Deliberazione della Giunta Regionale 20 dicembre 2024, n. 5-583
Regolamento UE 2016/679. Decreto legislativo 196/2003 e s.m.i.. Approvazione Piano triennale di Audit Privacy 2025-2027.

REGIONE PIEMONTE

Seduta N° **35** Adunanza 20 DICEMBRE 2024

Il giorno 20 del mese di dicembre duemilaventiquattro alle ore 10:10 si è svolta la seduta della Giunta regionale in via ordinaria, presso la sede della Regione Piemonte, Piazza Piemonte 1 - Torino con l'intervento di Elena Chiorino Presidente e degli Assessori Paolo Bongioanni, Enrico Bussalino, Marco Gabusi, Marco Gallo, Matteo Marnati, Maurizio Raffaello Marrone, Andrea Tronzano con l'assistenza di Guido Odicino nelle funzioni di Segretario Verbalizzante.
Assenti, per giustificati motivi: il Presidente Alberto CIRIO, gli Assessori Marina CHIARELLI - Federico RIBOLDI - Gian Luca VIGNALE

DGR 5-583/2024/XII

OGGETTO:
Regolamento UE 2016/679. Decreto legislativo 196/2003 e s.m.i.. Approvazione Piano triennale di Audit Privacy 2025-2027.

A relazione di: (Cirio), Chiorino

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:
a) 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;
b) 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.
Richiamate le seguenti deliberazioni della Giunta regionale:
- n. 1-6847 del 18 maggio 2018 con cui 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);
- n. 10-5171 del 14 giugno 2022 con cui la Responsabile del Settore "Programmazione, controlli e privacy" è stata nominata quale Responsabile per la protezione dei dati (RPD) della Regione Piemonte.

Dato atto che:
- il Responsabile Protezione Dati (RPD) ha, tra i suoi compiti, ai sensi dell'art. 39, paragrafo 1, lett. b) del Regolamento (UE) 2016/6799, quello 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 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;
- il piano triennale di Audit privacy 2022-2024, approvato con D.G.R. n. 41-5351 dell'8 luglio 2022, si concluderà a dicembre 2024 con la trasmissione delle osservazioni alle Direzioni regionali.
Dato atto, inoltre, che:
ad oggi sono stati effettuate le verifiche sulla base del precedente piano di Audit Privacy e, a titolo esemplificativo, sono stati sottoposti a controllo, a seguito di campionamento, i trattamenti di competenza delle Direzioni, le applicazioni web, la nomina degli incaricati, i soggetti in house di Regione Piemonte;
per il prossimo triennio sono stati introdotte ulteriori voci di controllo in materia, nello specifico la verifica della corretta nomina dei soggetti sub responsabili del trattamento, in conformità alle Linee Guida 22/2024 del 7 ottobre 2024 dello European Data Protection Board e della verifica, a campione, della corretta pubblicazione degli atti amministrativi sul Bollettino Ufficiale regionale.
il Responsabile Protezione Dati ha predisposto l'aggiornamento del Piano Triennale, tenuto conto degli esiti delle ricognizioni effettuate e degli obiettivi assegnati alle Direzioni regionali, fermo restando che gli Audit sulla sicurezza informatica sono effettuati dalla Direzione responsabile dei sistemi informativi.
Ritenuto, pertanto, opportuno:
- approvare il Piano Triennale di Audit Privacy per gli anni 2025, 2026 e 2027, di cui all'allegato al presente provvedimento quale parte integrante e sostanziale, stabilendo, in particolare, che:
a) nelle attività di Audit Privacy saranno coinvolte tutte le Direzioni, relativamente al trattamento dei dati di loro competenza;
b) l'attività di Audit sarà svolta in collaborazione con i referenti privacy di ciascuna Direzione;
c) gli Audit sulla sicurezza informatica sono effettuati dalla Direzione responsabile dei sistemi

informativi.
- demandare al Responsabile del Settore Programmazione, controlli e privacy l'adozione degli atti necessari per l'attuazione della presente deliberazione con i relativi programmi annuali di controllo.
Attestato che, ai sensi della DGR n. 8-8111 del 25 gennaio 2024 ed in esito all'istruttoria sopra richiamata, il presente provvedimento non comporta effetti contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte, in quanto l'attività di Audit Privacy è effettuata da personale interno al Settore Programmazione, controlli e privacy.
Attestata la regolarità amministrativa del presente provvedimento ai sensi della DGR n. 8-8111 del 25 gennaio 2024.
Tutto quanto premesso e considerato, la Giunta regionale, a voti unanimi resi nelle forme di legge;

delibera

1) di approvare, nell'ambito del Regolamento UE 2016/679 e del decreto legislativo 196/2003 e s.m.i., il Piano Triennale di Audit Privacy per gli anni 2025, 2026 e 2027, di cui all'allegato al presente provvedimento quale parte integrante e sostanziale, stabilendo, in particolare, che:
a) nelle attività di Audit Privacy saranno coinvolte tutte le Direzioni, relativamente al trattamento dei dati di loro competenza;
b) l'attività di Audit sarà svolta da personale regionale in collaborazione con i referenti privacy di ciascuna Direzione;
c) gli Audit sulla sicurezza informatica sono effettuati dalla Direzione responsabile dei sistemi informativi.
2) di demandare al Responsabile del Settore Programmazione, controlli e privacy l'adozione degli atti necessari per l'attuazione della presente deliberazione con i relativi programmi annuali di controllo;
3) che il presente provvedimento non comporta effetti contabili diretti né effetti prospettici sulla gestione finanziaria, economica e patrimoniale della Regione Piemonte, come in premessa attestato.

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.

Sono parte integrante del presente provvedimento gli allegati riportati a seguire [1], archiviati come file separati dal testo del provvedimento sopra riportato:

1. DGR-583-2024-All_1-allegato_alla_dgr_PIANO_triennale_AUDIT_privacy_2025_27.doc

Allegato

1 L'impronta degli allegati rappresentata nel timbro digitale QRCode in elenco è quella dei file pre-esistenti alla firma digitale con cui è stato adottato il provvedimento

Direzione della Giunta regionale
Settore Programmazione, controlli e privacy
Responsabile Protezione Dati (RPD)

PIANO TRIENNALE DI AUDIT PRIVACY 2025-2027

PIANO TRIENNALE DI AUDIT PRIVACY 2025-2027

Il presente piano di Audit Privacy è riferito al triennio 2025-2027, 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, di verificarne la rispondenza alla normativa contribuendo al suo miglioramento e limitando il rischio di sanzioni, proseguendo al contempo l'attività di diffusione della "cultura della privacy".

ATTIVITÀ DI AUDIT PRIVACY

Nell'attività di Audit Privacy saranno coinvolte tutte le Direzioni delegate al trattamento dei dati di loro competenza e ci si avvarrà della collaborazione dei referenti privacy di ciascuna Direzione; il Responsabile Protezione Dati potrà avvalersi anche della collaborazione di consulenze esterne.
Le attività di Audit svolte dal RPD riguarderanno anche i soggetti individuati come responsabili esterni del trattamento (art. 28 GDPR) sulla base di un campione predefinito.

Gli Audit verranno attuati attraverso la predisposizione di check list/questionari e di estrazioni a campione di documenti/atti/trattamenti/applicazioni mobili che, potenzialmente, trattano dati personali.
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 che attesta i risultati.

AUDIT SULLA CONFORMITÀ ALLA NORMATIVA PRIVACY (GDPR 2016/679).
Il Piano triennale di Audit Privacy 2025-2027, in attuazione delle previsioni della normativa in tema di privacy, prevede le seguenti azioni volte a rafforzare il "sistema privacy" della Regione Piemonte, a valutarne la conformità alla normativa e individuarne le possibili azioni di miglioramento:

- verifica, a campione, di applicativi complessi in uso di Regione Piemonte che contengono dati personali, su un campione selezionato;
- verifica, a campione, dei trattamenti inseriti nel registro (corretta descrizione, indicazione della base giuridica del trattamento, indicazione della tipologia di dati trattati, indicazione delle misure di sicurezza, individuazione del responsabile esterno, ecc);
- verifica, su campione selezionato, del collegamento tra DPM (data protection manager) e Procedo (applicativo mappatura processi, sottoprocessi, procedimenti);
- verifica della valutazione di impatto dei trattamenti ad alto rischio effettuata dalle strutture regionali, su un campione selezionato;
- Audit di conformità degli atti di nomina a responsabile esterno del trattamento, su un campione selezionato, rispetto alla normativa GDPR;
- Audit sull'adeguamento delle misure di sicurezza e applicazione della normativa GDPR nei confronti dei responsabili esterni del trattamento, su un campione selezionato;
- Verifica della corretta nomina dei soggetti sub responsabili del trattamento, in conformità alle Linee Guida 22/2024 del 7 ottobre 2024 dello European Data Protection Board;
- Verifica, a campione, della corretta pubblicazione degli atti amministrativi sul Bollettino Ufficiale regionale;
- Verifica, a campione su X Direzioni, della nomina e della relativa presa visione dei soggetti autorizzati al trattamento;
- verifiche, in collaborazione con il controllo successivo amministrativo, relativamente agli atti estratti su un campione selezionato;
- Verifica, a campione, di soggetti in house;
- eventuali interventi urgenti di Audit privacy.

I controlli sopra descritti verranno conclusi nel corso del triennio, fatte salve richieste urgenti da parte dell'Autorità Garante Privacy.