Codice A1019A
D.D. 12 luglio 2022, n. 337
Programmazione dell'attività di Audit in materia di Privacy per l'anno 2022 e modalità di svolgimento.

ATTO DD 337/A1019A/2022 DEL 12/07/2022

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 2022 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, curata 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:

- la Regione Piemonte, dal 2019, individua azioni volte a rafforzare il "sistema privacy" della Giunta regionale attraverso l'"Audit sulla conformità alla normativa privacy (GDPR 2016/679)".

- le azioni intraprese nell'ultima programmazione sono state:

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. 1-192del 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.

- l'Audit privacy 2020 ha avuto carattere ricognitivo, volto a fotografare il rispetto degli adempimenti prescritti dal Regolamento europeo e dal Codice per la protezione dei dati, come modificato dal D.Lgs. 101/2018, sia a livello generale sia a livello delle singole Direzioni e articolazioni dell'Ente anche attraverso la mappatura dello stato delle misure adottate. La ricognizione ha riguardato l'attività documentale/provvedimentale nonché gli adempimenti organizzativi adottati successivamente all'entrata in vigore del GDPR, e, segnatamente:

a) la ricognizione dei provvedimenti e atti del Titolare;
b) la predisposizione di un questionario alle Direzioni;
c) la ricognizione dei sistemi informativi;
d) la ricognizione del sistema di videosorveglianza.

- l'Audit privacy 2021 ha avuto l'obiettivo di estrarre a campione un numero pari a 20 trattamenti, individuati con metodo casuale dal registro dei trattamenti (DPM), verificandone della completezza nella compilazione dei campi previsti dal DPM stesso con particolare riferimento alle finalità del trattamento, alla presenza delle basi giuridiche che legittimano il trattamento, ai riferimenti normativi e legittimi interessi, all'origine dei dati, al tipo di banca dati, alle categorie di dati trattati, alle categorie di interessati, ai titolari selezionati, ai responsabili del trattamento, ai trasferimenti e comunicazioni, alle misure di sicurezza, al periodo di conservazione dei dati e, infine, sulla

presenza della valutazione di impatto in riferimento ai trattamenti considerati a *"rischio elevato per i diritti e le libertà delle persone"*;
Valutato quindi doveroso proseguire l'attività di audit, anche nel corso del 2022, 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;
Preso atto che l'attività di Audit è stata incardinata nel Settore "Programmazione, controlli e privacy", articolazione della Direzione della Giunta regionale, istituito con D-G.R. 7-4281 del 10.12.2021 e ritenuto opportuno procedere celermente a riorganizzare, all'interno del Settore, tale attività di Audit per il 2022;
Preso atto della DGR n. 41-5351 del 8/07/2022 che approva il Piano triennale di Audit Privacy 2022-2024;
Valutata l'opportunità di svolgere l'attività di Audit per l'anno 2022 nei seguenti ambiti:
- 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), secondo le modalità e la check list di cui all'allegato A al presente atto per farne parte integrante e sostanziale;
- la 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, secondo le modalità e la check list di cui all'allegato A al presente atto per farne parte integrante e sostanziale;
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 2022, sui seguenti ambiti:
- 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), secondo le modalità di cui all'allegato A al presente atto per farne parte integrante e sostanziale;
- 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, secondo le modalità di cui all'allegato

A al presente atto per farne parte integrante e sostanziale;
2. di approvare le modalità di svolgimento dell'attività di audit e la relativa check list di cui all'allegato A al presente atto per farne parte integrante e sostanziale;

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

Allegato

Allegato A)

Modalità di svolgimento dell'attività di Audit per l'anno 2022

Le attività di Audit per l'anno 2022 si concentreranno sui seguenti ambiti:

1) 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)

Le App sono state oggetto di attenzione e di raccomandazioni da parte dell'Autorità Garante per la Privacy.

A titolo informativo si segnala il parere rilasciato all'AgID, sullo schema di Linee guida per l'accesso telematico ai servizi della pubblica amministrazione, ai sensi dell'art. 64-bis del d.lgs. 82/2005 - 1° novembre 2021 [9714315], con cui l'Autorità Garante Privacy ha suggerito alcune indicazioni per assicurare opportune garanzie a tutela della privacy.

In conformità al citato parere, si ritiene utile procedere con una ricognizione dell'esistenza di applicazioni mobili di Titolarità di Regione Piemonte (App), verificando conseguentemente il rispetto della normativa privacy (Regolamento UE 2016/679).

Dal punto di vista procedurale verrà inviata una lettera alle Direzioni a cui verrà richiesto di comunicare l'esistenza di App in uso alla Direzione stessa (in riferimento anche a ciascun Settore appartenente alla Direzione) con la descrizione dei servizi offerti, delle misure tecniche e di sicurezza adottate.

2) 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

Tale verifica è conseguente all'adempimento, in corso di attuazione, in capo al Titolare, di aggiornamento del collegamento del programma HR con il registro dei trattamenti (DPM) finalizzato all'aggiornamento delle lettere di incarico al trattamento dati da trasmettere a tutti il personale regionale.

L'attività di Audit valuterà la corretta attuazione della misura in particolare verificando la predisposizione della lettera di incarico aggiornata da parte di tutte le Direzioni e della conseguente presa visione da parte del dipendente.

La verifica verrà effettuata direttamente sull'applicativo DPM (Registro dei trattamenti) con estrazione casuale di un campione di trattamenti (almeno il 5% rispetto al totale dei trattamenti e comunque verificando tutte le Direzioni della Giunta) generando un foglio Excel e procedendo nel seguente modo: dall'applicativo Microsoft Excel DATI/STATISTICHE/CAMPIONAMENTO.

La verifica, di cui al punto 1), verrà effettuata sulla base della check list di seguito proposta:

Checklist Audit 2022. Applicativi mobili di Regione Piemonte (App)

Verifica della conformità del rispetto della normativa privacy (Regolamento UE 2016/679) delle Applicazioni Mobili (App) di Titolarità della Giunta regionale.

DESCRIZIONE APP:

DOMANDE	SI	NO	NON APPLICABILE	NOTE
1) Sono individuate le finalità del trattamento?				
2) E' individuata la base giuridica che legittima il trattamento?				
3) Sono indicati i riferimenti normativi e legittimi interessi?				
4) E' indicata l'origine dei dati?				
5) E' indicato il tipo di banca dati?				
6) Sono indicate le categorie di dati oggetto del trattamento?				
7) Sono indicate le categorie di interessati oggetto del trattamento?				
8) E' indicato il Titolare del trattamento?				
9) E' indicato, se previsto, un responsabile del trattamento ex articolo 28 del GDPR?				
10) E' un trattamento comunicato ad altri Titolari?				
11) E' un trattamento che comporta trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale?				
12) Le misure di sicurezza sono indicate?				
13) E' indicato il periodo di conservazione dei dati?				
14) E' un trattamento che prevede *"un rischio elevato per i diritti e le libertà delle persone"?*				
15) Se la risposta al quesito 14 è SI, la valutazione d'impatto di cui all'articolo 35 del GDPR è stata				

effettuata?				

Eventuali osservazioni/criticità.

L’attività di verifica si concluderà con il verbale di controllo che darà conto degli esiti