					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII02					Dokumenttitel: **Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht**							
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 der PIMS-Rolle
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Führung und Rechenschaftspflicht
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	PIMS-Rollen, Verantwortlichkeiten und Befugnisse
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Rollenkompetenz
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Rollenbezogene Sensibilisierung
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Rollenkommunikation
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Rollenbezogene dokumentierte Information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Verantwortung für operative Steuerung
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Unabhängige Auditrolle
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Managementbewertung der Rechenschaftspflicht
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Rollenbezogene Nichtkonformität und Korrekturmaßnahme
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Verantwortung für Auftragsverarbeiterverträge
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Rollen und Verantwortlichkeiten gemeinsam Verantwortlicher
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Aufzeichnungen zur Rechenschaftspflicht
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Kundenvereinbarungen und Weisungen für Auftragsverarbeiter
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Zweckausrichtung von Auftragsverarbeitern
GDPR	Article 5(2)	Controller	Supporting	Nachweise zur Rechenschaftspflicht

GDPR	Article 24	Controller	Supporting	Verantwortung und Maßnahmen des Verantwortlichen
GDPR	Article 26	Joint Controller	Supporting	Vereinbarungen gemeinsam Verantwortlicher
GDPR	Article 28	Both	Supporting	Governance von Auftragsverarbeitern und Weisungen
GDPR	Article 30	Both	Supporting	Verarbeitungsaufzeichnungen und Verantwortungsnachweise
GDPR	Article 37	Conditional	Referenced	Benennung eines DPO, soweit anwendbar
GDPR	Article 38	Conditional	Supporting	Stellung und Unabhängigkeit des DPO, soweit anwendbar
GDPR	Article 39	Conditional	Supporting	Aufgaben des DPO, soweit anwendbar
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Akteure und Rollen im Datenschutzrahmenwerk
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Rechenschaftspflicht für Datenschutzkonformität
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Rollen und Funktionstrennung beim Schutz von PII
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Rollen und Verantwortlichkeiten in der Informationssicherheit
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Funktionstrennung

1. Geltungsbereich

1.1 Diese Richtlinie definiert das PIMS-Rollenmodell, die Struktur der Rechenschaftspflicht, Regeln zur Zuweisung von Verantwortlichkeiten, Regeln zur Rollenkombination, Erwartungen an Eskalationen und Nachweisanforderungen für die Datenschutz-Governance.

1.2 Diese Richtlinie gilt für Personal, Funktionen, Systeme, Lieferanten, Auftragsverarbeiter, Unterauftragsverarbeiter und Beziehungen gemeinsam Verantwortlicher, die an der Verarbeitung von PII innerhalb des PIMS-Geltungsbereichs beteiligt sind oder diese beeinflussen.

1.3 Diese Richtlinie gilt über Kontexte als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter hinweg.

1.4 Diese Richtlinie schafft keine neuen organisatorischen Stellenbezeichnungen. Sie definiert kanonische PIMS-Rollen, die bestehenden Personen oder Funktionen zugewiesen werden können, sofern Rollenzuweisung, Kompetenz, Unabhängigkeit und Anforderungen an Interessenkonflikte dokumentiert sind.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass PIMS-Verantwortlichkeiten eindeutig zugewiesen, verstanden, kommuniziert, nachgewiesen, überprüft und verbessert werden.

2.2 Diese Richtlinie ermöglicht der Organisation, Rechenschaftspflicht für Datenschutz-Governance, Verantwortung für PII-Verarbeitung, Rollenbestimmung als Verantwortlicher und Auftragsverarbeiter, Zuweisung der Verantwortlichkeiten gemeinsam Verantwortlicher, Bearbeitung von Weisungen an Auftragsverarbeiter, Datenschutzverantwortung von Lieferanten, unabhängige Überprüfung und rollenbasierte Eskalation nachzuweisen.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 die kanonischen PIMS-Rollen zu definieren, die im gesamten PIMS-Richtliniensatz verwendet werden;

3.1.2 sicherzustellen, dass jeder wesentlichen PIMS-Verantwortlichkeit eine rechenschaftspflichtige Rolle zugewiesen ist;

3.1.3 Rechenschaftspflicht als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter zu unterstützen;

3.1.4 praktikable Rollenkombinationen für kleine und mittlere Organisationen zu ermöglichen und zugleich Interessenkonflikte zu steuern;

3.1.5 die unabhängige Überprüfung durch Internal Audit / Compliance Reviewer zu wahren;

3.1.6 sicherzustellen, dass Rollenzuweisungen und Rollenänderungen in kanonischen Nachweisobjekten aufgezeichnet werden;

3.1.7 sicherzustellen, dass PIMS-Rolleninhaber angemessene Kommunikation und Sensibilisierung erhalten;

3.1.8 sicherzustellen, dass rollenbezogene Lücken, Konflikte und Nichtkonformitäten eskaliert und behoben werden.

4. Richtlinienaussagen

4.1 PIMS-Rollenmodell und Zuweisung

4.1.1 [All] Top Management MUSS das kanonische PIMS-Rollenmodell in REG01 vor der erstmaligen PIMS-Umsetzung und anschließend jährlich genehmigen.

4.1.2 [All] Privacy Lead / PIMS Manager MUSS namentliche PIMS-Rollenzuweisungen in REG01 vor der PIMS-Umsetzung und innerhalb von 10 Geschäftstagen nach personellen oder organisatorischen Änderungen pflegen.

4.1.3 [All] Privacy Lead / PIMS Manager MUSS den Verantwortungsumfang und die Befugnisebene für jede zugewiesene PIMS-Rolle in REG01 dokumentieren, bevor die Zuweisung wirksam wird.

4.1.4 [All] Process Owner / Business Owner MUSS für jede PII-Verarbeitungstätigkeit eine rechenschaftspflichtige verarbeitungsverantwortliche Rolle in REG02 zuweisen, bevor die Verarbeitungstätigkeit beginnt.

4.1.5 [All] System Owner / Application Owner MUSS den rechenschaftspflichtigen Systemverantwortlichen für jedes PII-verarbeitende System in REG02 dokumentieren, bevor das System produktiv gesetzt wird.

4.1.6 [All] Vendor / Procurement Owner MUSS den Verantwortlichen für die Beziehung zu jedem Auftragsverarbeiter, Unterauftragsverarbeiter, für jede Datenweitergabe an Dritte oder jede Beziehung gemeinsam Verantwortlicher in REG08 dokumentieren, bevor Onboarding oder Vereinbarungsgenehmigung erfolgen.

4.2 Rollenkombination, Funktionstrennung und Unabhängigkeit

4.2.1 [All] Privacy Lead / PIMS Manager MUSS jede PIMS-Rollenkombination in REG01 dokumentieren, bevor die Rollenkombination wirksam wird.

4.2.2 [All] Top Management MUSS Rollenkombinationen, die Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator oder Internal Audit / Compliance Reviewer betreffen, in REG01 vor der Zuweisung genehmigen.

4.2.3 [All] Internal Audit / Compliance Reviewer MUSS die Unabhängigkeit von dem zu überprüfenden PIMS-Prozess in REG12 dokumentieren, bevor jedes PIMS-Audit oder jede Überprüfung der Einhaltung beginnt.

4.2.4 [All] Privacy Lead / PIMS Manager MUSS kompensierende Kontrollen für unvermeidbare Konflikte der Funktionstrennung in REG12 aufzeichnen, bevor eine Rollenkombination genehmigt wird.

4.2.5 [All] Data Protection Officer / Privacy Advisor MUSS Bedenken hinsichtlich der Rollenunabhängigkeit oder Bedenken zu Interessenkonflikten in REG12 innerhalb von fünf Geschäftstagen nach Feststellung aufzeichnen.

[... 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 [All] Process Owner / Business Owner MUSS eine Ausnahme zur Rollen-Rechenschaftspflicht in REG12 beantragen, bevor eine PII-Verarbeitungstätigkeit ohne eine erforderliche zugewiesene Rolle betrieben wird.

9.1.2 [All] Privacy Lead / PIMS Manager MUSS die Auswirkungen und Minderung jeder Ausnahme zur Rollen-Rechenschaftspflicht in REG12 innerhalb von 10 Geschäftstagen nach Antrag bewerten.

9.1.3 [All] Top Management MUSS Ausnahmen zur Rollen-Rechenschaftspflicht, die 30 Tage überschreiten oder Verarbeitung mit hohem Risiko betreffen, in REG12 genehmigen, bevor die Ausnahme wirksam wird.

9.1.4 [All] Privacy Lead / PIMS Manager MUSS für jede genehmigte Ausnahme zur Rollen-Rechenschaftspflicht vor der Genehmigung ein Ablaufdatum von höchstens 90 Tagen in REG12 festlegen.

9.1.5 [All] Privacy Lead / PIMS Manager MUSS jede Ausnahme zur Rollen-Rechenschaftspflicht in REG12 innerhalb von fünf Geschäftstagen nach Ablauf schließen oder neu bewerten.

10. Durchsetzung

10.1.1 [All] Privacy Lead / PIMS Manager MUSS fehlende, unrichtige oder veraltete PIMS-Rollenzuweisungen als Nichtkonformitäten in REG12 innerhalb von fünf Geschäftstagen nach Feststellung aufzeichnen.

10.1.2 [All] Top Management MUSS bei wiederholten oder anhaltenden Versäumnissen der Rechenschaftspflicht Korrekturmaßnahmen in REG12 innerhalb von 15 Geschäftstagen verlangen.

10.1.3 [All] Process Owner / Business Owner MUSS die Produktivsetzung neuer oder geänderter PII-Verarbeitung verhindern, wenn erforderliche Rollen- und Rechenschaftsnachweise in REG02 oder REG08 fehlen.

10.1.4 [All] Internal Audit / Compliance Reviewer MUSS die Wirksamkeit von Korrekturmaßnahmen für Nichtkonformitäten der Rollen-Rechenschaftspflicht in REG12 beim nächsten geplanten Audit oder innerhalb von 60 Tagen nach Abschluss überprüfen, je nachdem, was zuerst eintritt.

11. Überprüfung und Pflege

11.1.1 [All] Privacy Lead / PIMS Manager MUSS diese Richtlinie jährlich und innerhalb von 30 Tagen nach einer wesentlichen Änderung am PIMS-Rollenmodell überprüfen.

11.1.2 [All] Data Protection Officer / Privacy Advisor MUSS vorgeschlagene Änderungen an dieser Richtlinie hinsichtlich ihrer Auswirkungen auf Datenschutzrollen in REG12 vor der Genehmigung überprüfen.

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

11.1.4 [All] Privacy Lead / PIMS Manager MUSS REG01 und REG11 innerhalb von 15 Geschäftstagen nach genehmigten Änderungen an PIMS-Rollen, Verantwortlichkeiten oder Kommunikationsanforderungen aktualisieren.

12. Verwandte Richtlinien

12.1 Diese Richtlinie wird durch die folgenden verwandten Richtlinien unterstützt:

12.2 PII01 - Richtlinie zum Datenschutz-Informationsmanagementsystem

12.3 PII03 - Richtlinie zum Verzeichnis der PII-Verarbeitung und zur Rechtsgrundlage

12.4 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

12.5 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen

12.6 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Dritte

12.7 PII14 - Richtlinie zur PII-Sicherheit und Zugriffskontrolle

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

12.9 PII16 - Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz

12.10 PII17 - Richtlinie zu dokumentierter Information und Nachweismanagement im 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** - Zugeordnet zur Bestimmung des PIMS-Rollenkontexts, der Anwendbarkeit für Verantwortliche und Auftragsverarbeiter, der Verarbeitungsverantwortung und der Aufzeichnungen zur Beziehungsverantwortung. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Zugeordnet zur Genehmigung durch Top Management, zur Aufsicht über Rechenschaftspflicht, zur jährlichen Managementbewertung, zu Kennzahlen zur Rechenschaftspflicht und zu Korrekturmaßnahmen bei Rollenversäumnissen. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Zugeordnet zur Zuweisung, Dokumentation, Kommunikation und Pflege von PIMS-Rollen, Verantwortlichkeiten, Befugnissen, Systemverantwortung, Verarbeitungsverantwortung, Verantwortung für Lieferantenbeziehungen, Verantwortung für Vorfalleskalation und Verantwortung für unabhängige Überprüfung. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Zugeordnet zu rollenspezifischer Kompetenz und Sensibilisierungsnachweisen für zugewiesene PIMS-Verantwortlichkeiten. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Zugeordnet zur Sensibilisierung für zugewiesene PIMS-Verantwortlichkeiten, zu Bestätigungsnachweisen und zur jährlichen Berichterstattung über rollenspezifische Sensibilisierung. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Zugeordnet zur Kommunikation von Rollenzuweisungen, Rollenänderungen, Eskalationen und Informationen zur Rollenübergabe. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Zugeordnet zu dokumentierter Information für PIMS-Rollenzuweisungen, Verantwortungsumfänge, Befugnisebenen, jährliche Nachweisaufbewahrung und Pflege der Rollenmatrix. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Zugeordnet zur Verantwortlichkeit für operative Steuerung bei Verarbeitungstätigkeiten, Systemen, Lieferanten, Auftragsverarbeitern, Unterauftragsverarbeitern, Beziehungen gemeinsam Verantwortlicher und Kontrollen zur Produktivsetzung. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Zugeordnet zum unabhängigen Audit und zur Überprüfung der Einhaltung von Nachweisen zur Rollenzuweisung, Nachweisen zur Rollenkombination, Nachweisen zur Unabhängigkeit, Feststellungen und Abschluss von Korrekturmaßnahmen. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Zugeordnet zur Managementbewertung der Vollständigkeit von PIMS-Rollenzuweisungen, Rollenkonflikten, Ausnahmen, Kennzahlen zur Rechenschaftspflicht und Ergebnissen der Überprüfung der Rechenschaftspflicht. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Zugeordnet zur Eskalation, Aufzeichnung von Nichtkonformitäten, Korrekturmaßnahmen, Schließung von Ausnahmen und Wirksamkeitsüberprüfung bei Fragen der Rollen-Rechenschaftspflicht. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Zugeordnet zur Zuweisung und Dokumentation der Verantwortung für Auftragsverarbeiterverträge und Eskalation von Verantwortlichkeiten Dritter vor Vertragsgenehmigung oder -verlängerung. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Zugeordnet zur Dokumentation der Zuweisung von Verantwortlichkeiten gemeinsam Verantwortlicher und Nachweisen zur Beziehungsverantwortung, bevor die

Verarbeitung als gemeinsam Verantwortliche beginnt. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Zugeordnet zur Pflege von Aufzeichnungen zur Rechenschaftspflicht für Verarbeitungsverantwortung als Verantwortlicher, Rollenklassifizierung und Nachweisverantwortung. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Zugeordnet zur Verantwortung für Kundenvereinbarungen des Auftragsverarbeiters, zur Verantwortlichkeit für Kundenweisungen und zu Nachweisen zur Beziehung des Auftragsverarbeiters. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Zugeordnet zur Ausrichtung von Zweck und Weisungen des Auftragsverarbeiters durch Verantwortlichkeit für Kundenweisungen und Überprüfung der Rolle als Verantwortlicher/Auftragsverarbeiter. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Zugeordnet zu Nachweisen zur Rechenschaftspflicht für Rollenzuweisungen, Verarbeitungsverantwortung, Rollenüberprüfungen, Nichtkonformitäten und Audit-Feststellungen. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Zugeordnet zur Verantwortung des Verantwortlichen, rechenschaftspflichtiger Verarbeitungsverantwortung, Aufsicht durch Top Management, jährlicher Überprüfung und Maßnahmen zur Rechenschaftspflicht. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Zugeordnet zur Dokumentation der Zuweisung von Verantwortlichkeiten gemeinsam Verantwortlicher und Nachweisen zur Beziehungsverantwortung, bevor die Verarbeitung als gemeinsam Verantwortliche beginnt. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Zugeordnet zur Zuweisung von Verantwortlichkeiten für Auftragsverarbeiter und Unterauftragsverarbeiter, zur Verantwortlichkeit für Kundenweisungen, zur Vertragsverantwortung und zu Eskalationswegen für Dritte. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Zugeordnet zu Verarbeitungsaufzeichnungen, Verarbeitungsverantwortung, PIMS-Rollenklassifizierung und Überprüfung der Rolle als Verantwortlicher/Auftragsverarbeiter. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Zugeordnet zur Dokumentation der Rolle Data Protection Officer / Privacy Advisor, wenn eine Benennung anwendbar ist oder freiwillig erfolgt. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Zugeordnet zur Stellung, Unabhängigkeit, Einbindung und Behandlung von Interessenkonflikten von Data Protection Officer / Privacy Advisor, soweit anwendbar. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Zugeordnet zu Datenschutzberatung, Beobachtungen aus der Überwachung, beratender Überprüfung und rollenbezogener Prüfung der Datenschutzauswirkungen durch Data Protection Officer / Privacy Advisor, soweit anwendbar. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Zugeordnet zu Akteuren des Datenschutzrahmenwerks und Rollenzuweisung für betroffene Personen, PII-Verantwortliche, PII-Auftragsverarbeiter, Dritte und PIMS-Rollenklassifizierung. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Zugeordnet zur Rechenschaftspflicht für Datenschutzkonformität, Rollennachweisen, Überprüfung, Audit-Feststellungen und Wirksamkeitsüberprüfung von Korrekturmaßnahmen. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Zugeordnet zur Definition von Rollen für den Schutz von PII, Rollendokumentation, Rollenkommunikation, Koordination von Sicherheit und Datenschutz sowie Funktionstrennung für den Schutz von PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Zugeordnet zur Definition, Zuweisung, Dokumentation, Kommunikation und Pflege von PIMS- und Informationssicherheitsverantwortlichkeiten. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Zugeordnet zu Funktionstrennung, Genehmigung von Rollenkombinationen, unabhängiger Überprüfung, Konfliktkontrollen und Wirksamkeitsüberprüfung von Korrekturmaßnahmen für Rollenkonflikte. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].