Politica per la protezione e il trattamento dei dati personali

ID documento: RPS_701_PO_Politica per la protezione e il trattamento dei dati personali_101

Versione: 01

Data di rilascio: 28/01/2026

Custode delle politiche: Sistemi Informativi e Qualità

Area di Applicazione: ISO/IEC 27701:2019, ISO/IEC 27001, 27017, 27018 – ISO 9001

Recensito e verificato da: RGSI

Approvato da: CEO

Classificazione: Pubblico

Revisioni

Ver.	Descrizione modifiche	Data	Responsabile
01	Prima emissione	28/01/2026	RGSI e PS

Indice

1. Scopo

La presente Politica definisce i principi, gli impegni e il modello di governance adottati da React Consulting S.r.l. per garantire la protezione e il trattamento lecito, corretto e trasparente dei dati personali, in conformità alla normativa applicabile in materia di protezione dei dati personali e ai requisiti della norma ISO/IEC 27701:2019.

La Politica costituisce il documento di riferimento di alto livello del Privacy Information Management System (PIMS) dell'Organizzazione e stabilisce il quadro generale entro il quale sono definiti, attuati e mantenuti i controlli e le misure di protezione dei dati personali.

Il PIMS è integrato e coerente con i seguenti sistemi di gestione adottati dall'Organizzazione:

- il Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) certificato secondo la norma ISO/IEC 27001, incluse le estensioni ISO/IEC 27017 e ISO/IEC 27018;
- il Sistema di Gestione per la Qualità conforme alla norma ISO 9001.

2. Campo di applicazione

La presente Politica si applica a React Consulting S.r.l., società consorziata del Consorzio Activa Digital S.c.a.r.l., con sede in Via Alessandro Severo, 52 – 00145 Roma (RM), e copre tutti i trattamenti di dati personali effettuati dall'Organizzazione.

In particolare, la Politica si applica:

- a tutti i trattamenti di dati personali svolti da React Consulting S.r.l.:
  - in qualità di Titolare del trattamento;
  - in qualità di Responsabile del trattamento, per conto dei propri clienti;
- a tutti i dipendenti, collaboratori, consulenti e soggetti terzi che operano sotto l'autorità dell'Organizzazione o per suo conto;
- a tutti i sistemi informativi, servizi, applicazioni e infrastrutture utilizzati per il trattamento dei dati personali, inclusi gli ambienti on-premise, cloud e hybrid cloud.

Il campo di applicazione del Privacy Information Management System (PIMS) è coerente e integrato con l'ambito di applicazione dei sistemi di gestione aziendali e comprende le seguenti attività:

Progettazione, sviluppo, conduzione e manutenzione di software e sistemi IT e ICT. Progettazione, sviluppo, conduzione, manutenzione ed erogazione di servizi sia on premise che in cloud e hybrid cloud con l'applicazione delle linee guida ISO/IEC 27017:2015, ISO/IEC 27018:2019 e 27701:2019. Attività di primo e secondo livello di Service Desk in ambito ICT.

3. Norme di riferimento

La presente Politica è redatta in conformità ai seguenti riferimenti normativi, legislativi e regolamentari, nonché alle norme tecniche applicabili in materia di protezione dei dati personali e sicurezza delle informazioni:

Normativa in materia di protezione dei dati personali

- **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 (Regolamento generale sulla protezione dei dati – GDPR);
- **Decreto Legislativo 30 giugno 2003**, n. 196, recante il Codice in materia di protezione dei dati personali, come modificato e integrato dal Decreto Legislativo 10 agosto 2018, n. 101;
- **Provvedimenti, Linee guida**, Raccomandazioni e Pareri adottati dall'Autorità Garante per la protezione dei dati personali, dal Comitato Europeo per la Protezione dei Dati (EDPB) e da altre autorità competenti, ove applicabili.

Norme e standard internazionali

- **ISO/IEC 27701:2019** – Tecniche di sicurezza – Estensione alla ISO/IEC 27001 e alla ISO/IEC 27002 per la gestione delle informazioni sulla privacy;
- **ISO/IEC 27001** – Sistemi di gestione per la sicurezza delle informazioni – Requisiti;

- **ISO/IEC 27002** – Controlli per la sicurezza delle informazioni;
- **ISO/IEC 27017:2015** – Codice di condotta per i controlli di sicurezza delle informazioni basato sulla ISO/IEC 27002 per i servizi cloud;
- **ISO/IEC 27018:2019** – Protezione delle informazioni personali identificabili (PII) nei cloud pubblici che operano in qualità di responsabili del trattamento;
- **ISO 9001** – Sistemi di gestione per la qualità – Requisiti.

Ulteriore normativa applicabile

- ulteriori disposizioni normative nazionali e internazionali applicabili in relazione alle attività svolte e ai contesti operativi dell'Organizzazione;
- obblighi di natura contrattuale assunti nei confronti di clienti, partner e fornitori, ove rilevanti ai fini della protezione dei dati personali.

4. Ruoli e Responsabilità

La governance del Privacy Information Management System (PIMS) di React Consulting S.r.l. è definita al fine di garantire una chiara attribuzione di ruoli, responsabilità e autorità in materia di protezione dei dati personali.

In particolare, sono individuati i seguenti ruoli:

Direzione

La Direzione è responsabile in ultima istanza dell'efficacia del PIMS e del suo allineamento agli obiettivi strategici dell'Organizzazione.

In particolare:

- approva la presente Politica e le politiche correlate;
- assicura la disponibilità delle risorse necessarie;
- effettua il riesame periodico del PIMS e ne promuove il miglioramento continuo.

Responsabile della Sicurezza (SEC – System, Privacy, Environment & Compliance).

Il ruolo di Responsabile SEC è ricoperto da Francesco D'Arrigo.

Il Responsabile SEC supporta la Direzione nel coordinamento e nell'integrazione dei sistemi di gestione (ISMS, PIMS e altri sistemi applicabili) e contribuisce alla definizione, attuazione e monitoraggio delle misure di sicurezza e di conformità in materia di protezione dei dati personali.

Responsabile della Protezione dei Dati (DPO) – esterno

Il DPO esterno svolge i compiti previsti dalla normativa applicabile in materia di protezione dei dati personali, operando in piena indipendenza.

In particolare:

- fornisce consulenza all'Organizzazione in merito agli obblighi normativi;
- sorveglia l'osservanza della normativa e delle politiche interne;
- coopera con l'Autorità di controllo e funge da punto di contatto.

Ufficio Privacy interno

L'Ufficio Privacy interno è responsabile della gestione operativa del PIMS e del supporto all'attuazione delle politiche e delle procedure in materia di protezione dei dati personali.

In particolare:

- coordina le attività operative di privacy;
- supporta la gestione dei diritti degli interessati, delle violazioni di dati personali e delle valutazioni dei rischi privacy;
- collabora con il DPO e con le funzioni aziendali coinvolte.

Responsabili di processo e di servizio

I Responsabili di processo e di servizio assicurano l'applicazione dei requisiti di protezione dei dati personali nei rispettivi ambiti di competenza, garantendo che i trattamenti siano svolti in conformità alla presente Politica e alle procedure aziendali applicabili.

Personale, collaboratori e terze parti

Tutto il personale, i collaboratori e i soggetti terzi che operano sotto l'autorità dell'Organizzazione sono tenuti a:

- rispettare la presente Politica e le procedure collegate;
- operare in conformità alle istruzioni ricevute e agli obblighi di riservatezza;
- partecipare alle attività di formazione e sensibilizzazione previste.

5. Contesto organizzativo e servizi

React Consulting S.r.l. opera nel settore dei servizi IT e di consulenza specialistica, fornendo soluzioni tecnologiche avanzate a clienti prevalentemente B2B. Le principali attività dell'Organizzazione includono:

- infrastrutture virtuali e servizi di cloud enabling;
- sviluppo e gestione di soluzioni CRM;
- servizi di Network Operations Center (NOC);
- consulenza IT specialistica;
- data **analytics e soluzioni di intelligenza artificiale.**

Nell'ambito delle proprie attività, React Consulting S.r.l. tratta diverse categorie di dati personali, tra cui:

- dati personali dei dipendenti e collaboratori;
- dati personali di clienti B2B;
- dati personali degli utenti finali dei clienti;
- log tecnici e dati di monitoraggio contenenti dati personali;
- dati di contatto commerciali;
- categorie particolari di dati personali, trattate esclusivamente in casi eccezionali, sulla base di idonee condizioni di liceità e mediante l'adozione di misure tecniche e organizzative rafforzate.

I trattamenti di dati personali sono effettuati esclusivamente all'interno dell'Unione Europea.

Per l'erogazione di alcuni servizi, React Consulting S.r.l. si avvale di sub-responsabili del trattamento qualificati, in particolare Microsoft (Azure) e IBM, selezionati e valutati in conformità ai requisiti di sicurezza delle informazioni e di protezione dei dati personali applicabili.

Con tali fornitori sono sottoscritti e applicati accordi contrattuali e misure di garanzia adeguate, incluse, ove applicabili, le Clausole Contrattuali Standard (Standard Contractual Clauses – SCC) e il Data Privacy Framework (DPF).

6. Principi per la protezione dei dati personali

React Consulting S.r.l. riconosce la protezione dei dati personali come un elemento fondamentale della propria responsabilità sociale, della fiducia dei clienti e della qualità dei servizi erogati. L'Organizzazione si impegna a promuovere una cultura aziendale orientata alla tutela della privacy, assicurando che i principi di protezione dei dati personali siano integrati in modo sistematico nei processi decisionali, operativi e tecnologici.

In tale contesto, React Consulting S.r.l. assicura che il trattamento dei dati personali avvenga nel rispetto dei principi stabiliti dalla normativa applicabile e dalla norma ISO/IEC 27701:2019, in particolare:

- **Liceità, correttezza e trasparenza:** i dati personali sono trattati in modo lecito, corretto e trasparente nei confronti degli interessati, fornendo informazioni chiare e comprensibili sulle modalità e finalità del trattamento;
- **Limitazione delle finalità:** i dati personali sono raccolti per finalità determinate, esplicite e legittime e non sono ulteriormente trattati in modo incompatibile con tali finalità;
- **Minimizzazione dei dati:** l'Organizzazione adotta misure volte a limitare la raccolta e il trattamento dei dati personali a quanto strettamente necessario rispetto alle finalità perseguite;
- **Esattezza:** React Consulting S.r.l. adotta misure ragionevoli per garantire che i dati personali siano accurati, completi e, ove necessario, aggiornati;
- **Limitazione della conservazione:** i dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un periodo di tempo non superiore a quello necessario al conseguimento delle finalità del trattamento;
- **Integrità e riservatezza:** i dati personali sono trattati garantendo un livello di sicurezza adeguato al rischio, attraverso l'adozione di misure tecniche e organizzative idonee a prevenire accessi non autorizzati, perdite, distruzioni o divulgazioni indebite;
- **Responsabilizzazione (accountability):** l'Organizzazione è in grado di dimostrare la conformità ai principi applicabili mediante l'adozione, l'attuazione e il mantenimento di politiche, procedure, controlli e registrazioni adeguate**.**

React Consulting S.r.l. si impegna inoltre a:

- promuovere la protezione dei dati fin dalla progettazione e per impostazione predefinita (privacy by design e by default) nello sviluppo di servizi, sistemi e soluzioni tecnologiche;
- garantire un'adeguata formazione e consapevolezza del personale e dei soggetti che operano sotto la propria autorità in materia di protezione dei dati personali;
- assicurare il coinvolgimento della Direzione nel definire, sostenere e migliorare continuamente il Privacy Information Management System (PIMS);
- perseguire il miglioramento continuo delle misure di protezione dei dati personali, anche attraverso il monitoraggio, la valutazione dei rischi e l'adeguamento alle evoluzioni normative, tecnologiche e organizzative.

7. Formazione e consapevolezza

L'Organizzazione assicura che il personale e i soggetti che operano sotto la propria autorità ricevano una formazione periodica in materia di protezione dei dati personali e sicurezza delle informazioni, proporzionata al ruolo, alle responsabilità e al livello di accesso ai dati.

La formazione di base è erogata tramite la piattaforma di formazione aziendale, è obbligatoria per tutti i dipendenti e deve essere svolta almeno una volta all'anno.

I percorsi formativi includono:

- una formazione di base sulla conformità al Regolamento (UE) 2016/679 (GDPR) e sui principi di protezione dei dati personali;
- una sezione dedicata alla sicurezza delle informazioni, basata sui requisiti e sui controlli dello standard ISO/IEC 27001:2022, con particolare riferimento alle buone pratiche di sicurezza di base.

L'Organizzazione assicura che le attività di formazione siano documentate e tracciate e siano oggetto di aggiornamento periodico, anche in funzione di evoluzioni normative, tecnologiche o organizzative, al fine di promuovere un adeguato livello di consapevolezza in materia di protezione dei dati personali e sicurezza delle informazioni.

8. Sicurezza delle informazioni e protezione dei dati personali

Le misure tecniche e organizzative adottate per la protezione dei dati personali sono definite sulla base di un approccio basato sul rischio e sono integrate nel Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) dell'Organizzazione, in conformità ai requisiti delle norme ISO/IEC 27001 e ISO/IEC 27701:2019.

Tali misure sono finalizzate a garantire un livello di sicurezza adeguato ai rischi per i diritti e le libertà delle persone fisiche e includono, tra l'altro:

- controllo degli accessi ai sistemi e ai dati, nonché segregazione dei ruoli e delle responsabilità;
- cifratura dei dati personali e ulteriori misure di protezione dei dati in transito e a riposo;
- registrazione degli eventi (logging) e attività di monitoraggio volte a individuare anomalie, accessi non autorizzati o incidenti di sicurezza;
- gestione degli incidenti di sicurezza delle informazioni, inclusa l'identificazione, l'analisi, il contenimento e la risposta agli incidenti che coinvolgono dati personali;
- sicurezza degli ambienti cloud, applicata in conformità alle linee guida delle norme ISO/IEC 27017:2015 e ISO/IEC 27018:2019.

Le misure di sicurezza sono oggetto di riesame periodico e di miglioramento continuo, tenendo conto dell'evoluzione dei rischi, delle tecnologie utilizzate, del contesto operativo e delle eventuali modifiche normative.

9. Documentazione a supporto e trasparenza

La Società adotta e mantiene una documentazione a supporto del Privacy Information Management System (PIMS) al fine di garantire la trasparenza, la tracciabilità e la dimostrabilità della conformità ai requisiti applicabili in materia di protezione dei dati personali.

La messa a disposizione della documentazione privacy al personale dell'Organizzazione costituisce uno strumento essenziale per la condivisione dei principi di protezione dei dati personali, per la diffusione della cultura della privacy e per il supporto all'applicazione coerente delle politiche e delle procedure aziendali.

In particolare:

- le informative privacy sono utilizzate quale strumento di trasparenza nei confronti degli interessati, al fine di fornire informazioni chiare e comprensibili sulle modalità e sulle finalità del trattamento dei dati personali;
- le informative e la restante documentazione privacy sono rese disponibili nella loro versione più aggiornata attraverso l'intranet aziendale, nella sezione dedicata "Privacy & Procedure", e sono consultabili da tutti i dipendenti;

- l'Organizzazione promuove attività di formazione e sensibilizzazione in materia di protezione dei dati personali, finalizzate a garantire che il personale e i soggetti che operano sotto la propria autorità comprendano e applichino correttamente i principi e le regole stabilite.

La documentazione in materia di protezione dei dati personali è soggetta a controllo delle versioni, riesame periodico e aggiornamento, in funzione di modifiche normative, organizzative, tecnologiche o operative rilevanti.

10. Diritti degli interessati

React Consulting S.r.l. riconosce e garantisce l'esercizio dei diritti degli interessati in conformità al Regolamento (UE) 2016/679 (GDPR), in particolare agli articoli da 12 a 22, nonché alle ulteriori disposizioni applicabili della normativa europea e nazionale in materia di protezione dei dati personali.

L'Organizzazione assicura che la gestione dei diritti degli interessati sia parte integrante del Privacy Information Management System (PIMS) e contribuisca alla dimostrabilità della conformità e alla tutela dei diritti e delle libertà fondamentali degli interessati.

10.1 Principi generali

L'Organizzazione assicura che l'esercizio dei diritti degli interessati avvenga nel rispetto dei seguenti principi:

- **trasparenza, correttezza e intelligibilità**, ai sensi dell'art. 12 del GDPR;
- **tempestività** e rispetto dei termini previsti dalla normativa applicabile;
- **gratuità**, salvo i casi espressamente previsti dalla normativa;
- **sicurezza e riservatezza**, incluse adeguate misure di verifica dell'identità del richiedente, proporzionate al rischio.

Le informazioni e le comunicazioni agli interessati sono fornite in forma chiara, semplice e accessibile, utilizzando un linguaggio comprensibile e, ove appropriato, mediante strumenti elettronici.

10.2 Diritti garantiti

React Consulting S.r.l. garantisce agli interessati l'esercizio dei seguenti diritti, nei limiti e secondo le modalità previste dalla normativa applicabile:

- **diritto di accesso** ai dati personali (art. 15 GDPR);
- **diritto di rettifica** dei dati inesatti o incompleti (art. 16 GDPR);
- **diritto alla cancellazione** dei dati personali ("diritto all'oblio"), nei casi previsti (art. 17 GDPR);
- **diritto di limitazione del trattamento** (art. 18 GDPR);
- **diritto alla portabilità dei dati**, ove applicabile (art. 20 GDPR);
- **diritto di opposizione** al trattamento, nei casi previsti dalla legge (art. 21 GDPR);
- **diritto a non essere sottoposti a decisioni basate unicamente su trattamenti automatizzati**, inclusa la profilazione, ove applicabile (art. 22 GDPR).

10.3 Modalità di esercizio dei diritti

Gli interessati possono esercitare i propri diritti attraverso i canali messi a disposizione dall'Organizzazione, indicati nelle informative privacy e nella documentazione a supporto del PIMS.

In particolare, le richieste possono essere presentate rivolgendosi al Responsabile della Protezione dei Dati (DPO) ai seguenti recapiti:

- **Responsabile della Protezione dei Dati (DPO)**: Riccardo Logozzo, dpo@activadigital.it;
- **Indirizzo email**: privacy@activadigital.it;
- **Indirizzo postale**: Via Alessandro Severo 52 – 00145 Roma (RM).

L'Organizzazione:

- registra ogni richiesta ricevuta;
- verifica l'identità del richiedente, adottando misure proporzionate al rischio e alla natura dei dati trattati;
- valuta l'ammissibilità della richiesta in conformità alla normativa applicabile;
- prende in carico le richieste senza ingiustificato ritardo e fornisce riscontro entro 30 giorni dal ricevimento.

Qualora, tenuto conto della complessità e del numero delle richieste, sia necessario un prolungamento dei termini, il periodo di risposta può essere esteso fino a ulteriori 60 giorni, ai sensi dell'art. 12, par. 3 del GDPR. In tali casi, l'Interessato è informato tempestivamente dell'estensione dei termini e delle relative motivazioni.

Nel caso in cui una richiesta non possa essere accolta, in tutto o in parte, l'Organizzazione fornisce all'Interessato una risposta motivata, indicando le ragioni del mancato accoglimento e informandolo della possibilità di:

- proporre reclamo all'Autorità di controllo competente;
- esercitare i rimedi giurisdizionali previsti dalla normativa vigente.

10.4 Ruolo di Titolare e di Responsabile del trattamento

Quando React Consulting S.r.l. opera in qualità di Titolare del trattamento, gestisce direttamente le richieste degli interessati e ne assicura l'evasione nei termini e secondo le modalità previste dalla normativa applicabile.

Quando opera in qualità di Responsabile del trattamento, l'Organizzazione:

- supporta il **Titolare del trattamento cliente** nell'adempimento degli obblighi relativi ai diritti degli interessati, ai sensi dell'art. 28, par. 3, lett. e) del GDPR;
- **trasmette tempestivamente** al Titolare le richieste ricevute, secondo quanto previsto dagli accordi contrattuali e dalle istruzioni documentate;
- **non agisce direttamente** sulle richieste degli interessati, salvo diversa autorizzazione del Titolare o obblighi di legge.

10.5 Limitazioni ed eccezioni

L'esercizio dei diritti degli interessati può essere limitato o differito esclusivamente nei casi previsti dalla normativa applicabile, inclusi, a titolo esemplificativo:

- obblighi legali di conservazione dei dati;
- tutela dei diritti e delle libertà di terzi;
- esigenze di sicurezza delle informazioni o di prevenzione e repressione di reati.

Eventuali limitazioni sono adeguatamente motivate, documentate e comunicate agli interessati, ove previsto.

10.6 Documentazione e tracciabilità

Tutte le richieste degli interessati e le decisioni adottate in merito sono:

- documentate;
- tracciate;
- conservate come evidenza di conformità, responsabilizzazione (accountability) e corretta applicazione del PIMS.

11. Registro dei trattamenti

React Consulting S.r.l. mantiene un Registro dei Trattamenti dei dati personali, redatto e aggiornato in conformità alla normativa applicabile e ai requisiti della norma ISO/IEC 27701:2019, quale strumento fondamentale di accountability e di governo dei trattamenti.

Il Registro dei Trattamenti descrive, per ciascuna attività di trattamento:

- le finalità del trattamento e le relative basi giuridiche;
- le categorie di dati personali trattati e le categorie di interessati;
- il ruolo dell'Organizzazione nel trattamento (Titolare del trattamento o Responsabile del trattamento);
- i destinatari dei dati personali e gli eventuali sub-responsabili del trattamento;
- i tempi di conservazione o i criteri utilizzati per determinarli;
- le misure tecniche e organizzative di sicurezza applicate.

Il Registro dei Trattamenti è oggetto di riesame e aggiornamento periodico, nonché in occasione di modifiche significative ai trattamenti, ai servizi o al contesto normativo e organizzativo.

I fornitori che trattano dati personali per conto dell'Organizzazione sono selezionati, qualificati e monitorati sulla base di criteri di sicurezza delle informazioni, affidabilità, competenza e conformità alla normativa applicabile in materia di protezione dei dati personali.

Prima dell'instaurazione del rapporto contrattuale, l'Organizzazione valuta l'adeguatezza dei fornitori e dei sub-responsabili del trattamento in relazione alla natura dei trattamenti, ai rischi per i diritti e le libertà degli interessati e alle misure tecniche e organizzative adottate.

I rapporti con i Responsabili e sub-responsabili del trattamento sono regolati da accordi contrattuali o altri atti giuridici vincolanti che definiscono, in conformità all'art. 28 del GDPR:

- l'oggetto e la durata del trattamento;
- la natura e le finalità del trattamento;
- le tipologie di dati personali e le categorie di interessati;
- gli obblighi in materia di protezione dei dati personali e le misure di sicurezza da adottare;
- le condizioni per l'eventuale ricorso a ulteriori sub-responsabili.

L'Organizzazione assicura il monitoraggio periodico dei fornitori e dei sub-responsabili rilevanti, anche mediante attività di verifica e riesame, al fine di garantire il mantenimento nel tempo dei requisiti di sicurezza e di conformità.

12. Incidenti e violazioni dei dati personali

Eventi che possano compromettere la riservatezza, l'integrità o la disponibilità dei dati personali sono gestiti attraverso processi strutturati e formalizzati, integrati con il Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) e con il Privacy Information Management System (PIMS).

In particolare, l'Organizzazione adotta processi dedicati di:

- gestione degli incidenti di sicurezza delle informazioni (incident management);

- gestione delle violazioni dei dati personali (data breach management);
- valutazione degli obblighi di notifica all'Autorità di controllo e di comunicazione agli interessati, ai sensi degli articoli 33 e 34 del GDPR.

Tali processi sono disciplinati da procedure formalizzate e supportati da moduli e strumenti operativi dedicati, che consentono di:

- rilevare e segnalare tempestivamente incidenti e violazioni;
- analizzare l'evento e valutarne l'impatto sui dati personali e sui diritti e le libertà degli interessati;
- adottare le misure di contenimento e mitigazione appropriate;
- documentare le decisioni assunte e le azioni intraprese, a fini di tracciabilità e accountability.

Le procedure di gestione degli incidenti e dei data breach sono oggetto di riesame periodico e di aggiornamento, anche in funzione di cambiamenti normativi, tecnologici o organizzativi.

13. Gestione del rischio e Valutazione d'Impatto sulla Protezione dei Dati (DPIA)

I rischi per i diritti e le libertà degli interessati derivanti dal trattamento dei dati personali sono identificati, analizzati e valutati nell'ambito del sistema di gestione integrato, in coerenza con l'approccio basato sul rischio adottato dall'Organizzazione e con i requisiti della norma ISO/IEC 27701:2019.

La gestione dei rischi privacy è integrata con i processi di risk assessment del Sistema di Gestione per la Sicurezza delle Informazioni (ISMS) e tiene conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei trattamenti, nonché delle potenziali conseguenze per gli interessati.

In caso di nuovi trattamenti di dati personali o di modifiche significative ai trattamenti esistenti:

- è effettuata una valutazione del rischio privacy, al fine di individuare e mitigare i rischi potenziali;
- quando previsto dalla normativa applicabile, è condotta una Valutazione d'Impatto sulla Protezione dei Dati (Data Protection Impact Assessment – DPIA), ai sensi dell'art. 35 del GDPR.

Le attività di valutazione del rischio e di DPIA sono disciplinate da procedure dedicate, adeguatamente documentate e soggette a riesame periodico, anche in funzione dell'evoluzione dei trattamenti e del contesto operativo.

14. Monitoraggio, audit e miglioramento continuo

L'efficacia del Privacy Information Management System (PIMS) è monitorata in modo sistematico al fine di garantire il mantenimento della conformità ai requisiti normativi applicabili e alle norme di riferimento, nonché il miglioramento continuo delle misure di protezione dei dati personali.

In particolare, il monitoraggio del PIMS avviene attraverso:

- indicatori di performance e di conformità, definiti e riesaminati periodicamente;
- audit interni, condotti a intervalli pianificati per verificare l'adeguatezza e l'efficacia del sistema;
- riesame della Direzione, integrato con i sistemi di gestione esistenti, al fine di valutare l'andamento del PIMS, le opportunità di miglioramento e la necessità di eventuali adeguamenti.

Eventuali non conformità, osservazioni o aree di miglioramento emerse nell'ambito delle attività di monitoraggio, audit o riesame sono gestite secondo il principio del miglioramento continuo, attraverso l'adozione di azioni correttive e, ove necessario, azioni preventive, adeguatamente documentate e tracciate.