					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII14					Dokumenttitel: **Richtlinie zur Sicherheit und Zugriffskontrolle für PII**							
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 / Maßnahme / Artikel	Anwendbarkeit	Abdeckungsart	Kommentar
ISO/IEC 27701:2025	Clause 6.1.3; Clause 8.1	Both	Primary	Planung und Betrieb von Sicherheitskontrollen für PII
ISO/IEC 27701:2025	Clause 7.5; Clause 9.1; Clause 10.2	Both	Supporting	Nachweise, Überwachung und Korrekturmaßnahmen
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9	Both	Primary	Identität und Zugriffsrechte für die Verarbeitung von PII
ISO/IEC 27701:2025	Annex A.3.22; Annex A.3.23	Both	Primary	Endpunktschutz und sichere Authentifizierung
ISO/IEC 27701:2025	Annex A.3.25; Annex A.3.26	Both	Primary	Protokollierung und kryptografischer Schutz
ISO/IEC 27701:2025	Annex A.3.28; Annex A.3.29	Both	Supporting	Anwendungssicherheit und sichere Architektur
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.15; Annex A.3.16	Both	Supporting	Schutz und Überprüfung von Aufzeichnungen
GDPR	Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32	Both	Primary	Sicherheit, Rechenschaftspflicht und Kontrollen für Auftragsverarbeiter
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Integration von ISMS-Kontrollen
ISO/IEC 27002:2022	Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24	Both	Supporting	Umsetzungshinweise für Sicherheitskontrollen
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Grundsätze der Informationssicherheit und der Einhaltung des Datenschutzes
ISO/IEC 29151:2022	Clause 9.4.2; Clause 9.4.3;	Both	Supporting	Sicherheitskontrollen zum Schutz von PII

	Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4			

1. Geltungsbereich

1.1 Diese Richtlinie definiert PII-spezifische Anforderungen an Sicherheit und Zugriffskontrolle für Systeme, Anwendungen, Services, Geräte, Cloud-Umgebungen und Betriebsprozesse, die PII speichern, übertragen, verarbeiten, darauf zugreifen, sie administrieren oder schützen.

1.2 Diese Richtlinie gilt für Kontexte als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter, in denen die Organisation Sicherheitskontrollen für die Verarbeitung von PII festlegt, betreibt, unterstützt oder sich auf diese stützt.

1.3 Diese Richtlinie umfasst die folgenden Sicherheitskontrollbereiche für PII:

1.3.1 Sicherheitsbasislinie für PII und Integration mit bestehenden Informationssicherheitsrichtlinien;

1.3.2 Zugriffskontrolle;

1.3.3 Authentifizierung;

1.3.4 privilegierter Zugriff;

1.3.5 Verschlüsselung und sichere Speicherung;

1.3.6 Protokollierung und Überwachung;

1.3.7 sichere Konfiguration und Schwachstellenmanagement;

1.3.8 Endpunkt- und Cloud-Zugriffskontrollen;

1.3.9 Nachweisverknüpfung über REG02, REG08, REG10 und REG12.

1.4 Diese Richtlinie ersetzt kein vollständiges Informationssicherheits-Managementsystem, keine Netzwerksicherheitsrichtlinie, keine Richtlinie für sichere Softwareentwicklung, keine Backup-Richtlinie, keine Endpunktrichtlinie, keine Cloud-Sicherheitsrichtlinie, keinen kryptografischen Standard, kein Verfahren zum Schwachstellenmanagement und kein Verfahren zur Reaktion auf Informationssicherheitsvorfälle. Soweit solche Richtlinien bereits bestehen, definiert diese Richtlinie die für PII erforderlichen Verknüpfungs- und Nachweisanforderungen für die PIMS-Assurance.

1.5 Diese Richtlinie dupliziert nicht:

1.5.1 das Verzeichnis der Verarbeitung von PII und die Zuständigkeit für die Rechtsgrundlage in PII03;

1.5.2 die Methodik für Datenschutz-Risikobeurteilung und DPIA in PII07;

1.5.3 Gates für Datenschutz durch Technikgestaltung in PII08;

1.5.4 Regeln für Erhebung, Nutzung, Offenlegung und Datenweitergabe in PII09;

1.5.5 die Durchführung von Aufbewahrung, Löschung und Entsorgung in PII10;

1.5.6 Governance des Lebenszyklus von Auftragsverarbeitern in PII12;

1.5.7 Kontrollen für Übermittlungsinstrumente bei internationalen Übermittlungen in PII13;

1.5.8 den Workflow für Vorfälle und Datenschutzverletzungen in PII15;

1.5.9 Governance für dokumentierte Informationen in PII17;

1.5.10 PIMS-Governance für Überwachung, Audit und Verbesserung in PII18.

1.6 Für diese Richtlinie sind Betriebsprotokolle, Ausgaben von Sicherheitswerkzeugen, Exporte aus Berechtigungsüberprüfungen, Schwachstellenberichte und Konfigurationsnachweise Nachweisquellen, die den kanonischen Nachweisobjekten beigefügt, darin zusammengefasst oder durch diese referenziert werden. Sie sind keine separaten PIMS-Register.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass PII während der gesamten Verarbeitung durch geeignete, risikoorientierte und auditierbare Sicherheits- und Zugriffskontrollen geschützt wird.

2.2 Diese Richtlinie ermöglicht der Organisation nachzuweisen, dass Sicherheitskontrollen für PII über REG02, REG08, REG10 und REG12 geplant, umgesetzt, überprüft, überwacht und verbessert werden, ohne doppelte Sicherheitsregister zu erstellen oder bestehende Informationssicherheitsrichtlinien zu ersetzen.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 eine Basislinie für die Zugriffskontrolle auf PII für Systeme und Verarbeitungstätigkeiten festzulegen;

3.1.2 sicherzustellen, dass Authentifizierungskontrollen der Sensitivität und dem Zugriffskontext von PII angemessen sind;

3.1.3 Prüfanforderungen für privilegierten und normalen Zugriff auf PII festzulegen;

3.1.4 Erwartungen an Verschlüsselung und sichere Speicherung für PII im Ruhezustand, während der Übertragung und in relevanten Cloud- oder Endpunktkontexten festzulegen;

3.1.5 Erwartungen an Protokollierung und Überwachung für den Zugriff auf PII, Änderungen an PII und die Administration von PII festzulegen;

3.1.6 Anforderungen an Nachweise zu sicherer Konfiguration und Schwachstellen für Systeme festzulegen, die PII verarbeiten;

3.1.7 Erwartungen an Endpunkt- und Cloud-Zugriff festzulegen, ohne eine vollständige Endpunkt- oder Cloud-Sicherheitsrichtlinie zu erstellen;

3.1.8 vermutete Sicherheitsvorfälle in Bezug auf PII mit REG10 zu verknüpfen, ohne den Vorfall-Workflow zu duplizieren;

3.1.9 mit bestehenden Informationssicherheitsrichtlinien zu integrieren, sofern vorhanden;

3.1.10 auditbereite Nachweise ausschließlich unter Verwendung von REG02, REG08, REG10 und REG12 zu führen.

4. Richtlinienaussagen

4.1 Sicherheitsbasislinie für PII und ISMS-Integration

4.1.1 [Both] Der Information Security Lead MUSS die Sicherheitsbasislinie für PII für jedes System oder jeden Service, der PII verarbeitet, in REG12 festlegen, bevor das System oder der Service in Produktion geht oder wesentlich geändert wird.

4.1.2 [Both] Der System Owner / Application Owner MUSS den Speicherort der Nachweise zu umgesetzten Sicherheitskontrollen für PII in REG12 erfassen, bevor er sich für die PIMS-Assurance auf eine bestehende Informationssicherheitskontrolle stützt.

4.1.3 [Controller] Der Process Owner / Business Owner MUSS die Sensitivität von PII, den Verarbeitungskontext und den Zugriffsbedarf in REG02 identifizieren, bevor neuer oder wesentlich geänderter Zugriff auf PII beantragt wird.

4.1.4 [Processor] Der Vendor / Procurement Owner MUSS Kundenweisungen zur Sicherheit, Verantwortungsgrenzen des Kunden und Sicherheitszusagen des Auftragsverarbeiters in REG08 erfassen, bevor der Zugriff des Auftragsverarbeiters auf Kunden-PII beginnt oder wesentlich geändert wird.

4.1.5 [Both] Der Privacy Lead / PIMS Manager MUSS verifizieren, dass Sicherheitsnachweise für PII mit REG02, REG08, REG10 oder REG12 verknüpft sind, bevor die Verarbeitungstätigkeit als PIMS-auditierbar akzeptiert wird.

4.2 Basislinie für Zugriffskontrolle

4.2.1 [Both] Der System Owner / Application Owner MUSS den Zugriff auf PII auf genehmigte Rollen und autorisierte Benutzer beschränken, die in REG02 oder REG12 erfasst oder nachvollziehbar sind, bevor der Zugriff aktiviert wird.

4.2.2 [Both] Der Process Owner / Business Owner MUSS den Geschäftszweck für den Zugriff auf PII in REG02 oder REG12 genehmigen, bevor der System Owner / Application Owner den Zugriff bereitstellt.

4.2.3 [Both] Der System Owner / Application Owner MUSS Benutzerzugriffe auf Systeme, die PII mit hoher Tragweite oder sensitive PII verarbeiten, mindestens vierteljährlich überprüfen und das Prüfergebnis in REG12 erfassen.

4.2.4 [Both] Der System Owner / Application Owner MUSS Benutzerzugriffe auf andere Systeme, die PII verarbeiten, mindestens jährlich überprüfen und das Prüfergebnis in REG12 erfassen.

4.2.5 [Both] Der System Owner / Application Owner MUSS den Zugriff auf PII innerhalb eines Geschäftstags nach Rollenänderung, Beendigung, Vertragsabschluss oder Wegfall der Erforderlichkeit des Zugriffs in REG12 entfernen oder anpassen.

4.2.6 [Processor] Der Vendor / Procurement Owner MUSS in REG08 bestätigen, dass der Zugriff des Auftragsverarbeiters auf Kunden-PII auf dokumentierte Weisungen des Kunden beschränkt ist, bevor der Zugriff aktiviert oder geändert wird.

4.2.7 [Subprocessor] Der Vendor / Procurement Owner MUSS in REG08 bestätigen, dass der Zugriff des Unterauftragsverarbeiters auf PII auf autorisierte Unterauftragsverarbeitungstätigkeiten beschränkt ist, bevor der Zugriff des Unterauftragsverarbeiters aktiviert oder geändert wird.

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

9. Ausnahmen

9.1.1 [Both] Der Information Security Lead MUSS jede Ausnahme von einer Sicherheits- oder Zugriffskontrollanforderung in Bezug auf PII in REG12 erfassen, bevor die Ausnahme aktiviert wird.

9.1.2 [Both] Der Data Protection Officer / Privacy Advisor MUSS zu Sicherheitsausnahmen mit höherem Risiko für PII in REG12 beraten, bevor die Genehmigung erfolgt.

9.1.3 [Both] Top Management MUSS Sicherheitsausnahmen für PII in REG12 vor der Aktivierung genehmigen, wenn die Ausnahme PII mit hoher Tragweite, sensitive PII, privilegierten Zugriff, Verschlüsselung, Protokollierung oder nicht behobene Hochrisiko-Schwachstellen betrifft.

9.1.4 [Both] Der Information Security Lead MUSS Ablaufdatum der Ausnahme, kompensierende Kontrolle und Prüfdatum in REG12 festlegen, bevor die Ausnahme genehmigt wird.

9.1.5 [Both] Der System Owner / Application Owner MUSS abgelaufene Sicherheitsausnahmen für PII innerhalb von fünf Geschäftstagen nach Ablauf in REG12 beheben, verlängern oder schließen.

9.1.6 [Processor] Der Vendor / Procurement Owner MUSS Sicherheitsausnahmen von Auftragsverarbeitern oder Unterauftragsverarbeitern, die Kunden-PII betreffen, vor der Annahme in REG08 und REG12 erfassen.

10. Durchsetzung

10.1.1 [Both] Der Privacy Lead / PIMS Manager MUSS Nichtkonformitäten aufgrund fehlender oder unvollständiger Sicherheitsnachweise für PII innerhalb von fünf Geschäftstagen nach Identifizierung in REG12 erfassen.

10.1.2 [Both] Der Information Security Lead MUSS innerhalb von fünf Geschäftstagen nach Validierung die Zuständigkeit für die Behebung von Ausfällen von Sicherheitskontrollen für PII in REG12 zuweisen.

10.1.3 [Both] Der System Owner / Application Owner MUSS unautorisierten, übermäßigen oder nicht belegten Zugriff auf PII innerhalb eines Geschäftstags nach Validierung deaktivieren oder beschränken und die Maßnahme in REG12 erfassen.

10.1.4 [Conditional] Der Incident Response Coordinator MUSS Durchsetzungsmaßnahmen innerhalb eines Geschäftstags mit REG10 verknüpfen, wenn die Durchsetzungsangelegenheit einen vermuteten oder bestätigten Vorfall in Bezug auf PII umfasst.

10.1.5 [Both] Top Management MUSS wiederholte oder risikoreiche Sicherheits-Nichtkonformitäten in Bezug auf PII in REG12 vor der Managementbewertung überprüfen.

11. Überprüfung und Pflege

11.1.1 [All] Der Privacy Lead / PIMS Manager MUSS diese Richtlinie mindestens jährlich gemeinsam mit dem Information Security Lead überprüfen und das Prüfergebnis in REG12 erfassen.

11.1.2 [Both] Der Information Security Lead MUSS die Sicherheitsbasislinie für PII in REG12 innerhalb von 30 Tagen nach einer wesentlichen Technologie-, Bedrohungs-, Audit-, Vorfalls- oder regulatorischen Änderung überprüfen, die die Sicherheit von PII betrifft.

11.1.3 [Both] Der System Owner / Application Owner MUSS Sicherheitsnachweise für PII auf Systemebene in REG12 innerhalb von 30 Tagen nach einer wesentlichen Architektur-, Zugriffs-, Konfigurations-, Schwachstellen- oder Protokollierungsänderung aktualisieren.

11.1.4 [Processor] Der Vendor / Procurement Owner MUSS Nachweise zu Sicherheitsverantwortlichkeiten von Auftragsverarbeitern und Unterauftragsverarbeitern in Bezug auf PII in REG08 innerhalb von 30 Tagen nach einer wesentlichen Service-, Kundenweisungs- oder Unterauftragsverarbeiteränderung überprüfen.

11.1.5 [All] Der Internal Audit / Compliance Reviewer MUSS Nachweise zur Richtlinienüberprüfung und ausgewählte Nachweise zu Sicherheitskontrollen für PII in REG12 gemäß dem genehmigten Auditplan verifizieren.

12. Zugehörige Richtlinien

12.1 Diese Richtlinie ist gemeinsam zu lesen mit:

12.2 PII01 - Richtlinie für das Datenschutz-Informationsmanagementsystem;

12.3 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht;

12.4 PII03 - Richtlinie zum Verzeichnis der Verarbeitung von PII und zur Rechtsgrundlage;

12.5 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA;

12.6 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen;

12.7 PII09 - Richtlinie zur Erhebung, Nutzung, Offenlegung und Weitergabe von PII;

12.8 PII10 - Richtlinie zur Aufbewahrung, Löschung und Entsorgung von PII;

12.9 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Dritte;

12.10 PII13 - Richtlinie zu internationalen Übermittlungen von PII;

12.11 PII15 - Richtlinie zum Management von Vorfällen und Datenschutzverletzungen in Bezug auf PII;

12.12 PII16 - Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz;

12.13 PII17 - Richtlinie zu dokumentierten Informationen und Nachweismanagement im PIMS;

12.14 PII18 - Richtlinie zu PIMS-Überwachung, Audit und Verbesserung.

13. Referenzstandards und Rahmenwerke

13.1 ISO/IEC 27701:2025 - Clause 6.1.3; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.7; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5; 5.1.4; 5.1.6; 6.1.2; 7.1.1; 7.1.2].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.5.5; 4.6.3; 4.6.4; 4.7.5; 5.1.2; 6.1.1; 6.1.3; 6.1.4; 7.1.3; 7.1.6; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 9.1.1; 10.1.1; 10.1.2; 11.1.1; 11.1.5].

13.3 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.3.1; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 10.1.3].

13.4 ISO/IEC 27701:2025 - Annex A.3.22; Annex A.3.23. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.8.1; 4.8.2; 4.8.3; 4.8.4; 4.8.5].

13.5 ISO/IEC 27701:2025 - Annex A.3.25; Annex A.3.26. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.6 ISO/IEC 27701:2025 - Annex A.3.28; Annex A.3.29. Addressed by clauses [4.1.1; 4.1.2; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 7.1.1; 7.1.2].

13.7 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.15; Annex A.3.16. Addressed by clauses [4.1.5; 4.2.3; 4.2.4; 4.4.2; 4.4.3; 4.6.2; 4.6.3; 4.6.4; 4.7.2; 4.7.3; 5.1.9; 6.1.6; 8.1.4; 10.1.1; 11.1.5].

13.8 GDPR - Article 5(1)(f); Article 5(2); Article 24; Article 28; Article 32. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.5; 4.2.6; 4.2.7; 4.3.2; 4.4.4; 4.5.1; 4.5.2; 4.6.1; 4.6.6; 4.7.5; 4.7.6; 4.7.7; 4.8.4; 4.8.5; 5.1.1; 5.1.7; 6.1.4; 7.1.4; 9.1.3; 10.1.4].

13.9 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.10 ISO/IEC 27002:2022 - Controls 8.1, 8.2, 8.3, 8.5, 8.8, 8.9, 8.15, 8.16, 8.20, 8.24. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.2; 4.4.1; 4.4.2; 4.5.1; 4.5.2; 4.6.1; 4.6.3; 4.7.1; 4.7.4; 4.7.5; 4.8.1; 4.8.2; 7.1.1; 7.1.2].

13.11 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.1; 4.5.1; 4.6.2; 4.6.6; 4.7.6; 5.1.2; 6.1.1; 8.1.4; 10.1.1; 11.1.1].

13.12 ISO/IEC 29151:2022 - Clause 9.4.2; Clause 9.4.3; Clause 9.4.4; Clause 9.4.5; Clause 10.1.2; Clause 10.1.3; Clause 12.1.5; Clause 18.1.5; Clause 18.2.2; Clause 18.2.3; Clause 18.2.4. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.7.1; 4.7.2; 4.7.4; 4.8.1; 4.8.2; 6.1.6; 11.1.5].