					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P16S					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 Standards und regulatorischen Vorgaben

Standard/Vorgabe	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 6.1.3, Klausel 8	Informationssicherheitsrisiken und erforderliche Kontrollen einschließlich Maskierung und Pseudonymisierung
ISO/IEC 27002:2022	Maßnahmen 8.11, 8.12	Leitlinien zur Maskierung und zur Vermeidung von Datenabfluss
NIST SP 800-53 Rev. 5	SC-12, SC-28, PT-2, PT-3	Datenverschleierung, datenschutzfördernde Technologien
EU-NIS2-Richtlinie	Artikel 21(2)(c)	Angemessene technische Maßnahmen, Pseudonymisierung als Kontrolle
EU-DORA-Verordnung	Artikel 10(1)	IKT-Risikokontrollen einschließlich Schutzmaßnahmen zur Datentransformation
COBIT 2019	DSS05.01, DSS06	Datenschutz, Verfahren zur Verschleierung und Pseudonymisierung
EU-DSGVO	Artikel 4(5), 5(1)(c), 32	Datenminimierung, Pseudonymisierung als technische Kontrolle

1. Zweck

1.1. Diese Richtlinie legt verbindliche Anforderungen für den Einsatz von Datenmaskierung und Pseudonymisierung zum Schutz sensibler, personenbezogener und vertraulicher Daten in kleinen und mittleren Unternehmen (KMU) fest.

1.2. Diese Verfahren sind verbindlich anzuwenden, wenn Echtdaten nicht erforderlich sind, etwa in Entwicklungs-, Analyse- oder Drittparteienszenarien, und tragen dazu bei, Risiken durch Offenlegung, Missbrauch oder Verstöße zu reduzieren.

1.3. Diese Richtlinie unterstützt unmittelbar die Einhaltung der Anforderungen für eine Zertifizierung nach ISO/IEC 27001:2022 sowie europäischer regulatorischer Vorgaben wie DSGVO, NIS2-Richtlinie und DORA-Verordnung.

1.4. Durch die Transformation von Daten vor ihrer Nutzung außerhalb ihres ursprünglichen geschäftlichen Kontexts begrenzt die Organisation Haftungsrisiken und verbessert ihre Fähigkeit, die gebotene Sorgfalt in Bezug auf Datenschutz und Informationssicherheit nachzuweisen.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für alle strukturierten oder unstrukturierten Daten, die als personenbezogen, vertraulich oder sensibel eingestuft sind und gespeichert oder verarbeitet werden:

2.1.1. in Produktiv-, Test- oder Entwicklungsumgebungen

2.1.2. auf lokalen Geräten, Servern oder Cloud-Plattformen

2.1.3. durch interne Mitarbeitende, Auftragnehmer oder Drittanbieter

2.2. Sie umfasst außerdem alle Werkzeuge zur Datentransformation (Maskierung, Tokenisierung, Pseudonymisierung), unabhängig davon, ob diese Open Source, kommerziell oder intern entwickelt sind.

2.3. Anwendungsfälle im Rahmen dieser Richtlinie umfassen:

2.3.1. die Aufbereitung von Testdatenbeständen oder Entwicklungsdatenbeständen

2.3.2. den Export von Daten in Analysesysteme

2.3.3. den Zugriff von Lieferanten oder Beratern auf operative Systeme

2.3.4. die Datenminimierung in Bezug auf betroffene Personen zur Reduzierung des Verarbeitungsrisikos

3. Ziele

3.1. Sicherstellen, dass echte personenbezogene oder sensible Daten niemals in Umgebungen mit geringerem Sicherheitsniveau offengelegt werden, in denen sie nicht zwingend erforderlich sind.

3.2. Die Anwendung von Maskierungs- oder Pseudonymisierungsverfahren vorschreiben, wenn reale Kennungen für die Aufgabe nicht zwingend erforderlich sind.

3.3. Unbefugten Zugriff oder Missbrauch von Daten verhindern, indem Transformationskontrollen vor der Datenübermittlung oder -verarbeitung durchgesetzt werden.

3.4. Gewährleisten, dass alle Maskierungs- und Pseudonymisierungsprozesse nachvollziehbar, auditierbar und mittels genehmigter Werkzeuge umgesetzt werden.

3.5. Die Einhaltung geltender rechtlicher und regulatorischer Anforderungen sicherstellen, die Datenminimierung, Vertraulichkeit und Schutzmaßnahmen zur Datentransformation verlangen.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführung

4.1.1. ist Eigentümerin dieser Richtlinie und genehmigt sie

4.1.2. stellt sicher, dass alle Abteilungen und Anbieter die Anforderungen an die Datentransformation einhalten

4.1.3. prüft Ausnahmen, Risikoanalysen und Transformationsprotokolle

4.1.4. koordiniert rechtliche, operative oder lieferantenbezogene Maßnahmen bei Verstößen

4.2. IT-Support-Dienstleister / Interne IT

4.2.1. wählt Werkzeuge zur Maskierung oder Pseudonymisierung aus und verwaltet diese

4.2.2. stellt sicher, dass geeignete Transformationsmethoden in Abhängigkeit vom Datentyp angewendet werden

4.2.3. führt Aufzeichnungen über transformierte Datenbestände und Verfahren zur Schlüsselverwaltung

4.2.4. stellt sicher, dass die Maskierung vor der Nutzung für Tests, durch Lieferanten oder für Analysen erfolgt

[... 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. Jährliche Überprüfung

9.1.1. Diese Richtlinie muss mindestens einmal jährlich durch die Geschäftsführung überprüft werden, um sicherzustellen, dass sie Folgendes berücksichtigt:

9.1.1.1. Aktualisierungen geltender regulatorischer Anforderungen (z. B. DSGVO, DORA)

9.1.1.2. neue Geschäftssysteme oder Datenaustausch mit Drittparteien

9.1.1.3. Rückmeldungen aus Audits oder Vorfällen mit der Nutzung unmaskierter Daten

9.2. Anlassbezogene Überprüfungen

9.2.1. Überprüfungen müssen auch erfolgen, wenn:

9.2.1.1. neue Anwendungen oder Plattformen eingeführt werden, die sensible Daten verarbeiten

9.2.1.2. ein wesentlicher Vorfall Lücken in den bestehenden Transformationskontrollen aufzeigt

9.2.1.3. Änderungen der Klassifizierungsstufen die Verfahren zur Datenverarbeitung beeinflussen

9.3. Versionskontrolle und Änderungsmanagement

9.3.1. Alle Änderungen an dieser Richtlinie müssen:

9.3.1.1. durch die Geschäftsführung genehmigt und in einem Änderungsprotokoll dokumentiert werden

9.3.1.2. den betroffenen Mitarbeitenden und Dienstleistern klar kommuniziert werden

9.3.1.3. sicher archiviert werden, wobei der Zugriff auf veraltete Versionen eingeschränkt sein muss

10. Zugehörige Richtlinien und Verknüpfungen

10.1. Diese Richtlinie ist gemeinsam mit den folgenden SME-Richtlinien anzuwenden, um einen konsistenten und durchsetzbaren Schutz sensibler Daten sicherzustellen:

10.1.1. P13S – Richtlinie zur Datenklassifizierung und Kennzeichnung: Definiert die Klassifizierungsstufen (z. B. „Vertraulich – Personenbezogen“), die festlegen, wann Maskierung oder Pseudonymisierung anzuwenden sind. Diese Richtlinie setzt Transformationsregeln auf Grundlage der Datensensibilität durch.

10.1.2. P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Stellt sicher, dass transformierte Datenbestände, einschließlich Backups mit maskierten oder pseudonymisierten Daten, nach den geltenden Vorgaben aufbewahrt und entsorgt werden, einschließlich der Löschung von Zuordnungsschlüsseln, wenn diese nicht mehr benötigt werden.

10.1.3. P17S – Richtlinie zu Datenschutz und Privatsphäre: Richtet Transformationsverfahren an weitergehenden Datenschutzpflichten aus, einschließlich DSGVO-Anforderungen zur Datenminimierung und zur Nutzung der Pseudonymisierung als Schutzmaßnahme für die Verarbeitung personenbezogener Daten.

10.1.4. P30S – Richtlinie zum Incident Response: Regelt Melde- und Eskalationsverfahren bei unbefugter Offenlegung von Daten, einschließlich der unzulässigen Nutzung oder Rückführung maskierter oder pseudonymisierter Daten.

10.1.5. P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Legt die Gesamtverantwortung für die Umsetzung der Richtlinie, die Risikoakzeptanz und die Genehmigung von Ausnahmen fest, vorrangig bei der Geschäftsführung.

10.2. Diese Richtlinien bilden ein integriertes Rahmenwerk zum Schutz von Daten und stellen sicher, dass Maßnahmen zur Maskierung und Pseudonymisierung die ISO/IEC-27001-Zertifizierung sowie die Einhaltung verschiedener regulatorischer Anforderungen unterstützen.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Klausel 6.1.3: Verlangt die Behandlung von Informationssicherheitsrisiken, einschließlich der Reduzierung von Offenlegungsrisiken durch Verfahren zur Datentransformation.

11.1.2. Klausel 8.1: Verlangt die Umsetzung der Kontrollen, die zur Erreichung der Sicherheitsziele erforderlich sind, einschließlich Pseudonymisierung und Maskierung.

11.2. ISO/IEC 27002

11.2.1. Maßnahme 8.11: Gibt Leitlinien zur Maskierung sensibler Daten in Test- und Entwicklungssystemen.

11.2.2. Maßnahme 8.12: Beschreibt Verfahren zur Vermeidung von Datenabfluss durch kontrollierte Transformation und geregelte Zugriffsverfahren.

11.3. NIST SP 800-53 Rev. 5

11.3.1. SC-12: Gewährleistet die Vertraulichkeit von Informationen durch Datenverschleierung.

11.3.2. SC-28: Schützt Informationen im Ruhezustand und während der Nutzung.

11.3.3. PT-2/PT-3: Fördern den Einsatz datenschutzfördernder Technologien, einschließlich Pseudonymisierung, bei der Verarbeitung personenbezogener Daten.

11.4. EU-DSGVO

11.4.1. Artikel 4(5): Definiert Pseudonymisierung rechtlich und verlangt Kontrollen über Zuordnungsschlüssel und Kennungen.

11.4.2. Artikel 5(1)(c): Unterstützt Grundsätze der Datenminimierung durch Maskierung.

11.4.3. Artikel 32: Erkennt Pseudonymisierung als technische Kontrolle an, die Datenschutzrisiken reduziert.

11.5. EU-NIS2-Richtlinie

11.5.1. Artikel 21(2)(c): Verlangt angemessene technische Maßnahmen zur Minimierung des Datensicherheitsrisikos, einschließlich Pseudonymisierung als Bestandteil der Risikokontrolle.

11.6. EU-DORA-Verordnung

11.6.1. Artikel 10(1): Verlangt IKT-bezogene Risikokontrollen, die Schutzmaßnahmen zur Datentransformation zur Aufrechterhaltung des Geschäftsbetriebs und der Vertraulichkeit bei Auslagerung und Systementwicklung umfassen.

11.7. COBIT 2019

11.7.1. DSS05.01: Verlangt den Schutz von Informationswerten, einschließlich Transformation, soweit möglich.

11.7.2. DSS06.06: Verlangt geeignete Verfahren zur Verschleierung und Pseudonymisierung, um die Datenexposition in Umgebungen mit geringerem Vertrauensniveau zu begrenzen.