					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P17					Dokumenttitel: **Richtlinie zu Datenschutz und Privatsphäre**							
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**

Anwendbare Normen und Vorschriften

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.1, 6.1.3, 8.1, 10	Relevante allgemeine, technische und organisatorische Kontrollen zur kontinuierlichen Verbesserung und zum Datenschutz
ISO/IEC 27002:2022	Maßnahmen 5.34, 8.10, 8.11, 8.12	Kontrollen für den Umgang mit personenbezogenen Daten, Aufbewahrung, Löschung, Anonymisierung und Rechte betroffener Personen
NIST SP 800-53 Rev.5	AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23	Anforderungen an Governance, Risikomanagement, Zugriffsmanagement, Protokollierung, Reaktion auf Datenschutzverletzungen und Datenschutzprogramme
EU GDPR	Artikel 5, 6, 12–23, 25, 28, 30, 32–34; Erwägungsgrund 78	Alle wesentlichen Grundsätze zu Datenschutz, Rechenschaftspflicht, Betroffenenrechten, Betroffenenanfragen, Datenschutzverletzungen sowie Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
EU NIS2	Artikel 21(2)(e), (f)	Risikobasierte Sicherheitskontrollen für wesentliche und wichtige Einrichtungen
EU DORA	Artikel 6(2)(d), 11(1)(c), 15(1), 17	Governance, Risiken durch Drittdienstleister und sichere Fristen für die Datenverarbeitung
COBIT 2019	APO12, DSS01, DSS05, MEA	Risikomanagement, sicherer Betrieb und Überwachung der Einhaltung

1. Zweck

1.1 Diese Richtlinie legt verbindliche organisatorische Grundsätze und technische Anforderungen für den Schutz personenbezogener Daten sowie für die Umsetzung von Datenschutz durch Technikgestaltung in allen Umgebungen fest.

1.2 Sie konkretisiert die Verantwortlichkeiten des Unternehmens nach internationalen Normen und regulatorischen Rahmenwerken und stellt sicher, dass personenbezogene Daten rechtmäßig, sicher und transparent erhoben, verarbeitet, aufbewahrt, weitergegeben und entsorgt werden.

1.3 Diese Richtlinie stärkt zudem die Einhaltung geltender Datenschutzgesetze und -rahmenwerke, einschließlich der EU-Datenschutz-Grundverordnung (GDPR), der EU-NIS2-Richtlinie, des Digital Operational Resilience Act (DORA) der EU, ISO/IEC 27001:2022 und COBIT 2019.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Organisationseinheiten, sämtliches Personal und alle Systeme, die an der Verarbeitung personenbezogener Daten beteiligt sind, einschließlich:

2.1.1 Mitarbeiter, Auftragnehmer, Berater sowie externe IT-Dienstleister.

2.1.2 Daten, die aus internen und externen Quellen über alle Geschäftsfunktionen hinweg erhoben werden.

2.1.3 Physische und digitale Medien, einschließlich Cloud-Diensten, SaaS-Plattformen, mobilen Geräten und papierbasierten Aufzeichnungen.

2.1.4 Alle Umgebungen, einschließlich Produktiv-, Entwicklungs-, Test- und Backup-Systemen, in denen personenbezogene Daten vorhanden sein können.

2.2 Sie umfasst alle Verarbeitungstätigkeiten, die nach geltenden Datenschutzgesetzen und Normen reguliert sind, einschließlich, aber nicht beschränkt auf:

2.2.1 Erhebung, Speicherung, Nutzung, Übermittlung und Entsorgung personenbezogener Daten.

2.2.2 Wahrnehmung der Rechte betroffener Personen, Dokumentation der Rechtsgrundlage und Einwilligungsmanagement.

2.2.3 Grenzüberschreitende Übermittlungen, Meldung von Datenschutzverletzungen und Weitergabe von Daten an Dritte.

2.2.4 Sichere Gestaltung und datenschutzfreundliche Voreinstellungen in Systemen und Prozessen.

3. Ziele

3.1 Gewährleistung einer rechtmäßigen, transparenten und rechenschaftspflichtigen Verarbeitung personenbezogener Daten im Einklang mit ISO/IEC 27001:2022 und den zugehörigen gesetzlichen Anforderungen.

3.2 Verankerung der Grundsätze Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen in allen Informationssystemen, Diensten und Geschäftsprozessen.

3.3 Umsetzung technischer und organisatorischer Maßnahmen (TOMs), die die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) personenbezogener Daten über ihren gesamten Lebenszyklus hinweg schützen.

3.4 Festlegung von Governance-Rollen und Rechenschaftsstrukturen für den Datenschutz, einschließlich der Verantwortlichkeiten des Datenschutzbeauftragten (DPO), der Informationssicherheit, der Rechtsabteilung und der Dateneigentümer.

3.5 Ermöglichung der vollständigen Einhaltung der Artikel 5, 6, 25, 30 und 32 der GDPR sowie der Anforderungen an Risikominderung und Resilienz nach NIS2 und DORA.

3.6 Wahrung der Rechte betroffener Personen, einschließlich Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Schutz vor automatisierter Entscheidungsfindung.

3.7 Minderung regulatorischer, reputationsbezogener, rechtlicher und operativer Risiken, die aus unbefugtem Zugriff, Missbrauch oder Verlust personenbezogener Daten entstehen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Stellt die strategische Aufsicht sicher und weist ausreichende Ressourcen zur Unterstützung des Datenschutzprogramms zu.

4.1.2 Genehmigt diese Richtlinie und stellt deren Umsetzung im gesamten Unternehmen sicher.

4.2 Datenschutzbeauftragter (DPO)

4.2.1 Handelt unabhängig, um die Einhaltung datenschutzrechtlicher Vorschriften zu überwachen.

4.2.2 Führt das Verzeichnis von Verarbeitungstätigkeiten (RoPA) gemäß Artikel 30 GDPR.

4.2.3 Leitet die Kommunikation mit Aufsichtsbehörden, führt Datenschutz-Folgenabschätzungen (DPIAs) durch und steuert Prozesse zur Meldung von Datenschutzverletzungen.

4.2.4 Prüft Datenschutzausnahmen und führt das Datenschutz-Ausnahmenregister.

[... 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 unter den folgenden Bedingungen zu überprüfen:

9.1.1 Wesentliche gesetzliche oder regulatorische Aktualisierungen (z. B. Änderungen der GDPR, DORA-Fristen)

9.1.2 Neue Systeme oder Verarbeitungstätigkeiten mit personenbezogenen Daten

9.1.3 Feststellungen aus internen Audits, die auf Richtlinienlücken hinweisen

9.1.4 Wesentliche Datenschutzverletzungen oder Rückmeldungen von Aufsichtsbehörden

9.2 Verantwortlichkeiten für die Überprüfung

9.2.1 Der DPO leitet die Überprüfung dieser Richtlinie ein und koordiniert sie mit Recht, Risikomanagement, Informationssicherheit und Geschäftsleitung.

9.2.2 Alle Aktualisierungen müssen im Register der ISMS-Dokumentenlenkung erfasst und an betroffene Interessenträger verteilt werden.

9.3 Änderungssteuerung

9.3.1 Jede Überarbeitung dieser Richtlinie muss formell durch die Geschäftsleitung genehmigt werden.

9.3.2 Veraltete Versionen sind sicher zu archivieren, und die aktualisierte Version muss eine dokumentierte Versionshistorie enthalten.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P1 – Informationssicherheitsrichtlinie. Legt die übergeordneten Grundsätze der Sicherheitsgovernance fest, die dieser Datenschutzrichtlinie zugrunde liegen. P1 unterstützt die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) personenbezogener Daten über alle Systeme und Dienste hinweg.

10.2 P6 – Risikomanagement-Richtlinie. Definiert die Methodik der Organisation zur Risikobehandlung, die für die Bewertung von Datenschutzrisiken, DPIA-Prozesse und Restrisikobewertungen gemäß GDPR und ISO/IEC 27001 Klausel 6.1.3 wesentlich ist.

10.3 P13 – Richtlinie zur Datenklassifizierung und Kennzeichnung. Regelt die Kategorisierung personenbezogener und sensibler Daten und bildet die Grundlage für die Anwendung geeigneter Datenschutzkontrollen, einschließlich Umsetzung von Aufbewahrung, Zugriffsbeschränkung und sicherer Entsorgung.

10.4 P14 – Richtlinie zur Datenaufbewahrung und Entsorgung. Unterstützt unmittelbar die Datenschutzanforderungen nach Artikel 5(1)(e) und 17 GDPR und stellt sicher, dass personenbezogene Daten nur so lange wie erforderlich aufbewahrt und im Einklang mit gesetzlichen Verpflichtungen sicher entsorgt werden.

10.5 P16 – Richtlinie zur Datenmaskierung und Pseudonymisierung. Legt Kontrollen zur Verringerung der Identifizierbarkeit personenbezogener Daten durch technische Maßnahmen wie Tokenisierung, dynamische Maskierung und Pseudonymisierung fest und setzt dadurch Artikel 32 GDPR und Maßnahme 5.34 der ISO/IEC 27002 um.

10.6 P30 – Incident-Response-Richtlinie (P30). Beschreibt die verbindlichen Protokolle zur Reaktion auf Datenschutzverletzungen, die in die Behandlung von Datenschutzvorfällen und die gemäß Artikel 33 und 34 GDPR erforderlichen Meldefristen integriert sind.

10.7 P33 – Richtlinie zur Audit- und Compliance-Überwachung. Erzwingt geplante Bewertungen der Wirksamkeit des Datenschutzprogramms, der Umsetzung von Richtlinien und der Nachverfolgung von Korrekturmaßnahmen über Organisationseinheiten und Auftragsverarbeiter Dritter hinweg.

11. Referenznormen und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 5.1 – Führung und Verpflichtung: Legt die Verantwortung auf Führungsebene für den Schutz personenbezogener Daten und die Umsetzung von Datenschutzgrundsätzen fest.

11.1.2 Klausel 6.1.3 – Informationssicherheitsrisikobehandlung: Unterstützt die Identifizierung, Bewertung und Behandlung von Datenschutzrisiken mittels DPIAs und Ausnahmen.

11.1.3 Klausel 8.1 – Operative Planung und Steuerung: Erfordert technische und prozessuale Schutzmaßnahmen, um eine sichere Verarbeitung personenbezogener Daten sicherzustellen.

11.1.4 Klausel 10.1 – Kontinuierliche Verbesserung: Verlangt die regelmäßige Bewertung und Anpassung des Datenschutzprogramms.

11.2 ISO/IEC 27002:2022 Maßnahmen 5.34, 8.10, 8.11, 8.12: Gibt Leitlinien für den Umgang mit personenbezogenen Daten, die Umsetzung von Aufbewahrung, Löschung, Anonymisierung und Transparenz in Bezug auf Rechte betroffener Personen.

11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5: Definieren Governance, Rollen, Rechenschaftspflicht und Verantwortlichkeiten für Datenschutzschulungen.

11.3.2 PL-2, PL-8: Verlangen die Integration von Datenschutzkontrollen in den Systemlebenszyklus und die Unternehmensarchitektur.

11.3.3 AC-2, AC-6: Erzwingen das Prinzip der minimalen Berechtigung und Kontenmanagement zum Schutz personenbezogener Daten.

11.3.4 AU-2, AU-6, AU-9: Schreiben Protokollierung, Rückverfolgbarkeit und Integrität von Audits für Zugriffe auf personenbezogene Daten vor.

11.3.5 IR-4, IR-5, IR-6: Definieren strukturierte Prozesse zur Erkennung, Analyse und Meldung von Datenschutzverletzungen.

11.3.6 PM-1, PM-21, PM-23: Etablieren ein umfassendes Datenschutzprogramm im Einklang mit strategischen Risiko- und Daten-Governance-Zielen.

11.4 EU GDPR (2016/679)

11.4.1 Artikel 5, 6, 12–23, 25, 28, 30, 32–34: Regelt die rechtmäßige Verarbeitung, Zweckbindung, Rechte betroffener Personen, Rechenschaftspflicht, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Verpflichtungen Dritter sowie das Management von Datenschutzverletzungen.

11.4.2 Erwägungsgrund 78: Bekräftigt die Grundsätze des Datenschutzes durch Technikgestaltung.

11.5 EU NIS2-Richtlinie (2022/2555)

11.5.1 Artikel 21(2)(e) und (f): Verlangt die Umsetzung risikobasierter Sicherheitskontrollen und den Schutz personenbezogener Daten im Anwendungsbereich wesentlicher und wichtiger Einrichtungen.

11.6 EU DORA (2022/2554)

11.6.1 Artikel 6(2)(d): Erzwingt interne Governance für IKT-Risiken im Zusammenhang mit der Datenverarbeitung.

11.6.2 Artikel 11(1)(c): Schreibt die Überwachung von Risiken Dritter für datenbezogene Dienste vor.

11.6.3 Artikel 15(1) und 17: Verlangen sichere Datenverarbeitung durch Dienstleister und fristgerechte Meldungen an Aufsichtsbehörden nach IKT-bezogenen Vorfällen.

11.7 COBIT 2019

11.7.1 APO12 – Risikomanagement: Verankert Datenschutzrisiken in der übergreifenden Überwachung von Unternehmensrisiken.

11.7.2 DSS01 – Gesteuerter Betrieb und DSS05 – Sicherheitsdienste verwalten: Stellen einen sicheren Betrieb sicher, einschließlich Zugriffskontrolle, Aufbewahrung und Systemintegrität.

11.7.3 MEA03 – Überwachung der Einhaltung: Verlangt die fortlaufende Überprüfung des Einhaltungsstatus gegenüber regulatorischen und richtlinienbasierten Datenschutzverpflichtungen.