REGIONE AUTÒNOMA DE SARDIGNA
REGIONE AUTONOMA DELLA SARDEGNA

DELIBERAZIONE N. 51/3 DEL 16.10.2018

Oggetto: **Modello organizzativo e adempimenti finalizzati all'applicazione del Regolamento europeo in materia di protezione dei dati personali con riguardo alla sicurezza dei dati personali: procedura di gestione delle violazioni di dati personali (data breach).**

Il Presidente ricorda che, il Regolamento (UE) 2016/679 del Parlamento e del Consiglio del 27 aprile 2016 recante la nuova disciplina sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46 /CE (regolamento generale sulla protezione dei dati) è pienamente applicabile in via diretta in tutti i Paesi dell'Unione Europea.

Evidenzia altresì che la Regione Sardegna, con la deliberazione della Giunta regionale n. 21/8 del 24 aprile 2018 ha emanato le direttive regionali in materia di attuazione del Regolamento (UE) 2016 /679, le quali definiscono le misure di governance e procedimentali finalizzate al perseguimento e all'attuazione dei principi e delle disposizioni del Regolamento, applicabili immediatamente sia al complesso degli uffici dell'Amministrazione regionale sia, previo recepimento e adattamento, secondo gli specifici assetti istituzionali, agli enti e alle agenzie che costituiscono il Sistema Regione ai sensi dell'art. 1, comma 2 bis della legge regionale n. 31 del 1998.

Ancora, il Presidente dà conto di aver provveduto, con propri decreti del 23 maggio 2018, numero 10068/47 e 25 maggio 2018, numero 10331/51, rispettivamente alla nomina del responsabile della protezione dei dati dell'Amministrazione regionale e all'attribuzione delle correlative funzioni di coordinatore dell'Unità di Progetto denominata "Responsabile della protezione dei dati per il sistema Regione".

Il Presidente prosegue sottolineando che il Regolamento definisce i diversi soggetti cui sono demandati ruoli e responsabilità volte ad applicare la normativa ivi disciplinata, nonché, in generale, le modalità con le quali questo obiettivo deve essere assicurato. Ruoli e responsabilità imperniate sul concetto di accountability secondo cui al titolare del trattamento è attribuito il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali.

Il Presidente, a questo proposito, precisa che il principio di accountability deve essere letto sotto un duplice profilo: esso non solo è il principio che ispira l'adeguamento/l'adempimento degli enti alla

normativa europea, ma è anche il punto di partenza per dimostrare rispetto e aderenza alla norma europea dell'Ente interessato; di conseguenza il concetto di accountability si deve intendere riferito al fatto che tutti i soggetti coinvolti in materia di protezione di dati personali non dovranno più ragionare in termini di mero adempimento alla norma di riferimento, come finora accaduto nella vigenza del Codice della Privacy ma, bensì, in termini di adesione sostanziale ai principi formalizzati nel nuovo Regolamento.

Il Presidente prosegue ricordando che con la deliberazione n. 24/27 del 14 maggio 2018 è stato formalizzato il modello organizzativo della gestione documentale della Regione con una prima indicazione delle misure urgenti da attuare per garantire modalità di gestione rispondenti al dettato del Regolamento (UE) 2016/679 e individuati il Coordinatore della gestione documentale e il Responsabile della conservazione.

Tra le misure prioritarie che l'Amministrazione intende perseguire, oltre a un generale riordino dei flussi documentali e degli archivi di deposito, è ritenuta determinante la totale digitalizzazione delle attività di tutte le strutture regionali al fine di eliminare la produzione di documentazione cartacea e dei conseguenti archivi.

Infatti, una corretta digitalizzazione implica la riduzione di costi per la conservazione degli archivi analogici, per la relativa manutenzione e per le correlate misure di sicurezza. Ad oggi, l'uso parallelo dei documenti cartacei e della loro digitalizzazione (spesso con modalità non appropriate) comporta una duplicazione della produzione documentale con aggravio dei costi che devono essere sostenuti per garantire entrambe le modalità di trattamento documentale a norma oltre ad accrescere l'esposizione a rischi di violazioni di dati personali.

Al fine di attuare una concreta riorganizzazione della gestione documentale e un coordinamento aperto alla partecipazione delle strutture sono stati attivati dal Coordinatore della gestione documentale dei gruppi di lavoro sui principali ambiti d'intervento, previa condivisione con le Direzioni generali dell'Amministrazione regionale. Il gruppo che cura la gestione della violazione della sicurezza dei dati (c.d. data breach) ha definito una procedura per la gestione delle violazioni di dati personali o presunte tali, individuando, inoltre, l'esigenza di revisione di alcuni punti della deliberazione n. 21/8 del 24 aprile 2018 riguardanti la gestione del data breach per eliminare alcuni dubbi interpretativi e dare riferimenti puntuali ai destinatari delle direttive. In particolare: a pag.1, parte finale del quarto capoverso, l'assunto “Il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 è abrogato” deve intendersi nel senso:

“L'applicazione del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n.196 è sospeso per le parti in contrasto con il Regolamento (UE) 2016/679 nelle more della sua modifica per l'adeguamento della normativa nazionale al Regolamento succitato”. (Il Decreto legislativo 10 agosto 2018, n. 101 – G.U del 4 settembre 2018, n. 205 ha disposto le modifiche di adeguamento al D.Lgs. 30 giugno 2003, n. 196).

All'art. 3 dell'allegato (pag. 3) è aggiunta la lettera 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”.

Il comma 2 dell'art. 7 dell'allegato è sostituito nel modo seguente: “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 .

Altresì 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”.

Il comma 3 dell'art. 7 dell'allegato è sostituito nel modo seguente: “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”.

Il comma 4 dell'art. 7 dell'allegato è sostituito nel modo seguente: “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".

Il comma 5 dell'art. 7 dell'allegato è eliminato in quanto il suo contenuto è stato assorbito nei commi precedenti.

È aggiunto l'articolo 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".

Il Presidente rappresenta la necessità di procedere all'adeguamento della deliberazione n. 21/8 del 24 aprile 2018 e all'approvazione delle rettifiche proposte e della procedura "data breach" definita nell'allegato alla presente deliberazione di cui dà lettura. Il Presidente evidenzia che detta procedura potrà essere adottata dagli Enti del Sistema regione anche adattandola alle loro specificità.

Il Presidente evidenzia che è opportuno garantire al Coordinatore della gestione documentale risorse idonee all'attuazione degli interventi di adeguamento della gestione documentale alle disposizioni del Regolamento (UE) 2016/679 con particolare riferimento alle urgenze.

La Giunta regionale, condividendo quanto rappresentato e proposto dal Presidente, e acquisito il parere favorevole di legittimità del Direttore generale della Centrale regionale di committenza

DELIBERA

- di approvare le modifiche alla deliberazione n. 21/8 del 24 aprile 2018 come di seguito evidenziate:

  a pag 1, parte finale del quarto capoverso l'assunto "Il Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 è abrogato" deve intendersi nel senso: "L'applicazione del Codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196 è sospeso per le parti in contrasto con il Regolamento (UE) 2016/679 nelle more della sua modifica per l'adeguamento della normativa nazionale al Regolamento succitato". (Il Decreto legislativo 10 agosto 2018, n. 101 – G.U del 4 settembre 2018 , n. 205 ha disposto le modifiche di adeguamento al D.Lgs. 30 giugno 2003, n. 196).

All'art. 3 dell'allegato (pag. 3) è aggiunta la lettera 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”.

Il comma 2 dell'art. 7 dell'allegato è sostituito nel modo seguente: “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.

Altresì 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”.

Il comma 3 dell'art. 7 dell'allegato è sostituito nel modo seguente: “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”.

Il comma 4 dell'art. 7 dell'allegato è sostituito nel modo seguente: “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”.

Il comma 5 dell'art.7 dell'allegato è eliminato in quanto il suo contenuto è stato assorbito nei commi precedenti.

È aggiunto l'articolo 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”;

- di approvare l'allegato alla presente deliberazione denominato “Procedura Data Breach”;
- di dare mandato all'Assessore della Programmazione, Bilancio, Credito e Assetto del Territorio per l'attribuzione delle risorse necessarie agli interventi prioritari di adeguamento della gestione documentale alle disposizioni del Regolamento (UE) 2016/679 e alla corretta attuazione del modello organizzativo di cui alla Delib.G.R. n. 24/27 del 14 maggio 2018;
- di allegare alla presente deliberazione il testo coordinato dell'allegato alla Delib.G.R. n. 21/8 del 24 aprile 2018 con le modifiche e integrazioni qui introdotte.

Letto, confermato e sottoscritto.

Il Direttore Generale	Il Presidente
Alessandro De Martini	Francesco Pigliaru