| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Inserire qui la denominazione dell'entità giuridica registrata | | | | | | | |
| Numero del documento:<br>P17 | | | | | Titolo del documento:<br>**Politica di protezione dei dati e della privacy** | | | | | | | |
| Versione:<br>1.0 | | Data di entrata in vigore:<br>01.01.2025 | | | Proprietario del documento: | | | | | | | |
| X | Politica | | Standard | | Procedura | | Modulo | | Registro | | Altro | |

| **Cronologia delle revisioni** | | | | |
|---|---|---|---|---|
| **Numero di revisione** | **Data di revisione** | **Modifiche** | **Riesaminato da** | **Proprietario del processo** |
| | | | | |
| | | | | |

| **Approvazioni** | | | |
|---|---|---|---|
| **Nome** | **Ruolo** | **Data** | **Firma** |
| | | | |
| | | | |

Allineata a norme e regolamenti

| Standard/Regolamento | Clausola/Articolo | Commento |
|---|---|---|
| ISO/IEC 27001:2022 | Clausole 5.1, 6.1.3, 8.1, 10 | Controlli generali, tecnici e di miglioramento continuo pertinenti alla protezione dei dati |
| ISO/IEC 27002:2022 | Controlli 5.34, 8.10, 8.11, 8.12 | Controlli relativi al trattamento dei dati personali identificabili, alla conservazione, cancellazione, anonimizzazione e ai diritti degli interessati |
| NIST SP 800-53 Rev.5 | AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23 | Requisiti in materia di governance, rischio, gestione degli accessi, logging, risposta alle violazioni e programma privacy |
| GDPR UE | Articoli 5, 6, 12–23, 25, 28, 30, 32–34; Considerando 78 | Requisiti fondamentali in materia di privacy, accountability, diritti degli interessati, richieste degli interessati, violazioni dei dati personali, protezione dei dati fin dalla progettazione e per impostazione predefinita |
| NIS2 UE | Articolo 21(2)(e), (f) | Controlli di sicurezza basati sul rischio per soggetti essenziali e importanti |
| DORA UE | Articoli 6(2)(d), 11(1)(c), 15(1), 17 | Governance, rischio di terze parti e requisiti di tempestività per il trattamento sicuro |
| COBIT 2019 | APO12, DSS01, DSS05, MEA | Gestione del rischio, operazioni sicure, monitoraggio della conformità |

## 1. Finalità

1.1 La presente politica stabilisce principi organizzativi vincolanti e requisiti tecnici per la protezione dei dati personali e l'applicazione della protezione dei dati fin dalla progettazione in tutti gli ambienti.

1.2 Formalizza le responsabilità dell'organizzazione ai sensi degli standard internazionali e dei quadri normativi applicabili, assicurando che i dati personali siano raccolti, trattati, conservati, condivisi e smaltiti in modo lecito, sicuro e trasparente.

1.3 La presente politica rafforza inoltre la conformità alle leggi e ai quadri normativi applicabili in materia di privacy, inclusi il Regolamento generale sulla protezione dei dati (GDPR) dell'UE, la Direttiva NIS2 dell'UE, il Regolamento DORA dell'UE, la ISO/IEC 27001:2022 e COBIT 2019.

## 2. Ambito di applicazione

**2.1 La presente politica si applica a tutte le unità organizzative, al personale e ai sistemi coinvolti nel trattamento dei dati personali, inclusi:**

2.1.1 dipendenti, collaboratori esterni, consulenti e fornitori di servizi terzi.

2.1.2 dati raccolti da fonti interne ed esterne nell'ambito di tutte le funzioni aziendali.

2.1.3 supporti fisici e digitali, inclusi servizi cloud, piattaforme SaaS, dispositivi mobili e documentazione cartacea.

2.1.4 tutti gli ambienti, inclusi sistemi di produzione, sviluppo, test e backup in cui possono essere presenti dati personali.

**2.2 Essa copre tutte le attività di trattamento disciplinate dalle leggi e dalle norme applicabili in materia di privacy, incluse, a titolo esemplificativo e non esaustivo:**

2.2.1 raccolta, archiviazione, utilizzo, trasmissione e smaltimento dei dati personali.

2.2.2 applicazione dei diritti degli interessati, documentazione della base giuridica, gestione del consenso.

2.2.3 trasferimenti transfrontalieri, notifica delle violazioni e condivisione dei dati con terze parti.

2.2.4 progettazione sicura e applicazione della protezione dei dati per impostazione predefinita nei sistemi e nei processi.

## 3. Obiettivi

3.1 Garantire il trattamento lecito, trasparente e responsabile dei dati personali in allineamento con la ISO/IEC 27001:2022 e i relativi obblighi di legge.

3.2 Integrare i principi di protezione dei dati fin dalla progettazione e per impostazione predefinita in tutti i sistemi informativi, servizi e processi aziendali.

3.3 Applicare misure tecniche e organizzative (TOM) che tutelino la riservatezza, l'integrità e la disponibilità (CIA) dei dati personali per tutto il loro ciclo di vita.

3.4 Definire ruoli di governance e strutture di responsabilità per la protezione dei dati, incluse le responsabilità del Responsabile della protezione dei dati (DPO), della Sicurezza delle informazioni, della Funzione legale e compliance e dei Titolari delle informazioni.

3.5 Consentire la piena conformità agli articoli 5, 6, 25, 30 e 32 del GDPR, nonché ai requisiti di riduzione del rischio e resilienza previsti da NIS2 e DORA.

3.6 Garantire i diritti degli interessati, inclusi accesso, rettifica, cancellazione, limitazione, portabilità, opposizione e tutela rispetto ai processi decisionali automatizzati.

3.7 Mitigare i rischi normativi, reputazionali, legali e operativi derivanti da accessi non autorizzati, uso improprio o perdita di dati personali.

## 4. Ruoli e responsabilità

### 4.1 Direzione esecutiva

4.1.1 Fornisce supervisione strategica e assegna risorse adeguate a supporto del programma privacy.

4.1.2 Approva la presente politica e ne assicura l'attuazione in tutta l'organizzazione.

### 4.2 Responsabile della protezione dei dati (DPO)

4.2.1 Opera in autonomia nel vigilare sulla conformità alla normativa in materia di protezione dei dati.

4.2.2 Mantiene il registro delle attività di trattamento (RoPA) ai sensi dell'articolo 30 del GDPR.

4.2.3 Gestisce i rapporti con le autorità competenti, conduce le valutazioni d'impatto sulla protezione dei dati (DPIA) e governa i processi di notifica delle violazioni.

4.2.4 Riesamina le eccezioni privacy e mantiene il Registro delle eccezioni privacy.

[ ... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ... ]

## 9. Requisiti di riesame e aggiornamento

**9.1 La presente politica deve essere riesaminata almeno annualmente o prima al ricorrere delle seguenti condizioni:**

9.1.1 aggiornamenti normativi o regolatori significativi (ad esempio modifiche al GDPR, scadenze DORA).

9.1.2 nuovi sistemi o attività di trattamento che coinvolgono dati personali.

9.1.3 risultanze dell'audit interno che evidenziano lacune della politica.

9.1.4 incidenti di violazione rilevanti o rilievi dell'autorità di controllo.

**9.2 Responsabilità del riesame**

9.2.1 Il DPO deve avviare il riesame della politica, coordinandosi con la Funzione legale, la Funzione rischio, la Sicurezza delle informazioni e la Direzione esecutiva.

9.2.2 Tutti gli aggiornamenti devono essere registrati nel Registro dei documenti del SGSI e distribuiti alle parti interessate coinvolte.

**9.3 Controllo delle modifiche**

9.3.1 Qualsiasi revisione della presente politica deve essere formalmente approvata dalla Direzione esecutiva.

9.3.2 Le versioni obsolete devono essere archiviate in modo sicuro e la versione aggiornata deve includere una cronologia delle modifiche documentata.

## 10. Politiche correlate e collegamenti

10.1 P1 – Politica per la sicurezza delle informazioni. Stabilisce i principi generali di governance della sicurezza che costituiscono il fondamento della presente politica privacy. La P1 supporta la riservatezza, l'integrità e la disponibilità (CIA) dei dati personali in tutti i sistemi e servizi.

10.2 P6 – Politica di gestione del rischio. Definisce la metodologia dell'organizzazione per il trattamento del rischio, essenziale per valutare i rischi privacy, i processi DPIA e le valutazioni del rischio residuo richieste dal GDPR e dalla clausola 6.1.3 della ISO/IEC 27001.

10.3 P13 – Politica di classificazione ed etichettatura dei dati. Fornisce i criteri per la categorizzazione dei dati personali e sensibili, costituendo la base per l'applicazione di adeguati controlli privacy, inclusi applicazione della conservazione, limitazione dell'accesso e smaltimento sicuro.

10.4 P14 – Politica di conservazione e smaltimento dei dati. Supporta direttamente i requisiti privacy di cui agli articoli 5(1)(e) e 17 del GDPR, assicurando che i dati personali siano conservati solo per il tempo necessario e smaltiti in modo sicuro in conformità agli obblighi di legge.

10.5 P16 – Politica di mascheramento dei dati e pseudonimizzazione. Stabilisce controlli per ridurre l'identificabilità dei dati personali attraverso misure tecniche quali tokenizzazione, mascheramento dinamico e pseudonimizzazione, dando così attuazione all'articolo 32 del GDPR e al controllo 5.34 della ISO/IEC 27002.

10.6 P30 – Politica di risposta agli incidenti (P30). Definisce i protocolli obbligatori di risposta alle violazioni che si integrano con la gestione delle violazioni privacy e con le tempistiche di notifica richieste dagli articoli 33 e 34 del GDPR.

10.7 P33 – Politica di monitoraggio dell'audit e della conformità. Applica valutazioni pianificate dell'efficacia del programma privacy, dell'applicazione della politica e del monitoraggio delle azioni correttive nelle unità organizzative e presso i responsabili del trattamento terzi.

## 11. Standard e quadri di riferimento

**11.1 ISO/IEC 27001**

11.1.1 Clausola 5.1 – Leadership e impegno: stabilisce la responsabilità a livello esecutivo per la protezione dei dati personali e l'applicazione dei principi privacy.

11.1.2 Clausola 6.1.3 – Trattamento del rischio per la sicurezza delle informazioni: supporta l'identificazione, la valutazione e il trattamento del rischio privacy tramite DPIA ed eccezioni.

11.1.3 Clausola 8.1 – Pianificazione e controllo operativi: richiede misure tecniche e procedurali di sicurezza per assicurare che i dati personali siano trattati in modo sicuro.

11.1.4 Clausola 10.1 – Miglioramento continuo: prescrive la valutazione periodica e l'adeguamento del programma privacy.

11.2 ISO/IEC 27002:2022 controlli 5.34, 8.10, 8.11, 8.12: fornisce indicazioni sul trattamento dei dati personali identificabili, sull'applicazione della conservazione, sulla cancellazione, sull'anonimizzazione e sulla trasparenza rispetto ai diritti degli interessati.

**11.3 NIST SP 800-53 Rev.5**

11.3.1 AR-1, AR-2, AR-4, AR-5: definiscono governance, ruoli, responsabilità e obblighi di formazione privacy.

11.3.2 PL-2, PL-8: richiedono l'integrazione dei controlli privacy nel ciclo di vita dei sistemi e nell'architettura aziendale.

11.3.3 AC-2, AC-6: applicano il principio del privilegio minimo e la gestione degli account per la protezione dei dati personali.

11.3.4 AU-2, AU-6, AU-9: prescrivono logging, tracciabilità e integrità dell'audit per l'accesso ai dati personali.

11.3.5 IR-4, IR-5, IR-6: definiscono processi strutturati di rilevazione, analisi e segnalazione per le violazioni privacy.

11.3.6 PM-1, PM-21, PM-23: istituiscono un programma privacy completo, allineato agli obiettivi strategici aziendali di rischio e governance dei dati.

**11.4 GDPR UE (2016/679)**

11.4.1 Articoli 5, 6, 12–23, 25, 28, 30, 32–34: disciplinano trattamento lecito, limitazione della finalità, diritti degli interessati, accountability, protezione dei dati fin dalla progettazione e per impostazione predefinita, obblighi delle terze parti e gestione delle violazioni.

11.4.2 Considerando 78: rafforza i principi di protezione dei dati fin dalla progettazione.

**11.5 Direttiva NIS2 UE (2022/2555)**

11.5.1 Articolo 21(2)(e) e (f): richiede l'attuazione di controlli di sicurezza basati sul rischio e la protezione dei dati personali nell'ambito dei soggetti essenziali e importanti.

**11.6 DORA UE (2022/2554)**

11.6.1 Articolo 6(2)(d): impone una governance interna del rischio ICT relativo al trattamento dei dati.

11.6.2 Articolo 11(1)(c): prescrive la supervisione del rischio di terze parti per i servizi correlati ai dati.

11.6.3 Articoli 15(1) e 17: richiedono il trattamento sicuro dei dati da parte dei fornitori di servizi e tempestive comunicazioni alle autorità di vigilanza a seguito di incidenti correlati alle ICT.

**11.7 COBIT 2019**

11.7.1 APO12 – Gestione del rischio: integra il rischio privacy nella più ampia supervisione del rischio aziendale.

11.7.2 DSS01 – Managed Operations e DSS05 – DSS05: assicurano operazioni sicure, incluso controllo degli accessi, conservazione e integrità dei sistemi.

11.7.3 MEA03 – Monitoraggio della conformità: richiede il riesame continuo dello stato di conformità rispetto agli obblighi privacy di natura normativa e derivanti dalle politiche.