					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P16					Titolo del documento: **Politica 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**

Allineamento a norme e regolamenti

Standard/Regolamento	Clausola/Articolo	Commento
ISO/IEC 27001:2022	Clausola 6.1	Requisiti generali per la gestione del rischio e i controlli operativi relativi al mascheramento dei dati e alla pseudonimizzazione
ISO/IEC 27002:2022	Controlli 8.11, 8	Indicazioni di controllo per l'applicazione del mascheramento dei dati e della pseudonimizzazione
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Controlli di privacy e riservatezza per la minimizzazione dei dati, la trasformazione dei dati e la limitazione dell'accesso
GDPR UE	Articoli 4(5), 5(1)(c,f), 32	Base giuridica e requisiti per la pseudonimizzazione e le misure di protezione dei dati
NIS2 UE	Articolo 21(2)(c)	Obbligo di adottare misure tecniche e organizzative, incluse tecnologie a tutela della privacy
DORA UE	Articoli 10(1), 10(2)(e)	Gestione del rischio ICT e controlli di riservatezza per il mascheramento dei dati e la pseudonimizzazione
COBIT 2019	DSS05.01, DSS06.06, MEA	Controlli di governance per la protezione dei dati mediante mascheramento e per la valutazione della conformità

Finalità

1.1 La presente politica definisce l'approccio dell'organizzazione all'applicazione del mascheramento dei dati e della pseudonimizzazione quali tecnologie a tutela della privacy, al fine di ridurre l'identificabilità e l'esposizione dei dati personali o sensibili.

1.2 Essa supporta l'utilizzo sicuro delle informazioni nelle attività di test, analisi e operative, nel rispetto dei requisiti di legge e regolamentari, mitigando l'impatto di una violazione dei dati e applicando i principi di minimizzazione dei dati e riservatezza.

1.3 La politica è allineata alla ISO/IEC 27001:2022, supporta l'articolo 4(5) del GDPR sulla pseudonimizzazione e integra un'applicazione basata sul rischio coerente con gli standard NIST, NIS2, DORA e COBIT 2019.

2. Ambito di applicazione

2.1 La presente politica si applica a:

2.1.1 tutti i dipendenti, i collaboratori esterni, le terze parti e i fornitori che hanno accesso a sistemi che trattano informazioni personali, riservate o sensibili.

2.1.2 tutti gli ambienti dati, inclusi produzione, sviluppo, test e staging.

2.1.3 tutte le forme di mascheramento dei dati (ad esempio statico, dinamico, deterministico, tokenizzazione) e le tecniche di pseudonimizzazione utilizzate per ridurre i rischi per la privacy.

2.1.4 tutti i tipi di dati (strutturati o non strutturati), sistemi (on-premise o asset ospitati in cloud) e applicazioni che coinvolgono dati personali o soggetti a regolamentazione.

2.2 L'ambito di applicazione include l'utilizzo in:

2.2.1 sviluppo applicativo e ambienti di quality assurance (QA)/test

2.2.2 piattaforme di analisi o reportistica

2.2.3 scambio di dati con terze parti o fornitori di servizi

2.2.4 sistemi di backup, archiviazione documentale o ripristino

3. Obiettivi

3.1 Garantire un'applicazione coerente ed efficace del mascheramento dei dati e della pseudonimizzazione per ridurre i rischi di esposizione dei dati o di uso improprio.

3.2 Garantire che i dati reali non siano mai utilizzati in ambienti non di produzione, salvo che siano stati sottoposti a trasformazione mediante tecniche a tutela della privacy approvate.

3.3 Mantenere l'integrità referenziale, l'usabilità e i metodi di preservazione del formato quando richiesto per la coerenza operativa.

3.4 Applicare rigorosi controlli di accesso ai dati originali, ai dati mascherati e alle chiavi di reidentificazione.

3.5 Trattare i set di dati mascherati o pseudonimizzati come dati sensibili, soggetti alla registrazione di audit degli accessi, ai controlli di conservazione e ai protocolli di risposta agli incidenti.

3.6 Convalidare l'efficacia di tali controlli attraverso test continui, monitoraggio e procedure di audit.

4. Ruoli e responsabilità

4.1 Direzione esecutiva

4.1.1 Approva la presente politica e ne garantisce l'attuazione nell'ambito delle più ampie iniziative di governance IT e protezione dei dati.

4.2 Chief Information Security Officer (CISO) / Responsabile del SGSI

4.2.1 Supervisiona l'attuazione e la conformità continuativa.

4.2.2 Garantisce l'allineamento con la clausola 6.1.3 della ISO/IEC 27001 (trattamento del rischio) e la clausola 8.1 (controllo operativo).

4.2.3 Riesamina i log di audit e convalida l'efficacia dei controlli.

[... 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 in caso di:

9.1.1 modifiche normative che incidono sul mascheramento dei dati o sulla pseudonimizzazione

9.1.2 adozione di nuovi sistemi IT che trattano dati sensibili

9.1.3 modifiche sostanziali allo schema di classificazione dei dati dell'organizzazione

9.1.4 risultanze dell'audit che indichino carenze nei controlli

9.1.5 comparsa di nuove minacce o tecnologie di mascheramento

9.2 Il Responsabile del SGSI deve guidare il riesame in consultazione con il Responsabile della protezione dei dati (DPO), i Titolari delle informazioni, la Sicurezza IT e la Funzione legale e compliance. Gli aggiornamenti devono essere soggetti al controllo di versione, approvati dalla Direzione esecutiva e comunicati a tutte le parti interessate coinvolte.

10. Politiche correlate e collegamenti

10.1 P13 - Politica di classificazione ed etichettatura dei dati. Le decisioni in materia di mascheramento dei dati e pseudonimizzazione dipendono direttamente dalla classificazione dei campi dati e dai livelli di sensibilità definiti nella P13.

10.2 P14 - Politica di conservazione e smaltimento dei dati. I set di dati trasformati devono essere conservati e smaltiti in conformità alle regole del ciclo di vita definite nella P14, garantendo che i dati mascherati e pseudonimizzati siano trattati come dati sensibili.

10.3 P17 - Politica di protezione dei dati e privacy. Fornisce i principi in materia di privacy e i fondamenti normativi per applicare la pseudonimizzazione quale attività di trattamento conforme ai sensi del GDPR e di normative analoghe.

10.4 P22 - Politica di registrazione e monitoraggio. Consente audit centralizzati e l'emissione di avvisi sugli eventi di mascheramento dei dati e pseudonimizzazione in conformità con protocolli strutturati di monitoraggio della sicurezza.

11. Standard e quadri di riferimento

11.1 ISO/IEC 27001

11.1.1 Clausola 6.1.3 - Piano di trattamento del rischio: stabilisce il mascheramento dei dati e la pseudonimizzazione come meccanismi di trattamento del rischio per ridurre l'identificabilità dei dati sensibili in ambienti di trattamento non essenziali.

11.1.2 Clausola 8.1 - Pianificazione e controllo operativo: richiede controlli tecnici e procedurali per la trasformazione sicura dei dati durante il trattamento, l'archiviazione o il trasferimento.

11.2 ISO/IEC 27002:2022

11.2.1 Controlli 8.11, 8: indicazioni sul mascheramento dei dati e sulla pseudonimizzazione per minimizzare i rischi di reidentificazione e perdita di dati.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Protezione dei dati personali identificabili: applicazione di tecnologie a tutela della privacy quali mascheramento dei dati e pseudonimizzazione.

11.3.2 PT-2, PT-3: minimizzazione e sicurezza del trattamento dei dati personali identificabili - trasformazione per ridurre l'identificabilità e applicare il controllo degli accessi.

11.3.3 SC-12, SC-28, SC-30: riservatezza e integrità dei dati - controlli di riservatezza e offuscamento per l'archiviazione, la trasmissione e l'utilizzo.

11.4 GDPR UE (2016/679)

11.4.1 Articolo 4(5): definizione formale di pseudonimizzazione.

11.4.2 Articolo 32: sicurezza del trattamento - misure organizzative e tecniche per la pseudonimizzazione.

11.4.3 Articolo 5(1)(c,f): minimizzazione dei dati e riservatezza mediante pseudonimizzazione/mascheramento dei dati.

11.5 Direttiva UE NIS2 (2022/2555)

11.5.1 Articolo 21(2)(c): richiede tecnologie a tutela della privacy quali mascheramento dei dati e pseudonimizzazione come misure di sicurezza.

11.6 DORA UE (2022/2554)

11.6.1 Articolo 10(1): il quadro di riferimento per la gestione del rischio ICT include controlli di mascheramento dei dati e pseudonimizzazione.

11.6.2 Articolo 10(2)(e): richiede l'uso di tecnologie di trasformazione per proteggere dati personali e dati finanziari.

11.7 COBIT 2019

11.7.1 DSS05.01: proteggere gli asset informativi - requisiti per mascheramento dei dati e pseudonimizzazione.

11.7.2 DSS06.06: test e analisi sicuri - mascheramento in ambienti esterni alla produzione.

11.7.3 MEA03: monitoraggio della conformità per l'efficacia del mascheramento dei dati e della pseudonimizzazione.