					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P17S					Titolo del documento: **Politica di protezione dei dati e della privacy**							
Versione: 1.0		Data di entrata in vigore: 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**

Allineamento a norme e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausole 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Controlli 5.34, 8.10–8.12	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
GDPR UE	Articoli 5, 6, 12-23, 30, 32-34	
NIS2 UE	Articolo 21(2)(e), 21(2)(f)	
DORA UE	Articoli 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

1. Finalità

1.1. La presente politica definisce le modalità con cui l'organizzazione protegge i dati personali in conformità agli obblighi di legge, ai requisiti normativi e agli standard internazionali di sicurezza.

1.2. Essa garantisce che i dati personali, relativi a clienti, personale o partner, siano raccolti, utilizzati, conservati e cancellati in modo lecito, corretto e sicuro.

1.3. La presente politica contribuisce inoltre alla conformità alla ISO/IEC 27001:2022 e supporta la capacità di dimostrare tale conformità in sede di audit, imponendo un approccio coerente e basato sul rischio alla tutela della privacy.

1.4. Attraverso la presente politica, l'organizzazione dimostra accountability e rafforza la fiducia dei clienti, dando priorità alla trasparenza, alla minimizzazione dei dati e a una solida governance della privacy.

2. Ambito di applicazione

2.1. La presente politica si applica a:

2.1.1. Tutti i dipendenti, collaboratori esterni o fornitori di servizi che accedono a dati personali, oppure li trattano o li gestiscono

2.1.2. Qualsiasi sistema, applicazione o ubicazione in cui i dati personali sono conservati o trasmessi

2.1.3. Tutti i dati personali, indipendentemente dal fatto che siano conservati in formato elettronico, cartaceo, in sistemi cloud o su dispositivi mobili

2.2. La presente politica si applica ai dati relativi a clienti, personale, fornitori e a qualsiasi altra persona identificata o identificabile.

2.3. La politica resta applicabile indipendentemente dal fatto che i dati siano trattati internamente o da fornitori di servizi terzi.

3. Obiettivi

3.1. Garantire che i dati personali siano trattati in conformità alla normativa in materia di privacy e agli standard di sicurezza, inclusi GDPR, NIS2 e ISO 27001.

3.2. Proteggere i dati personali da accessi non autorizzati, uso improprio, alterazione o perdita mediante controlli tecnologici e organizzativi chiaramente definiti.

3.3. Rispettare i diritti degli interessati, inclusi il diritto di accesso, rettifica e cancellazione dei propri dati.

3.4. Definire ruoli e responsabilità chiari per la protezione dei dati all'interno dell'organizzazione.

3.5. Applicare la minimizzazione dei dati, la conservazione sicura e la cancellazione tempestiva in tutti i sistemi e processi.

3.6. Ridurre il rischio di non conformità, sanzioni legali, danni reputazionali o perdita di fiducia da parte dei clienti.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. Approva la presente politica e ne garantisce l'attuazione

4.1.2. Fornisce le risorse necessarie per gestire i rischi per la privacy e rispondere agli incidenti

4.1.3. Mantiene la responsabilità complessiva della conformità alla normativa e agli standard in materia di privacy

4.2. Referente privacy (interno o esternalizzato)

4.2.1. Mantiene le registrazioni delle attività di trattamento dei dati

4.2.2. Gestisce le richieste degli interessati e delle autorità di controllo

4.2.3. Supporta le valutazioni del rischio, la formazione e l'attuazione della politica

4.2.4. Documenta le violazioni dei dati personali e notifica le autorità quando richiesto

[... 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. Riesami pianificati

9.1.1. La presente politica deve essere sottoposta a riesame almeno una volta ogni 12 mesi dal Referente privacy e approvata dal Direttore generale

9.1.2. Il riesame deve valutare la rilevanza della politica, l'allineamento normativo e l'efficacia operativa

9.2. Eventi che attivano un riesame intermedio

9.2.1. Gli aggiornamenti della politica devono essere avviati anche in risposta a:

9.2.1.1. nuove o modificate normative sulla protezione dei dati, ad esempio GDPR o DORA

9.2.1.2. incidenti di sicurezza o violazioni della privacy che coinvolgono dati personali

9.2.1.3. introduzione di nuovi sistemi, strumenti o servizi che trattano dati personali

9.2.1.4. risultanze di audit significative o raccomandazioni delle autorità di controllo

9.3. Controllo delle modifiche e comunicazione

9.3.1. Tutte le modifiche alla politica devono essere formalmente documentate in un registro delle modifiche

9.3.2. Le versioni aggiornate devono essere distribuite a tutto il personale e ai collaboratori esterni interessati

9.3.3. Le versioni archiviate devono essere conservate per garantire la tracciabilità ai fini dell'audit di conformità

10. Politiche correlate e collegamenti

10.1. La presente politica opera congiuntamente ad altre politiche SME per creare un quadro completo e applicabile per la privacy:

10.1.1. P13S – Politica di classificazione ed etichettatura dei dati: garantisce che i dati personali siano classificati correttamente, in modo che le misure di tutela della privacy possano essere applicate in base al rischio.

10.1.2. P14S – Politica di conservazione e smaltimento dei dati: definisce regole chiare sulla durata di conservazione dei dati personali e sui metodi sicuri per il loro smaltimento alla scadenza.

10.1.3. P16S – Politica di mascheramento dei dati e pseudonimizzazione: specifica come gli identificativi personali devono essere trasformati prima che i dati siano utilizzati in ambienti non di produzione o condivisi esternamente.

10.1.4. P30S – Politica di risposta agli incidenti: disciplina le fasi necessarie per rispondere alle violazioni dei dati personali, inclusa la notifica alle autorità di controllo e agli interessati entro i tempi previsti.

10.1.5. P2S – Politica sui ruoli e sulle responsabilità di governance: chiarisce la struttura delle responsabilità e i ruoli decisionali applicabili all'attuazione e alla supervisione della privacy.

10.2. Tali politiche correlate devono essere riesaminate e applicate congiuntamente per assicurare una copertura end-to-end della privacy su sistemi, personale e fornitori.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 5.1 – Richiede che l'alta direzione dimostri leadership e impegno nella protezione dei dati personali.

11.1.2. Clausola 6.1.3 – Richiede il trattamento dei rischi connessi al trattamento delle informazioni personali.

11.1.3. Clausola 8.1 – Richiede l'attuazione di controlli operativi per proteggere i dati lungo l'intero ciclo di vita.

11.2. ISO/IEC 27002

11.2.1. Controllo 5.34 – Fornisce indicazioni applicative sulla protezione della privacy e sulla gestione sicura dei dati personali identificabili.

11.2.2. Controllo 8.10 – Riguarda lo smaltimento sicuro dei dati personali per prevenire divulgazioni residue.

11.2.3. Controllo 8.11 – Supporta l'uso del mascheramento dei dati e della pseudonimizzazione ai fini della minimizzazione dei dati.

11.2.4. Controllo 8.12 – Previene perdite di dati non autorizzate mediante controlli sull'accesso e sull'uso dei dati.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – Assegna ruoli e responsabilità per la gestione del rischio per la privacy.

11.3.2. PL-5 – Richiede la documentazione di un piano per la privacy che disciplini l'uso e la protezione dei dati.

11.3.3. AC-6 – Richiede l'applicazione del principio del privilegio minimo e di controlli degli accessi per i dati personali.

11.3.4. IR-4 – Richiede processi di gestione degli incidenti per le violazioni che coinvolgono dati personali.

11.4. GDPR UE

11.4.1. Articolo 5 – Definisce i principi fondamentali del trattamento dei dati lecito, corretto e trasparente.

11.4.2. Articolo 6 – Richiede una valida base giuridica per ogni attività di trattamento dei dati personali.

11.4.3. Articoli 12–23 – Definiscono i diritti degli interessati, inclusi accesso, rettifica, cancellazione e opposizione.

11.4.4. Articolo 30 – Richiede le registrazioni delle attività di trattamento.

11.4.5. Articolo 32 – Richiede misure di sicurezza tecniche e organizzative adeguate.

11.4.6. Articoli 33–34 – Definiscono gli obblighi di notifica delle violazioni alle autorità e agli interessati.

11.5. NIS2 UE

11.5.1. Articolo 21(2)(e) – Richiede misure per garantire la protezione dei dati in allineamento con le politiche di cibersicurezza.

11.5.2. Articolo 21(2)(f) – Richiede meccanismi per gestire la sicurezza dei dati personali e riservati nei sistemi ICT.

11.6. DORA UE

11.6.1. Articolo 6 – Richiede assetti di governance interni per la gestione del rischio e la protezione dei dati.

11.6.2. Articolo 15 – Impone alle entità finanziarie di garantire che i fornitori terzi proteggano i dati personali e supportino la conformità normativa.

11.6.3. Articolo 17 – Richiede che le imprese assicurino che i sistemi ICT che trattano dati personali siano sicuri, resilienti e monitorati.

11.7. COBIT 2019

11.7.1. APO12 – Gestire il rischio: richiede l'identificazione e il trattamento dei rischi per la privacy e la protezione dei dati.

11.7.2. DSS05 – Gestire i servizi di sicurezza: richiede misure di sicurezza per prevenire l'accesso non autorizzato ai dati personali.

11.7.3. MEA03 – Monitorare, valutare e verificare la conformità: richiede alle organizzazioni di garantire la conformità continua alla normativa sulla privacy e sulla protezione dei dati.