CONSIGLIO REGIONALE DEL PIEMONTE - Deliberazione dell'Ufficio di Presidenza
Deliberazione 22 luglio 2026, n. 265
ADOZIONE DEL PIANO TRIENNALE DI AUDIT PRIVACY 2026-2028. (SS/FD'A)

Documento allegato

CONSIGLIO REGIONALE DEL PIEMONTE

Ufficio di Presidenza

Delibera n. 265/2026 - Cl. 6.4.2

Oggetto ADOZIONE DEL PIANO TRIENNALE DI AUDIT PRIVACY 2026-2028. (SS/FD'A)

Seduta n. 32

L'anno 2026, il giorno 22 luglio alle ore 13.45 - presso la sede di Palazzo Lascaris, via Alfieri n. 15, Torino - si è riunito l'Ufficio di Presidenza del Consiglio Regionale.

Sono presenti: *il Presidente NICCO, il Vice Presidente RAVETTI, i Consiglieri Segretari CAROSSO, CERA.*

Non sono presenti: *il Vice Presidente GRAGLIA, il Consigliere Segretario CASTELLO.*

A relazione del Presidente NICCO

ADOZIONE DEL PIANO TRIENNALE DI AUDIT PRIVACY 2026-2028. (SS/FD'A)

Premesso che il quadro normativo in materia di protezione dei dati personali è costituito:
dal regolamento UE 2016/679 (GDPR-General Data Protection Regulation), di seguito regolamento UE 2016/679, in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione degli stessi, approvato dal Parlamento europeo e dal Consiglio europeo in data 27 aprile 2016, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016 che, dopo un periodo di transizione di due anni, è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio

2018;

dal decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), adeguato alle disposizioni di cui al Regolamento UE con 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";

considerato che il regolamento UE:

è stato istituito per tutelare i diritti e le libertà fondamentali delle persone fisiche, attraverso un'applicazione uniforme e omogenea delle norme sulla protezione dei dati personali con regole equivalenti a livello europeo (Considerando 10), e offre un quadro di riferimento aggiornato e basato sul principio di responsabilizzazione (c.d. principio di accountability) con particolare riferimento agli articoli:
5, par. 2, secondo il quale il Titolare è responsabile del rispetto dei principi applicabili al trattamento, enunciati al par. 1, e deve essere in grado di comprovarlo;
24, che richiede al Titolare di mettere in atto misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare che il trattamento sia attuato conformemente al regolamento UE;
impone un cambiamento culturale nell'approccio al modello di gestione della privacy, che richiede un ripensamento delle misure di sicurezza da adottarsi nelle amministrazioni, le quali 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;

rilevato che l'audit privacy è lo strumento di controllo a disposizione del Titolare del trattamento per dimostrare la conformità dell'azione dell'amministrazione alla disciplina sul trattamento dei dati personali;

richiamata la deliberazione 23 luglio 2025, n. 189 "Adempimenti regolamento UE n. 679/2016 'regolamento generale sulla protezione dei dati personali'", con la quale l'Ufficio di Presidenza:
- ha dato atto che, ai sensi dell'articolo 4, par. 1, punto 7, del Regolamento UE, il Consiglio regionale del Piemonte, rappresentato ai fini previsti dello stesso dall'Ufficio di Presidenza, è il Titolare di tutti i trattamenti posti in essere ai fini dello svolgimento delle competenze attribuite dallo Statuto, dal Regolamento interno e dalla normativa regionale;
- ha provveduto a modificare e rafforzare la governance relativa alla protezione dei dati, con l'approvazione della nuova versione del registro delle attività di trattamento del Titolare;
- ha aggiornato il sistema di gestione della funzione inerente alla protezione dei dati personali, integrando e modificando quanto previsto originariamente dalla deliberazione n. 113/2018;

- ha confermato la nomina del responsabile della protezione dei dati personali (di seguito RPD), attribuendogli i compiti previsti dall'articolo 39 del GDPR e fornendogli le garanzie dell'articolo 38;

- ha disposto, al fine di garantire la corretta osservanza degli obblighi discendenti dal regolamento UE e dalla normativa nazionale, la costituzione di un organismo tecnico stabile, denominato "Gruppo dei referenti privacy", preposto allo svolgimento di compiti operativi di analisi, implementazione, gestione, approfondimento e soluzione delle problematiche applicative della normativa in materia di privacy;

richiamata, inoltre, la deliberazione dell'Ufficio di Presidenza del 22 luglio 2026, n. 264 con la quale è stata data attuazione alla deliberazione dell'Ufficio di Presidenza n. 189 del 23 luglio 2025, con l'approvazione del registro delle attività di trattamento nella versione risultante dalle attività svolte nel corso dell'anno dai delegati del trattamento, nonché si è provveduto ad approvare lo schema di informativa, ai sensi degli articoli 13 e 14 del Regolamento UE 679/2016, e a ridefinire la composizione, i compiti e il funzionamento del Gruppo dei referenti privacy;

dato atto che il Responsabile della protezione dei dati, ai sensi dell'articolo 39, paragrafo 1, lettera b) del Regolamento (UE) 2016/679, esercita funzioni di sorveglianza sull'osservanza della normativa e delle politiche interne in materia di protezione dei dati personali, operando in piena indipendenza e senza assumere compiti o responsabilità operative;

considerato che il sistema di audit privacy si colloca su un piano distinto rispetto alle attività di sorveglianza attribuite al Responsabile della protezione dei dati e non comporta l' attribuzione allo stesso di responsabilità operative o gestionali nell'ambito delle attività di verifica;

rilevato altresì che gli esiti delle attività di audit possono essere utilizzati dal Responsabile della protezione dei dati, unitamente agli ulteriori elementi acquisiti nell'esercizio delle proprie funzioni, quale base informativa per le attività di analisi, monitoraggio e sorveglianza di cui all'articolo 39 del Regolamento (UE) 2016/679, ferma restando l'autonomia di valutazione dello stesso e la possibilità di formulare osservazioni, raccomandazioni e richieste di approfondimento da rappresentare mediante le relazioni periodiche previste dalla deliberazione dell'Ufficio di Presidenza 23 luglio 2025, n. 189;

considerato opportuno procedere alla formalizzazione di un sistema strutturato di audit privacy, tenuto conto delle risultanze e delle esigenze di sviluppo della funzione progressivamente

emerse nell’ambito delle attività di monitoraggio e sorveglianza previste dall’articolo 39 del Regolamento (UE) 2016/679, al fine di conferire maggiore organicità, sistematicità e documentabilità alle attività di verifica e monitoraggio, nonché di rendere più esplicita l'attuazione del principio di responsabilizzazione (accountability) del Titolare;

preso atto che le attività di audit possono articolarsi su più livelli, in funzione dei soggetti coinvolti e delle finalità di controllo. In particolare, l’audit di prima parte costituisce il primo livello di verifica ed è svolto da professionalità interne all’Ente, per valutare e documentare il grado di conformità dei trattamenti di dati personali alla normativa privacy; l’audit di seconda parte che attiene alle verifiche sui fornitori di beni o servizi per la PA, per garantire la qualità e il rispetto dei contratti; mentre l’audit di terza parte è svolto da enti indipendenti esterni al fine dell’ ottenimento della certificazione;

rilevata la necessità di procedere alla verifica degli aspetti di prima e di seconda parte, al fine di assicurare un adeguato livello di conformità alla normativa in materia di protezione dei dati personali;

considerato che tali attività sono finalizzate a contribuire al miglioramento della governance della funzione inerente la protezione dei dati personali e al rafforzamento dell’effettiva attuazione del principio di responsabilizzazione (accountability), nonché a favorire l’individuazione di eventuali criticità, aree di miglioramento e possibili interventi correttivi o organizzativi;

ritenuto opportuno, anche alla luce dell’attuale fase di aggiornamento e revisione del sistema inerente la protezione dei dati personali del Consiglio regionale, nonché al fine di disporre di un quadro conoscitivo organico e aggiornato e di rafforzarne il monitoraggio nel tempo, prevedere lo svolgimento di una fase di verifica sistematica dei trattamenti rispetto ai requisiti normativi applicabili, finalizzata alla definizione di un quadro di riferimento del sistema inerente la protezione dei dati personali, utile per la valutazione del livello di conformità alla normativa in materia di protezione dei dati personali e per il monitoraggio nel tempo delle misure adottate, anche con riguardo ai rapporti con i fornitori;

valutato, valutato, di conseguenza, di prevedere che, per l’anno 2026, le attività di audit assumono carattere di prima attuazione del sistema e non configurano un ciclo completo di programmazione annuale, che sarà definito a decorrere dall’anno 2027 mediante l’adozione del primo Programma annuale di audit, quale strumento attuativo del Piano triennale di audit privacy;

precisato che il Piano triennale di audit privacy definisce la cornice generale del sistema, gli indirizzi, gli obiettivi, gli ambiti di controllo e il modello organizzativo delle attività di audit, mentre i Programmi annuali individuano, in modo puntuale, le attività di verifica da svolgere, le priorità di intervento, i processi e gli ambiti da sottoporre a controllo, nonché le modalità operative e gli eventuali strumenti metodologici utilizzati;

ritenuto di prevedere che le attività di audit siano organizzate e svolte secondo quanto disciplinato dal Piano triennale di audit privacy 2026-2028 di cui all'Allegato A, parte integrante e sostanziale della presente deliberazione, in ordine al modello organizzativo, ai criteri, ai soggetti coinvolti e alle modalità operative;

ritenuto, altresì, che le verifiche devono essere condotte nel rispetto del principio di separazione tra funzioni di gestione e funzioni di controllo, con esclusione della partecipazione di soggetti direttamente coinvolti nei trattamenti oggetto di audit, assicurando, pertanto, la separazione tra funzioni di gestione e funzioni di verifica;

ritenuto opportuno precisare che gli ambiti di controllo individuati nel presente Piano (Allegato A) hanno natura programmatoria e possono essere oggetto di rimodulazione, integrazione o aggiornamento nel corso del periodo di riferimento, laddove ciò si renda necessario in relazione a sopravvenute esigenze organizzative, normative o operative, ovvero alle specifiche caratteristiche dei processi e delle attività da sottoporre a verifica, al fine di garantire efficacia, flessibilità e adeguatezza dell'attività di audit;

valutato di demandare al Direttore della Direzione Amministrazione, Personale, Sistemi Informativi e Organismi di Garanzia l'adozione del Programma annuale di audit entro il 31 marzo di ciascun anno, in ragione delle competenze organizzative e gestionali attribuite alla medesima Direzione e della necessità di assicurare il coordinamento delle risorse coinvolte nell' attuazione del presente Piano (**Allegato A)**, fermo restando il coinvolgimento dei delegati competenti per i trattamenti oggetto di verifica e la responsabilità degli stessi in ordine all'attuazione delle eventuali azioni correttive;

ritenuto opportuno che, a decorrere dall'attuazione dei Programmi annuali di audit, le risultanze delle attività svolte siano adeguatamente formalizzate e rese disponibili all'Ufficio di Presidenza, in qualità di Titolare del trattamento, ai fini delle valutazioni e delle eventuali determinazioni di competenza in ordine alle eventuali criticità riscontrate, alle aree di

miglioramento e ai possibili interventi correttivi o organizzativi, ferma restando la necessità di portare all'attenzione del Titolare eventuali criticità di particolare rilievo emerse anche nella fase di prima attuazione del sistema;

precisato che le strutture competenti per i trattamenti di dati personali, nell'ambito delle rispettive responsabilità, assicurano il presidio e il controllo continuo dei trattamenti di propria competenza, nell'ambito della gestione ordinaria, attraverso l' attuazione delle misure organizzative e di sicurezza e la verifica della loro applicazione, attività che si collocano su un piano distinto sia dalle verifiche sui responsabili del trattamento sia dalle attività di audit del Titolare;

richiamato che le verifiche (in sede di autocontrollo) sui responsabili del trattamento di cui all'articolo 28 del Regolamento (UE) 2016/679 sono svolte dalle strutture competenti, in attuazione delle responsabilità del Titolare del trattamento, per i trattamenti di dati personali nell'ambito delle attività di gestione e controllo dei rapporti contrattuali e che le medesime verifiche non esauriscono le attività di audit del Titolare, che possono essere svolte su tali ambiti mediante i soggetti incaricati, secondo quanto previsto dal presente Piano (**Allegato A**);

ritenuto, pertanto, opportuno approvare il Piano triennale di audit privacy per gli anni 2026, 2027 e 2028, di cui all'**Allegato A,** che costituisce parte integrante e sostanziale della presente deliberazione, e stabilire che le attività di audit privacy interessano tutte le Direzioni e i Settori con riferimento ai trattamenti di dati personali di rispettiva competenza, fermo restando che le verifiche specialistiche inerenti i profili tecnici di sicurezza informatica sono svolte dalla Direzione responsabile dei sistemi informativi;

considerato, infine, di disporre la riservatezza dell'**Allegato A**, ritenendo che la sua diffusione possa esporre il Consiglio regionale a un rischio di elusione del proprio sistema di sicurezza;

L'Ufficio di Presidenza, all'***unanimità dei presenti***,

D E L I B E R A

1. di dare atto che le premesse costituiscono parte integrante e sostanziale della presente deliberazione;

2. di approvare il Piano triennale di audit privacy per gli anni 2026, 2027 e 2028, di cui all'**Allegato A**, che costituisce parte integrante e sostanziale della presente deliberazione;

3. di stabilire che le attività di audit privacy interessano tutte le Direzioni e i Settori con riferimento ai trattamenti di dati personali di rispettiva competenza, fermo restando che le verifiche specialistiche inerenti i profili tecnici di sicurezza informatica sono svolte dalla Direzione responsabile dei sistemi informativi;

4. di dare atto che le attività di audit sono organizzate e svolte secondo quanto previsto dal Piano triennale di audit privacy 2026-2028 (**Allegato A**) in ordine al modello organizzativo, ai criteri, ai soggetti coinvolti e alle modalità operative, nel rispetto del principio di separazione tra funzioni di gestione e funzioni di verifica;

5. di stabilire che, per l'anno 2026, le attività di audit assumono carattere di prima attuazione del sistema e non configurano un ciclo completo di programmazione annuale, che sarà definito a decorrere dall'anno 2027 mediante l'adozione del primo Programma annuale di audit;

6. di stabilire che, a decorrere dall'attuazione dei Programmi annuali di audit, le risultanze delle attività svolte siano formalizzate e rese disponibili all'Ufficio di Presidenza, in qualità di Titolare del trattamento, secondo quanto previsto dal Piano triennale di audit privacy 2026-2028 (**Allegato A**), ferma restando la necessità di portare alla sua attenzione eventuali criticità di particolare rilievo;

7. di demandare al Direttore della Direzione Amministrazione, Personale, Sistemi Informativi e Organismi di Garanzia l'adozione del Programma annuale di audit entro il 31 marzo di ciascun anno, in ragione delle competenze organizzative e gestionali attribuite alla medesima Direzione e della necessità di assicurare il coordinamento delle risorse coinvolte nell'attuazione del Piano triennale di audit privacy 2026-2028 (**Allegato A**), fermo restando il coinvolgimento dei delegati competenti per i trattamenti oggetto di verifica e la responsabilità degli stessi in ordine all'attuazione delle eventuali azioni correttive;

8. di disporre la riservatezza dell'**Allegato A**.