					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII18					Dokumenttitel: **Richtlinie zur PIMS-Überwachung, zu Audits und zur Verbesserung**							
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**

Rechtlicher Hinweis (Urheberrecht und Nutzungsbeschränkungen)

(C) 2025 Clarysec LLC. All rights reserved.

Dieses Dokument ist geistiges Eigentum der Clarysec LLC. Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Genehmigung für kommerzielle oder Implementierungszwecke kopiert, wiederverwendet, verbreitet oder verändert werden.
Die unbefugte Nutzung ist streng untersagt und kann rechtliche Schritte nach sich ziehen.
Für Lizenzierungsanfragen kontaktieren Sie bitte: info@clarysec.com

Ausgerichtet an Standards und Vorschriften

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 6.2	Both	Supporting	Messung der Datenschutzziele
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentierte Information zu Überwachung, Audit und Verbesserung
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Überwachung der operativen Planung und Steuerung
ISO/IEC 27701:2025	Clause 9.1	Both	Primary	Überwachung, Messung, Analyse 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.1.2.9	Controller	Supporting	Verarbeitungsaufzeichnungen des Verantwortlichen, die für Audits verwendet werden
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Nachweise zu Vereinbarungen mit Auftragsverarbeitern und zur Auditkooperation
GDPR	Article 5(2)	Controller	Supporting	Nachweise zur Rechenschaftspflicht
GDPR	Article 24	Controller	Supporting	Maßnahmen des Verantwortlichen und Überprüfung der Wirksamkeit
GDPR	Article 28	Both	Supporting	Governance für Audits und Kooperation von Auftragsverarbeitern
GDPR	Article 30	Both	Supporting	Verarbeitungsaufzeichnungen, die für Audits verwendet werden
GDPR	Article 32	Both	Supporting	Testen und Bewerten von Sicherheitsmaßnahmen
GDPR	Article 39	Conditional	Supporting	Überwachung und Auditberatung durch den DPO, soweit anwendbar

ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Datenschutzkonformität, Audit und unabhängige Aufsicht
ISO/IEC 29151:2022	Clause 18.2.2; Clause 18.2.3; Clause 18.2.4	Both	Supporting	Überprüfung des PII-Schutzes und Konformitätsprüfungen
ISO/IEC 27001:2022	Clause 9.1	Both	Supporting	Überwachung und Bewertung der Informationssicherheit
ISO/IEC 27001:2022	Clause 9.2	Both	Supporting	Unterstützung interner ISMS-Audits
ISO/IEC 27001:2022	Clause 9.3	Both	Supporting	Unterstützung der ISMS-Managementbewertung
ISO/IEC 27001:2022	Clause 10.1	Both	Supporting	Unterstützung der kontinuierlichen Verbesserung des ISMS
ISO/IEC 27001:2022	Clause 10.2	Both	Supporting	Unterstützung bei Nichtkonformitäten und Korrekturmaßnahmen im ISMS
ISO/IEC 27002:2022	Control 5.35	Both	Supporting	Unabhängige Überprüfung der Informationssicherheit
ISO/IEC 27002:2022	Control 5.36	Both	Supporting	Überprüfung der Einhaltung von Richtlinien und Standards
ISO 19011:2018	Clause 4; Clause 5; Clause 6; Clause 7	Both	Supporting	Grundsätze, Programm, Durchführung und Kompetenz für Managementsystemaudits

1. Geltungsbereich

1.1 Diese Richtlinie definiert die Anforderungen der Organisation an PIMS-Überwachung, Messung, Analyse, Bewertung, internes Audit, Managementbewertung, Behandlung von Nichtkonformitäten, Korrekturmaßnahmen und kontinuierliche Verbesserung.

1.2 Diese Richtlinie gilt für Folgendes:

1.2.1 alle PIMS-Prozesse, Kontrollen, Richtlinien, Register, Nachweisobjekte, Systeme, Lieferanten, Auftragsverarbeiter, Unterauftragsverarbeiter und Vereinbarungen zur Datenweitergabe innerhalb des PIMS-Geltungsbereichs;

1.2.2 die Kontexte der Organisation als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter;

1.2.3 die konsolidierte Überwachung der PIMS-Leistung, Datenschutzziele, des Umsetzungsstatus der Kontrollen, der Audit-Feststellungen, Nichtkonformitäten, Korrekturmaßnahmen, Maßnahmen aus der Managementbewertung und Verbesserungsmaßnahmen;

1.2.4 in REG12 aufbewahrte Nachweise sowie unterstützende Quellnachweise, die in REG01 bis REG11 aufbewahrt werden.

1.3 Diese Richtlinie ersetzt nicht die in anderen PIMS-Richtlinien definierten Anforderungen an die operative Überwachung. Sie legt den konsolidierten Zyklus zur Leistungsbewertung, zum Audit, zur Überprüfung und zur Verbesserung des PIMS fest.

1.4 Für diese Richtlinie bedeutet eine wesentliche PIMS-Nichtkonformität ein Versagen, das den PIMS-Geltungsbereich, Datenschutzziele, die Rechenschaftspflicht für PII-Verarbeitung, die Datenschutz-Risikobehandlung, Rechte betroffener Personen, die Sicherheit der Verarbeitung, die Governance für Auftragsverarbeiter oder Unterauftragsverarbeiter, die Bereitschaft zur Behandlung von Datenschutzverletzungen, die Integrität dokumentierter Nachweise, den Geltungsbereich der Zertifizierung oder das wiederholte Versagen derselben Anforderung innerhalb eines Zeitraums von 12 Monaten wesentlich beeinträchtigt.

1.5 Für diese Richtlinie bedeutet eine wesentliche Änderung jede Änderung, die den PIMS-Geltungsbereich, Zwecke der PII-Verarbeitung, PII-Kategorien, Kategorien betroffener Personen, Verarbeitungsorte, die Zuweisung der Rollen als Verantwortlicher oder Auftragsverarbeiter, die Systemarchitektur, Lieferanten- oder Unterauftragsverarbeitervereinbarungen, das Datenschutz-Risikoprofil, anwendbare gesetzliche oder vertragliche Verpflichtungen, den Auditumfang, die Überwachungsmethode oder den Geltungsbereich der Zertifizierung betrifft.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass die Organisation die PIMS-Leistung bewertet, die PIMS-Konformität verifiziert, Nichtkonformitäten identifiziert, Kontrollschwächen korrigiert und das PIMS auf Grundlage objektiver Nachweise kontinuierlich verbessert.

2.2 Diese Richtlinie ermöglicht der Organisation nachzuweisen, dass PIMS-Überwachung, Audits, Managementbewertung und Verbesserungsaktivitäten geplant, soweit erforderlich unabhängig, nachweisbasiert, fristgerecht und bis zu verantwortlichen Rollen und kanonischen Nachweisobjekten nachvollziehbar sind.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 einen konsolidierten Prozess für PIMS-Überwachung und -Messung zu definieren;

3.1.2 sicherzustellen, dass Datenschutzziele und die Leistung der PIMS-Kontrollen anhand dokumentierter Nachweise gemessen werden;

3.1.3 ein risikobasiertes internes Auditprogramm für das PIMS einzurichten;

3.1.4 Unabhängigkeit und Objektivität bei PIMS-Audittätigkeiten zu wahren;

3.1.5 sicherzustellen, dass der Managementbewertung vollständige und aktuelle Eingaben zur PIMS-Leistung vorliegen;

3.1.6 sicherzustellen, dass Nichtkonformitäten aufgezeichnet, bewertet, korrigiert und verifiziert werden;

3.1.7 sicherzustellen, dass Korrekturmaßnahmen bis zum Abschluss verfolgt und auf Wirksamkeit überprüft werden;

3.1.8 wiederkehrende Schwächen und Verbesserungsmöglichkeiten zu identifizieren;

3.1.9 die Auditbereitschaft für Zertifizierungen und ein rechenschaftspflichtiges Nachweismanagement zu unterstützen;

3.1.10 eine Dopplung operativer Kennzahlen zu vermeiden, die bereits in zugehörigen PIMS-Richtlinien definiert sind.

4. Richtlinienaussagen

4.1 Rahmenwerk für PIMS-Überwachung und -Messung

4.1.1 [Both] The Privacy Lead / PIMS Manager MUSS das konsolidierte PIMS-Überwachungsprogramm vor dem erstmaligen PIMS-Betrieb und danach jährlich in REG12 definieren.

4.1.2 [Both] The Privacy Lead / PIMS Manager MUSS für jede PIMS-Kennzahl vor Beginn des Messzyklus die Messmethode, Häufigkeit, Nachweisquelle, Zielvorgabe und verantwortliche Rolle in REG12 definieren.

4.1.3 [Both] The Process Owner / Business Owner MUSS dem Privacy Lead / PIMS Manager vierteljährlich Eingaben zur Überwachung von PII-Verarbeitungstätigkeiten aus REG02 bereitstellen.

4.1.4 [Both] The Information Security Lead MUSS dem Privacy Lead / PIMS Manager vierteljährlich Eingaben zum Status der PII-Sicherheitskontrollen aus REG03 bereitstellen.

4.1.5 [Both] The Vendor / Procurement Owner MUSS dem Privacy Lead / PIMS Manager vierteljährlich Eingaben zum Status der Vertrauenssicherung für Auftragsverarbeiter, Unterauftragsverarbeiter, Datenweitergaben an Dritte und Lieferanten aus REG08 bereitstellen.

4.1.6 [All] The Incident Response Coordinator MUSS dem Privacy Lead / PIMS Manager monatlich und innerhalb von 10 Geschäftstagen nach Abschluss eines wesentlichen Vorfalls Eingaben zu Trends bei Datenschutzvorfällen und Verletzungen des Schutzes personenbezogener Daten aus REG10 bereitstellen.

4.1.7 [Both] The Privacy Lead / PIMS Manager MUSS die Ergebnisse der PIMS-Überwachung vierteljährlich in REG12 konsolidieren.

4.2 Internes PIMS-Auditprogramm

4.2.1 [All] The Internal Audit / Compliance Reviewer MUSS jährlich vor dem ersten geplanten PIMS-Auditzyklus ein risikobasiertes internes PIMS-Auditprogramm in REG12 erstellen.

4.2.2 [All] The Internal Audit / Compliance Reviewer MUSS für jedes PIMS-Audit vor Beginn der Audit-Feldarbeit Ziel, Kriterien, Umfang, Methode, Stichprobengrundlage und Berichtsfrist in REG12 definieren.

4.2.3 [All] The Internal Audit / Compliance Reviewer MUSS vor jeder Auditzuweisung Prüfungen der Unabhängigkeit der Auditoren und auf Interessenkonflikte in REG12 aufzeichnen.

4.2.4 [All] The Privacy Lead / PIMS Manager MUSS angeforderte gelenkte dokumentierte PIMS-Informationen und Registernachweise innerhalb von 10 Geschäftstagen nach einer genehmigten Auditanfrage über REG12 verfügbar machen.

4.2.5 [Both] The Internal Audit / Compliance Reviewer MUSS während jedes PIMS-Audits den Umsetzungsstatus anwendbarer PIMS-Kontrollen anhand von REG03 testen.

4.2.6 [Both] The Internal Audit / Compliance Reviewer MUSS während jedes PIMS-Audits die ausgewählte Stichprobe der PII-Verarbeitungsnachweise in REG12 aufzeichnen.

4.2.7 [All] The Internal Audit / Compliance Reviewer MUSS die PIMS-Auditergebnisse innerhalb von 15 Geschäftstagen nach Abschluss des Audits in REG12 aufzeichnen.

4.2.8 [All] The Privacy Lead / PIMS Manager MUSS innerhalb von 10 Geschäftstagen nach Annahme der Auditergebnisse in REG12 Verantwortliche für Korrekturmaßnahmen zu akzeptierten PIMS-Audit-Feststellungen zuweisen.

[... 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 Ausnahmen bei Überwachung, Audit und Verbesserung

9.1.1 [All] The Process Owner / Business Owner MUSS jede Ausnahme von dieser Richtlinie in REG12 beantragen, bevor die Abweichung eintritt.

9.1.2 [All] The Privacy Lead / PIMS Manager MUSS die Auswirkungen jeder beantragten Ausnahme auf Datenschutz, Zertifizierung, Audit und Korrekturmaßnahmen innerhalb von 10 Geschäftstagen nach Antragstellung in REG12 bewerten.

9.1.3 [All] The Data Protection Officer / Privacy Advisor MUSS vor Genehmigung jeder Ausnahme, die gesetzliche Verpflichtungen, Rechte betroffener Personen, DPIA-Zusagen, Kundenauditverpflichtungen oder risikoreiche Verarbeitung betrifft, Beratung in REG12 aufzeichnen.

9.1.4 [All] Top Management MUSS Ausnahmen, die den Abschluss des Auditplans, die Managementbewertung, wesentliche Nichtkonformitäten, den Geltungsbereich der Zertifizierung oder risikoreiche Verarbeitung betreffen, in REG12 genehmigen, bevor die Ausnahme wirksam wird.

9.1.5 [All] The Privacy Lead / PIMS Manager MUSS für jede genehmigte Ausnahme bei Überwachung, Audit oder Verbesserung in REG12 ein Ablaufdatum festlegen, das 90 Tage nicht überschreitet.

9.1.6 [All] The Privacy Lead / PIMS Manager MUSS jede Ausnahme bei Überwachung, Audit oder Verbesserung innerhalb von fünf Geschäftstagen nach Ablauf in REG12 schließen oder neu bewerten.

10. Durchsetzung

10.1 Durchsetzung der Anforderungen an Überwachung, Audit und Verbesserung

10.1.1 [All] The Privacy Lead / PIMS Manager MUSS einen versäumten Überwachungszyklus, ein versäumtes PIMS-Audit, eine überfällige Managementbewertung, fehlende Auditnachweise, eine überfällige Korrekturmaßnahme oder eine überfällige Verbesserungsmaßnahme innerhalb von fünf Geschäftstagen nach Identifizierung als Nichtkonformität in REG12 aufzeichnen.

10.1.2 [All] The Internal Audit / Compliance Reviewer MUSS den Schweregrad von Audit-Feststellungen vor Herausgabe des Auditberichts in REG12 aufzeichnen.

10.1.3 [All] Top Management MUSS für jede wesentliche PIMS-Nichtkonformität innerhalb von 10 Geschäftstagen nach Eskalation in REG12 eine Korrekturmaßnahme verlangen.

10.1.4 [All] The Process Owner / Business Owner MUSS die Produktivsetzung oder Einreichung externer Vertrauenssicherung für risikoreiche Verarbeitung verhindern, wenn erforderliche

Nachweise zu Korrekturmaßnahmen vor der Produktivsetzung oder Einreichung in REG12 fehlen.

10.1.5 [All] The Privacy Lead / PIMS Manager MUSS wiederholt versäumte Fristen für Überwachung oder Korrekturmaßnahmen innerhalb von fünf Geschäftstagen nach dem zweiten Auftreten in einem Zeitraum von 12 Monaten in REG12 an Top Management eskalieren.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUSS den Abschluss von Durchsetzungsmaßnahmen beim nächsten geplanten Audit oder innerhalb von 60 Tagen nach gemeldetem Abschluss in REG12 verifizieren, je nachdem, was zuerst eintritt.

11. Überprüfung und Pflege

11.1 Überprüfung und Pflege der Richtlinie

11.1.1 [All] The Privacy Lead / PIMS Manager MUSS diese Richtlinie jährlich und innerhalb von 30 Tagen nach einer wesentlichen Änderung der Anforderungen an PIMS-Überwachung, Audit, Managementbewertung, Korrekturmaßnahmen oder Zertifizierung in REG12 überprüfen.

11.1.2 [All] The Internal Audit / Compliance Reviewer MUSS die Wirksamkeit des PIMS-Auditprogramms jährlich nach dem letzten geplanten Audit für das PIMS-Betriebsjahr in REG12 überprüfen.

11.1.3 [All] The 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] The Privacy Lead / PIMS Manager MUSS REG01 und REG03 innerhalb von 15 Geschäftstagen nach genehmigten Änderungen an dieser Richtlinie aktualisieren, die den PIMS-Geltungsbereich oder die Anwendbarkeit von Kontrollen ändern.

11.1.6 [All] The 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 Verzeichnis der PII-Verarbeitung und zur Rechtsgrundlage

12.5 PII04 - Richtlinie zu Datenschutzhinweis und Transparenz

12.6 PII05 - Richtlinie zum Einwilligungs- und Präferenzmanagement

12.7 PII06 - Richtlinie zum Management der Rechte betroffener Personen

12.8 PII07 - Richtlinie zur 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 personenbezogener Daten

12.11 PII10 - Richtlinie zur Aufbewahrung, Löschung und Entsorgung personenbezogener Daten

12.12 PII11 - Richtlinie zur Richtigkeit und Qualität personenbezogener Daten

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

12.14 PII13 - Richtlinie zur internationalen Übermittlung personenbezogener Daten

12.15 PII14 - Richtlinie zur PII-Sicherheit und Zugriffskontrolle

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

12.17 PII16 - Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz

12.18 PII17 - Richtlinie zu dokumentierten PIMS-Informationen und Nachweismanagement

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 diese umsetzen oder unterstützen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.2** - Zugeordnet zur Definition, Messung, Berichterstattung und Überprüfung von PIMS-Zielen und PIMS-Leistungskennzahlen. Addressed by clauses [4.1.2; 4.3.4; 8.1.1].

13.2.2 **Clause 7.5** - Zugeordnet zur Pflege dokumentierter Informationen zu Überwachungsergebnissen, Auditprogrammen, Auditergebnissen, Nachweisen der Managementbewertung, Nichtkonformitäten, Korrekturmaßnahmen und Verbesserungsmaßnahmen. Addressed by clauses [4.1.7; 4.2.4; 4.2.7; 4.3.1; 4.4.1; 7.1.8; 11.1.1].

13.2.3 **Clause 8.1** - Zugeordnet zum Betrieb des geplanten Zyklus für PIMS-Überwachung, Audit, Korrekturmaßnahmen und Verbesserung als Teil der operativen PIMS-Steuerung. Addressed by clauses [4.1.1; 4.2.1; 7.1.1; 7.1.6].

13.2.4 **Clause 9.1** - Zugeordnet zur Definition dessen, was überwacht und gemessen wird, zur Konsolidierung von Überwachungsergebnissen, zur Bewertung der PIMS-Leistung und zur Pflege von Messnachweisen. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.1.7; 8.1.1; 8.1.2; 8.1.4; 8.1.7].

13.2.5 **Clause 9.2** - Zugeordnet zur Pflege des internen Auditprogramms, Auditplanung, Prüfungen der Unabhängigkeit der Auditoren, Nachweisstichproben, Auditergebnissen und Nachverfolgung von Audit-Feststellungen. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 8.1.3; 10.1.2].

13.2.6 **Clause 9.3** - Zugeordnet zur Planung der Managementbewertung, Überprüfung der PIMS-Leistung, Überprüfung von Audit- und Korrekturmaßnahmentrends, Genehmigung von Ergebnissen und Ressourcenentscheidungen. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 6.1.7].

13.2.7 **Clause 10.1** - Zugeordnet zur Identifizierung, Genehmigung, Umsetzung und Nachverfolgung von Möglichkeiten zur kontinuierlichen Verbesserung der Eignung, Angemessenheit und Wirksamkeit des PIMS. Addressed by clauses [4.3.7; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 7.1.6].

13.2.8 **Clause 10.2** - Zugeordnet zur Aufzeichnung von Nichtkonformitäten, Ursachenanalyse, Planung von Korrekturmaßnahmen, Umsetzung von Korrekturmaßnahmen, Wirksamkeitsverifizierung, Eskalation und Durchsetzung. Addressed by clauses [4.2.8; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 10.1.1; 10.1.3; 10.1.6].

13.2.9 **Annex A.1.2.9** - Zugeordnet zu Verarbeitungsaufzeichnungen des Verantwortlichen, die als Nachweisquellen für Überwachung, Auditstichproben und Kennzahlen zur Aktualität des Verarbeitungsinventars verwendet werden. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.2.10 **Annex A.2.2.2** - Zugeordnet zu Nachweisen zu Vereinbarungen mit Auftragsverarbeitern, Kundenaudits, Antworten zur Vertrauenssicherung und Kooperation von Auftragsverarbeitern,

die über Prozesse zur Lieferanten- und Kundenvertrauenssicherung nachverfolgt werden. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3 GDPR

13.3.1 **Article 5(2)** - Zugeordnet zu Nachweisen der Rechenschaftspflicht für Überwachung, Audit, Managementbewertung, Korrekturmaßnahmen und kontinuierliche Verbesserung. Addressed by clauses [4.1.7; 4.2.7; 4.3.2; 4.4.2; 4.5.1].

13.3.2 **Article 24** - Zugeordnet zu Governance-Maßnahmen des Verantwortlichen, Wirksamkeitsüberprüfung, Managementbewertung, Korrekturmaßnahmen und dokumentierten Verbesserungsnachweisen. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.5.2; 10.1.3].

13.3.3 **Article 28** - Zugeordnet zu Nachweisen zu Auftragsverarbeitern, Unterauftragsverarbeitern, Kundenaudits, Vertrauenssicherung durch Dritte und Lieferantenkooperation. Addressed by clauses [4.1.5; 5.1.7; 7.1.5; 8.1.8].

13.3.4 **Article 30** - Zugeordnet zu Verarbeitungsaufzeichnungen, die als Nachweise für Überwachung, Auditstichproben, Vollständigkeit von Nachweisobjekten und Aktualität des Verarbeitungsinventars verwendet werden. Addressed by clauses [4.1.3; 4.2.6; 8.1.7].

13.3.5 **Article 32** - Zugeordnet zur Überwachung und Bewertung des Status von PII-Sicherheitskontrollen, technischen Kontrollnachweisen und sicherheitsbezogenen Wirksamkeitsnachweisen. Addressed by clauses [4.1.4; 4.2.5; 5.1.4; 7.1.4; 8.1.2].

13.3.6 **Article 39** - Zugeordnet zu Datenschutzberatung, Überwachungsbeobachtungen, Auditunterstützung und Überprüfung von Trends der Einhaltung von Datenschutzanforderungen durch the Data Protection Officer / Privacy Advisor, soweit anwendbar. Addressed by clauses [5.1.3; 6.1.6; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.12** - Zugeordnet zur Verifizierung der Einhaltung von Datenschutzanforderungen, internen oder unabhängigen Audits, internen Kontrollen, Aufsichtsmechanismen und Nachweisen zur Datenschutz-Risikobeurteilung. Addressed by clauses [4.2.1; 4.2.3; 4.2.7; 4.5.1; 6.1.6; 8.1.7].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 18.2.2; Clause 18.2.3; Clause 18.2.4** - Zugeordnet zur unabhängigen Überprüfung der PII-bezogenen Informationssicherheit, zur Einhaltung von Richtlinien und Standards sowie zur technischen Konformitätsprüfung für den PII-Schutz. Addressed by clauses [4.2.3; 4.2.5; 7.1.4; 8.1.2; 10.1.6].

13.6 ISO/IEC 27001:2022

13.6.1 **Clause 9.1** - Zugeordnet zu Eingaben aus der Überwachung und Bewertung der Informationssicherheit, die die PIMS-Leistungsmessung und den Status der PII-Sicherheitskontrollen unterstützen. Addressed by clauses [4.1.4; 8.1.2].

13.6.2 **Clause 9.2** - Zugeordnet zur Unterstützung interner ISMS-Audits für PIMS-Auditplanung, Auditnachweise, Auditergebnisse und Abschluss des Auditprogramms. Addressed by clauses [4.2.1; 4.2.2; 4.2.7; 8.1.3].

13.6.3 **Clause 9.3** - Zugeordnet zu Eingaben und Ergebnissen der Managementbewertung für eine integrierte Aufsicht über PIMS- und Informationssicherheitsleistung. Addressed by clauses [4.3.1; 4.3.2; 4.3.5; 4.3.6].

13.6.4 **Clause 10.1** - Zugeordnet zur kontinuierlichen Verbesserung des PIMS und der unterstützenden Kontrollumgebung der Informationssicherheit. Addressed by clauses [4.5.1; 4.5.2; 4.5.6].

13.6.5 **Clause 10.2** - Zugeordnet zur Behandlung von Nichtkonformitäten, Planung von Korrekturmaßnahmen, Umsetzung von Korrekturmaßnahmen und Wirksamkeitsverifizierung. Addressed by clauses [4.4.2; 4.4.4; 4.4.6; 4.4.7; 10.1.1].

13.7 ISO/IEC 27002:2022

13.7.1 Control 5.35 - Zugeordnet zur unabhängigen Überprüfung, zu Prüfungen der Unabhängigkeit der Auditoren, zum Testen von Auditnachweisen und zur unabhängigen Verifizierung der Wirksamkeit von Korrekturmaßnahmen. Addressed by clauses [4.2.3; 4.2.5; 4.4.7; 10.1.6].

13.7.2 Control 5.36 - Zugeordnet zur Konformitätsprüfung von PIMS- und Informationssicherheitsrichtlinien, zum Umsetzungsstatus von Kontrollen und zu Nachweisen der Normenkonformität. Addressed by clauses [4.1.4; 4.2.5; 4.5.3; 8.1.2].

13.8 ISO 19011:2018

13.8.1 **Clause 4; Clause 5; Clause 6; Clause 7** - Zugeordnet zu Auditgrundsätzen, Management des Auditprogramms, Auditdurchführung, nachweisbasierter Auditberichterstattung, Audit-Follow-up und Kompetenzerwartungen an Auditoren für PIMS-Audits. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.6; 4.2.7; 4.4.7; 5.1.9; 11.1.2].