



**REGIONE AUTÓNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA**

Allegato alla Delib.G.R. n. 21/8 del 24.4.2018

Direttive regionali in materia di attuazione del Regolamento (UE) 2016/679 del Parlamento 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 (regolamento generale sulla protezione dei dati).

Direttive

Art. 1 – Oggetto

Art. 2 – Titolare del trattamento

Art. 3 – Delega delle funzioni del titolare del trattamento

Art. 4 – Incaricati del trattamento

Art. 5 – Responsabile della protezione dei dati Art. 6 –

Registro del titolare del trattamento

Art. 7 – Procedimento in caso di violazione dei dati personali (data breach)

Art. 8 - Presidio data breach



**REGIONE AUTÓNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA**

Art. 1

Oggetto

1. Le presenti direttive hanno per oggetto le misure organizzative e procedurali mediante le quali la Regione Autonoma della Sardegna 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 nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Art. 2

Titolare del trattamento

1. Con riferimento ai dati trattati dall'Amministrazione regionale, il titolare del trattamento è la Regione in persona del Presidente, suo rappresentante legale pro tempore.
2. Il titolare del trattamento assicura il rispetto dei principi e delle disposizioni del Regolamento anche mediante delega delle relative funzioni ai direttori generali, ai coordinatori delle unità di progetto e ai responsabili apicali degli uffici, secondo le rispettive competenze e responsabilità. I direttori generali possono esercitare le predette funzioni anche delegandole, a propria volta, ai direttori di servizio secondo le relative competenze e responsabilità.

Art. 3

Delega delle funzioni del titolare del trattamento

1. Con proprio decreto il Presidente della Regione delega le funzioni relative all'attuazione dei principi dettati in materia di trattamento dei dati personali dall'articolo 5 del Regolamento e, in particolare, i compiti previsti dal Regolamento aventi ad oggetto:
 - a) la comunicazione delle informazioni nei termini indicati dall'articolo 13 del Regolamento qualora i dati personali siano raccolti presso l'interessato;
 - b) la comunicazione delle informazioni nei termini indicati dall'articolo 14 del Regolamento qualora i dati personali non siano stati ottenuti presso l'interessato;
 - c) l'esercizio del diritto di accesso dell'interessato ai sensi dell'articolo 15 del Regolamento;
 - d) l'esercizio del diritto di rettifica da parte dell'interessato ai sensi dell'articolo 16 del Regolamento;
 - e) l'esercizio del diritto alla cancellazione da parte dell'interessato ai sensi dell'articolo 17 del Regolamento;
 - f) l'esercizio del diritto di limitazione del trattamento da parte dell'interessato ai sensi dell'articolo 18 del Regolamento;

- g) la notifica in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento ai sensi dell'articolo 19 del Regolamento;
- h) l'esercizio del diritto alla portabilità dei dati ai sensi dell'articolo 20 del Regolamento;
- i) l'esercizio del diritto di opposizione ai sensi dell'articolo 21 del Regolamento;
- j) l'esercizio del diritto di cui all'articolo 22 del Regolamento;
- k) l'adozione, e ove necessario riesame e aggiornamento, delle misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al Regolamento. Tali misure devono comunque essere adeguate a garantire un livello di sicurezza adeguato al rischio secondo quanto statuito dall'articolo 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;
- l) l'adozione delle misure tecniche e 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);
- m) l'adozione delle misure tecniche e 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);
- n) lo svolgimento degli adempimenti correlati, per quanto di competenza, all'attuazione degli articoli 26 e 28 del Regolamento, concernenti, rispettivamente, gli obblighi correlati alla situazione di contitolarità del trattamento e disciplina del responsabile del trattamento;
- o) la formale individuazione, nelle rispettive strutture, degli incaricati del trattamento;
- p) la tenuta del registro delle attività di trattamento in modo da assicurarne, per gli aspetti di competenza, la corretta compilazione e il costante aggiornamento e revisione;
- q) la rilevazione e la segnalazione al responsabile della protezione dei dati (DPO), secondo quanto indicato nell'articolo 35 del Regolamento e nelle Linee guida adottate sul tema dal Gruppo di lavoro europeo (WP29), dei casi nei quali effettuare la valutazione d'impatto sulla protezione dei dati personali e lo svolgimento della valutazione di impatto secondo le direttive e previa consultazione del DPO, provvedendo, ove necessario anche alla consultazione preventiva ai sensi dell'articolo 36 del Regolamento;
- r) la collaborazione, per quanto di competenza, con il responsabile della protezione dei dati della Regione Sardegna, nell'esecuzione dei compiti ad esso attribuiti;
- s) la cooperazione, per quanto di competenza, con l'autorità di controllo, nell'esecuzione dei compiti ad essa attribuiti;
- t) la gestione delle violazioni di dati personali (data breach), con particolare riferimento alla decisione di notifica, fermo restando quanto disposto dall'art. 7 e relativa procedura. Detta funzione non è ulteriormente delegabile.

Art. 4

Incaricati del trattamento

Sono incaricati del trattamento i dipendenti e collaboratori che agiscono sotto l'autorità del titolare del trattamento, i quali, ai sensi dell'articolo 29 del Regolamento, hanno accesso ai dati personali e al loro trattamento previa formale designazione e dopo essere stati debitamente istruiti e formati.

Art. 5

Responsabile della protezione dei dati

1. Il responsabile della protezione dei dati della Regione Sardegna, con le competenze e le prerogative previste dagli articoli 37, 38 e 39 del Regolamento, è individuato tra i dipendenti dell'Amministrazione regionale o degli enti, agenzie, aziende e istituti regionali che costituiscono il Sistema regione, come definito dal comma 2 bis dell'articolo 1 della legge regionale 13 novembre 1998, n.31.
2. Al fine di consentire al responsabile della protezione dei dati di eseguire i compiti ad esso attribuiti dal Regolamento, l'Amministrazione regionale fornisce al medesimo le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

Art. 6

Registro del titolare del trattamento

1. Il registro delle attività di trattamento svolte sotto la responsabilità della Regione Sardegna, è compilato, per gli aspetti di competenza, da ciascuna articolazione organizzativa dirigenziale della Amministrazione, che ne cura il costante aggiornamento e revisione.
2. Il registro del titolare del trattamento può essere detenuto, previa specifica delega, dal responsabile della protezione dei dati.

Art. 7

Procedimento in caso di violazione dei dati personali (data breach)

1. Per violazione dei dati personali (data breach) si intende 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 dall'Amministrazione regionale.
2. Al fine della corretta gestione dei casi di data breach, il titolare del trattamento designa con proprio decreto un dirigente (referente data breach) e un suo sostituto con competenze adeguate per supportare le valutazioni per individuare le conseguenze sui diritti degli interessati e supportare l'attuazione della corretta procedura da seguire in relazione alle specificità della violazione di dati personali in attuazione degli artt. 33 e 34 del Regolamento (UE) 2016/679.

Altresi il titolare del trattamento designa con proprio decreto il/i responsabile/i IT al fine di prevenire e gestire gli interventi di attenuazione/eliminazione dei danni, compreso il ripristino delle funzionalità e il supporto alla valutazione delle circostanze e conseguenze tecnico informatiche determinate dalla violazione.

3. Ogni dipendente o collaboratore dell'Amministrazione regionale, qualora abbia conoscenza del verificarsi di una violazione di dati personali avvisa con immediatezza il delegato del titolare ai sensi dell'art. 3 e il dirigente o responsabile della struttura presso la quale presta servizio. Secondo le modalità stabilite da apposita direttiva ed entro 24 ore dalla conoscenza della violazione da parte del dipendente o collaboratore, la stessa deve essere comunicata dal delegato del Titolare al Referente data breach e ai soggetti ivi indicati.
4. Non appena il titolare del trattamento nelle persone dei delegati di cui all'art. 3 è a conoscenza di un data breach che comporta un rischio per i diritti e la libertà delle persone fisiche notifica, per il tramite del referente data breach di cui al comma 2, la violazione dei dati personali al Garante, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è a conoscenza secondo quanto previsto dall'art. 33 e, ove ne ricorrano i presupposti, agli interessati ai sensi dell'art. 34 del Regolamento (UE) 2016/679 e nel rispetto delle modalità stabilite da apposita direttiva di cui al precedente comma 3.

Art. 8

Presidio data breach

Per garantire la gestione di eventuali data breach nei giorni festivi o nei giorni di chiusura obbligatoria degli uffici regionali è attivato un servizio di reperibilità dei soggetti attivi e relativo personale di supporto. Le fasi attuative saranno oggetto di apposita direttiva della Direzione generale dell'organizzazione e del personale.