Deliberazione n. 18/24

Oggetto: **Approvazione Linee Guida relative al modello organizzativo e agli adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati. (Sostituzione delle precedenti direttive approvate con delibere del Consiglio di Amministrazione n° 20 del 18/10/2018 e n° 36 del 10/12/2018)**

L'anno duemilaventiquattro in data 23 aprile alle ore 9:30, presso gli uffici dell'ERSU in Via Coppino n° 18, a Sassari è stato convocato il Consiglio di Amministrazione nelle persone:

		P	A
Daniele Maoddi	Presidente	X	
Eliana Fois	Consigliere	X	
Giovanni Luigi Testoni	Consigliere	X	
Eraldo Sanna Passino	Consigliere	X	
Pietro Mongiu	Consigliere	X	

Per il Collegio dei Revisori contabili, assistono:

Mario Graziano Marras	Presidente	X	
Michele Raimondo Mura	Componente		X
Daniela Manca	Componente		X

Il Presidente, constatata la presenza del numero legale, dichiara aperta la seduta. Svolge le funzioni di Segretario, il Direttore generale dell'Ente arch. Libero Meloni.

DELIBERA DEL CONSIGLIO DI AMMINISTRAZIONE

Oggetto: **Approvazione Linee Guida relative al modello organizzativo e agli adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati. Sostituzione delle precedenti direttive approvate con delibere del Consiglio di Amministrazione n° 20 del 18/10/2018 e n° 36 del 10/12/2018**

il Consiglio di Amministrazione

VISTA la L.R. n. 37 del 14 settembre 1987 recante norme per l'attuazione del diritto allo studio universitario in Sardegna*;*

VISTA la L.R. n. 20 del 23 agosto 1995 che detta norme in tema di semplificazione e razionalizzazione dell'ordinamento degli Enti strumentali della Regione sarda;

VISTA la L.R. n. 14 del 15 maggio 1995 avente ad oggetto *"Indirizzo, controllo, vigilanza e tutela sugli enti, istituti ed aziende regionali"*;

VISTA la L.R. n. 31 del 13 novembre 1998 e ss.mm.ii. sulla disciplina del personale regionale e dell'organizzazione degli uffici della Regione Autonoma della Sardegna;

VISTO il decreto del Presidente della Regione Sardegna n. 13 del 23/02/2024 con il quale è stato prorogato fino al 28 settembre 2026 al dott. arch. Libero Meloni l'incarico di direttore generale dell'Ente Regionale per il diritto allo Studio Universitario (da ora anche E.R.S.U.) di Sassari, a suo tempo conferito con il Decreto del Presidente della Regione Sardegna n. 66 del 29 settembre 2021*;*

VISTI i Decreti del Presidente della Regione Sardegna n. 1 del 5 gennaio 2024 e n. 2 del 8 gennaio 2024 con i quali si è provveduto alla costituzione del Consiglio di Amministrazione dell'Ente;

VISTO il Regolamento UE 2016/679, entrato in vigore il 25/05/2018, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, di seguito denominato "Regolamento";

PREMESSO **che** la Regione Sardegna con le deliberazioni della Giunta regionale n. 21/8 del 24 aprile 2018 e n. 51/3 del 16 ottobre 2018, definiva le prime misure organizzative e tecniche finalizzate al perseguimento e all'attuazione del Regolamento, applicabili, secondo gli specifici assetti istituzionali, agli Enti e alle Agenzie che costituiscono il sistema regione;

che l'Ente regionale per il Diritto allo studio di Sassari (di seguito Ersu) recepiva, tenuto conto delle specificità dell'Ente, le deliberazioni sopra citate, attraverso il Consiglio di Amministrazione di cui alle deliberazioni n. 20 del 18/10/2018 avente ad oggetto "Regolamento Ue N. 679/16: approvazione Manuale operativo di buone prassi per la protezione dei dati personali" e n. 36 del 10/12/2018 avente ad oggetto "Regolamento UE n. 679/16 e D.lgs. 101/2018: approvazione Linee guida applicative";

che l'Ersu di Sassari nel maggio del 2018 si dotava del Registro dei trattamenti cosi come previsto dal Regolamento 679/16 art. 30 aderendo alla proposta di utilizzo dell'applicativo messo a disposizione dalla Regione Sardegna, come da nota prot. 5033 del 15/03/2018 (ns prot. 2753 acquisito in pari data);

che l'Ersu di Sassari sulla base della deliberazione n. 21/8 del 24 aprile 2018 ricorreva alla facoltà di avvalersi del Responsabile Protezione Dati (R.P.D.) della Regione Sardegna, nominato con decreto presidenziale n. 47 del 23/5/2018, designando il dott. Alessandro

Inghilleri quale R.P.D. dell'Ente con delibera commissariale n° 47 del 24/5/2018 e rinnovando tale incarico, conformemente alle determinazioni della Giunta regionale, con successivi provvedimenti dell'Organo politico, da ultimo con Deliberazione del Commissario Straordinario n. 14 del 4/04/2023;

che il dott. Alessandro Inghilleri con nota del 4/7/2023, acquisita al protocollo dell'Ente con n° 5299 nella medesima data, comunicava la cessazione dell'incarico di Responsabile protezione Dati per la Regione Sardegna e per il sistema regionale nel suo complesso, Enti ed Agenzie;

che la Regione Sardegna aggiornava e in parte sostituiva le precedenti direttive con deliberazione n. 45/3 del 20/12/2023 avente ad oggetto "Modello organizzativo e adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati. Indirizzi e aggiornamento delle direttive regionali. Sostituzione delle direttive contenute nelle deliberazioni della Giunta regionale n.21/8 del 24 aprile 2018 e n.51/3 del 16 ottobre 2018";

DATO ATTO **che,** nelle more della nuova nomina del Responsabile protezione dati della Regione Sardegna e di una possibile estensione delle sue funzioni agli Enti e Agenzia del comparto, l'Ente ha nominato, con determinazione n. 111 del 30/10/2023 del Direttore generale, come Responsabile Protezione Dati (RPD) dell'Ersu, la Società Karanoa S.r.l., che ha individuato come referente l'avv. Giacomo Crovetti;

che con nota del 16/10/2023 ns prot. 14720 l'Ente confermava l'adesione al servizio di supporto offerto dall' Ufficio speciale del Responsabile della protezione dei dati per il sistema Regione in merito alla detenzione del Registro delle attività di trattamento e alle conseguenti attività di erogazione dei servizi informatici di manutenzione, evoluzione e gestione;

CONSIDERATO che, sulla base delle premesse di cui sopra, in particolare della deliberazione regionale n.45/3 del 20/12/2023, si rende necessario adeguare le misure organizzative e tecniche dell'Ente finalizzate al perseguimento e all'attuazione dei principi del Regolamento, attraverso delle linee guida, allegate alla presente deliberazione per farne parte integrante e sostanziale;

PRESO ATTO che l'adozione delle linee guida sostituisce le precedenti misure tecniche organizzative adottate con le deliberazioni del Consiglio di Amministrazione n. 20 del 18/10/2018 avente ad oggetto "Regolamento Ue N. 679/16: approvazione Manuale operativo di buone prassi per la protezione dei dati personali" e n. 36 del 10/12/2024 avente ad oggetto "Regolamento UE n. 679/16 e D.lgs. 101/2018: approvazione Linee guida applicative";

DATO ATTO **che** la proposta del presente provvedimento è stata curata dal Responsabile del *Settore comunicazione istituzionale, Eventi culturali propri, Transizione digitale, ICT, Privacy* Dott.ssa Maria Elena Soddu e dalla stessa sottoposta all'attenzione del Direttore Generale;

che la stessa è stata sottoposta al parere preventivo del Responsabile della Protezione Dati dell'Ente, il quale ha espresso parere positivo;

DATO ATTO altresì dell'assenza di conflitto di interessi da parte dei sottoscrittori del presente atto nonché di coloro che hanno preso parte al procedimento correlato al presente provvedimento, ai sensi dell'art. 6 e 7 del D.P.R. n. 62/2013;

TENUTO CONTO che il presente provvedimento sarà assoggettato alle procedure finalizzate all'assolvimento degli obblighi in tema di trasparenza e di pubblicazione (d.lgs. 33/2013);

ACQUISITO il parere di legittimità ex art. 5 della Legge Regionale 15.05.1995 n. 14, rilasciato dal Direttore Generale attraverso la sottoscrizione del presente atto;

delibera all'unanimità

per le motivazioni in premessa da intendersi qui integralmente richiamate

1. Di approvare le Linee Guida relative al modello organizzativo e agli adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, allegate al presente provvedimento per farne parte integrante e sostanziale.
2. Di dare atto che le presenti Linee Guida sostituiscono le precedenti misure tecniche organizzative adottate con deliberazioni del Consiglio di Amministrazione n. 20 del 18/10/2018 avente ad oggetto "Regolamento Ue N. 679/16: approvazione Manuale operativo di buone prassi per la protezione dei dati personali" e n. 36 del 10/12/2024 avente ad oggetto "Regolamento UE n. 679/16 e D.lgs. 101/2018: approvazione Linee guida applicative";
3. Di dare mandato al Direttore generale per gli atti conseguenti.

Il Direttore Generale
Arch. Libero Meloni
(firmato digitalmente ai sensi D.lgs. 82/05)

MELONI
LIBERO
24.04.2024
11:29:54
GMT+01:00

Il Presidente
Dott. Daniele Maoddi
(firmato digitalmente ai sensi D.lgs. 82/05)

Daniele
Maoddi
24.04.2024
10:38:51
GMT+00:00

Visto per il parere di legittimità
ex art. 5 L.R. 15.05.1995 n. 14
Il Direttore Generale
Arch. Libero Meloni
(firmato digitalmente ai sensi D.lgs. 82/05)

MELONI LIBERO
24.04.2024
11:29:54
GMT+01:00

Ente Regionale pro su Deretu a s'Istùdiu Universitàriu de Tàtari
Ente Regionale per il diritto allo Studio Universitario
Sassari

REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

Allegato alla Delibera C.d.A. n° 18 del 23.04.2024

MODELLO ORGANIZZATIVO E ADEMPIMENTI FINALIZZATI ALL'APPLICAZIONE DEL REGOLAMENTO (UE) 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI NONCHÉ ALLA LIBERA CIRCOLAZIONE DI TALI DATI

MELONI
LIBERO
24.04.2024
11:29:54
GMT+01:00

PREMESSA

Le presenti direttive hanno per oggetto le misure organizzative mediante le quali l'Ente regionale per il Diritto allo studio di Sassari (di seguito ERSU) attua i principi e le disposizioni del Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 (di seguito indicato come Regolamento) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

Art. 1 - DEFINIZIONI

Ai fini della presente documento, in conformità al Regolamento, si intende per:

a) "dato personale": qualsiasi informazione riguardante una persona fisica identificata e identificabile ("interessato");
b) "trattamento": qualsiasi operazione e insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati, applicate ai dati personali o insieme di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, la limitazione, la cancellazione o la distruzione;
c) "titolare del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o l'organismo che determina le finalità e i mezzi del trattamento dei dati personali;
d) "delegato del titolare": il direttore generale al quale il titolare abbia delegato - nei limiti dell'ambito delle rispettive competenze e dei connessi trattamenti – le funzioni e i compiti connessi all'attuazione dei principi di cui all'art. 5 del Regolamento. Il delegato del titolare può esercitare le predette funzioni delegandole, a propria volta, ai Direttori di Servizio nei limiti dell'ambito delle rispettive competenze e dei connessi trattamenti;
e) "responsabile della protezione dati" (di seguito denominato "RPD"): il soggetto, nominato dal titolare del trattamento, chiamato a svolgere le funzioni e i compiti previsti dagli artt. 37, 38 e 39 del Regolamento;
f) "responsabile esterno del trattamento": la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, sulla base dell'art. 28 del Regolamento;
g) "violazione dei dati personali": la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;
h) "registro del trattamento": il registro nel quale il titolare del trattamento annota le informazioni, relative ai trattamenti di competenza, indicate nell'art. 30 del Regolamento;
i) "valutazione d'impatto sulla protezione dei dati": la valutazione – effettuata dal titolare del trattamento ai sensi degli art. 35 e 36 del Regolamento – dell'impatto del trattamento da avviare sui diritti e le libertà degli interessati;
j) "autorizzati al trattamento" dei dati personali: coloro che, debitamente istruiti e formati in materia a cura del titolare del trattamento, accedono ai dati e li trattano sotto l'autorità del titolare stesso e previa sua formale designazione;
k) "referente privacy": individuato con atto formale tra i dipendenti dell'Ente, rappresenta il punto di contatto tra l'RPD e i Servizi dell'Ente;

l) "dati di natura particolare": dati che rilevano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona;

m) "dati genetici": i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica che ne consentono o confermano l'identificazione univoca, quali immagini facciale o dati dattiloscopici;

n) "dati relativi alla salute": i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rilevano informazioni relative al suo stato di salute;

Art. 2 - TITOLARE DEL TRATTAMENTO

1. Il titolare del trattamento è l'ERSU di Sassari, nella persona del suo rappresentante legale, il Presidente dell'Ente, cui spetta la promozione di misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento.
2. Al Consiglio di Amministrazione compete:
    a) l'adozione degli indirizzi relativamente alle misure tecniche e organizzative rispetto agli adempimenti previsti dal Regolamento;
    b) l'attribuzione di funzioni e compiti ai soggetti delegati degli adempimenti previsti dalla normativa in materia di trattamento dei dati personali;
    c) la nomina del RPD con l'attribuzione di funzioni e compiti sulla base di quanto previsto al Regolamento agli artt. 37, 38 e 39;
    d) l'allocazione di adeguate risorse per la formazione del personale in materia di protezione dei dati e sicurezza informatica e per l'adeguamento dell'Ente alla normativa vigente.
3. Il titolare del trattamento assicura il rispetto dei principi e delle disposizioni del Regolamento e della normativa statale vigente in materia di protezione dei dati personali, anche mediante delega dei compiti al Direttore Generale. Il Direttore Generale può esercitare le predette funzioni delegandole, a propria volta, ai Direttori di Servizio nei limiti delle rispettive competenze e dei connessi trattamenti.

Art. 3 - DELEGATI DEL TITOLARE

1. Ai sensi del comma 3 del precedente art. 2, il Presidente dell'Ente, previa deliberazione del Consiglio di Amministrazione, delega al Direttore Generale, i seguenti compiti:

    a. la predisposizione dell'informativa relativa a ciascuno dei trattamenti di dati personali in conformità agli articoli 13 e 14 del Regolamento;
    b. la creazione delle condizioni volte a facilitare l'esercizio dei diritti previsti dagli articoli dal 15 al 22 del Regolamento ed il tempestivo riscontro alle istanze degli interessati;
    c. l'adozione, e ove necessario il riesame e l'aggiornamento, delle misure tecniche e organizzative adeguate a garantire e poter dimostrare che il trattamento è effettuato conformemente al Regolamento. Tali misure devono comunque essere adeguate a garantire un livello di sicurezza correlato al livello di rischio secondo quanto statuito dall'art. 32 del Regolamento. Fatte salve eventuali misure particolari correlate alle specificità delle finalità del trattamento, le predette misure possono consistere in interventi conformi a linee guida e policy da applicare secondo standard comuni a tutti gli uffici dell'Amministrazione;

d. l'adozione delle misure tecniche ed organizzative adeguate ad attuare in modo efficace e fin dalla progettazione i principi di protezione dei dati personali e integrare nel trattamento le garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati (privacy by design - *rif. art. 25 comma 1 del Regolamento);*
e. l'adozione delle misure tecniche ed organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento (privacy by default – *rif. art. 25 comma 2 del Regolamento*);
f. lo svolgimento degli adempimenti correlati, per quanto di competenza, all'attuazione degli artt. 26 e 28 del Regolamento, concernenti, rispettivamente, gli obblighi correlati alla situazione di contitolarità del trattamento e la disciplina del responsabile esterno del trattamento;
g. la formale individuazione, nelle rispettive strutture, degli autorizzati al trattamento ai sensi dell'art. 29 del Regolamento, fornendo agli stessi specifiche istruzioni per il corretto trattamento dei dati;
h. la tenuta del registro delle attività di trattamento in modo da assicurarne, per gli aspetti di competenza, la corretta compilazione ed il costante aggiornamento e revisione, art. 30 del Regolamento;
i. l'individuazione dei trattamenti di competenza per i quali è obbligatorio, o comunque opportuno, effettuare la valutazione di impatto sulla protezione dei dati personali, conduzione della stessa, previa consultazione del RPD, e della conseguente consultazione preventiva dell'Autorità Garante per la protezione dei dati personali (di seguito denominata "Garante") ai sensi dell'art. 36 del Regolamento;
j. la designazione degli amministratori di sistema in aderenza alle norme vigenti in materia;
k. la collaborazione, per quanto di competenza, con il RPD dell'Ente, nell'esecuzione dei compiti ad esso attribuiti;
l. la cooperazione, per quanto di competenza, con l'autorità di controllo nell'esecuzione dei compiti ad essa attribuiti.

Il Direttore Generale può esercitare le predette funzioni delegandole, a propria volta, ai Direttori di Servizio nei limiti delle rispettive competenze e dei connessi trattamenti.
I delegati del titolare si avvalgono, nell'esercizio dei propri compiti, del personale afferente al Servizio che svolge funzioni di: coordinamento, responsabile del procedimento/trattamento, redazione del Registro dei trattamenti e del personale autorizzato al trattamento.

Art. 4 - AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

1. I dirigenti, nella misura in cui operano al di fuori della delega delle funzioni e dei compiti del Titolare o dei suoi delegati, i dipendenti, i collaboratori e tutti coloro che agiscono sotto l'autorità del Titolare, ai sensi dell'articolo 29 del Regolamento e dell'articolo 2-quaterdecies del Codice in materia di protezione dei dati personali, hanno accesso ai dati personali e al loro trattamento dopo essere stati debitamente istruiti e formati e previa formale designazione nella quale sono definiti i profili di autorizzazione, i dati trattati, le operazioni di trattamento effettuate e le istruzioni da seguire.

2. Il personale tratta i dati nel rispetto delle istruzioni ricevute, del Regolamento e della vigente normativa in materia di protezione dei dati personali e di ogni altra buona pratica e procedura interna adottata dal Titolare e partecipa alla formazione erogata dal Titolare in materia.

3. Il personale si attiene, nel trattamento dei dati personali, alle seguenti istruzioni di carattere generale, fermo restando il rispetto delle altre misure organizzative e procedurali adottate:

a) trattare i dati personali in modo lecito, corretto e trasparente nei confronti degli interessati, esclusivamente nei limiti di quanto necessario per l'adempimento delle mansioni assegnate e per le connesse finalità;
b) accertare, per quanto di competenza, che i dati personali trattati siano esatti, aggiornati, adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono raccolti, nel rispetto del principio di minimizzazione dei dati;
c) custodire i dati personali in modo da garantirne la sicurezza contro i rischi di distruzione, perdita, anche accidentale, modifica o accesso non autorizzati, attenendosi alle misure di sicurezza tecniche e organizzative adottate dal Titolare o dai suoi delegati;
d) accedere alla postazione e alle risorse di rete messe a disposizione dal Titolare mediante le credenziali di autenticazione assegnate e periodicamente modificate; ogni autorizzato al trattamento adotta le necessarie cautele per assicurarne la segretezza, evitando di lasciare incustodite le credenziali o accessibile il terminale assegnato durante una sessione di trattamento. Le credenziali di autenticazione informatica sono individuali e non possono essere condivise;
e) ridurre al minimo l'utilizzo di supporti rimovibili, controllare periodicamente il contenuto dei supporti stessi e procedere alla cancellazione dei contenuti obsoleti;
f) non asportare supporti informatici o cartacei contenenti dati personali, né farne copia alcuna, senza la previa autorizzazione del delegato del trattamento o del proprio dirigente;
g) conservare con il massimo riserbo e riporre alla fine di ogni giornata lavorativa negli armadi o cassetti debitamente chiusi a chiave i documenti cartacei contenenti dati personali;
h) rispettare le misure tecniche e organizzative adottate dal Titolare o dai delegati del Titolare ai sensi dell'articolo 32 del Regolamento;
i) rispettare, mantenere efficienti ed utilizzare in maniera appropriata le misure di sicurezza, anche fisiche, segnalando eventuali disfunzioni o possibili situazioni di rischio al delegato del Titolare e al RPD;
j) nel trattamento dei dati personali far uso esclusivamente delle attrezzature e dei servizi forniti dal Titolare, salva diversa autorizzazione del Titolare stesso o del delegato del trattamento;
k) non creare banche dati senza espressa autorizzazione del delegato del Titolare e in caso di nuovo trattamento di dati personali informare il delegato del Titolare e il referente privacy e procedere all'aggiornamento del Registro delle attività di trattamento secondo le procedure individuate dall'Ente (vedi art. successivo Registro trattamenti);
l) rispettare i divieti di comunicazione e diffusione dei dati personali secondo la vigente normativa;
m) accertare la sussistenza del fondamento di liceità e della base giuridica che giustificano la comunicazione e la pubblicazione di dati personali e applicare il principio di minimizzazione dei dati;
n) portare ad immediata conoscenza del delegato del Titolare ogni richiesta indirizzata dai soggetti interessati e relativa all'esercizio dei diritti di cui agli articoli dal 15 al 22 del Regolamento;
o) informare il delegato del Titolare di ogni questione rilevante in materia di trattamento dei dati personali che dovesse sorgere durante l'espletamento delle proprie mansioni;
p) interrompere, in caso di cessazione del rapporto di lavoro ovvero nel caso di cessazione delle attività autorizzate (ad esempio in caso di trasferimento presso altra struttura dell'Amministrazione), ogni operazione di trattamento di dati personali e, su istruzione del delegato del Titolare, provvedere all'immediata restituzione degli stessi al Titolare, senza trattenerne copia. Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dei dati dovranno essere osservati anche in seguito a cessazione del rapporto di lavoro con il Titolare. Contestualmente alla cessazione del rapporto di lavoro o al trasferimento presso altra struttura dell'Amministrazione, informare gli uffici competenti per consentire la cancellazione di ogni

credenziale di accesso a sistemi informativi, piattaforme e similari il cui accesso è strettamente collegato al ruolo cessato;

q) rivolgersi tempestivamente per difficoltà o questioni inerenti la sicurezza informatica (ad esempio apertura di PEC o e-mail di dubbia provenienza, malfunzionamento o blocco della propria postazione) al proprio referente informatico o amministratore di sistema dandone comunicazione, se il problema persiste, anche al proprio dirigente e al delegato del Titolare;

r) al fine di prevenire l'accesso ai dati personali di persone non autorizzate, ritirare immediatamente i documenti inviati in stampa e, laddove disponibili, utilizzare preferibilmente il badge o altre forme di identificazione obbligatoria sul posto o la funzionalità di stampa sicura; distruggere personalmente i documenti cartacei contenenti dati personali allorquando non sono più necessari e in caso di copia erronea o non correttamente leggibile, utilizzando preferibilmente un apparato specifico distruggi documenti.

4. Il Titolare del trattamento si riserva la facoltà di integrare ed adeguare le istruzioni generali in ottemperanza all'evoluzione normativa in materia e alle buone pratiche e policy adottate nel tempo. Oltre alle istruzioni generali indicate nel comma 3 del presente articolo, i delegati del Titolare impartiscono, anche per gruppi omogenei di attività, istruzioni specifiche in rapporto alla peculiarità e complessità del trattamento, alle operazioni di trattamento attribuite, alla tipologia dei dati trattati e dei soggetti interessati. Le autorizzazioni al trattamento sono date avvalendosi dello specifico modello approvato con delibera regionale n° 45/3 del 20/12/2023 presente nel Registro dei trattamenti e personalizzato secondo le specifiche dell'Ente.

Art. 5 - REFERENTE PRIVACY

Il delegato del titolare designa tra i funzionari o altri dipendenti con idonee capacità un referente privacy. Il referente privacy costituisce il punto di contatto e di raccordo tra l'RPD e l'Ente, in via principale ma non esclusiva.
Il referente privacy supporta il titolare e i delegati del titolare attraverso:

- la gestione delle utenze applicative all'interno del Registro delle attività di trattamento;
- l'assistenza, laddove richiesto e necessario, nella creazione e aggiornamento delle schede del Registro delle attività di trattamento, fermo restano la responsabilità delle stesse in capo ai delegati del titolare e ai redattori individuati con atto del Direttore generale;
- la partecipazione al processo di analisi e valutazione dei rischi effettuato, con il supporto del RPD, dai delegati del titolare;
- il raccordo tra l'RPD e i Servizi coinvolti nella gestione delle istanze degli interessati per l'esercizio dei diritti, ai sensi degli articoli dal 15 al 22 del Regolamento.

Art. 6 - RESPONSABILE DELLA PROTEZIONE DATI

1. Il Responsabile della protezione dati (RPD), con le competenze e le prerogative previste dagli articoli 37, 38 e 39 del Regolamento, può essere individuato tra i dipendenti dell'Ente. Nel caso di assenza di personale interno, in possesso dei requisiti previsti dalla normativa vigente, il ruolo può essere assunto da soggetti esterni e assolvere i compiti in base a un contratto di servizio. L'ERSU di Sassari in qualità di Agenzia del sistema Regione potrà avvalersi del RPD designato dall'amministrazione regionale se previsto dalla Giunta regionale e nei limiti indicati da quest'ultima.
2. Il responsabile della protezione dei dati è incaricato dei seguenti compiti:
   a) informare e fornire consulenza al titolare del trattamento o responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento nonché da altre disposizioni dell'Unione relative alla protezione dei dati;

b) sorvegliare l'osservanza del Regolamento, di altre disposizioni dell'Unione Europea e delle disposizioni statali 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'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

3. Il RPD è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.
4. Il parere del RPD, deve essere in ogni caso richiesto:
   - nell'ambito della valutazione di impatto del trattamento, secondo quanto previsto dall'articolo 35 del Regolamento;
   - nell'ambito della valutazione del "data breach" (violazione dei dati personali).

Art. 7 - I RESPONSABILI ESTERNI DEL TRATTAMENTO

1. Sono designati responsabili del trattamento i soggetti esterni all'amministrazione che trattano dati personali per conto del titolare; la scelta del responsabile esterno è effettuata secondo quanto previsto dall'articolo 28 del Regolamento, valutando l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.
2. Il Titolare dà istruzioni in merito al trattamento all'interno di contratti o convenzioni e, in ogni caso, in aderenza al modello presente nel Registro dei trattamenti, adottato dalla Regione Sardegna e disponibile tra i modelli presenti nel Registro trattamenti.

Art. 8 - AMMINISTRATORI DI SISTEMA

L'Autorità Garante per la protezione dei dati personali con il provvedimento del 27 novembre 2008, ancora in vigore, definisce "l'amministratore di sistema" come la figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, facendo però rientrare in essa altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di rete e di apparati di sicurezza e gli amministratori di sistemi complessi.

Il Titolare del trattamento individua i propri amministratori con nomina scritta, che ne individua l'ambito di operatività.

Art. 9 - REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO DELLA ERSU DI SASSARI

1. Il Registro delle attività di trattamento previsto dall'art. 30 del Regolamento (di seguito "Registro") è detenuto dal Titolare. Il Registro è un documento che impegna ufficialmente il Titolare, anche nei confronti dell'Autorità Garante per la protezione dei dati personali, pertanto deve essere compilato con attenzione e mantenuto aggiornato nel corso del tempo.
2. Il Registro è realizzato tramite un applicativo informatico fornito dalla Regione Sardegna, in particolare dall'Ufficio speciale del Responsabile della protezione dei dati per il sistema Regione, che ne cura la

manutenzione, evoluzione e gestione. Il Registro in uso prevede una scheda tipo per il trattamento all'interno della quale sono generati per ogni trattamento:

a) Modello d'informativa
b) Modello lettera di autorizzazione

Il Registro prevede inoltre le seguenti funzionalità per ogni scheda:

a) Supporto all'analisi dei rischi e utilizzo della metodologia Enisa
b) Assessment misure di sicurezza: il sistema consente di specificare in maniera completa le misure di sicurezza già in essere o pianificate per un trattamento, allegando un documento tecnico di maggiore dettaglio. In alternativa, è possibile effettuare l'assessmente direttamente a sistema, utilizzando uno strumento messo a disposizione dall'Enisa.

3. Il Registro è un atto pubblico dell'Ente e il suo contenuto deve rappresentare correttamente i trattamenti di dati personali in essere. Ogni trattamento deve essere riportato in un'apposita scheda del Registro includendo le informazioni minime obbligatorie previste dalla normativa e gli ulteriori elementi ritenuti utili per un corretto censimento dei trattamenti.
4. Ai delegati del Titolare è demandata l'individuazione e l'aggiornamento dei trattamenti all'interno del Registro sulla base di quelli afferenti al proprio Servizio, inteso come Direzione Generale, Servizio Amministrativo e Servizio Utenze. I delegati del titolare possono avvalersi per la creazione, compilazione e aggiornamento delle schede di personale abilitato con il ruolo di redattore. L'approvazione delle schede compilate in bozza dai redattori compete ai delegati del titolare, ai quali compete anche, per il medesimo trattamento, il rilascio dell'informativa e delle lettere di autorizzazione al trattamento dei dati.
5. Le utenze del Registro sono così suddivise: visitatori, redattori e delegati del Titolare. La gestione delle utenze applicative, di raccordo con il Titolare, compete al referente per la privacy previsto all'art. 5.

Art. 10 - PROCEDIMENTO IN CASO DI VIOLAZIONE DEI DATI PERSONALI (DATA BREACH)

1. Per violazione dei dati personali (data breach) si intende la violazione che comporta, accidentalmente o in modo illecito, distruzione, perdita, modifica, indisponibilità, divulgazione o accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ersu di Sassari.
2. Ogni dipendente o collaboratore dell'amministrazione e tutti coloro che agiscono sotto l'autorità del titolare del trattamento, qualora abbiano conoscenza del verificarsi di una violazione di dati personali avvisano con immediatezza il Direttore generale o il dirigente responsabile del Servizio presso il quale prestano servizio, i quali rivestono ai fini della privacy anche la funzione del Delegato del Titolare.
   - Se dalla prima analisi da parte del Delegato del Titolare emergono elementi tali da escludere la possibile violazione dei dati personali, l'anomalia viene gestita all'interno del Servizio/Direzione interessata.
   - Se, invece, dalla prima analisi emergono gli estremi per una probabile violazione, si procede ai necessari approfondimenti. La seconda parte del processo è, pertanto, soltanto eventuale e si verifica quanto il Delegato del Titolare, nella cui struttura si è verificato l'evento, ravvisi un "data breach" o ritiene che tale evento possa configurarsi come un "data breach"; in questo caso procede entro ventiquattro ore dalla conoscenza della violazione da parte del dipendente a segnalare l'episodio al gruppo d'intervento.
3. Il Gruppo d'intervento è costituito dal Delegato del Titolare il cui Servizio/Direzione è interessato all'evento e dai seguenti soggetti:
   - il referente data breach per il supporto giuridico/procedurale
   - il responsabile IT
   - il responsabile per la protezione dati
   - il responsabile per la conservazione

Il Direttore generale partecipa ai lavori del gruppo e il referente del "data breach" è supportato nell'adempimento dei suoi compiti dal RPD.

4. Il referente per il "data breach", in presenza dei presupposti previsti dall'articolo 33 del Regolamento, procede alla notificazione della violazione dei dati personali all'Autorità Garante della protezione dei dati personali senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui è accertata la violazione e, ove ne ricorrano i presupposti, anche avvalendosi del Delegato al trattamento interessato dalla violazione, effettua la comunicazione agli interessati ai sensi dell'articolo 34 del Regolamento, nel rispetto delle modalità stabilite dalla procedura data breach.
5. L'Ersu di Sassari utilizza, per la valutazione della gravità delle violazioni dei dati personali, la procedura individuata dall'Amministrazione regionale, sulla base delle indicazioni fornite dall'ENISA (European union agency for Cybersecurity) presente all'interno del Registro trattamenti.
6. L'Ersu di Sassari si avvale anche del Registro violazioni, messo a disposizione all'interno del Registro dei trattamenti in uso dalla Regione Sardegna, previsto dall'art. 33 comma 5 del GDPR che dispone *"Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio"*.
   Nel Registro delle violazioni sono annotate a cura del Referente data breach tutte le informazioni richieste dalla normativa vigente, quali, a titolo esemplificativo ma non esaustivo: a) le circostanze relative alla violazione, b) le conseguenze, c) i provvedimenti adottati per contrastarla e limitarne gli effetti, d) i dati personali coinvolti.
7. L'Ersu di Sassari adotta inoltre un "Registro delle segnalazioni" in formato elettronico, dove vengono annotati gli eventi non rientranti nel registro delle violazioni, ma ritenuti comunque significativi al fine di migliorare le procedure di rafforzamento di tutela della privacy. Il registro è detenuto dallo stesso incaricato del Registro violazioni di cui al punto precedente.

Art. 11 - ANALISI DEI RISCHI E VALUTAZIONE DI IMPATTO

1. I delegati del Titolare possono effettuare l'analisi del rischio inerente a ciascuno dei trattamenti di competenza in rapporto ai diritti e alle libertà degli interessati. A tal fine, utilizzano gli standard e la metodologia per l'analisi dei rischi adottati da ENISA (European Union Agency for Cybersecurity) e integrati a cura dell'Ufficio del RPD regionale all'interno del registro del trattamento.
2. I delegati del Titolare individuano i trattamenti di competenza per i quali è obbligatorio o comunque opportuno effettuare la valutazione di impatto sulla protezione dei dati personali (Data Protection Impact Assessment-DPIA) ed effettuano la stessa, previa consultazione e con il supporto del RPD, secondo quanto disposto dall'articolo 35 del Regolamento, adottando la metodologia elaborata e messa a disposizione dalla CNIL (Commission nationale de l'informatique et des libertés).
3. Le metodologie per l'analisi dei rischi e per la valutazione di impatto possono essere oggetto di successive integrazioni o modificazioni adottate dal Titolare, anche su proposta del RPD.
4. I delegati del Titolare possono utilizzare metodologie diverse di analisi, motivando le ragioni e indicando chiaramente i criteri alla base della metodologia utilizzata.

Art. 12 - MISURE DI SICUREZZA

1. Il titolare del trattamento e ciascun delegato del titolare devono metter in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e la libertà delle persone fisiche.
2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono ai sensi dell'art. 32 del GDPR: la pseudonimizzazione - la minimizzazione - la cifratura dei

dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative, a titolo esemplificativo e non esaustivo, che possono essere adottate da ciascun Servizio a cui afferisce il trattamento:
   a) sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus, firewall, antintrusione);
   b) misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi, sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso ai dati in caso di incidente fisico o tecnico.
4. La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza. Il titolare del trattamento, tramite i suoi delegati, impartisce adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso ai dati personali.

Art. 13 - DIRITTI DELL'INTERESSATO.

1. Il Regolamento, agli articoli da 15 a 22 e all'art. 77, prevede che il soggetto interessato goda dei seguenti diritti:
   a) di avere accesso ai propri dati personali e alle informazioni previste dall'art. 15;
   b) di ottenere la rettifica dei dati personali inesatti (art. 16), la totale cancellazione (art. 17), la limitazione di trattamento (art. 18);
   c) di ottenere la comunicazione prevista dall'art. 19 sull'obbligo di notifica;
   d) di portabilità dei dati (art. 20);
   e) di opporsi al trattamento (art. 21);
   f) di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona;
   g) di proporre reclamo all'autorità di controllo (Garante Privacy) (art. 77).
2. L'esercizio dei diritti da parte degli interessati avviene, sulla base di quanto previsto all'art. 12 del Regolamento, rivolgendosi al Titolare del trattamento o al Delegato del Titolare nei seguenti modi:
   - inviando una raccomandata A.R. all'indirizzo: E.R.S.U. di Sassari, Via Michele Coppino n. 18, 07100 Sassari,
   - inviando una e-mail a: affarigenerali@ersusassari.it,
   - inviando una PEC a: affarigenerali@pec.ersusassari.it.

   L'Ente ha adottato a tal fine il modello definito dalla Regione Sardegna.

Art. 14 - DISPOSIZIONI FINALI

Le presenti direttive recepiscono, la delibera regionale n° 45/3 del 20/12/2023 avente ad oggetto *"Modello organizzativo e adempimenti finalizzati all'applicazione del Regolamento (UE) 2016/79 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati. Indirizzi e aggiornamento delle direttive regionali. Sostituzione delle direttive*

contenute nella deliberazione della Giunta regionale n° 21/8 del 24 aprile 2018 e n° 51/3 del 16 ottobre 2018", adeguandola e rimodulandola rispetto a quelle che sono le specificità del proprio Ente.

Allo stesso tempo la presente direttiva sostituisce le precedenti delibere del Consiglio di Amministrazione dell'ERSU la n° 20 del 18/10/2018 avente ad oggetto *"Regolamento UE n° 279/16: approvazione Manuale operativo di buone prassi per la protezione dei dati personali"* e n° 36/18 del 10/12/2018 avente ad oggetto *"Regolamento UE n° 679/16 e D.lgs. n° 101/2018: approvazione Linee guida applicative"*, che recepivano le precedenti delibere regionali sopra richiamate sostituite dalla delibera n° 45/3 del 20/12/2023.

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del GDPR e tutte le sue norme attuative vigenti.