					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII23					Dokumenttitel: **Richtlinie für Cloud-PII-Auftragsverarbeiter**							
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 4.1; Clause 6.1.3	Processor	Supporting	PIMS-Rolle und Anwendbarkeit von Kontrollen
ISO/IEC 27701:2025	Clause 7.5; Clause 8.1	Processor	Primary	Dokumentierte Nachweise für Cloud-Auftragsverarbeiter und operative Kontrolle
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Processor	Supporting	Überwachung, Nichtkonformität und Korrekturmaßnahme
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Kundenvereinbarungen, Weisungen, Unterstützung und Aufzeichnungen
ISO/IEC 27701:2025	Annex A.2.3.2	Processor	Primary	Kundenunterstützung für Verpflichtungen gegenüber betroffenen Personen
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Primary	Temporäre Dateien, Rückgabe, Übertragung, Entsorgung und Übermittlungskontrollen
ISO/IEC 27701:2025	Annex A.2.5.2; Annex A.2.5.3	Processor	Supporting	Übermittlungsgrundlage und Orte
ISO/IEC 27701:2025	Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Offenlegungsaufzeichnungen und Bearbeitung von Offenlegungsersuchen
ISO/IEC 27701:2025	Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9	Processor	Primary	Offenlegung, Beauftragung und Änderungsmitteilung zu Unterauftragsverarbeitern
ISO/IEC 27701:2025	Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25	Processor	Supporting	Nachweise zu Zugriff, Aufzeichnungen, Backup und Protokollierung
GDPR	Article 28	Processor	Primary	Auftragsverarbeiter, Unterauftragsverarbeiter, Unterstützung, Audit, Löschung und Rückgabe
GDPR	Article 30	Processor	Supporting	Aufzeichnungen von Auftragsverarbeitern

GDPR	Article 32; Article 33	Processor	Supporting	Sicherheit und Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen
GDPR	Article 44	Conditional	Referenced	Steuerung internationaler Übermittlungen
ISO/IEC 29100:2020	Clause 5.3; Clause 5.5; Clause 5.6	Processor	Supporting	Zweckbindung, Minimierung, Nutzung, Aufbewahrung und Begrenzung der Offenlegung
ISO/IEC 29100:2020	Clause 5.10; Clause 5.11; Clause 5.12	Processor	Supporting	Rechenschaftspflicht, Informationssicherheit und Einhaltung
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2	Processor	Supporting	Bewertung, Überwachung, Änderung und Aufbewahrungskontrollen für Auftragsverarbeiter
ISO/IEC 27001:2022	Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23	Processor	Supporting	Anwendbarkeit von Kontrollen, operative Kontrolle und Lieferanten-/Cloud-Kontrollen
ISO/IEC 27002:2022	Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16	Processor	Supporting	Lieferanten-, Cloud-, Lösch-, Protokollierungs- und Überwachungskontrollen
ISO/IEC 27018:2020	Annex A.2.1; Annex A.3.1	Processor	Primary	Kundenunterstützung durch Cloud-Auftragsverarbeiter und Zweckbindung
ISO/IEC 27018:2020	Annex A.6.1; Annex A.6.2; Annex A.8.1	Processor	Primary	Cloud-Offenlegungsmitteilung, Offenlegungsaufzeichnungen und Transparenz zu Unterauftragsverarbeitern
ISO/IEC 27018:2020	Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1	Processor	Primary	Cloud-Schnittstelle für Verletzungen des Schutzes personenbezogener Daten, Exit, Vertragsmaßnahmen, Unteraufträge und Standortaufzeichnungen
ISO/IEC 27036-2:2022	Clause 6.1.1; Clause 6.1.2	Processor	Supporting	Strategie und Governance für Lieferbeziehungen

ISO/IEC 27036-2:2022	Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5	Processor	Supporting	Planung, Vereinbarung, Management, Überwachung und Beendigung von Lieferantenbeziehungen
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Processor	Supporting	Löschrahmenwerk und Dokumentation
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Processor	Supporting	Umsetzung der Löschung und Ausnahmen

1. Geltungsbereich

1.1 Diese Richtlinie legt verbindliche Datenschutzanforderungen für Cloud-Services fest, bei denen die Organisation als PII-Auftragsverarbeiter oder Unterauftragsverarbeiter handelt, einschließlich SaaS-, PaaS-, IaaS-, gehosteter Anwendungs-, Managed-Cloud-, Cloud-Support-, Cloud-Speicher-, Cloud-Analyse- und Cloud-Infrastrukturdienste, die PII im Auftrag von Kunden verarbeiten.

1.2 Diese Richtlinie gilt für Cloud-Verarbeitung, die im Rahmen von Kundenvereinbarungen, dokumentierten Kundenweisungen, Weisungen vorgelagerter Auftragsverarbeiter, Unterauftragsverarbeitervereinbarungen, Cloud-Region-Konfiguration, Cloud-Support-Zugriff, Serviceadministration, Backup, Replikation, Protokollierung, Überwachung, Löschung, Rückgabe, Unterstützung bei Verletzungen des Schutzes personenbezogener Daten, Auditunterstützung und Unterstützungspflichten gegenüber Kunden erfolgt.

1.3 Diese Richtlinie umfasst:

1.3.1 Geltungsbereich der Cloud-PII-Verarbeitung und Weisungsaufzeichnungen;

1.3.2 Kundenvereinbarungen und Nachweise zur geteilten Verantwortung;

1.3.3 Nachweise zu Mandantentrennung, Cloud-Zugriff, administrativem Zugriff und Protokollierung;

1.3.4 Governance für Unterauftragsverarbeiter und Cloud-Lieferkette;

1.3.5 Standort, Fernzugriff und Steuerung internationaler Übermittlungen;

1.3.6 Nachweise zu Rückgabe, Übermittlung, Löschung, Entsorgung und Exit;

1.3.7 Kundenunterstützung bei Rechten betroffener Personen, DPIAs, Audits und Reaktion auf Verletzungen des Schutzes personenbezogener Daten;

1.3.8 Nachweise zu Überwachung, Ausnahme, Durchsetzung und Verbesserung.

1.4 Diese Richtlinie erstellt kein separates Kundenvertragsregister, Register für Cloud-Services, Register zur Mandantentrennung, Zugriffsregister, Protokollregister, Löschregister, Register für Supportanfragen, Auditnachweisregister, Register für Datenschutzverletzungen, Unterauftragsverarbeiterregister oder Cloud-Governance-Gremium.

1.5 Diese Richtlinie ersetzt nicht:

1.5.1 PII03 für Verarbeitungsinventar und Zuständigkeit für Rechtsgrundlagen;

1.5.2 PII06 für den vollständigen Workflow zu Rechten betroffener Personen;

1.5.3 PII07 für Datenschutzrisiko- und DPIA-Methodik;

1.5.4 PII08 für Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen;

1.5.5 PII09 für allgemeine Kontrollen zu Erhebung, Nutzung, Offenlegung und Weitergabe;

1.5.6 PII10 für die Methodik zu Aufbewahrung, Löschung und Entsorgung;

1.5.7 PII12 für allgemeine Lifecycle-Governance für Auftragsverarbeiter, Unterauftragsverarbeiter und Drittparteien;

1.5.8 PII13 für die Bewertung internationaler Übermittlungsinstrumente;

1.5.9 PII14 für die vollständige PII-Sicherheits- und Zugriffskontrollarchitektur;

1.5.10 PII15 für den Workflow zum Management von Vorfällen und Datenschutzverletzungen;

1.5.11 PII17 für die Lenkung dokumentierter Information;

1.5.12 PII18 für PIMS-Governance zu Überwachung, Audit und Verbesserung.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass Cloud-Services von PII-Auftragsverarbeitern und Unterauftragsverarbeitern auf Grundlage dokumentierter Kundenweisungen, eines klaren

Verarbeitungsumfangs, kontrollierter Unterauftragsverarbeitervereinbarungen, angemessener Cloud-Sicherheitsverantwortlichkeiten, dokumentierter Standort- und Übermittlungssteuerung, Unterstützungspflichten gegenüber Kunden, Unterstützung bei Verletzungen des Schutzes personenbezogener Daten, Fähigkeit zur Löschung/Rückgabe und auditbereiter Nachweise betrieben werden.

2.2 Diese Richtlinie unterstützt die Auditbereitschaft für Zertifizierungen nach ISO/IEC 27701:2025 PIMS für Cloud-Auftragsverarbeiter und Cloud-Unterauftragsverarbeiter und bleibt zugleich in den bestehenden PIMS-Richtliniensatz und die kanonischen Nachweisobjekte integriert.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 Den Umfang der Cloud-PII-Verarbeitung vor Kunden-Onboarding oder wesentlicher Änderung festlegen.

3.1.2 Sicherstellen, dass Kundenweisungen aufgezeichnet, überprüft und befolgt werden.

3.1.3 Nachweise für Cloud-Auftragsverarbeiter und Unterauftragsverarbeiter in kanonischen PIMS-Registern pflegen.

3.1.4 Nachweise zu geteilter Verantwortung, Mandantentrennung, Zugriff, Protokollierung und Standort festlegen, ohne die PII-Sicherheitsrichtlinie zu duplizieren.

3.1.5 Nachweise zu Onboarding, Änderung, weiterzugebenden Verpflichtungen und Überwachung von Unterauftragsverarbeitern kontrollieren.

3.1.6 Kunden bei Rechten betroffener Personen, DPIAs, Auditanfragen und Reaktion auf Verletzungen des Schutzes personenbezogener Daten unterstützen.

3.1.7 Sicherstellen, dass Nachweise zu Rückgabe, Löschung, Übermittlung und Entsorgung beim Exit aufbewahrt werden.

3.1.8 Kontrollen für Cloud-Auftragsverarbeiter überwachen und Korrekturmaßnahmen über REG12 steuern.

4. Richtlinienaussagen

4.1 Umfang der Cloud-Verarbeitung und Kundenweisungen

4.1.1 [Processor] The Privacy Lead / PIMS Manager MUSS jeden Cloud-PII-Verarbeitungsservice, die Verarbeitungsrolle des Kunden, die Quelle der Kundenweisung, PII-Kategorien, Kategorien betroffener Personen, den Servicezweck, den Verarbeitungsort, die Abhängigkeit von Unterauftragsverarbeitern, die Löschabhängigkeit und die Übermittlungskennzeichnung in REG02 und REG08 aufzeichnen, bevor ein Kunden-Onboarding oder eine wesentliche Serviceänderung erfolgt.

4.1.2 [Processor] The Process Owner / Business Owner MUSS die dokumentierten Kundenweisungen für die Cloud-PII-Verarbeitung in REG08 aufzeichnen, bevor die Verarbeitung beginnt.

4.1.3 [Subprocessor] The Process Owner / Business Owner MUSS Weisungen des vorgelagerten Auftragsverarbeiters oder vom Kunden genehmigte Weisungen in REG08 aufzeichnen, bevor PII als Cloud-Unterauftragsverarbeiter verarbeitet wird.

4.1.4 [Processor] The Privacy Lead / PIMS Manager MUSS die Anwendbarkeit von Kontrollen für Cloud-Auftragsverarbeiter in REG03 aufzeichnen, bevor ein neuer Cloud-PII-Verarbeitungsservice freigegeben oder wesentlich geändert wird.

4.1.5 [Processor] The Data Protection Officer / Privacy Advisor MUSS jede Kundenweisung, die mit dokumentierten Kundenverpflichtungen, PIMS-Anforderungen oder dem genehmigten Serviceumfang unvereinbar erscheint, in REG12 prüfen, bevor die Organisation nach der Weisung handelt.

4.1.6 [Processor] The Process Owner / Business Owner MUSS jede vorgeschlagene Verarbeitung von Kunden-PII außerhalb dokumentierter Kundenweisungen in REG12 aufzeichnen und die Genehmigung von Privacy Lead / PIMS Manager einholen, bevor die Verarbeitung erfolgt.

4.2 Cloud-Konfiguration, Mandantentrennung, Zugriff und Protokollierung

4.2.1 [Processor] The Information Security Lead MUSS die Abgrenzung der geteilten Verantwortung in der Cloud für PII-Zugriff, Administration, Protokollierung, Backup, Verschlüsselung, Schwachstellenmanagement und Löschung in REG08 aufzeichnen, bevor ein Kunden-Onboarding oder eine wesentliche Serviceänderung erfolgt.

4.2.2 [Processor] The System Owner / Application Owner MUSS Kontrollen zur Mandantentrennung oder Kundentrennung in REG12 vor Produktivnutzung und nach wesentlicher Architekturänderung validieren.

4.2.3 [Processor] The System Owner / Application Owner MUSS administrativen Cloud-Zugriff auf Kunden-PII nur gewähren, nachdem der genehmigte geschäftliche Bedarf, der Zugriffsumfang, die Zugriffsdauer und die Überprüfungshäufigkeit in REG12 aufgezeichnet wurden.

4.2.4 [Processor] The Information Security Lead MUSS privilegierten Cloud-Zugriff, Support-Zugriff, Zugriff auf Kunden-PII und Protokollabdeckung mindestens vierteljährlich in REG12 überprüfen.

4.2.5 [Processor] The System Owner / Application Owner MUSS die Trennung von Produktiv-, Staging-, Test- und Supportumgebungen für Kunden-PII vor Freigabe und nach wesentlicher Umgebungsänderung in REG12 validieren.

4.2.6 [Processor] The System Owner / Application Owner MUSS Backup-, Replikations-, Protokollspeicher- und Support-Zugriffsorte für Cloud-Kunden-PII in REG02, REG08 oder REG09 aufzeichnen, bevor diese Orte aktiviert oder geändert werden.

[... 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 [Processor] The Process Owner / Business Owner MUSS eine Ausnahme für Cloud-Auftragsverarbeiter in REG12 vor Onboarding, Freigabe, Verlängerung oder fortgesetzter Nutzung beantragen, wenn erforderliche Nachweise zu Kundenweisung, Unterauftragsverarbeiter, Standort, Zugriff, Protokollierung, Löschung oder Vorfallschnittstelle unvollständig sind.

9.2 [Processor] The Data Protection Officer / Privacy Advisor MUSS datenschutzrelevante Ausnahmeanträge für Cloud-Auftragsverarbeiter in REG12 vor Genehmigung prüfen, wenn die Ausnahme Kundenweisungen, Unterstützung betroffener Personen, Übermittlungen, Unterauftragsverarbeiter, Löschung, Unterstützung bei Verletzungen des Schutzes personenbezogener Daten oder PII mit hoher Tragweite betrifft.

9.3 [Processor] Top Management MUSS risikobehaftete oder wesentliche Ausnahmen für Cloud-Auftragsverarbeiter in REG12 genehmigen, bevor die Ausnahme wirksam wird.

9.4 [Processor] The Privacy Lead / PIMS Manager MUSS für jede genehmigte Ausnahme für Cloud-Auftragsverarbeiter vor Genehmigung ein Ablaufdatum, einen Remediation Owner, ein Überprüfungsdatum und einen Restrisikovermerk in REG12 zuweisen.

10. Durchsetzung

10.1 [Processor] The Privacy Lead / PIMS Manager MUSS Kunden-Onboarding, Servicefreigabe, Verlängerung oder fortgesetzte Verarbeitung blockieren, wenn erforderliche

Nachweise in REG02, REG03, REG08, REG09, REG10 oder REG12 fehlen, bevor die Verarbeitung beginnt oder fortgesetzt wird.

10.2 [Processor] The System Owner / Application Owner MUSS nicht genehmigten Cloud-Zugriff, nicht genehmigte Regionsnutzung, nicht genehmigte Replikation, nicht genehmigten Support-Zugriff oder nicht genehmigten Datenfluss zu Unterauftragsverarbeitern innerhalb eines Geschäftstages nach einer Durchsetzungsentscheidung deaktivieren und den Abschluss in REG08 oder REG12 aufzeichnen.

10.3 [Processor] The Vendor / Procurement Owner MUSS neue PII-Verarbeitung durch einen nicht genehmigten oder nichtkonformen Cloud-Unterauftragsverarbeiter aussetzen, bis Korrekturmaßnahmen-Nachweise in REG08 vollständig sind.

10.4 [Processor] The Incident Response Coordinator MUSS versäumte Fristen für Kundenbenachrichtigungen bei Vorfällen innerhalb eines Geschäftstages nach Feststellung in REG10 und REG12 eskalieren.

10.5 [Processor] The Internal Audit / Compliance Reviewer MUSS die Wirksamkeit von Korrekturmaßnahmen bei wesentlichen oder wiederholten Nichtkonformitäten von Cloud-Auftragsverarbeitern innerhalb von 60 Tagen nach Abschluss der Korrekturmaßnahme in REG12 verifizieren.

11. Überprüfung und Pflege

11.1 [Processor] The Privacy Lead / PIMS Manager MUSS diese Richtlinie in REG12 jährlich und innerhalb von 30 Tagen nach einer wesentlichen Änderung der Verpflichtungen von Cloud-Auftragsverarbeitern, Cloud-Architektur, Governance für Unterauftragsverarbeiter, Kundenunterstützung, Löschfähigkeit oder Zertifizierungsanforderungen überprüfen.

11.2 [Processor] The Vendor / Procurement Owner MUSS Aufzeichnungen zu Cloud-Unterauftragsverarbeitern und Cloud-Service-Abhängigkeiten in REG08 mindestens jährlich und vor Verlängerung überprüfen.

11.3 [Processor] The System Owner / Application Owner MUSS Nachweise zu Mandantentrennung, privilegiertem Zugriff, Protokollierung, Backup, Replikation und Löschung in REG12 mindestens jährlich und nach wesentlicher Architekturänderung überprüfen.

11.4 [Processor] The Privacy Lead / PIMS Manager MUSS REG09-Aufzeichnungen zu Cloud-Standorten und Übermittlungssteuerung mindestens jährlich und innerhalb von 15 Geschäftstagen nach einer wesentlichen Änderung von Standort, Support-Zugriff, Backup oder Unterauftragsverarbeiter überprüfen.

11.5 [Processor] The Privacy Lead / PIMS Manager MUSS REG03 innerhalb von 15 Geschäftstagen nach genehmigten Richtlinienänderungen aktualisieren, die sich auf die Anwendbarkeit von Kontrollen für Cloud-Auftragsverarbeiter auswirken.

11.6 [All] Top Management MUSS wesentliche Überarbeitungen dieser Richtlinie in REG12 vor Veröffentlichung genehmigen.

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 PII06 - Richtlinie zum Management der Rechte betroffener Personen

12.6 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

12.7 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

12.8 PII09 - Richtlinie zu PII-Erhebung, -Nutzung, -Offenlegung und -Weitergabe

12.9 PII10 - Richtlinie zu PII-Aufbewahrung, -Löschung und -Entsorgung

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

12.11 PII13 - Richtlinie zur internationalen PII-Übermittlung

12.12 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle

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

12.14 PII17 - Richtlinie zum Management dokumentierter PIMS-Informationen und Nachweise

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

12.16 PII20 - Richtlinie zum Datenschutz von Kindern

12.17 PII21 - Richtlinie zu AI und automatisierter Entscheidungsfindung im Datenschutz

12.18 PII22 - Richtlinie zu Marketing-Datenschutz und Cookies

12.19 PII24 - Richtlinie zu CCTV und physischer Überwachung im Datenschutz

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, mit denen sie umgesetzt oder unterstützt werden.

13.2 ISO/IEC 27701:2025 - Clause 4.1; Clause 6.1.3. Addressed by clauses [4.1.1; 4.1.4; 5.2; 7.1; 11.5].

13.3 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.3.1; 4.4.1; 4.6.1; 4.7.1; 4.8.1; 7.1; 7.2; 7.3].

13.4 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.3.5; 4.6.6; 4.8.1; 4.8.2; 4.8.4; 6.1; 6.2; 8.1; 8.2; 8.3; 8.4; 8.5; 10.5; 11.1].

13.5 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.5; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.2; 4.1.3; 4.1.5; 4.1.6; 4.3.1; 4.7.5; 7.2].

13.6 ISO/IEC 27701:2025 - Annex A.2.3.2. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5].

13.7 ISO/IEC 27701:2025 - Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.8 ISO/IEC 27701:2025 - Annex A.2.5.2; Annex A.2.5.3. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.9 ISO/IEC 27701:2025 - Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.5.3; 4.5.4; 4.7.2; 4.7.5].

13.10 ISO/IEC 27701:2025 - Annex A.2.5.7; Annex A.2.5.8; Annex A.2.5.9. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6].

13.11 ISO/IEC 27701:2025 - Annex A.3.8; Annex A.3.9; Annex A.3.14; Annex A.3.24; Annex A.3.25. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.7.3; 5.4; 5.6; 11.3].

13.12 GDPR - Article 28. Addressed by clauses [4.1.2; 4.1.3; 4.3.1; 4.3.2; 4.3.4; 4.4.2; 4.4.3; 4.4.5; 4.6.1; 4.6.3; 4.6.5; 4.7.2].

13.13 GDPR - Article 30. Addressed by clauses [4.1.1; 4.1.3; 4.4.1; 4.8.1; 7.1].

13.14 GDPR - Article 32; Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 7.6].

13.15 GDPR - Article 44. Addressed by clauses [4.2.6; 4.4.4; 4.5.1; 4.5.2; 7.5; 11.4].

13.16 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.6; 4.2.6; 4.5.1; 4.6.1; 4.6.3].

13.17 ISO/IEC 29100:2020 - Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.4; 4.3.5; 4.8.1; 4.8.4; 6.1; 8.5; 10.5].

13.18 ISO/IEC 29151:2022 - Clause 15.1.2; Clause 15.2.2; Clause 15.2.3; Annex A.7; Annex A.7.2. Addressed by clauses [4.4.1; 4.4.6; 4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.8.3].

13.19 ISO/IEC 27001:2022 - Clause 6.1.3; Clause 8.1; Annex A controls 5.19; 5.20; 5.21; 5.22; 5.23. Addressed by clauses [4.1.4; 4.2.1; 4.4.1; 4.4.3; 4.4.6; 4.8.1; 4.8.3; 6.1; 7.1; 11.5].

13.20 ISO/IEC 27002:2022 - Control 5.19; Control 5.20; Control 5.21; Control 5.22; Control 5.23; Control 8.10; Control 8.15; Control 8.16. Addressed by clauses [4.2.1; 4.2.4; 4.4.1; 4.4.3; 4.4.6; 4.6.1; 4.6.3; 4.7.3; 4.8.3; 11.3].

13.21 ISO/IEC 27018:2020 - Annex A.2.1; Annex A.3.1. Addressed by clauses [4.1.2; 4.1.6; 4.3.1; 4.3.2; 4.3.3; 4.3.5].

13.22 ISO/IEC 27018:2020 - Annex A.6.1; Annex A.6.2; Annex A.8.1. Addressed by clauses [4.4.1; 4.4.2; 4.4.5; 4.5.3; 4.5.4].

13.23 ISO/IEC 27018:2020 - Annex A.10.1; Annex A.10.3; Annex A.11.11; Annex A.11.12; Annex A.12.1. Addressed by clauses [4.2.6; 4.4.3; 4.4.4; 4.6.1; 4.6.3; 4.6.5; 4.7.1; 4.7.2; 4.7.5].

13.24 ISO/IEC 27036-2:2022 - Clause 6.1.1; Clause 6.1.2. Addressed by clauses [4.1.1; 4.2.1; 4.4.1; 4.4.6; 6.1; 7.2].

13.25 ISO/IEC 27036-2:2022 - Clause 7.1; Clause 7.2; Clause 7.3; Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.4.6; 4.8.2; 4.8.3; 10.3; 11.2].

13.26 ISO/IEC 27555:2025 - Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6].

13.27 ISO/IEC 27555:2025 - Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7. Addressed by clauses [4.6.2; 4.6.3; 4.6.4; 4.6.5; 4.6.6; 9.1; 9.4].