

Codice A1019A

D.D. 17 maggio 2023, n. 261

Programmazione dell'attività di Audit in materia di Privacy per l'anno 2023 e modalità di svolgimento.



ATTO DD 261/A1019A/2023

DEL 17/05/2023

DETERMINAZIONE DIRIGENZIALE

A1000A - DIREZIONE DELLA GIUNTA REGIONALE

A1019A - Programmazione, controlli e privacy

OGGETTO: Programmazione dell'attività di Audit in materia di Privacy per l'anno 2023 e modalità di svolgimento.

Premesso che:

- il 24 maggio 2016 è entrato in vigore il Regolamento UE 2016/679, 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 (d.lgs. 196/2003) 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)*”;
- il Regolamento UE 2016/679 impone un cambiamento culturale nell’approccio al modello di gestione della Privacy introducendo, 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 nel rispetto della normativa sulla privacy, essendo uno strumento di verifica della conformità dell’amministrazione sia dal punto di vista della conservazione del trattamento dei dati sia di una particolare 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;
- il presupposto giuridico dell’Audit privacy è rinvenibile nei Considerando del Regolamento UE 2016/679 (GDPR), dal 74 al 79, i quali, in particolare, stabiliscono che:
 - *il titolare deve mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del*

contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche (cit. Considerando 74).

- *La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento (78).*

- l'Audit privacy, curato dal DPO con il supporto dei referenti privacy, individuati formalmente da ciascuna Direzione, consente altresì al Titolare di individuare le aree di rischio su cui occorre agire attraverso misure adeguate per minimizzare i rischi;

Considerato che:

- con D.G.R 41-5351 del 1°8 luglio 2022 è stato adottato Piano triennale di Audit Privacy 2022-2024 stabilendo che :

1. nelle attività di Audit Privacy saranno coinvolte tutte le Direzioni, relativamente al trattamento dei dati di loro competenza;
2. l'attività di Audit sarà svolta da personale regionale in collaborazione con i referenti privacy di ciascuna Direzione;
3. gli Audit sulla sicurezza informatica sono effettuati dalla Direzione responsabile dei sistemi informativi;

- con D.D. n. 337/A1019A/2022 del 12/07/2022, in attuazione al Piano triennale di Audit Privacy 2022-2024 si è stabilito di svolgere l'attività di Audit, per l'anno 2022, sui seguenti ambiti:

- a. ricognizione dell'esistenza di applicazioni mobili di Titolarità di Regione Piemonte (App), con particolare riferimento alla verifica del rispetto della normativa privacy (Regolamento UE 2016/679);
- b. verifica di un adempimento, in corso di attuazione, in capo al Titolare, di aggiornamento del collegamento del programma HR con il registro dei trattamenti (DPM) per l'integrazione e l'aggiornamento delle lettere di incarico al trattamento dati;

Valutato quindi doveroso proseguire l'attività di audit, anche nel corso del 2023, nell'ottica della corretta applicazione della normativa sulla privacy, anche individuando le aree di rischio e definendo le azioni di prevenzione delle attività in materia di protezione dei dati personali in conformità al Piano Triennale di Audit 2022-2024;

Ritenuto opportuno, quindi, incentrare l'attività di audit sui seguenti ambiti:

- a. verifica, a campione, di un numero pari a 20 trattamenti estratti con metodo casuale dal registro dei trattamenti (DPM), secondo le modalità e la check list di cui all'allegato A alla presente determinazione;
- b. la verifica dell'aggiornamento del collegamento del programma HR con il registro dei trattamenti (DPM) per la predisposizione delle lettere di incarico al trattamento dati, relativamente al personale neoassunto, a completamento dell'Audit avviato nel corso del 2022.

Preso atto della DGR n. 41-5351 del 8/07/2022 che approva il Piano triennale di Audit Privacy 2022-2024;

Dato atto che il presente provvedimento non comporta impegni di spesa a carico della Regione Piemonte;

Attestata la regolarità amministrativa del presente provvedimento ai sensi della D.G.R. n. 1-4046 del 17/10/2016, come modificata dalla D.G.R. n. 1-3361 del 14 giugno 2021.

LA DIRIGENTE

Richiamati i seguenti riferimenti normativi:

- il Regolamento UE 2016/679;
- la Deliberazione Giunta Regionale 18/05/2018 , n. 1 - 6847;
- la Deliberazione Giunta Regionale 28/09/2018 , n. 1 - 7574;
- la Deliberazione Giunta Regionale 18/10/2019 , n. 1 - 387;
- la Deliberazione Giunta Regionale 09/08/2019 , n. 1 - 192;
- la Deliberazione Giunta Regionale 27/08/2020, n. 19 - 1177;
- la Deliberazione Giunta Regionale 10/12/2021, n. 7 - 4281;
- la Deliberazione Giunta Regionale 8/07/2022, n. 41 - 5351;

DETERMINA

1. di svolgere l'attività di Audit, per l'anno 2023, sui seguenti ambiti:

- a. verifica, a campione, di un numero pari a 20 trattamenti estratti con metodo casuale dal registro dei trattamenti (DPM), secondo le modalità e la check list di cui all'allegato A alla presente determinazione;
- b. la verifica dell'aggiornamento del collegamento del programma HR con il registro dei trattamenti (DPM) per la predisposizione delle lettere di incarico al trattamento dati, relativamente al personale neoassunto, a completamento dell'Audit avviato nel corso del 2022.

Il presente provvedimento, non comportando spesa, non assume rilevanza contabile.

La presente Determinazione non è soggetta agli obblighi di pubblicazione di cui al D.Lgs 33/2013.

Avverso la presente determinazione è ammessa proposizione di ricorso giurisdizionale al Tribunale Amministrativo Regionale del Piemonte entro 60 giorni ovvero proposizione di ricorso straordinario al Capo dello Stato entro 120 giorni dalla data di comunicazione o di piena conoscenza dell'atto, ovvero l'azione innanzi al Giudice Ordinario, per tutelare un diritto soggettivo, entro il termine di prescrizione previsto dal Codice Civile.

La presente determinazione sarà pubblicata sul Bollettino Ufficiale della Regione Piemonte ai sensi dell'articolo 61 dello Statuto e dell'articolo 5 della legge regionale 12 ottobre 2010, n. 22.

LA DIRIGENTE (A1019A - Programmazione, controlli e privacy)
Firmato digitalmente da Tiziana Zaniolo