					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P17S					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**

Ausgerichtet an Standards und Vorschriften

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Maßnahmen 5.34, 8.10–8.12	
NIST SP 800-53 Rev. 5	AR-2, PL-5, AC-6, IR-4	
EU-DSGVO	Artikel 5, 6, 12–23, 30, 32–34	
EU-NIS2	Artikel 21(2)(e), 21(2)(f)	
EU-DORA	Artikel 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

1. Zweck

1.1. Diese Richtlinie legt fest, wie die Organisation personenbezogene Daten im Einklang mit gesetzlichen Verpflichtungen, regulatorischen Anforderungen und internationalen Sicherheitsstandards schützt.

1.2. Sie stellt sicher, dass personenbezogene Daten – unabhängig davon, ob sie von Kunden, Mitarbeitenden oder Partnern stammen – rechtmäßig, nach Treu und Glauben und sicher erhoben, genutzt, gespeichert und gelöscht werden.

1.3. Diese Richtlinie unterstützt zudem die Einhaltung der ISO/IEC 27001:2022 und die Auditbereitschaft durch die Umsetzung eines konsistenten, risikobasierten Ansatzes zum Schutz der Privatsphäre.

1.4. Mit dieser Richtlinie weist die Organisation Rechenschaftspflicht nach und stärkt das Vertrauen der Kunden, indem sie Transparenz, Datenminimierung und eine wirksame Datenschutz-Governance priorisiert.

2. Geltungsbereich

2.1. Diese Richtlinie gilt für:

2.1.1. alle Mitarbeitenden, Auftragnehmer und Dienstleister, die auf personenbezogene Daten zugreifen, diese verarbeiten oder verwalten

2.1.2. jedes System, jede Anwendung und jeden Standort, an dem personenbezogene Daten gespeichert oder übertragen werden

2.1.3. sämtliche personenbezogenen Daten, unabhängig davon, ob sie elektronisch, in Papierform, in cloudbasierten Systemen oder auf mobilen Geräten gespeichert sind

2.2. Diese Richtlinie gilt für Daten von Kunden, Mitarbeitenden, Lieferanten und sonstigen identifizierbaren Personen.

2.3. Die Richtlinie gilt unabhängig davon, ob Daten intern oder durch externe Dienstleister verarbeitet werden.

3. Ziele

3.1. Sicherzustellen, dass personenbezogene Daten in Übereinstimmung mit Datenschutzgesetzen und Sicherheitsstandards, einschließlich DSGVO, NIS2 und ISO 27001, verarbeitet werden.

3.2. Schutz personenbezogener Daten vor unbefugtem Zugriff, Missbrauch, Veränderung oder Verlust durch klare technische und organisatorische Maßnahmen.

3.3. Wahrung der Datenschutzrechte betroffener Personen, einschließlich des Rechts auf Auskunft, Berichtigung und Löschung ihrer Daten.

3.4. Festlegung klarer Rollen und Verantwortlichkeiten für den Datenschutz innerhalb der Organisation.

3.5. Durchsetzung von Datenminimierung, sicherer Aufbewahrung und fristgerechter Löschung über alle Systeme und Prozesse hinweg.

3.6. Verringerung des Risikos von Nichteinhaltung, rechtlichen Sanktionen, Reputationsschäden oder Vertrauensverlust bei Kunden.

4. Rollen und Verantwortlichkeiten

4.1. Geschäftsführer (GM)

4.1.1. genehmigt diese Richtlinie und stellt ihre Durchsetzung sicher

4.1.2. stellt die erforderlichen Ressourcen bereit, um Datenschutzrisiken zu steuern und auf Vorfälle zu reagieren

4.1.3. trägt die Gesamtverantwortung für die Einhaltung von Datenschutzgesetzen und Standards

4.2. Datenschutzkoordinator (intern oder extern)

4.2.1. führt Verzeichnisse von Verarbeitungstätigkeiten

4.2.2. bearbeitet Datenschutzanfragen betroffener Personen und Anfragen von Aufsichtsbehörden

4.2.3. unterstützt Risikoanalysen, Schulungen und die Umsetzung der Richtlinie

4.2.4. dokumentiert Datenschutzverletzungen und benachrichtigt Behörden, sofern erforderlich

[... 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. Planmäßige Überprüfungen

9.1.1. Diese Richtlinie muss mindestens alle 12 Monate durch den Datenschutzkoordinator überprüft und durch den Geschäftsführer genehmigt werden

9.1.2. Die Überprüfung muss die Relevanz der Richtlinie, die regulatorische Ausrichtung und die operative Wirksamkeit bewerten

9.2. Auslöser für außerplanmäßige Überprüfungen

9.2.1. Aktualisierungen der Richtlinie müssen zudem veranlasst werden als Reaktion auf:

9.2.1.1. neue oder überarbeitete Datenschutzgesetze (z. B. DSGVO, DORA)

9.2.1.2. Sicherheitsvorfälle oder Datenschutzverletzungen mit Bezug zu personenbezogenen Daten

9.2.1.3. die Einführung neuer Systeme, Werkzeuge oder Services, die personenbezogene Daten verarbeiten

9.2.1.4. wesentliche Auditfeststellungen oder Empfehlungen von Aufsichtsbehörden

9.3. Änderungssteuerung und Kommunikation

9.3.1. Alle Änderungen an der Richtlinie müssen formell in einem Änderungsprotokoll dokumentiert werden

9.3.2. Überarbeitete Versionen müssen an alle Mitarbeitenden und einschlägigen Auftragnehmer verteilt werden

9.3.3. Archivierte Versionen müssen zur Nachvollziehbarkeit der Compliance aufbewahrt werden

10. Verwandte Richtlinien und Verknüpfungen

10.1. Diese Richtlinie gilt in Verbindung mit anderen SME-Richtlinien, um ein vollständiges und durchsetzbares Datenschutzrahmenwerk zu schaffen:

10.1.1. P13S – Richtlinie zur Datenklassifizierung und Kennzeichnung: Stellt sicher, dass personenbezogene Daten angemessen klassifiziert werden, damit Datenschutzmaßnahmen risikobasiert angewendet werden können.

10.1.2. P14S – Richtlinie zur Datenaufbewahrung und Entsorgung: Legt klare Regeln dafür fest, wie lange personenbezogene Daten aufzubewahren sind und welche sicheren Verfahren nach Ablauf der Aufbewahrungsfrist für ihre Entsorgung anzuwenden sind.

10.1.3. P16S – Richtlinie zur Datenmaskierung und Pseudonymisierung: Legt fest, wie personenbezogene Identifikatoren umgewandelt werden müssen, bevor Daten in einer Nicht-Produktionsumgebung verwendet oder extern weitergegeben werden.

10.1.4. P30S – Richtlinie zur Reaktion auf Sicherheitsvorfälle: Beschreibt die erforderlichen Schritte zur Reaktion auf Datenschutzverletzungen, einschließlich der Benachrichtigung von Aufsichtsbehörden und betroffenen Personen innerhalb der vorgeschriebenen Fristen.

10.1.5. P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Stellt die Rechenschaftsstruktur und Entscheidungsrollen klar, die für die Durchsetzung und Überwachung des Datenschutzes gelten.

10.2. Diese zugehörigen Richtlinien müssen gemeinsam überprüft und angewendet werden, um einen durchgängigen Datenschutz über Systeme, Mitarbeitende und Lieferanten hinweg sicherzustellen.

11. Referenzstandards und Rahmenwerke

11.1. ISO/IEC 27001

11.1.1. Klausel 5.1 – Verlangt, dass die oberste Leitung Führung und Verpflichtung zum Schutz personenbezogener Daten nachweist.

11.1.2. Klausel 6.1.3 – Verlangt die Behandlung von Risiken im Zusammenhang mit der Verarbeitung personenbezogener Daten.

11.1.3. Klausel 8.1 – Verlangt die Umsetzung operativer Kontrollen zum Schutz von Daten über ihren gesamten Lebenszyklus hinweg.

11.2. ISO/IEC 27002

11.2.1. Maßnahme 5.34 – Gibt Umsetzungshinweise zum Schutz der Privatsphäre und zum sicheren Umgang mit personenbezogenen Daten.

11.2.2. Maßnahme 8.10 – Behandelt die sichere Entsorgung personenbezogener Daten, um eine verbleibende Offenlegung zu verhindern.

11.2.3. Maßnahme 8.11 – Unterstützt den Einsatz von Maskierung und Pseudonymisierung zur Datenminimierung.

11.2.4. Maßnahme 8.12 – Verhindert unbefugten Datenabfluss durch Kontrollen für Datenzugriff und Datennutzung.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AR-2 – Weist Rollen und Verantwortlichkeiten für das Management von Datenschutzrisiken zu.

11.3.2. PL-5 – Verlangt die Dokumentation eines Datenschutzplans, der Datennutzung und Datenschutzmaßnahmen abdeckt.

11.3.3. AC-6 – Verlangt das Prinzip der minimalen Berechtigung und Zugriffskontrollen für personenbezogene Daten.

11.3.4. IR-4 – Verlangt Verfahren zum Umgang mit Informationssicherheitsvorfällen bei Verstößen mit Bezug zu personenbezogenen Daten.

11.4. EU-DSGVO

11.4.1. Artikel 5 – Definiert die Grundsätze der rechtmäßigen, nach Treu und Glauben erfolgenden und transparenten Datenverarbeitung.

11.4.2. Artikel 6 – Verlangt eine gültige Rechtsgrundlage für jede Verarbeitungstätigkeit personenbezogener Daten.

11.4.3. Artikel 12–23 – Beschreiben die Rechte betroffener Personen, einschließlich Auskunft, Berichtigung, Löschung und Widerspruch.

11.4.4. Artikel 30 – Verlangt Verzeichnisse von Verarbeitungstätigkeiten.

11.4.5. Artikel 32 – Verlangt angemessene technische und organisatorische Maßnahmen.

11.4.6. Artikel 33–34 – Legen Meldepflichten bei Datenschutzverletzungen gegenüber Behörden und betroffenen Personen fest.

11.5. EU-NIS2

11.5.1. Artikel 21(2)(e) – Verlangt Maßnahmen zur Sicherstellung des Datenschutzes im Einklang mit Cybersicherheitsrichtlinien.

11.5.2. Artikel 21(2)(f) – Verlangt Mechanismen zur Steuerung der Sicherheit personenbezogener und vertraulicher Daten in IKT-Systemen.

11.6. EU-DORA

11.6.1. Artikel 6 – Verlangt interne Governance-Rahmenwerke zur Steuerung von Datenrisiken und Datenschutz.

11.6.2. Artikel 15 – Verpflichtet Finanzunternehmen sicherzustellen, dass Drittanbieter personenbezogene Daten schützen und die regulatorische Compliance unterstützen.

11.6.3. Artikel 17 – Verlangt, dass Unternehmen sicherstellen, dass IKT-Systeme, die personenbezogene Daten verarbeiten, sicher, resilient und überwacht sind.

11.7. COBIT 2019

11.7.1. APO12 – Risiken managen: Verlangt die Identifizierung und Behandlung von Datenschutz- und Datenrisiken.

11.7.2. DSS05 – Sicherheitsdienste verwalten: Verlangt Schutzmaßnahmen zur Verhinderung unbefugten Zugriffs auf personenbezogene Daten.

11.7.3. MEA03 – Compliance überwachen: Verlangt von Organisationen, die fortlaufende Einhaltung von Datenschutzgesetzen und Datenschutzvorgaben sicherzustellen.