Deliberazione della Giunta Regionale 18 ottobre 2019, n. 1-387
Regolamento UE 2016/679. Decreto legislativo 196/2003. Approvazione Piano triennale di Audit Privacy 2019-2021.

A relazione del Presidente Cirio:

Premesso che:
il 24 maggio 2016 è entrato in vigore il Regolamento UE 2016/679, comunemente noto come GDPR "*General Data Protection Regulation*", relativo alla protezione delle persone fisiche, con riguardo al trattamento dei dati personali ed alla libera circolazione di tali dati, che ha trovato applicazione diretta a partire dal 25 maggio 2018 in tutti i Paesi facenti parte dell'Unione Europea;
in Italia il quadro normativo in materia di tutela dei dati personali è disciplinato oltre che dal suddetto Regolamento Europeo dal Codice Privacy novellato dal Decreto Legislativo 10 agosto 2018 n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 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 (regolamento generale sulla protezione dei dati)*";
la normativa consente la protezione del dato personale sotto un duplice profilo:
- la dimensione della sicurezza del trattamento, l'aspetto normativo/documentale, finalizzato a garantire che il flusso sui dati non leda i diritti fondamentali dell'interessato;
- la dimensione della sicurezza del trattamento, l'aspetto tecnologico/organizzativo, che mira a garantire l'integrità e la disponibilità del dato personale, nel passaggio attraverso l'infrastruttura operativa;

il Regolamento UE 2016/679 impone un cambiamento culturale nell'approccio al modello di gestione della Privacy, richiede infatti un ripensamento delle misure di sicurezza da adottarsi nelle amministrazioni, che devono essere adeguate al singolo contesto organizzativo ed elaborate a seguito di un'attenta analisi dei rischi, tipico dei sistemi di gestione di audit interno;
il suddetto regolamento introduce, in particolare, il principio di accountability secondo il quale il titolare del trattamento dei dati deve dimostrare di aver adottato adeguati modelli organizzativi e idonee misure di sicurezza fisiche e logiche, per proteggere i dati;
"l'audit privacy" rappresenta, quindi, la prova di una costante attenzione verso i trattamenti effettuati in conformità alla normativa privacy, essendo uno strumento di verifica della conformità dell'amministrazione dal punto di vista della conservazione del trattamento dei dati, specifica attenzione al sistema informatico, inteso come l'insieme di processi, risorse e tecnologie tesi alla protezione dei sistemi e del patrimonio informativo in termini di riservatezza, integrità e disponibilità.
Richiamato che:
- con la D.G.R. n. 1-6847 del 18 maggio 2018 sono stati recepiti i primi adempimenti in attuazione 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 ed è stata istituita la figura del Responsabile protezione dati (RPD);
- il Responsabile Protezione Dati (RPD) ha, tra i suoi compiti, ai sensi dell'art. 39, paragr. 1, lett. b) del Regolamento (UE) 2016/6799, "sorvegliare l'osservanza del regolamento (UE) 2016/679, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare 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".
Dato atto che:

- il RPD deve pianificare opportune verifiche ispettive (Audit) con lo scopo di accertare lo stato di compliance del sistema Privacy al Regolamento, di prevenire l'insorgere di eventuali anomalie, difformità e criticità del sistema e di definire, nel caso, opportune azioni correttive e/o di miglioramento.

- è opportuno, a tale fine, prevedere non essendo possibile verificare eventuali scostamenti dallo standard o miglioramenti rispetto alle non conformità riscontrate in precedenza, una prima fase in cui il RPD proceda alla verifica dello stato di attuazione delle disposizioni adottate dalla Giunta regionale in tema di Privacy per definire una baseline sulla quale misurare successive evoluzioni ed alla cui conclusione, predisponga una relazione che segnali ogni mancata conformità o suggerimento e proponga un piano di rimedi e scadenze per le diverse azioni richieste, che saranno successivamente oggetto di ulteriore verifica.

Ritenuto, pertanto, opportuno approvare il Piano Triennale di Audit Privacy per gli anni 2019, 2020 e 2021, di cui all'allegato al presente provvedimento quale parte integrante e sostanziale, stabilendo, in particolare, che:

- per le attività di audit il Responsabile Protezione Dati potrà avvalersi della collaborazione del Settore Audit Interno, fermo restando che nell'attività di Audit Privacy saranno coinvolte tutte le Direzioni relativamente al trattamento dei dati di loro competenza e ci si avvarrà della collaborazione dei referenti privacy di ciascuna Direzione e che gli Audit sulla sicurezza informatica sono effettuati dalla Direzione responsabile dei sistemi informativi.

Visto il Regolamento generale sulla protezione dei dati 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016;

visto il Decreto Legislativo 10 agosto 2018 n. 101;

vista la D.G.R. n. 1-6847 del 18.5.2018;

vista la D.G.R. n. 1-192 del 9.8.2019.

Attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. n. 1- 4046 del 17.10.2016.

Tutto quanto premesso e considerato;

la Giunta regionale, a voti unanimi resi nelle forme di legge,

delibera

- di approvare, nell'ambito del Regolamento UE 2016/679 e del decreto legislativo 196/2003, il Piano Triennale di Audit Privacy per gli anni 2019, 2020 e 2021, di cui all'allegato al presente provvedimento quale parte integrante e sostanziale, stabilendo, in particolare, che:

- per le attività di audit il Responsabile Protezione Dati potrà avvalersi della collaborazione del Settore Audit Interno, fermo restando che nell'attività di Audit Privacy saranno coinvolte tutte le Direzioni delegate relativamente al trattamento dei dati di loro competenza e ci si avvarrà della collaborazione dei referenti privacy di ciascuna Direzione e che gli Audit sulla sicurezza informatica sono effettuati dalla Direzione responsabile dei sistemi informativi;

- di dare atto che il presente provvedimento non comporta oneri a carico del bilancio regionale.

La presente deliberazione sarà pubblicata sul B.U. della Regione Piemonte ai sensi dell'art. 61 dello Statuto e dell'art. 5 della L.R. 22/2010.

(omissis)

Allegato

Direzione Affari Istituzionali ed Avvocatura

Responsabile Protezione Dati (RPD)

PIANO TRIENNALE DI AUDIT PRIVACY 2019-2021

PIANO DI AUDIT PRIVACY TRIENNALE 2019-2021

Il presente piano di Audit Privacy è riferito al triennio 2019-2021, con eventuale aggiornamento annuale.

AMBITO DI APPLICAZIONE

- Regolamento (UE) 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.

- Provvedimenti del Titolare per l'adeguamento alla normativa.

Il 27 aprile 2016 è stato approvato il Regolamento (UE) 2016/679 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).

Il Regolamento (GDPR) nasce per proteggere i diritti e le libertà fondamentali delle persone fisiche, in particolare per assicurare un'applicazione coerente e omogenea delle norme a protezione dei dati personali con regole equivalenti a livello europeo (considerando 10) ed offre un quadro di riferimento aggiornato e fondato sul principio di responsabilizzazione (*accountability*).

Il Regolamento introduce la figura del Responsabile Protezione Dati (RPD) che ha, tra i suoi compiti (art. 39, paragr. 1, lett. b) Regolamento (UE) 2016/679), l'incarico di "sorvegliare l'osservanza del regolamento (UE) 2016/679, di altre disposizioni nazionali o dell'Unione relative alla protezione dei dati nonché delle politiche del titolare 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".

Il Regolamento introduce concetti e strumenti nuovi tra i quali, particolare rilievo, rivestono: l'istituzione del Registro dei trattamenti e la valutazione d'impatto sulla protezione dei dati (DPIA).

Il GDPR, introduce il principio di *accountability* secondo il quale il titolare del trattamento dei dati deve dimostrare di aver adottato adeguati modelli organizzativi e idonee misure di sicurezza fisiche e logiche, per proteggere i dati.

A tal fine il RPD deve pianificare opportune verifiche ispettive (Audit) con lo scopo di accertare lo stato di compliance del sistema Privacy al Regolamento, prevenendo l'insorgere di eventuali anomalie, difformità e criticità del sistema e, nel caso, definendo opportune azioni correttive e/o di miglioramento.

OBIETTIVO

L'obiettivo del programma di Audit Privacy è quello di pianificare la verifica dell'attuazione e dell'efficacia delle misure privacy adottate e di verificarne la rispondenza alla normativa contribuendo al suo miglioramento e limitando il rischio di sanzioni.

ATTIVITÀ DI AUDIT PRIVACY

Il responsabile protezione dati, nello svolgere le attività di cui al presente Piano, potrà avvalersi anche della collaborazione del Settore Audit Interno, previo idoneo provvedimento di impegno di spesa.

Nell'attività di Audit Privacy, anche al fine di coordinare analoghe attività ed evitare sovrapposizioni, saranno coinvolte tutte le Direzioni relativamente al trattamento dei dati di loro competenza e ci si avvarrà della collaborazione dei referenti privacy di ciascuna Direzione.

Inoltre le attività di Audit, svolte dal RPD, riguarderanno anche i soggetti individuati come responsabili esterni del trattamento da un campione predefinito.

Gli Audit verranno attuati attraverso la predisposizione di questionari somministrati alle singole Direzioni regionali.

Ciascun Audit Privacy è condotto con lo scopo di verificare al giusto livello di dettaglio l'applicazione dei requisiti del GDPR.

Le evidenze reperite durante le verifiche saranno valutate a fronte dei seguenti riferimenti:

- i requisiti della norma;
- i controlli previsti dalla norma stessa;
- la documentazione che costituisce l'impianto di *accountability*.

Le eventuali "non conformità" e "osservazioni" saranno gestite attraverso il follow-up delle raccomandazioni fornite in sede di Audit privacy.

Dagli Audit si potrà trarre profitto in merito alle osservazioni e commenti degli auditor e si potranno identificare e attuare opportunità di miglioramento.

Al termine del ciclo di Audit annuale sarà effettuata una relazione dal RPD che attesta i risultati.

AUDIT SULLA CONFORMITÀ ALLA NORMATIVA PRIVACY (GDPR 2016/679).

Il Piano triennale di Audit Privacy 2019-2021, in attuazione delle previsioni della normativa in tema di privacy, prevede le seguenti azioni volte a rafforzare il "sistema privacy" della Giunta regionale, a valutarne la conformità alla normativa e le possibili azioni di miglioramento:

1) Rappresentazione dell'organigramma "sistema privacy", che evidenzia le figure previste dal Regolamento europeo.

2) Mappatura e aggiornamento dei trattamenti, da parte dei referenti privacy come da DGR n. 1-192 del 9 agosto 2019, con validazione da parte dei Delegati;

3) Valutazione di impatto per tutti i trattamenti per cui è obbligatorio per legge effettuarla in ambito regionale, da parte dei referenti privacy, previa validazione da parte dei Delegati, come da DGR n. 1-192 del 9 agosto 2019.

4) Verifica della valutazione di impatto dei trattamenti ad alto rischio effettuata dalle strutture regionali, su un campione selezionato.

5) Audit di conformità, dell'adeguamento alla normativa GDPR, sugli atti di nomina a responsabile esterno del trattamento, su un campione selezionato.

4) Audit sull'adeguamento delle misure di sicurezza e applicazione della normativa GDPR nei confronti dei responsabili esterni del trattamento, su un campione selezionato.

5) Audit sulla sicurezza informatica delle misure adottate dalla Direzione Segretariato in quanto responsabile dei sistemi informativi.

6) Diffusione della cultura dell'Audit privacy.

7) Interventi urgenti di Audit privacy.