Allegato 1 alla Delibera

Disposizioni generali sulla protezione dei dati personali in attuazione del Regolamento (UE) 2016/679 del Parlamento e del Consiglio -Recepimento direttive regionali emanate con DGR n.45/3 del 20.12.2023

Art. 1 – Oggetto

Art. 2 – Titolare del trattamento

Art. 3 – Delega delle funzioni del titolare del trattamento

Art. 4 – Referenti privacy

Art. 5 – Autorizzati al trattamento

Art. 6 – Amministratori di sistema

Art. 7- Responsabile della protezione dei dati

Art. 8 – Registro delle attività di trattamento della Regione

Art. 9 – Procedimento in caso di violazione dei dati personali

Art. 10 – I responsabili esterni del trattamento

Art. 11 – Analisi dei rischi e valutazione di impatto

Art. 12 – Adozione di atti generali

Art. 1

Oggetto

1. La presente direttiva ha per oggetto il recepimento delle misure organizzative attuate dalla Regione Sardegna e mediante le quali attuare 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, nonché alla libera circolazione di tali dati.

Art. 2

Titolare del trattamento

1. Con riferimento ai trattamenti dell'Agenzia, il titolare del trattamento è la stessa Agenzia Fo.Re.S.T.A.S. in persona dell'Amministratore Unico pro tempore, che la rappresenta legalmente, cui spetta la promozione dell'adozione di misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento.

2. All'Amministratore Unico compete:

a. l'adozione, anche su proposta dei suoi delegati, degli atti amministrativi generali previsti dagli articoli 2-ter e 2-sexies del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 e successive modifiche e integrazioni);
b. l'adozione degli indirizzi relativamente alle misure tecniche e organizzative di carattere generale non delegabili ai singoli Servizi;
c. l'individuazione dei requisiti di nomina del RPD e dei compiti ulteriori assegnati rispetto a quelli previsti dal Regolamento;
d. l'attribuzione di funzioni e compiti ai soggetti delegati degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
e. l'allocazione di adeguate risorse per la formazione del personale in materia di protezione dei dati e sicurezza informatica e per l'adeguamento dell'amministrazione 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 e ai Direttori dei Servizi, Centrali e Territoriali, nei limiti delle rispettive competenze e dei connessi trattamenti.

4. I delegati del trattamento, nell'esercizio dei propri compiti, si avvalgono della fattiva collaborazione dei referenti privacy e del personale autorizzato al trattamento, adeguatamente istruito.

Art. 3

Delega delle funzioni del titolare del trattamento

1. L'Amministratore Unico delega al Direttore Generale e ai Direttori dei Servizi Centrali e Territoriali, nei limiti delle rispettive competenze e dei connessi trattamenti, i seguenti compiti:

a. ricognizione dei dati personali, giudiziari e di natura particolare trattati e verifica della liceità, proporzionalità e trasparenza dei trattamenti;
b. analisi del rischio dei singoli trattamenti per i diritti e le libertà degli interessati;
c. compilazione e costante aggiornamento, con riferimento ai trattamenti di competenza, del registro delle attività di trattamento del titolare, ai sensi dell'articolo 30 del Regolamento;
d. individuazione dei soggetti autorizzati a compiere operazioni di trattamento, ai sensi dell'articolo 29 del Regolamento e dell'articolo 2-quaterdecies del decreto legislativo n. 196/2003, fornendo agli stessi specifiche istruzioni per il corretto trattamento dei dati e sovraintendendo e vigilando sull'attuazione delle istruzioni impartite;
e. designazione degli amministratori di sistema in aderenza alle norme vigenti in materia;
f. creazione delle condizioni volte a facilitare l'esercizio dei diritti previsti dagli articoli da 15 a 22 del Regolamento e tempestivo riscontro alle istanze degli interessati (diritti dell'interessato);
g. realizzazione degli adempimenti correlati, per quanto di competenza, all'attuazione degli articoli 26 e 28 del Regolamento, concernenti, rispettivamente, la contitolarità del trattamento e la designazione del responsabile del trattamento; nei casi in cui l'Agenzia, sia investita del compito di trattare dati personali per conto di altri titolari, il ruolo di responsabile del trattamento è attribuito all'Agenzia, che si avvale dei delegati per gli adempimenti conseguenti, compresa la mappatura del trattamento nella sezione dedicata del registro delle attività;
h. individuazione dei trattamenti di competenza per i quali è obbligatorio, o comunque opportuno, effettuare la valutazione di impatto sulla protezione dei dati personali e 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'articolo 36 del Regolamento;
i. coinvolgimento tempestivo e adeguato del RPD in tutte le questioni attinenti al trattamento dei dati personali;

j. adozione delle misure tecniche e organizzative adeguate ad attuare in modo efficace i principi di protezione dei dati personali e integrazione nel trattamento delle garanzie volte a soddisfare i requisiti del regolamento e tutelare i diritti degli interessati (privacy by design);
k. adozione delle misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari in relazione a ciascuna specifica finalità del trattamento (privacy by default);
l. attuazione per quanto di competenza, delle prescrizioni contenute nei provvedimenti comunicati dal Garante;
m. gestione della prima fase di una violazione di dati personali, nel rispetto della specifica procedura adottata dal titolare;
n. adozione delle misure di sicurezza tecniche e organizzative idonee a garantire che il trattamento sia effettuato conformemente al Regolamento e alla normativa statale vigente in materia di protezione dei dati personali, nonché conformi a linee guida e policy da applicare secondo standard comuni a tutti i Servizi dell'Agenzia (es. Regolamento Privacy e Regolamento Informatico);
o. mera predisposizione dell'informativa relativa a ciascuno dei trattamenti di dati personali di rispettiva competenza, in conformità agli articoli 13 e 14 del Regolamento, da sottoporre poi alla firma del titolare del trattamento.

2. I delegati del titolare esercitano le funzioni e i compiti delegati nel rispetto del Regolamento e della normativa vigente in materia di protezione dei dati personali, delle linee guida e dei provvedimenti del Garante, degli atti amministrativi di indirizzo adottati dalla Giunta Regionale, anche ai sensi degli articoli 2-ter e 2-sexies del decreto legislativo n. 196/2003, e delle buone pratiche e policy adottate dal titolare.

3. Il delegato del titolare richiede per ogni dipendente i permessi adeguati all'ambito di trattamento consentito per l'accesso ai sistemi informativi dell'Agenzia, verifica periodicamente la sussistenza delle condizioni per la conservazione del profilo di autorizzazione assegnato e si accerta che sia fornita comunicazione tempestiva agli uffici competenti per l'adeguamento del profilo.

4. Nell'ambito dei compiti previsti dalla lettera n) del comma 1, gli interventi e le misure tecniche atte a prevenire e contrastare, in termini uniformi per tutta l'Agenzia, i rischi connessi alla sicurezza informatica correlati alla tutela della riservatezza, integrità e disponibilità dei dati personali, sono delegati al Servizio Infrastrutture, Patrimonio e sicurezza (IPS) che, limitatamente a tal fine, coordina l'attività dell'Agenzia.

5. Si precisa che nel suddetto Servizio IPS, in quanto responsabile della cura del Patrimonio, è incardinata altresì l'organizzazione e la gestione della Videosorveglianza, per la quale si rimanda al relativo Regolamento e framework documentale per la conformità del Sistema di videosorveglianza che sarà in carico al Gruppo di lavoro privacy con la supervisione del DPO.

Art. 4

Referenti privacy

1. Nell'ottica del soddisfacimento dell'esigenza di coordinamento e di sinergia tra i Servizi dell'Agenzia nell'adempimento degli obblighi derivanti dall'entrata in vigore del Regolamento, il Direttore Generale, delegato del titolare, sentiti i Direttori dei Servizi, designa tra i funzionari o altri dipendenti con idonee capacità, almeno un referente privacy e un sostituto che svolgano la funzione di punto di contatto e raccordo tra il Responsabile per la protezione dei dati e la struttura di appartenenza, ferma restando la possibilità del delegato del titolare, tenuto conto della complessità e del numero dei trattamenti facenti capo all'Agenzia, di costituire un gruppo di lavoro a supporto del Responsabile per la protezione dei dati o uno specifico ufficio dedicato. L'atto di designazione del referente privacy, del suo sostituto e dell'eventuale gruppo di lavoro o ufficio dedicato è trasmesso al Responsabile per la protezione dei dati.

2. Il referente privacy costituisce il primo riferimento, all'interno della struttura di appartenenza, per la risoluzione delle problematiche e delle questioni in materia di protezione dei dati personali, supporta il delegato del titolare e le persone autorizzate al trattamento nell'adempimento dei propri compiti in materia di protezione dei dati personali e, in particolare, si occupa di:

- caricare le schede, compilare e aggiornare il registro delle attività di trattamento;
- gestire le utenze applicative all'interno del registro delle attività di trattamento;
- fornire il supporto nella gestione dei casi di possibile violazione dei dati personali e il necessario raccordo tra l'Agenzia, il referente data breach e il Responsabile per la protezione dei dati;
- fornire il supporto nei processi di analisi e valutazione dei rischi;
- fornire un raccordo tra il Responsabile per la protezione dei dati e l'Agenzia nella gestione delle istanze degli interessati per l'esercizio dei diritti, ai sensi degli articoli da 15 a 22 del Regolamento;
- fornire supporto nella formulazione delle richieste di consulenza al Responsabile per la protezione dei dati;
- collaborare con il Responsabile per la protezione dei dati e con gli altri referenti privacy, al fine di condividere problemi e soluzioni;
- con riferimento alle attività di sorveglianza svolte dal Responsabile per la protezione dei dati, raccordare i diversi Servizi e il Responsabile per la protezione dei dati e fornire supporto alle attività svolte presso l'intera Agenzia;
- facilitare il raccordo tra il Responsabile per la protezione dei dati e l'Agenzia in caso di ispezioni da parte del Garante.

3. La rete dei referenti privacy delle strutture dell'Amministrazione regionale si riunisce periodicamente e collabora, anche attraverso l'eventuale costituzione di un gruppo ristretto temporaneo o permanente, all'elaborazione e all'aggiornamento, con il coordinamento del Responsabile per la protezione dei dati e del suo ufficio, dei principali documenti e policy adottati dal titolare in materia di protezione dei dati personali.

Art. 5

Autorizzati al trattamento dei dati personali

1. 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 decreto legislativo n. 196 del 2003, hanno accesso ai dati personali e al loro trattamento dopo essere stati debitamente istruiti 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. L'Agenzia Fo.Re.S.T.A.S., al fine di migliorare la sensibilità e la preparazione dei dipendenti sulle tematiche privacy, si impegna nell'organizzazione della formazione specifica.
3. 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 e partecipa alla formazione erogata dal titolare in materia.
4. 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 Responsabile per la protezione dei dati;
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; nel caso di utilizzo di cartelle condivise segnalare al delegato del titolare o comunque al proprio dirigente la presenza di file contenenti dati personali al fine di individuare le corrette misure di protezione dei dati;
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 da 15 a 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 altro Servizio o Settore dell'Agenzia), 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 sono osservati anche in seguito a cessazione del rapporto di lavoro con il titolare. Contestualmente alla cessazione del rapporto di lavoro o al trasferimento presso altro Servizio/Settore dell'Agenzia, il personale che ha cessato il rapporto di lavoro o che è stato trasferito informa 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 (compresa la cancellazione/modifica delle nomine di autorizzati al trattamento);
q. rivolgersi tempestivamente per difficoltà o questioni inerenti alla 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.

5. Il titolare del trattamento si riserva la facoltà di integrare e 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, 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.

Art.6
Amministratore di Sistema

In base al provvedimento del Garante della Privacy del 27 novembre 2008, denominato **"***Misure ed accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*"**,** con tale denominazione ci si riferisce a chi svolge sul sistema informatico un'attività contraddistinta da un elevato profilo autorizzativo, che gli permetta di accedere a tutte le risorse del sistema, della rete, dei servizi web, delle attività legate al backup e al ripristino dei dati, delle attività legate alla manutenzione ed alla sicurezza dei sistemi informatici.

L'amministratore di sistema ha, di conseguenza, il compito di sovrintendere alle risorse del sistema operativo di uno strumento elettronico o di un sistema di base dati e di consentirne l'utilizzazione.

Sulla base degli elevati privilegi di accesso ai dati da parte dell'Amministratore di Sistema, il Titolare del trattamento deve mettere in atto degli accorgimenti e delle misure preventive nella scelta e nella successiva gestione di questa figura:

- l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;
- la designazione quale amministratore di sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
- gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante;

- nel caso di servizi di amministrazione di sistema affidati in *outsourcing* il titolare del trattamento deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema;
- l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari o dei responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti;
- devono essere adottati sistemi idonei alla registrazione degli accessi logici (*access log*) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema.
  Le registrazioni devono:
  - avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste;
  - comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate;
  - essere conservate per un congruo periodo, non inferiore a sei mesi.

  Nell'ambito del Modello Organizzativo di Fo.Re.S.T.A.S. la funzione di Amministratore di Sistema è assegnata a soggetti che presentino le competenze tecniche necessarie allo svolgimento delle predette funzioni.

Art. 7

Responsabile della protezione dei dati

1. Il responsabile della protezione dei dati (RPD) dell'Agenzia, con le competenze e le prerogative previste dagli articoli 37, 38 e 39 del Regolamento, può essere individuato tra i dipendenti dell'Agenzia, dell'Amministrazione regionale o degli enti, agenzie, aziende regionali che costituiscono il sistema Regione, come definito dal comma 2-bis dell'articolo 1 della legge regionale 13 novembre 1998, n. 31 (Disciplina del personale regionale e dell'organizzazione degli uffici della Regione). Nel caso di assenza di personale interno dotato dei requisiti previsti dalla normativa vigente, l'incarico può essere ricoperto anche da soggetti esterni.

2. L'Agenzia Fo.Re.S.T.A.S. ha provveduto a nominare un Responsabile per la protezione dei dati esterno, con la Deliberazione n.7 del 31.07.2024, al quale l'Agenzia fornisce le risorse necessarie per assolvere i compiti e accedere ai dati personali e ai trattamenti per mantenere la propria competenza specialistica.

3. Il responsabile della protezione dei dati è incaricato dei seguenti compiti:

a. informare e fornire consulenza al titolare del trattamento, nonché ai delegati del titolare e ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal Regolamento e da altre disposizioni dell'Unione relative alla protezione dei dati;
b. sorvegliare l'osservanza del Regolamento e di altre disposizioni dell'Unione europea, delle disposizioni statali e regionali 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.

4. Al responsabile della protezione dei dati, col supporto del referente privacy, sono delegate le funzioni di impulso, proposta e raccordo tra i Servizi dell'Agenzia, finalizzate all'attuazione dei compiti posti in capo al titolare del trattamento in materia di protezione dei dati personali.

5. Il Responsabile per la protezione dei dati è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. Le richieste di parere, corredate dalla previa istruttoria della struttura richiedente, sono inviate all'indirizzo dpo@forestas.it

Nei casi in cui il Responsabile per la protezione dei dati esprima parere negativo all'avvio o alla prosecuzione di un trattamento, il titolare o il suo delegato formalizza le motivazioni che giustificano comunque l'esecuzione dell'attività o l'implementazione della soluzione tecnologica, in contrasto alle indicazioni fornite dal Responsabile per la protezione dei dati.

6. Il parere del Responsabile per la protezione dei dati è in ogni caso richiesto:
   - nell'ambito della valutazione di impatto del trattamento, secondo quanto previsto dall'articolo 35 del regolamento;
   - nell'ambito della valutazione della violazione dei dati personali.

Art. 8

Registro delle attività di trattamento dell'Agenzia Fo.Re.S.T.A.S.

1. Il registro delle attività di trattamento previsto dall'articolo 30 del Regolamento (di seguito "registro") è unico per tutta l'Agenzia ed è compilato dai delegati del titolare con il supporto dei referenti privacy che ne curano il costante aggiornamento e la revisione per le parti di competenza.
2. Il registro è un atto dell'Agenzia e il suo contenuto rappresenta correttamente i trattamenti di dati personali in essere. Ogni trattamento è 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.

3. L'Agenzia, in quanto parte del sistema Regione, ha richiesto l'utilizzo dell'applicativo regionale per i trattamenti di propria competenza. Il Registro dei trattamenti è disponibile all'indirizzo https://rpd.regione.sardegna.it/registrotrattamento/login.php
4. L'Agenzia potrà valutare l'utilizzo di sistemi informatici alternativi in base alle esigenze che si verificheranno nel corso del tempo.
5. Ciascun Delegato del Titolare dell'Agenzia individua autonomamente gli utenti abilitati all'accesso al registro per le finalità di visione, aggiornamento e approvazione delle schede di trattamento. La gestione delle utenze applicative e l'aggiornamento delle schede dei trattamenti, con relativa richiesta di approvazione, vengono delegati ai referenti previsti all'articolo
6. L'approvazione ufficiale delle schede compete ai delegati del titolare del trattamento in base alle rispettive competenze e ai connessi trattamenti.
7. All'interno del registro vi è una specifica sezione dedicata alla formazione dei referenti e dei dipendenti, sviluppata dall'Ufficio Responsabile per la protezione dei dati della Regione Sardegna, in cui è fruibile del materiale informativo e la registrazione dei corsi formativi per il tempo necessario a garantire l'aggiornamento.

Art. 9

Procedimento in caso di violazione dei dati personali

1. L'articolo 4 del Regolamento UE 2016/679 (d'ora in poi GDPR) definisce "data breach" 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 presso una Azienda o una Pubblica Amministrazione. Gli articoli 33 e 34 del GDPR si occupano rispettivamente di disciplinare la notifica di una violazione dei dati personali all'autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato.

2. Qualsiasi dipendente o collaboratore dell'Agenzia, a prescindere dal ruolo rivestito, e tutti coloro che agiscono sotto l'autorità del titolare del trattamento, qualora abbiano conoscenza di un episodio di potenziale data breach, avvisano con immediatezza un Delegato del Titolare (il Direttore Generale o il Direttore del Servizio presso il quale prestano servizio); tale delegato del titolare è indicato come referente data breach. Quest'ultimo, senza indugio, segnala l'episodio al Gruppo di intervento costituito dallo stesso e dai seguenti soggetti:

- il Responsabile per la protezione dei dati, il quale darà parere tecnico sulla questione;

- i Referenti privacy;

- il Responsabile IT;

- il Responsabile della conservazione.

3. Il Referente data breach del Servizio in cui si è verificata la violazione, senza indugio, da avviso della potenziale violazione stessa a ciascun altro Referente data breach degli altri Servizi eventualmente colpiti

Art. 10

I responsabili esterni del trattamento

1. Tutti i delegati del titolare individuano e nominano, in base ai trattamenti di propria competenza, i responsabili del trattamento, ovvero 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. I delegati, in accordo col titolare, forniscono istruzioni in merito al trattamento all'interno di contratti o convenzioni e, in ogni caso, in aderenza a quanto inserito nel modello di nomina.

Art. 11

Analisi dei rischi e valutazione di impatto

1. I delegati del titolare effettuano 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 messi a disposizione da Istituzioni e Studi di Settore (ad esempio ENISA, ISO 31.000) e che vengono integrati 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 ed effettuano la stessa, previa consultazione del Responsabile per la protezione dei dati, 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.

Art. 12

Adozione di atti generali

1. Le proposte di regolamento e gli atti amministrativi generali che prevedono il trattamento

di categorie particolari di dati personali necessari per motivi di interesse pubblico rilevante specificano, coerentemente con quanto disposto dall'articolo 2-sexies del decreto legislativo n. 196 del 2003:

a) i tipi di dati che possono essere trattati;

b) le operazioni eseguibili;

c) il motivo di interesse pubblico rilevante;

d) le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

2. I proponenti degli atti previsti al comma 1 consultano, già in fase di elaborazione, l'ufficio del Responsabile per la protezione dei dati e ne danno atto nel testo proposto.