorno Diciotto del mese di Aprile, in Sassari, nella sede legale dell'Azienda Ospedaliero-Universitaria.

PRESO ATTO della proposta di Deliberazione avente per oggetto: "*Adempimenti GDPR - Regolamento UE 679/2016 – Nomina Responsabile Protezione Dati (RPD/DPO) ex articolo 37 paragrafo 1 e deleghe ai Responsabili delle SC Affari Generali, Convenzioni e Rapporti con l'Università e ICT-Tecnologie della Comunicazione e dell'Informazione.*";

DATO ATTO che il Direttore Amministrativo e il Direttore Sanitario hanno espresso parere favorevole;

D E L I B E R A

Per i motivi espressi in premessa, che qui si richiamano integralmente, di adottare la proposta di deliberazione di cui sopra e conseguentemente:

1) **DI PROCEDERE** alla nomina del Responsabile della Protezione dati (RPD/DPO), obbligatoria ai sensi dell'art. 37, par. 1 del Reg. UE 679/2016;

2) **DI NOMINARE,** come RPD/DPO, la Dott.ssa Ivette Podda, Collaboratore Amministrativo Professionale cat. D, organicamente in forza al *Servizio ICT - Tecnologie dell'Informazione e della Comunicazione*, dotata di adeguate qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, nonché della capacità di assolvere i compiti - conformemente a quanto previsto nelle "*Linee Guida sui Responsabili della Protezione Dati – WP243*";

3) **DI PREVEDERE** che il Titolare si assicuri che il RPD/DPO sia tempestivamente coinvolto in tutte le questioni riguardanti la protezione dei dati e che questo venga costantemente sostenuto nell'esecuzione dei compiti allo stesso assegnati, fornendogli le risorse necessarie per assolvere tali compiti e per mantenere la propria conoscenza specialistica;

4) **DI STABILIRE** che il RPD/DPO, nell'esercizio delle sue funzioni tipiche, debba occuparsi delle seguenti attività:
   - notificazione all'Autorità Garante in caso di avvenuta violazione a seguito di Data Breach;
   - verifica della regolare tenuta del registro delle violazioni;
   - verifica di conformità al GDPR dell'informativa privacy e dei moduli di raccolta del consenso;
   - tenuta del registro dei trattamenti, sotto la responsabilità del titolare o del responsabile;
   - verifica di conformità al GDPR della DPIA e dei Codici di condotta;
   - consulenza preventiva e verifica di conformità al GDPR su tutte le misure tecniche ed organizzative predisposte dal Titolare o dai Responsabili del trattamento (interni ed esterni);
   - consulenza al Titolare ed al Responsabile del trattamento in ogni ambito che possa coinvolgere la protezione dei dati personali;

5) **DI STABILIRE** che il RPD/DPO possa svolgere all'interno del *Servizio ICT - Tecnologie dell'Informazione e della Comunicazione* anche altre attività compatibili con la predetta nomina, purché le stesse siano neutre rispetto ai compiti tipici del RPD/DPO, in quanto non concorrono a determinare le finalità o le modalità dei trattamenti;

6) **DI DARE ATTO** che il conferimento della funzione di RPD/DPO non comporta nuovi oneri a carico dell'Azienda;

7) **DI STABILIRE** che gli adempimenti a carico del Titolare vengano dallo stesso ripartiti secondo la seguente modalità, salvo quanto verrà stabilito e delegato con successivi atti formali:
   - **adempimenti propri del *Titolare***: nomina del RPD/DPO; adozione di tutte le misure tecniche ed organizzative adeguate per la tutela dei dati personali, tramite delega ai Direttori delle SC/SS/SSD/Dipartimenti;

- **adempimenti del Direttore della *SC Affari Generali, Convenzioni e Rapporti con l'Università*:** adempimenti inerenti la gestione delle deleghe verso i responsabili del trattamento interni ed esterni; redazione delle informative privacy e dei moduli di raccolta dei relativi consensi; redazione dei codici di condotta; DPIA – valutazione di impatto sui diritti e libertà degli interessati dei trattamenti analogici effettuati in azienda; predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza delle informazioni su supporto cartaceo su delega del Titolare; predisposizione del regolamento generale sulla privacy.
- **adempimenti del Direttore della *SC ICT – Tecnologie dell'Informazione e Comunicazione*:** definizione delle procedure per la gestione dei c.d. *data breach*; predisposizione e tenuta del registro delle violazioni; DPIA – valutazione di impatto sui diritti e libertà degli interessati dei trattamenti informatici effettuati in azienda; predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza informatica su delega del Titolare;
- **adempimenti dei *Responsabili del Trattamento (Direttori SC/SS/SSD/Dipartimento)*:** attuazione delle misure tecniche ed organizzative adeguate per la tutela dei dati personali negli ambiti di relativa competenza e in tutti i settori delegati dal Titolare; individuazione e nomina dei soggetti autorizzati al trattamento dati.

8) **DI DELEGARE**, pertanto, il Direttore della *SC Affari Generali, Convenzioni e Rapporti con L'Università*, dott. Antonio Solinas, della redazione delle informative privacy e dei moduli di raccolta dei relativi consensi; della redazione dei codici di condotta; della Valutazione di impatto sui diritti e libertà degli interessati - DPIA - dei trattamenti analogici effettuati in azienda; della predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza delle informazioni su supporto cartaceo su delega del Titolare; della predisposizione del regolamento generale sulla privacy;

9) **DI DELEGARE**, parimenti, il Direttore della SC *ICT – Tecnologie dell'Informazione e Comunicazione,* Dott. Luigi Spanu, della definizione delle procedure per la gestione dei c.d. *data breach*; della predisposizione e tenuta del registro delle violazioni; della Valutazione di impatto sui diritti e libertà degli interessati - DPIA - dei trattamenti digitale effettuati in azienda; della predisposizione di tutte le misure tecniche ed organizzative in materia di sicurezza informatica su delega del Titolare;

10) **DI PREVEDERE** che il nominativo del RPD/DPO:

- venga comunicato al Garante per la Protezione dei Dati Personali per agevolare i contatti con l'Autorità;
- venga indicato, assieme ai recapiti, nell'informativa privacy fornita agli interessati;
- venga pubblicato, unitamente ai contatti, sul sito web nella sezione "*amministrazione trasparente*";
- venga comunicato agli interessati in caso di violazione dei dati personali.

IL DIRETTORE GENERALE
(Dott. Antonio D'Urso)
Antonio D'Urso 18 Aprile 2018

La presente Deliberazione è in pubblicazione all'Albo Pretorio elettronico del sito dell'Azienda Ospedaliero Universitaria di Sassari dal 18.04.2018 *per la durata di quindici giorni*

Il Direttore della SC Affari Generali, Convenzioni e Rapporti con l'Università

(Dott. Antonio Solinas)