					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII01					Dokumenttitel: **Richtlinie zum Datenschutz-Informationsmanagementsystem**							
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 / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Kontext und Bestimmung der PIMS-Rolle
ISO/IEC 27701:2025	Clause 4.2	Both	Primary	Interessierte Parteien und Anforderungen
ISO/IEC 27701:2025	Clause 4.3	Both	Primary	PIMS-Geltungsbereich
ISO/IEC 27701:2025	Clause 4.4	Both	Primary	Einrichtung und Verbesserung des PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Führung und Verpflichtung
ISO/IEC 27701:2025	Clause 5.2	Both	Primary	Datenschutzrichtlinie
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Rollen und Befugnisse
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	Risiken und Chancen
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Datenschutz-Risikobeurteilung
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Datenschutz-Risikobehandlung und SoA
ISO/IEC 27701:2025	Clause 6.2	Both	Primary	Datenschutzziele
ISO/IEC 27701:2025	Clause 6.3	Both	Primary	Geplante PIMS-Änderungen
ISO/IEC 27701:2025	Clause 7.1	Both	Primary	Ressourcen
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Kompetenz
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Sensibilisierung
ISO/IEC 27701:2025	Clause 7.4	Both	Primary	Kommunikation
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentierte Information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Operative Planung und Steuerung
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operative Datenschutz-Risikobeurteilung

ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operative Datenschutz-Risikobehandlung
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Überwachung und Bewertung
ISO/IEC 27701:2025	Clause 9.2	Both	Primary	Internes Audit
ISO/IEC 27701:2025	Clause 9.3	Both	Primary	Managementbewertung
ISO/IEC 27701:2025	Clause 10.1	Both	Primary	Kontinuierliche Verbesserung
ISO/IEC 27701:2025	Clause 10.2	Both	Primary	Nichtkonformität und Korrekturmaßnahme
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	Governance-Aufzeichnungen für Verantwortliche
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3	Processor	Primary	Vereinbarung und Zwecke des Auftragsverarbeiters
ISO/IEC 27701:2025	Annex A.3.3	Both	Primary	Verknüpfung mit der PII-Sicherheitsrichtlinie
GDPR	Article 5(2)	Controller	Supporting	Nachweise der Rechenschaftspflicht
GDPR	Article 24	Controller	Supporting	Maßnahmen und Richtlinie des Verantwortlichen
GDPR	Article 26	Joint Controller	Supporting	Regelungen für gemeinsam Verantwortliche
GDPR	Article 28	Both	Supporting	Governance für Auftragsverarbeiter
GDPR	Article 30	Both	Supporting	Verarbeitungsaufzeichnungen
GDPR	Article 32	Both	Supporting	Sicherheit der Verarbeitung
GDPR	Article 35	Controller	Supporting	DPIA-Governance
ISO/IEC 29100:2020	Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12	Both	Supporting	Datenschutzkontrollen und Grundsätze
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	PIA-Prozess und Vorbereitung
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2; Annex A.2	Controller	Supporting	PII-Schutzprogramm und Richtlinie

ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integration organisatorischer Datenschutzrisiken

1. Geltungsbereich

1.1 Diese Richtlinie richtet das Privacy Information Management System der Organisation für die Verarbeitung von PII in Kontexten als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter ein.

1.2 Diese Richtlinie gilt für Folgendes:

1.2.1 PIMS-Geltungsbereich, Kontext, interessierte Parteien und organisatorische Grenzen;

1.2.2 Bestimmung der PIMS-Rolle für Verarbeitungstätigkeiten mit PII;

1.2.3 Datenschutzrichtlinie, Datenschutzziele, Datenschutz-Risikobeurteilung, Datenschutz-Risikobehandlung und die PIMS-Erklärung zur Anwendbarkeit;

1.2.4 PIMS-Governance, Überwachung, Internes Audit, Managementbewertung, Nichtkonformität, Korrekturmaßnahmen und kontinuierliche Verbesserung;

1.2.5 dokumentierte Information und Nachweise, die erforderlich sind, um PIMS-Konformität und Rechenschaftspflicht nachzuweisen.

1.3 Für diese Richtlinie bezeichnet eine wesentliche Änderung jede Änderung, die den PIMS-Geltungsbereich, PII-Verarbeitungszwecke, PII-Kategorien, Kategorien betroffener Personen, Verarbeitungsorte, Rollenzuweisung als Verantwortlicher oder Auftragsverarbeiter, Systemarchitektur, Lieferanten- oder Unterauftragsverarbeiterregelungen, Datenschutz-Risikoprofil, anwendbare rechtliche oder vertragliche Verpflichtungen oder den Geltungsbereich der Zertifizierung betrifft.

2. Zweck

2.1 Diese Richtlinie definiert die verbindlichen Governance-Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung, Überwachung und kontinuierliche Verbesserung des PIMS.

2.2 Zweck dieser Richtlinie ist sicherzustellen, dass die Organisation eine rechenschaftspflichtige, risikobasierte und nachweisgestützte Steuerung der Verarbeitung von PII über die anwendbaren PIMS-Rollen hinweg nachweisen kann.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 den PIMS-Geltungsbereich, Kontext, Grenzen und Rollen-Anwendbarkeit zu definieren;

3.1.2 die Governance-Rechenschaftspflicht für das PIMS unter Verwendung kanonischer PIMS-Rollen zuzuweisen;

3.1.3 Datenschutzziele und messbare Erwartungen an die PIMS-Leistung festzulegen;

3.1.4 eine PIMS-Erklärung zur Anwendbarkeit für ausgewählte und ausgeschlossene Kontrollen aufrechtzuerhalten;

3.1.5 Datenschutz-Risikobeurteilung, Datenschutz-Risikobehandlung und DPIA-Governance in den PIMS-Betrieb zu integrieren;

3.1.6 sicherzustellen, dass Verpflichtungen als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter vor Beginn der Verarbeitung identifiziert werden;

3.1.7 auditbereite Nachweise für Auditbereitschaft für Zertifizierungen und kontinuierliche Verbesserung aufrechtzuerhalten;

3.1.8 unnötige Rollen, Register, Formulare und doppelte operative Kontrollen zu vermeiden.

4. Richtlinienaussagen

4.1 Einrichtung, Kontext und Geltungsbereich des PIMS

4.1.1 [Both] Top Management MUSS den PIMS-Geltungsbereich in REG01 vor der erstmaligen PIMS-Umsetzung und innerhalb von 30 Tagen nach jeder wesentlichen Änderung genehmigen.

4.1.2 [Both] Privacy Lead / PIMS Manager MUSS externe und interne Datenschutz-Kontextthemen in REG01 jährlich und innerhalb von 30 Tagen nach jeder wesentlichen Änderung dokumentieren.

4.1.3 [Both] Privacy Lead / PIMS Manager MUSS relevante interessierte Parteien und deren PIMS-Anforderungen in REG01 jährlich und innerhalb von 30 Tagen nach jeder wesentlichen Änderung dokumentieren.

4.1.4 [Both] Privacy Lead / PIMS Manager MUSS die Zusammenfassung der PIMS-Prozessinteraktionen in REG01 vor jeder Managementbewertung aufrechterhalten.

4.2 Bestimmung der PIMS-Rolle

4.2.1 [Both] Process Owner / Business Owner MUSS die PIMS-Rolle der Organisation für jede Verarbeitungstätigkeit mit PII in REG02 klassifizieren, bevor die Verarbeitungstätigkeit beginnt.

4.2.2 [Joint Controller] Vendor / Procurement Owner MUSS die Zuweisung der Verantwortlichkeiten gemeinsam Verantwortlicher in REG08 dokumentieren, bevor die gemeinsame Verarbeitung beginnt.

4.2.3 [Processor] Vendor / Procurement Owner MUSS Kundenverarbeitungsanweisungen für Tätigkeiten als Auftragsverarbeiter in REG08 vor dem Service-Onboarding dokumentieren.

4.2.4 [Subprocessor] Vendor / Procurement Owner MUSS vorgelagerte Kundenanweisungen und genehmigte Unterauftragsverarbeitungsregelungen in REG08 dokumentieren, bevor die Unterauftragsverarbeitung beginnt.

[... 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 Ausnahmeantrag und Genehmigung

9.1.1 [All] Process Owner / Business Owner MUSS jede beantragte Ausnahme von dieser Richtlinie in REG12 dokumentieren, bevor die Abweichung erfolgt.

9.1.2 [Both] Privacy Lead / PIMS Manager MUSS das Datenschutzrisiko jeder beantragten Ausnahme in REG04 vor Genehmigung bewerten.

9.1.3 [Both] Top Management MUSS Ausnahmen, die akzeptierte Datenschutz-Risikoschwellen überschreiten, in REG12 vor Umsetzung genehmigen.

9.1.4 [Both] Privacy Lead / PIMS Manager MUSS aktive PIMS-Ausnahmen in REG12 vierteljährlich bis zum Abschluss überprüfen.

9.2 Abschluss von Ausnahmen

9.2.1 [All] Process Owner / Business Owner MUSS Nachweise zum Abschluss der Ausnahme in REG12 bis zum genehmigten Ablaufdatum der Ausnahme dokumentieren.

9.2.2 [Both] Internal Audit / Compliance Reviewer MUSS Nachweise zum Abschluss abgelaufener Ausnahmen in REG12 während des nächsten geplanten Internen Audits verifizieren.

10. Durchsetzung

10.1 Behandlung von Nichtkonformitäten

10.1.1 [All] Privacy Lead / PIMS Manager MUSS vermutete Nichtkonformitäten mit dieser Richtlinie in REG12 innerhalb von fünf Geschäftstagen nach Identifizierung erfassen.

10.1.2 [All] Process Owner / Business Owner MUSS genehmigte Korrekturmaßnahmen in REG12 bis zum zugewiesenen Fälligkeitstermin nach Genehmigung der Nichtkonformität umsetzen.

10.1.3 [All] Top Management MUSS ungelöste wesentliche PIMS-Nichtkonformitäten in REG12 bei jeder Managementbewertung überprüfen.

10.1.4 [All] Internal Audit / Compliance Reviewer MUSS die Wirksamkeit von Korrekturmaßnahmen in REG12 innerhalb von 30 Tagen nach gemeldetem Abschluss verifizieren.

10.2 Eskalation

10.2.1 [All] Privacy Lead / PIMS Manager MUSS überfällige wesentliche Korrekturmaßnahmen innerhalb von fünf Geschäftstagen nach dem Fälligkeitstermin in REG12 an Top Management eskalieren.

10.2.2 [All] Top Management MUSS Entscheidungen zu überfälligen wesentlichen Korrekturmaßnahmen in REG12 innerhalb von 15 Geschäftstagen nach Eskalation erfassen.

11. Überprüfung und Pflege

11.1 Richtlinienüberprüfung

11.1.1 [All] Privacy Lead / PIMS Manager MUSS diese Richtlinie in REG12 jährlich und innerhalb von 30 Tagen nach jeder wesentlichen Änderung des rechtlichen, organisatorischen, verarbeitungsbezogenen, technologischen oder Geltungsbereichs der Zertifizierung überprüfen.

11.1.2 [All] Data Protection Officer / Privacy Advisor MUSS dokumentierte Beratung in REG12 vor Richtliniengenehmigung bereitstellen, wenn sich wesentliche Datenschutzverpflichtungen ändern.

11.1.3 [All] Top Management MUSS wesentliche Änderungen an dieser Richtlinie in REG12 vor Veröffentlichung genehmigen.

11.1.4 [All] Privacy Lead / PIMS Manager MUSS REG01 und REG03 innerhalb von 15 Geschäftstagen nach genehmigten Richtlinienänderungen aktualisieren, die den PIMS-Geltungsbereich oder die Anwendbarkeit von Kontrollen ändern.

11.1.5 [All] Privacy Lead / PIMS Manager MUSS die Kommunikation genehmigter Richtlinienänderungen in REG11 innerhalb von 30 Tagen nach Veröffentlichung erfassen.

12. Verwandte Richtlinien

12.1 Diese Richtlinie wird durch die folgenden verwandten Richtlinien unterstützt:

12.2 PII02 - Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht-Richtlinie

12.3 PII03 - Richtlinie zum PII-Verarbeitungsinventar und zur Rechtsgrundlage

12.4 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

12.5 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

12.6 PII12 - Richtlinie zu Auftragsverarbeitern, Unterauftragsverarbeitern und Datenweitergabe

12.7 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle

12.8 PII15 - Richtlinie zum Management von PII-Vorfällen und Datenschutzverletzungen

12.9 PII16 - Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz

12.10 PII17 - Richtlinie zum Management dokumentierter Information und Nachweise des PIMS

12.11 PII18 - Richtlinie zu PIMS-Überwachung, Audit und Verbesserung

13. Referenzstandards und Rahmenwerke

13.1 Diese Richtlinie ist den folgenden Standards und Vorschriften zugeordnet. Die Zuordnung erläutert, wie die Richtlinie die genannten Anforderungen unterstützt, und identifiziert die internen Klauseln, die sie umsetzen oder unterstützen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Abgebildet auf die Bestimmung des organisatorischen Kontexts, von Datenschutz-Kontextthemen und der Anwendbarkeit der Rolle als Verantwortlicher oder Auftragsverarbeiter für PIMS-Tätigkeiten. Addressed by clauses [4.1.2; 4.2.1; 6.1.3].

13.2.2 **Clause 4.2** - Abgebildet auf die Identifizierung interessierter Parteien, betroffener Personen, Kunden, Aufsichtsbehörden, Auftragsverarbeiter, Unterauftragsverarbeiter und deren relevante PIMS-Anforderungen. Addressed by clauses [4.1.3; 7.2.1; 11.1.1].

13.2.3 **Clause 4.3** - Abgebildet auf die Definition, Genehmigung, Aufrechterhaltung und Änderung des dokumentierten PIMS-Geltungsbereichs. Addressed by clauses [4.1.1; 6.1.3; 11.1.4].

13.2.4 **Clause 4.4** - Abgebildet auf die Einrichtung, Umsetzung, Aufrechterhaltung und Verbesserung von PIMS-Prozessen und deren Wechselwirkungen. Addressed by clauses [4.1.4; 7.1.1; 7.2.1].

13.2.5 **Clause 5.1** - Abgebildet auf Genehmigung durch Top Management, Ressourcen, Governance-Überprüfung und Führung in Bezug auf PIMS-Wirksamkeit und Verbesserung. Addressed by clauses [4.3.1; 5.1.1; 6.1.1; 8.1.4; 10.1.3].

13.2.6 **Clause 5.2** - Abgebildet auf die Aufrechterhaltung dieser Datenschutzrichtlinie als genehmigte dokumentierte Information und die Kommunikation von Richtlinienänderungen. Addressed by clauses [4.3.1; 11.1.1; 11.1.3; 11.1.5].

13.2.7 **Clause 5.3** - Abgebildet auf die Zuweisung und Kommunikation von PIMS-Rollen, Verantwortlichkeiten und Befugnissen. Addressed by clauses [5.1.1; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.8 **Clause 6.1.1** - Abgebildet auf die Planung von Maßnahmen für PIMS-Risiken und -Chancen unter Nutzung von Kontext, Anforderungen interessierter Parteien, Zielen und Verbesserungseingaben. Addressed by clauses [4.1.2; 4.1.3; 4.4.1; 6.1.1; 8.1.1].

13.2.9 **Clause 6.1.2** - Abgebildet auf die Verpflichtung zur Datenschutz-Risikobeurteilung vor neuer oder wesentlich geänderter Verarbeitung und zur Aufrechterhaltung von Datenschutz-Risikonachweisen. Addressed by clauses [4.4.1; 5.1.3; 8.2.4; 9.1.2].

13.2.10 **Clause 6.1.3** - Abgebildet auf Datenschutz-Risikobehandlung, Kontrollauswahl, Verknüpfung mit dem Informationssicherheitsprogramm und Pflege der Erklärung zur Anwendbarkeit. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.3; 7.1.4; 8.2.2].

13.2.11 **Clause 6.2** - Abgebildet auf die Festlegung, Messung, Überwachung, Kommunikation und Aktualisierung von PIMS-Zielen. Addressed by clauses [4.3.1; 4.3.2; 8.1.2; 8.1.4].

13.2.12 **Clause 6.3** - Abgebildet auf geplante PIMS-Änderungen und die Steuerung von Änderungen, die Geltungsbereich, Rollen, Kontrollen und dokumentierte Information betreffen. Addressed by clauses [4.1.1; 6.1.3; 7.1.1; 11.1.4].

13.2.13 **Clause 7.1** - Abgebildet auf die Bestimmung und Bereitstellung von Ressourcen für Einrichtung, Betrieb, Aufrechterhaltung und Verbesserung des PIMS. Addressed by clauses [5.1.1; 6.1.1; 7.1.1].

13.2.14 **Clause 7.2** - Abgebildet auf Kompetenzerwartungen und Nachweise, die PIMS-Verantwortlichkeiten und Rollenausübung unterstützen. Addressed by clauses [5.1.3; 5.1.8; 11.1.5].

13.2.15 **Clause 7.3** - Abgebildet auf Sensibilisierung für die Datenschutzrichtlinie, Beitrag zur PIMS-Wirksamkeit und Auswirkungen von Nichtkonformität. Addressed by clauses [11.1.5; 10.1.1; 10.2.1].

13.2.16 **Clause 7.4** - Abgebildet auf interne und externe Kommunikation, die für PIMS-Governance, Richtlinienänderungen und Eskalation relevant ist. Addressed by clauses [6.2.1; 10.2.1; 11.1.5].

13.2.17 **Clause 7.5** - Abgebildet auf Erstellung, Pflege, Steuerung, Nachweisbereitschaft und Aufbewahrung dokumentierter Information. Addressed by clauses [4.5.1; 4.5.3; 7.1.6; 11.1.4].

13.2.18 **Clause 8.1** - Abgebildet auf Planung, Umsetzung und Steuerung operativer PIMS-Prozesse und extern bereitgestellter Prozesse. Addressed by clauses [4.4.4; 7.1.3; 7.1.5; 7.2.1].

13.2.19 **Clause 8.2** - Abgebildet auf die Durchführung von Datenschutz-Risikobeurteilungen in geplanten Abständen sowie wenn wesentliche Änderungen vorgeschlagen werden oder eintreten. Addressed by clauses [4.4.1; 8.2.4; 9.1.2].

13.2.20 **Clause 8.3** - Abgebildet auf die Umsetzung von Plänen zur Datenschutz-Risikobehandlung und die Aufbewahrung von Nachweisen zu Behandlungsergebnissen. Addressed by clauses [4.4.3; 7.1.3; 8.2.2].

13.2.21 **Clause 9.1** - Abgebildet auf Überwachung, Messung, Analyse, Bewertung, Kennzahlen und Berichterstattung zur PIMS-Wirksamkeit. Addressed by clauses [8.1.1; 8.1.2; 8.1.4; 8.2.1; 8.2.2; 8.2.3; 8.2.4].

13.2.22 **Clause 9.2** - Abgebildet auf Planung interner Audits, Stichproben von Nachweisen, Auditergebnisse und unabhängige Überprüfung. Addressed by clauses [5.1.9; 6.2.1; 8.1.3; 9.2.2].

13.2.23 **Clause 9.3** - Abgebildet auf Eingaben für die Managementbewertung, Leistungsüberprüfung, Ergebnisse der Managementbewertung und Verbesserungsentscheidungen. Addressed by clauses [6.1.1; 6.1.2; 8.1.4; 10.1.3].

13.2.24 **Clause 10.1** - Abgebildet auf kontinuierliche Verbesserung durch Managementbewertung, Kennzahlen, Verfolgung von Korrekturmaßnahmen und Richtlinienpflege. Addressed by clauses [6.1.1; 6.2.2; 10.1.4; 11.1.1].

13.2.25 **Clause 10.2** - Abgebildet auf Behandlung von Nichtkonformitäten, Korrekturmaßnahmen, Eskalation, Abschluss und Verifizierung der Wirksamkeit. Addressed by clauses [4.5.2; 6.2.2; 6.2.3; 10.1.1; 10.1.2; 10.1.4; 10.2.1; 10.2.2].

13.2.26 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Abgebildet auf Aufzeichnungen zu Verarbeitungszwecken auf Seite des Verantwortlichen, Verknüpfung mit der Rechtsgrundlage, Bestimmung des DPIA-Bedarfs, Zuweisung der Verantwortung gemeinsam Verantwortlicher und Nachweisaufzeichnungen zur Verarbeitung. Addressed by clauses [4.2.1; 4.2.2; 4.4.2; 4.5.1; 7.1.2; 8.2.1].

13.2.27 **Annex A.2.2.2; Annex A.2.2.3** - Abgebildet auf Kundenvereinbarungen des Auftragsverarbeiters, dokumentierte Kundenanweisungen und Zweckbeschränkungen des Auftragsverarbeiters. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.2.28 **Annex A.3.3** - Abgebildet auf Verknüpfung mit der PII-Sicherheitsrichtlinie, Verantwortlichkeit für die Baseline der PII-Sicherheitskontrollen und Status von Informationssicherheitskontrollen in der PIMS-Erklärung zur Anwendbarkeit. Addressed by clauses [4.3.4; 5.1.4; 7.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Abgebildet auf Nachweise der Rechenschaftspflicht, Richtliniengenehmigung, Klassifizierung der Verarbeitungsrolle, Anwendbarkeit von Kontrollen, Überwachung, Audit und Aufzeichnungen zu Korrekturmaßnahmen. Addressed by clauses [4.3.1; 4.5.1; 4.5.2; 6.1.1; 8.1.3].

13.3.2 **Article 24** - Abgebildet auf Governance-Maßnahmen des Verantwortlichen, Richtliniengenehmigung, PIMS-Ziele, Überprüfung der Wirksamkeit und dokumentierte Nachweise der Rechenschaftspflicht des Verantwortlichen. Addressed by clauses [4.3.1; 4.3.2; 6.1.1; 8.1.4; 11.1.1].

13.3.3 **Article 26** - Abgebildet auf die Bestimmung und Dokumentation der Zuweisung der Verantwortlichkeiten gemeinsam Verantwortlicher, bevor die gemeinsame Verarbeitung beginnt. Addressed by clauses [4.2.2; 5.1.7; 7.1.5].

13.3.4 **Article 28** - Abgebildet auf Governance-Aufzeichnungen für Auftragsverarbeiter und Unterauftragsverarbeiter, Kundenverarbeitungsanweisungen und Steuerung extern bereitgestellter Prozesse. Addressed by clauses [4.2.3; 4.2.4; 5.1.7; 7.1.5].

13.3.5 **Article 30** - Abgebildet auf Aufzeichnungen zu Verarbeitungstätigkeiten, Rollenklassifizierung, Rechenschaftsaufzeichnungen zur Verarbeitung und für Auditierbarkeit aufbewahrte Nachweise. Addressed by clauses [4.2.1; 5.1.5; 7.1.2; 8.2.1].

13.3.6 **Article 32** - Abgebildet auf Governance der PII-Sicherheitsbaseline, Verantwortlichkeit für Sicherheitskontrollen, Status der Sicherheitsumsetzung und Bestätigung operativer Kontrollen. Addressed by clauses [4.3.4; 4.4.4; 5.1.4; 7.1.4].

13.3.7 **Article 35** - Abgebildet auf Bestimmung des DPIA-Bedarfs und Datenschutz-Risikobeurteilung, bevor eine Verarbeitung als Verantwortlicher mit hohem Risiko oder eine wesentlich geänderte Verarbeitung als Verantwortlicher fortgesetzt wird. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.1; Clause 5.11; Clause 5.12** - Abgebildet auf Identifizierung von Datenschutzkontrollen, Datenschutzgrundsätze, Informationssicherheit, Einhaltung des Datenschutzes, Audit, Nachweise und risikobasierte Datenschutz-Governance. Addressed by clauses [4.3.3; 4.3.4; 4.4.1; 4.5.1; 8.1.3; 10.1.4].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Abgebildet auf PIA-Governance, Bestimmung von DPIA-Auslösern, PIA-Vorbereitung, Datenschutz-Risikokriterien und dokumentierte Nachweise der Datenschutz-Risikobeurteilung. Addressed by clauses [4.4.1; 4.4.2; 5.1.3; 8.2.4; 9.1.2].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2; Annex A.2** - Abgebildet auf Anforderungen an das PII-Schutzprogramm, Identifizierung von PII-Schutzanforderungen, datenschutzrisikobasierte Kontrollauswahl und richtungsweisende PII-Schutzrichtlinie. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 7.1.4].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Abgebildet auf organisatorische Datenschutz-Risikogrundsätze, Führungsverpflichtung, Integration von Datenschutzrisiken in die PIMS-Governance und Verständnis der Rolle der Organisation bei der Verarbeitung von PII. Addressed by clauses [4.1.2; 4.2.1; 4.4.1; 4.4.3; 6.1.1].