					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P16					Dokumenttitel: **Richtlinie zur Datenmaskierung und Pseudonymisierung**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Abgleich mit Normen und regulatorischen Anforderungen

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 6.1	Allgemeine Anforderungen an Risikomanagement und operative Kontrollen für Maskierung und Pseudonymisierung
ISO/IEC 27002:2022	Maßnahmen 8.11, 8	Leitlinien für die Umsetzung von Maskierung und Pseudonymisierung
NIST SP 800-53 Rev. 5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Datenschutz- und Vertraulichkeitskontrollen für Datenminimierung, Datentransformation und Zugriffsbeschränkung
EU-DSGVO	Artikel 4(5), 5(1)(c,f), 32	Rechtsgrundlage und Anforderungen für Pseudonymisierung und Datenschutzmaßnahmen
EU-NIS2	Artikel 21(2)(c)	Verpflichtung zu technischen und organisatorischen Maßnahmen einschließlich datenschutzfördernder Technologien
EU-DORA	Artikel 10(1), 10(2)(e)	IKT-Risikomanagement und Vertraulichkeitskontrollen für Datenmaskierung und Pseudonymisierung
COBIT 2019	DSS05.01, DSS06.06, MEA	Governance-Kontrollen zum Schutz von Daten durch Maskierung sowie zur Bewertung der Einhaltung

1. Zweck

1.1 Diese Richtlinie legt den Ansatz der Organisation zur Umsetzung von Datenmaskierung und Pseudonymisierung als datenschutzfördernde Technologien fest, um die Identifizierbarkeit und Offenlegung personenbezogener oder sensibler Daten zu verringern.

1.2 Sie unterstützt die sichere Nutzung von Informationen in Test-, Analyse- und Betriebsprozessen, stellt die Einhaltung gesetzlicher und regulatorischer Anforderungen sicher, mindert die Auswirkungen von Datenschutzverletzungen und setzt die Grundsätze der Datenminimierung und Vertraulichkeit durch.

1.3 Diese Richtlinie ist an ISO/IEC 27001:2022 ausgerichtet, unterstützt Artikel 4 Absatz 5 DSGVO zur Pseudonymisierung und integriert eine risikobasierte Umsetzung im Einklang mit NIST, NIS2, DORA und COBIT 2019.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Mitarbeitenden, Auftragnehmer, Dritten oder Lieferanten mit Zugriff auf Systeme, die personenbezogene, vertrauliche oder sensible Informationen verarbeiten.

2.1.2 alle Datenumgebungen, einschließlich Produktions-, Entwicklungs-, Test- und Staging-Umgebungen.

2.1.3 alle Formen der Datenmaskierung, z. B. statisch, dynamisch, deterministisch und Tokenisierung, sowie Pseudonymisierungstechniken, die zur Reduzierung von Datenschutzrisiken eingesetzt werden.

2.1.4 alle Datentypen, ob strukturiert oder unstrukturiert, Systeme, ob lokal betrieben oder cloudbasiert, und Anwendungen mit personenbezogenen oder regulierten Daten.

2.2 Der Geltungsbereich umfasst die Nutzung in:

2.2.1 Anwendungsentwicklung sowie Qualitätssicherungs- und Testumgebungen

2.2.2 Analyse- oder Berichtsplattformen

2.2.3 Datenaustausch mit Dritten oder Dienstleistern

2.2.4 Backup-, Archivierungs- oder Wiederherstellungssystemen

3. Ziele

3.1 Die konsistente und wirksame Anwendung von Maskierung und Pseudonymisierung ist sicherzustellen, um Risiken der Datenoffenlegung oder missbräuchlichen Nutzung zu reduzieren.

3.2 Es ist sicherzustellen, dass in Nicht-Produktionsumgebungen niemals Echtdaten verwendet werden, sofern diese nicht mittels genehmigter datenschutzfördernder Technologien transformiert wurden.

3.3 Referenzielle Integrität, Nutzbarkeit und formatwahrende Transformationen sind aufrechtzuerhalten, soweit dies für die operative Konsistenz erforderlich ist.

3.4 Für Originaldaten, maskierte Daten und Reidentifizierungsschlüssel sind strenge Zugriffskontrollen durchzusetzen.

3.5 Maskierte oder pseudonymisierte Datenbestände sind als sensible Daten zu behandeln und der Zugriffsprotokollierung, Aufbewahrungskontrollen sowie Incident-Response-Verfahren zu unterwerfen.

3.6 Die Wirksamkeit dieser Kontrollen ist durch kontinuierliche Tests, Überwachung und Audits zu validieren.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt diese Richtlinie und stellt deren Durchsetzung als Teil übergeordneter IT-Governance- und Datenschutzinitiativen sicher.

4.2 Chief Information Security Officer (CISO) / ISMS-Manager

4.2.1 Überwacht die Umsetzung und fortlaufende Einhaltung.

4.2.2 Stellt die Ausrichtung an ISO/IEC 27001, Klausel 6.1.3 (Risikobehandlung), und Klausel 8.1 (operative Planung und Steuerung) sicher.

4.2.3 Prüft Audit-Logs und validiert die Wirksamkeit der Kontrollen.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1 Diese Richtlinie ist mindestens jährlich oder früher zu überprüfen, wenn eines der folgenden Ereignisse eintritt:

9.1.1 regulatorische Änderungen mit Auswirkungen auf Maskierung oder Pseudonymisierung

9.1.2 Einführung neuer IT-Systeme, die sensible Daten verarbeiten

9.1.3 wesentliche Änderungen am Klassifizierungsschema der Organisation

9.1.4 Auditfeststellungen, die auf Kontrollmängel hinweisen

9.1.5 Auftreten neuer Bedrohungen oder Maskierungstechnologien

9.2 Der ISMS-Manager leitet die Überprüfung in Abstimmung mit dem Datenschutzbeauftragten (DPO), den Dateneigentümern, der Informationssicherheit und der Rechtsabteilung. Aktualisierungen müssen versionskontrolliert, von der obersten Führungsebene genehmigt und allen betroffenen Stakeholdern mitgeteilt werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P13 - Richtlinie zur Datenklassifizierung und Kennzeichnung. Entscheidungen zu Maskierung und Pseudonymisierung hängen unmittelbar von der in P13 festgelegten Klassifizierung von Datenfeldern und Sensibilitätsstufen ab.

10.2 P14 - Richtlinie zur Datenaufbewahrung und Entsorgung. Transformierte Datenbestände sind gemäß den Lebenszyklusregeln in P14 aufzubewahren und zu entsorgen; dabei ist sicherzustellen, dass maskierte und pseudonymisierte Daten als sensibel behandelt werden.

10.3 P17 - Richtlinie zu Datenschutz und Privatsphäre. Diese Richtlinie definiert Datenschutzgrundsätze und regulatorische Grundlagen für die Anwendung der Pseudonymisierung als konforme Verarbeitungstätigkeit nach DSGVO und vergleichbaren Gesetzen.

10.4 P22 - Richtlinie zu Protokollierung und Überwachung. Diese Richtlinie ermöglicht die zentrale Auditierung und Alarmierung von Maskierungs- und Pseudonymisierungsereignissen gemäß strukturierten Verfahren der Sicherheitsüberwachung.

11. Referenznormen und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 6.1.3 - Risikobehandlungsplan: Legt Maskierung und Pseudonymisierung als Mechanismen der Risikobehandlung zur Verringerung der Identifizierbarkeit sensibler Daten in nicht essenziellen Verarbeitungsumgebungen fest.

11.1.2 Klausel 8.1 - Operative Planung und Steuerung: Verlangt technische und prozessuale Kontrollen für die sichere Datentransformation bei Verarbeitung, Speicherung oder Übertragung.

11.2 ISO/IEC 27002:2022

11.2.1 Maßnahmen 8.11, 8: Leitlinien zur Datenmaskierung und Pseudonymisierung zur Minimierung von Risiken der Reidentifizierung und des Datenabflusses.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PM-17 - Schutz personenbezogener Daten: Umsetzung datenschutzfördernder Technologien wie Maskierung und Pseudonymisierung.

11.3.2 PT-2, PT-3: Minimierung und Sicherheit der Verarbeitung personenbezogener Daten - Transformation zur Reduzierung der Identifizierbarkeit und Durchsetzung von Zugriffskontrolle.

11.3.3 SC-12, SC-28, SC-30: Datenvertraulichkeit und -integrität - Vertraulichkeits- und Verschleierungskontrollen für Speicherung, Übertragung und Nutzung.

11.4 EU-DSGVO (2016/679)

11.4.1 Artikel 4(5): Formale Definition der Pseudonymisierung.

11.4.2 Artikel 32: Sicherheit der Verarbeitung - organisatorische und technische Maßnahmen zur Pseudonymisierung.

11.4.3 Artikel 5(1)(c,f): Datenminimierung und Vertraulichkeit durch Pseudonymisierung und Maskierung.

11.5 EU-NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(c): Verlangt datenschutzfördernde Technologien wie Maskierung und Pseudonymisierung als Sicherheitsmaßnahmen.

11.6 EU-DORA (2022/2554)

11.6.1 Artikel 10(1): Das IKT-Risikomanagementrahmenwerk umfasst Kontrollen zu Maskierung und Pseudonymisierung.

11.6.2 Artikel 10(2)(e): Verlangt den Einsatz von Transformationstechnologien zum Schutz personenbezogener und finanzieller Daten.

11.7 COBIT 2019

11.7.1 DSS05.01: Schutz von Informationswerten - Anforderungen an Maskierung und Pseudonymisierung.

11.7.2 DSS06.06: Sichere Tests und Analysen - Maskierung in Umgebungen außerhalb der Produktion.

11.7.3 MEA03: Überwachung der Einhaltung hinsichtlich der Wirksamkeit von Maskierung und Pseudonymisierung.