					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII17					Dokumenttitel: **PIMS-Richtlinie zum Management dokumentierter Informationen und Nachweise**							
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 6.1.3	Both	Supporting	Dokumentierte Information zur Erklärung zur Anwendbarkeit
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentierte PIMS-Information
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Steuerung operativer Nachweise
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Überwachungsnachweise
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Auditnachweise
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Nachweise der Managementbewertung
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Nachweise zu Nichtkonformität und Korrekturmaßnahmen
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Verarbeitungsaufzeichnungen des Verantwortlichen
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Nachweise zu Auftragsverarbeitervereinbarung und Weisungen
ISO/IEC 27701:2025	Annex A.3.14	Both	Primary	Schutz von Aufzeichnungen
GDPR	Article 5(2)	Controller	Supporting	Nachweise zur Rechenschaftspflicht
GDPR	Article 24	Controller	Supporting	Maßnahmen und Nachweise des Verantwortlichen
GDPR	Article 28	Both	Supporting	Dokumentation des Auftragsverarbeiters
GDPR	Article 30	Both	Supporting	Verarbeitungsaufzeichnungen
GDPR	Article 32	Both	Supporting	Schutz von Nachweisen
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Nachweise der Einhaltung im Datenschutz
ISO/IEC 29151:2022	Clause 18.1.4	Both	Supporting	Schutz von Aufzeichnungen
ISO/IEC 27001:2022	Clause 7.5	Both	Supporting	Steuerung dokumentierter Information
ISO/IEC 27002:2022	Control 5.33	Both	Supporting	Schutz von Aufzeichnungen

ISO/IEC 27002:2022	Control 5.34	Both	Supporting	Schutz der Privatsphäre und von PII

1. Geltungsbereich

1.1 Diese Richtlinie definiert verbindliche Anforderungen für die Erstellung, Genehmigung, Versionierung, den Schutz, die Aufbewahrung, den Abruf, die Übersetzung, die Zurückziehung und die Nachweisführung für dokumentierte PIMS-Informationen.

1.2 Diese Richtlinie gilt für PIMS-Richtlinien, Register, dokumentierte Genehmigungen, Nachweisaufzeichnungen, Auditnachweise, Aufzeichnungen der Managementbewertung, Nachweise zu Korrekturmaßnahmen und gesteuerte Übersetzungen, die zum Nachweis der PIMS-Konformität verwendet werden.

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

1.4 Diese Richtlinie schafft kein separates Dokumentenregister. Nachweise zur Steuerung dokumentierter Information werden über die kanonischen PIMS-Nachweisobjekte REG01 bis REG12 geführt; REG03 und REG12 werden für Nachweise zur Anwendbarkeit von Kontrollen, zu Audits, Nichtkonformitäten, Korrekturmaßnahmen und Verbesserungen verwendet.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass dokumentierte PIMS-Informationen korrekt, gesteuert, für autorisierte Benutzer zugänglich, gegen unbefugte Änderungen oder Offenlegung geschützt, zur Auditierbarkeit aufbewahrt und bei Veraltung zurückgezogen werden.

2.2 Diese Richtlinie unterstützt die Auditbereitschaft für Zertifizierungen, indem sie sicherstellt, dass Nachweise, die zur Darlegung der PIMS-Konformität erforderlich sind, aufgefunden, verifiziert, abgerufen und mit anwendbaren Richtlinien, Kontrollen, Verarbeitungstätigkeiten, Risiken, Audits und Korrekturmaßnahmen verknüpft werden können.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 Anforderungen an die Steuerung dokumentierter PIMS-Informationen zu definieren;

3.1.2 die Integrität der Nachweise über REG01 bis REG12 hinweg aufrechtzuerhalten;

3.1.3 sicherzustellen, dass die Genehmigung von Richtlinien und Nachweisen nachvollziehbar ist;

3.1.4 sicherzustellen, dass Versionshistorie und Entscheidungen zur Zurückziehung dokumentiert werden;

3.1.5 PIMS-Nachweise mit der Erklärung zur Anwendbarkeit und Richtlinienzuordnungen zu verknüpfen;

3.1.6 den Zugriff auf PIMS-Dokumente und Nachweisaufzeichnungen zu steuern;

3.1.7 die mehrsprachige Versionskontrolle von Richtlinien und Nachweisen zu unterstützen;

3.1.8 den rechtzeitigen Abruf von Auditnachweisen zu ermöglichen;

3.1.9 unnötige Bürokratie bei der Dokumentensteuerung zu vermeiden;

3.1.10 auditbereite Aufzeichnungen für Zertifizierung, Vertrauensbildung bei Kunden und kontinuierliche Verbesserung aufzubewahren.

4. Richtlinienaussagen

4.1 Steuerung dokumentierter PIMS-Informationen

4.1.1 [All] Privacy Lead / PIMS Manager MUSS vor der ersten PIMS-Veröffentlichung und danach vierteljährlich einen Index dokumentierter PIMS-Informationen in REG12 pflegen.

4.1.2 [All] Process Owner / Business Owner MUSS vor Beginn der Verarbeitungstätigkeit und danach jährlich die für jede eigene PII-Verarbeitungstätigkeit erforderliche dokumentierte Information in REG02 identifizieren.

4.1.3 [All] Privacy Lead / PIMS Manager MUSS vor jeder Richtlinienfreigabe und innerhalb von 15 Arbeitstagen nach jeder wesentlichen Änderung der Anwendbarkeit von Kontrollen die anwendbaren PIMS-Richtlinien, Kontrollen und Nachweispflichten mit REG03 verknüpfen.

4.1.4 [All] Privacy Lead / PIMS Manager MUSS jeder Kategorie dokumentierter PIMS-Informationen in REG12 eine Zugriffsstufe und Sensitivitätsklassifizierung für Nachweise zuweisen, bevor die Kategorie verwendet wird.

4.2 Erstellung, Genehmigung, Versionierung und Veröffentlichung

4.2.1 [All] Privacy Lead / PIMS Manager MUSS vor der Veröffentlichung dokumentierter PIMS-Informationen in REG12 eine Dokumentenkennung, einen Verantwortlichen, eine Versionsnummer, einen Genehmigungsstatus, ein Wirksamkeitsdatum und ein Überprüfungsdatum zuweisen.

4.2.2 [All] Top Management MUSS Kernrichtlinien des PIMS und wesentliche Richtlinienänderungen vor der Veröffentlichung in REG12 genehmigen.

4.2.3 [All] Privacy Lead / PIMS Manager MUSS PIMS-Nachweisvorlagen oder eingebettete Registerabschnitte vor der operativen Nutzung in REG12 genehmigen.

4.2.4 [All] Privacy Lead / PIMS Manager MUSS vor der Freigabe aktualisierter dokumentierter PIMS-Informationen die Versionshistorie und die Begründung für Änderungen in REG12 aufzeichnen.

4.2.5 [All] Privacy Lead / PIMS Manager MUSS die Kommunikation genehmigter Änderungen dokumentierter PIMS-Informationen innerhalb von 30 Tagen nach Veröffentlichung in REG11 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 Ausnahmen für dokumentierte Information oder Nachweissteuerung in REG12 beantragen, bevor von dieser Richtlinie abgewichen wird.

9.1.2 [All] Privacy Lead / PIMS Manager MUSS jede Ausnahme für dokumentierte Information oder Nachweissteuerung innerhalb von 10 Arbeitstagen nach Antragstellung in REG12 bewerten.

9.1.3 [All] Data Protection Officer / Privacy Advisor MUSS vor der Genehmigung jeder Ausnahme, die die Offenlegung von PII-Nachweisen, Übersetzungsabweichungen, Aufbewahrungskonflikte oder Beschränkungen von Auditnachweisen betrifft, Beratung in REG12 aufzeichnen.

9.1.4 [All] Top Management MUSS Ausnahmen zu dokumentierter Information, die 30 Tage überschreiten oder Zertifizierung, risikoreiche Verarbeitung oder externe Vertrauensbildung betreffen, in REG12 genehmigen, bevor die Ausnahme wirksam wird.

9.1.5 [All] Privacy Lead / PIMS Manager MUSS für jede genehmigte Ausnahme zu dokumentierter Information oder Nachweissteuerung in REG12 ein Ablaufdatum festlegen, das 90 Tage nicht überschreitet.

9.1.6 [All] Privacy Lead / PIMS Manager MUSS jede Ausnahme zu dokumentierter Information oder Nachweissteuerung innerhalb von fünf Arbeitstagen nach Ablauf in REG12 schließen oder neu bewerten.

10. Durchsetzung

10.1.1 [All] Privacy Lead / PIMS Manager MUSS fehlende, unrichtige, ungesteuerte, veraltete oder nicht abrufbare dokumentierte PIMS-Informationen innerhalb von fünf Arbeitstagen nach Identifizierung als Nichtkonformität in REG12 aufzeichnen.

10.1.2 [All] Privacy Lead / PIMS Manager MUSS die Veröffentlichung dokumentierter PIMS-Informationen verhindern, wenn erforderliche Genehmigungs-, Versions-, Verantwortlichen- oder Wirksamkeitsdatumsnachweise in REG12 fehlen.

10.1.3 [All] Process Owner / Business Owner MUSS die Einreichung von Verarbeitungsnachweisen für Audits verhindern, wenn erforderliche Nachweise zu Verantwortlichem, Datum, Status oder Genehmigung in REG02 fehlen.

10.1.4 [All] System Owner / Application Owner MUSS unbefugten Zugriff auf Repositories dokumentierter PIMS-Informationen entfernen und die Entfernung innerhalb eines Arbeitstages nach Identifizierung in REG12 aufzeichnen.

10.1.5 [All] Internal Audit / Compliance Reviewer MUSS die Wirksamkeit von Korrekturmaßnahmen für Nichtkonformitäten dokumentierter Information beim nächsten geplanten Audit oder innerhalb von 60 Tagen nach Abschluss, je nachdem, was zuerst eintritt, in REG12 verifizieren.

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 der Anforderungen an dokumentierte PIMS-Informationen überprüfen.

11.1.2 [All] Privacy Lead / PIMS Manager MUSS diese Richtlinie innerhalb von 30 Tagen nach einer wesentlichen Auditfeststellung, Zertifizierungsnichtkonformität, Änderung der Repository-Plattform oder Änderung des Prozesses für mehrsprachige Veröffentlichungen überprüfen.

11.1.3 [All] Data Protection Officer / Privacy Advisor MUSS datenschutzrelevante Änderungen an dieser Richtlinie vor der Genehmigung in REG12 überprüfen.

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

11.1.5 [All] Privacy Lead / PIMS Manager MUSS die Kommunikation genehmigter Änderungen an dieser Richtlinie innerhalb von 30 Tagen nach Veröffentlichung in REG11 aufzeichnen.

12. Zugehörige Richtlinien

12.1 Diese Richtlinie wird durch die folgenden zugehörigen Richtlinien unterstützt:

12.2 PII01 - Richtlinie zum Datenschutz-Informationsmanagementsystem

12.3 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht

12.4 PII03 - Richtlinie zum PII-Verarbeitungsinventar und zur Rechtsgrundlage

12.5 PII04 - Richtlinie zu Datenschutzhinweis und Transparenz

12.6 PII05 - Richtlinie zum Management von Einwilligungen und Präferenzen

12.7 PII06 - Richtlinie zum Management der Rechte betroffener Personen

12.8 PII07 - Richtlinie zu Datenschutz-Risikobeurteilung und DPIA

12.9 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

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

12.11 PII10 - Richtlinie zur Aufbewahrung, Löschung und Entsorgung von PII

12.12 PII11 - Richtlinie zu Richtigkeit und Qualität von PII

12.13 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Drittparteien

12.14 PII13 - Richtlinie zur internationalen Übermittlung von PII

12.15 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle

12.16 PII15 - Richtlinie zum Management von PII-Vorfällen und Verletzungen des Schutzes personenbezogener Daten

12.17 PII16 - Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz

12.18 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 6.1.3** - Zugeordnet zur Pflege der PIMS-Erklärung zur Anwendbarkeit, der Aufzeichnungen zur Anwendbarkeit von Kontrollen und der Verknüpfung von Richtlinien mit Nachweisen. Addressed by clauses [4.1.3; 4.3.3; 6.1.3; 7.1.2].

13.2.2 **Clause 7.5** - Zugeordnet zur Identifizierung dokumentierter Information, Genehmigung, Versionskontrolle, Zugriff, Abruf, Aufbewahrung, Zurückziehung, Verknüpfung von Übersetzungsversionen und Aufbewahrungsmetadaten. Addressed by clauses [4.1.1; 4.1.4; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.5; 4.4.1; 4.4.2; 4.4.4; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.1; 4.6.2; 4.6.3; 4.6.4].

13.2.3 **Clause 8.1** - Zugeordnet zu Nachweisen für operative Planung und Steuerung in Bezug auf Verarbeitungsaufzeichnungen, Nachweisvorlagen, Qualität operativer Nachweise und extern bereitgestellte Nachweise. Addressed by clauses [4.1.2; 4.2.3; 4.3.2; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1** - Zugeordnet zur Pflege dokumentierter Nachweise zu Messung, Abrufleistung, Nachweislücken, Übersetzungsabweichungen und Abschluss der Überprüfung des Repository-Zugriffs. Addressed by clauses [8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6].

13.2.5 **Clause 9.2** - Zugeordnet zum Abruf von Auditnachweisen, zu Auditstichproben, zur Nachvollziehbarkeit von Auditnachweisen und zu Auditfeststellungen im Zusammenhang mit der Steuerung dokumentierter Information. Addressed by clauses [4.3.4; 4.4.4; 6.1.3; 8.1.3; 10.1.5].

13.2.6 **Clause 9.3** - Zugeordnet zu Nachweisen der Managementbewertung, der Berücksichtigung der Steuerung dokumentierter Information in der Managementbewertung und der Überprüfung der Leistung der Nachweissteuerung durch Top Management. Addressed by clauses [6.1.2; 8.1.1; 8.1.2; 11.1.4].

13.2.7 **Clause 10.2** - Zugeordnet zu Nichtkonformitäten dokumentierter Information, Korrekturmaßnahmen, Ausnahmebehandlung, Abschluss und Wirksamkeitsverifizierung. Addressed by clauses [4.3.4; 6.1.4; 9.1.1; 9.1.2; 9.1.4; 9.1.5; 9.1.6; 10.1.1; 10.1.5].

13.2.8 **Annex A.1.2.9** - Zugeordnet zu Verarbeitungsaufzeichnungen des Verantwortlichen, Aufzeichnungen zur Rechenschaftspflicht, Qualität von Verarbeitungsnachweisen und Aufbewahrung von Nachweisen zur Unterstützung der Pflichten des Verantwortlichen. Addressed by clauses [4.1.2; 4.3.2; 4.5.1; 7.1.3].

13.2.9 **Annex A.2.2.2** - Zugeordnet zu Auftragsverarbeitervereinbarung, Kundenweisung, extern bereitgestellten Nachweisen und Steuerung von Nachweisen zur Auftragsverarbeiterbeziehung. Addressed by clauses [5.1.7; 7.1.4].

13.2.10 **Annex A.3.14** - Zugeordnet zum Schutz von PIMS-Aufzeichnungen gegen Verlust, unbefugte Änderung, unbefugten Zugriff, unbefugte Freigabe und unsachgemäße Entsorgung. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.2; 4.5.4; 4.5.5; 10.1.4].

13.3 GDPR

13.3.1 **Article 5(2)** - Zugeordnet zu Nachweisen zur Rechenschaftspflicht, Nachvollziehbarkeit von Nachweisen, Nachweisabruf, Nichtkonformitätsaufzeichnungen und auditbereiten Aufzeichnungen, die Einhaltung darlegen. Addressed by clauses [4.1.1; 4.3.2; 4.3.3; 4.4.4; 4.5.4; 6.1.3; 8.1.3; 10.1.1].

13.3.2 **Article 24** - Zugeordnet zu Governance-Nachweisen des Verantwortlichen, Genehmigungsaufzeichnungen, Richtliniensteuerung, Maßnahmen zur Rechenschaftspflicht, dokumentierter Überprüfung und Aufsicht durch Top Management. Addressed by clauses [4.2.2; 4.3.3; 6.1.2; 9.1.4; 11.1.4].

13.3.3 **Article 28** - Zugeordnet zur Dokumentation von Auftragsverarbeitern und Unterauftragsverarbeitern, zu Nachweisen von Kundenweisungen, extern bereitgestellten Prozessnachweisen und Steuerung der Offenlegung von Nachweisen. Addressed by clauses [4.4.5; 5.1.7; 7.1.4].

13.3.4 **Article 30** - Zugeordnet zu Nachweisen für Verarbeitungsaufzeichnungen, Qualitätsanforderungen an Nachweise, Referenzen zu Verarbeitungstätigkeiten und Metadaten zu Verantwortlichem und Status von Verarbeitungsnachweisen. Addressed by clauses [4.1.2; 4.3.2; 7.1.3; 10.1.3].

13.3.5 **Article 32** - Zugeordnet zum Schutz von Nachweis-Repositories, Zugriffsbeschränkungen, Zugriffsgenehmigungen, Überprüfung des Repository-Schutzes und Entfernung unbefugter Zugriffe. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Zugeordnet zu Nachweisen der Einhaltung im Datenschutz, Abruf von Auditnachweisen, Nachvollziehbarkeit von Nachweisen, Unterstützung unabhängiger Überprüfung und Nachweisen zu Korrekturmaßnahmen. Addressed by clauses [4.3.3; 4.4.4; 4.6.3; 6.1.3; 8.1.3; 10.1.5].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.1.4** - Zugeordnet zum Schutz PII-bezogener Aufzeichnungen, zur Aufbewahrung von Aufzeichnungen sowie zu Zugriffskontrollen und Löschkontrollen für Nachweis-Repositories. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.5.2; 4.5.5; 10.1.4].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 7.5** - Zugeordnet zur Identifizierung dokumentierter Information, Genehmigung, Verfügbarkeit, Schutz, Versionskontrolle, Aufbewahrung, Disposition und Steuerung extern erforderlicher dokumentierter Information. Addressed by clauses [4.1.1; 4.2.1; 4.2.4; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.5.3; 4.6.1; 4.6.2; 4.6.4].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.33 - Zugeordnet zum Schutz von PIMS-Aufzeichnungen gegen Verlust, Zerstörung, Fälschung, unbefugten Zugriff, unbefugte Freigabe und unsachgemäße Entsorgung. Addressed by clauses [4.1.4; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 10.1.4].

13.7.2 Control 5.34 - Zugeordnet zum Schutz der Privatsphäre und von PII in dokumentierter Information, Nachweis-Repositories, Offenlegungen und zugriffsgesteuerten Aufzeichnungen. Addressed by clauses [4.1.4; 4.4.2; 4.4.3; 4.4.5; 4.5.5; 6.1.5].