					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P16S					Titolo del documento: **Politica P16S sul mascheramento dei dati e sulla pseudonimizzazione**							
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**

Allineata a norme e regolamenti

Norma/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 6.1.3, Clausola 8	Rischi per la sicurezza delle informazioni e controlli necessari, inclusi mascheramento e pseudonimizzazione
ISO/IEC 27002:2022	Controlli 8.11, 8.12	Linee guida sul mascheramento e sulla prevenzione della perdita di dati
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Offuscamento dei dati, tecnologie a tutela della privacy
UE NIS2	Articolo 21(2)(c)	Misure tecniche proporzionate, pseudonimizzazione come controllo
UE DORA	Articolo 10(1)	Controlli del rischio ICT, incluse misure di salvaguardia per la trasformazione dei dati
COBIT 2019	DSS05.01, DSS06	Protezione dei dati, tecniche di offuscamento/pseudonimizzazione
UE GDPR	Articoli 4(5), 5(1)(c), 32	Minimizzazione dei dati, pseudonimizzazione come controllo tecnico

1. Finalità

1.1. La presente politica definisce requisiti vincolanti per l'uso del mascheramento dei dati e della pseudonimizzazione al fine di proteggere i dati sensibili, personali e riservati nelle piccole e medie imprese (PMI).

1.2. Tali tecniche sono obbligatorie quando i dati reali non sono necessari, ad esempio in scenari di sviluppo, analisi o servizi erogati da terze parti, contribuendo a ridurre i rischi di esposizione, uso improprio o violazione dei dati.

1.3. La presente politica supporta direttamente la conformità ai requisiti per la certificazione ISO/IEC 27001:2022, nonché agli obblighi normativi europei quali GDPR, Direttiva NIS2 e Regolamento DORA.

1.4. Trasformando i dati prima del loro utilizzo al di fuori del contesto aziendale originario, l'organizzazione limita la propria esposizione al rischio e rafforza la capacità di dimostrare la dovuta diligenza in materia di privacy e sicurezza.

2. Ambito di applicazione

2.1. La presente politica si applica a tutti i dati strutturati o non strutturati classificati come personali, riservati o sensibili, sia archiviati sia trattati:

2.1.1. In ambienti di produzione, test o sviluppo

2.1.2. Su dispositivi locali, server o piattaforme cloud

2.1.3. Da personale interno, appaltatori e fornitori di servizi terzi

2.2. Si applica inoltre a tutti gli strumenti di trasformazione dei dati (mascheramento, tokenizzazione, pseudonimizzazione), siano essi open source, commerciali o sviluppati internamente.

2.3. I casi d'uso disciplinati dalla presente politica includono:

2.3.1. Preparazione di set di dati per test o sviluppo

2.3.2. Esportazione di dati verso sistemi di analisi

2.3.3. Accesso di fornitori o consulenti ai sistemi operativi

2.3.4. Minimizzazione dei dati relativi agli interessati per ridurre il rischio di trattamento

3. Obiettivi

3.1. Garantire che dati personali o sensibili reali non siano mai esposti in ambienti con livelli di sicurezza inferiori, salvo ove strettamente necessario.

3.2. Rendere obbligatorie tecniche di mascheramento o pseudonimizzazione quando gli identificativi reali non sono strettamente necessari per l'attività da svolgere.

3.3. Prevenire accessi non autorizzati o usi impropri dei dati applicando controlli di trasformazione prima del trasferimento o del trattamento dei dati.

3.4. Garantire che tutti i processi di mascheramento e pseudonimizzazione siano tracciabili, verificabili in sede di audit e applicati tramite strumenti approvati.

3.5. Rispettare le norme legali e regolamentari applicabili che richiedono minimizzazione dei dati, riservatezza e misure di salvaguardia per la trasformazione dei dati.

4. Ruoli e responsabilità

4.1. Direttore generale (GM)

4.1.1. È il titolare della presente politica e la approva

4.1.2. Assicura che tutti i reparti e i fornitori rispettino i requisiti di trasformazione

4.1.3. Riesamina eccezioni, valutazioni del rischio e registri delle trasformazioni

4.1.4. Coordina le azioni legali, operative o nei confronti dei fornitori in caso di violazioni

4.2. Fornitore di supporto IT / IT interno

4.2.1. Seleziona e gestisce gli strumenti di mascheramento o pseudonimizzazione

4.2.2. Assicura che siano applicati metodi di trasformazione adeguati in base alla tipologia di dato

4.2.3. Mantiene le registrazioni dei set di dati trasformati e delle procedure di gestione delle chiavi

4.2.4. Assicura che il mascheramento sia applicato prima dell'utilizzo per test, da parte di fornitori o per analisi

[... 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. Riesame annuale

9.1.1. La presente politica deve essere riesaminata almeno una volta all'anno dal Direttore generale per assicurare che rifletta:

9.1.1.1. Gli aggiornamenti delle normative applicabili (ad es. GDPR, DORA)

9.1.1.2. Nuovi sistemi aziendali o nuovi scambi di dati con terze parti

9.1.1.3. Feedback derivante da audit o incidenti che coinvolgono l'uso di dati non mascherati

9.2. Riesami intermedi

9.2.1. I riesami devono inoltre essere effettuati quando:

9.2.1.1. Vengono introdotte nuove applicazioni o piattaforme che trattano dati sensibili

9.2.1.2. Un incidente rilevante evidenzia carenze negli attuali controlli di trasformazione

9.2.1.3. Modifiche ai livelli di classificazione incidono sulle procedure di trattamento dei dati

9.3. Controllo delle versioni e gestione delle modifiche

9.3.1. Tutte le modifiche alla politica devono essere:

9.3.1.1. Approvate dal GM e documentate in un registro delle modifiche

9.3.1.2. Comunicate chiaramente ai dipendenti e ai fornitori di servizi interessati

9.3.1.3. Archiviate in modo sicuro con accesso limitato alle versioni obsolete

10. Politiche correlate e collegamenti

10.1. La presente politica deve essere applicata congiuntamente alle seguenti politiche SME per garantire una protezione coerente e vincolante dei dati sensibili:

10.1.1. P13S – Politica di classificazione ed etichettatura dei dati: definisce i livelli di classificazione (ad es. Riservato – Personale) che determinano quando devono essere applicati mascheramento o pseudonimizzazione. La presente politica applica regole di trasformazione in base ai livelli di sensibilità dei dati.

10.1.2. P14S – Politica di conservazione e smaltimento dei dati: assicura che i set di dati trasformati, inclusi i backup contenenti dati mascherati o pseudonimizzati, siano conservati e smaltiti secondo le regole applicabili, inclusa la cancellazione delle chiavi di mappatura quando non più necessarie.

10.1.3. P17S – Politica di protezione dei dati e privacy: allinea le pratiche di trasformazione ai più ampi obblighi in materia di privacy, inclusi i requisiti del GDPR relativi alla minimizzazione dei dati e all'uso della pseudonimizzazione come misura di sicurezza per il trattamento dei dati personali.

10.1.4. P30S – Politica di risposta agli incidenti: disciplina le procedure di segnalazione ed escalation in caso di divulgazione non autorizzata di dati, incluso l'uso improprio o il ripristino di dati mascherati o pseudonimizzati.

10.1.5. P2S – Politica sui ruoli e sulle responsabilità di governance: assegna la responsabilità complessiva per l'applicazione della politica, l'accettazione del rischio e l'approvazione delle eccezioni, principalmente al Direttore generale.

10.2. Tali politiche costituiscono un quadro integrato di protezione dei dati, assicurando che le attività di mascheramento e pseudonimizzazione supportino la certificazione ISO 27001 e la conformità a più normative.

11. Standard e quadri di riferimento

11.1. ISO/IEC 27001

11.1.1. Clausola 6.1.3: richiede il trattamento dei rischi per la sicurezza delle informazioni, inclusa la mitigazione dell'esposizione mediante tecniche di trasformazione dei dati.

11.1.2. Clausola 8.1: richiede l'applicazione dei controlli necessari per soddisfare gli obiettivi di sicurezza, inclusi pseudonimizzazione e mascheramento.

11.2. ISO/IEC 27002

11.2.1. Controllo 8.11: fornisce linee guida sul mascheramento dei dati sensibili nei sistemi di test e sviluppo.

11.2.2. Controllo 8.12: fornisce strategie per prevenire la perdita di dati attraverso pratiche controllate di trasformazione e accesso.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12: assicura la riservatezza delle informazioni attraverso l'offuscamento dei dati.

11.3.2. SC-28: protegge le informazioni a riposo e in uso.

11.3.3. PT-2/PT-3: promuovono l'uso di tecnologie a tutela della privacy, inclusa la pseudonimizzazione, nel trattamento di dati personali identificabili.

11.4. UE GDPR

11.4.1. Articolo 4(5): definisce giuridicamente la pseudonimizzazione e richiede controlli sulle chiavi di mappatura e sugli identificativi.

11.4.2. Articolo 5(1)(c): supporta i principi di minimizzazione dei dati attraverso il mascheramento.

11.4.3. Articolo 32: riconosce la pseudonimizzazione come controllo tecnico che riduce i rischi per la privacy.

11.5. Direttiva UE NIS2

11.5.1. Articolo 21(2)(c): richiede misure tecniche proporzionate per minimizzare il rischio per la sicurezza dei dati, inclusa la pseudonimizzazione come parte del controllo del rischio.

11.6. Regolamento UE DORA

11.6.1. Articolo 10(1): richiede controlli del rischio correlato alle ICT che includano misure di salvaguardia per la trasformazione dei dati a supporto della continuità e della riservatezza durante l'esternalizzazione e lo sviluppo dei sistemi.

11.7. COBIT 2019

11.7.1. DSS05.01: richiede la protezione degli asset informativi, inclusa la trasformazione ove possibile.

11.7.2. DSS06.06: richiede tecniche appropriate di offuscamento e pseudonimizzazione per limitare l'esposizione dei dati in ambienti a minore affidabilità.