

				Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII21				Dokumenttitel: Datenschutzrichtlinie für KI und automatisierte Entscheidungsfindung							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025		Dokumentverantwortlicher:							
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 7.5; Clause 8.1	Both	Primary	Dokumentierte Information und operative Steuerung für Nachweise zur Verarbeitung durch KI, Profiling und automatisierte Entscheidungsfindung
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Überwachung, Nichtkonformität und Korrekturmaßnahmen für Datenschutzkontrollen im Zusammenhang mit KI
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9	Controller	Primary	Zweck, Rechtsgrundlage, Datenschutz-Folgenabschätzung und Aufzeichnungen des Verantwortlichen
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.1.2.8	Controller	Supporting	Verträge mit Auftragsverarbeitern und Verantwortlichkeiten gemeinsam Verantwortlicher für KI-bezogene Verarbeitung personenbezogener Daten
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4	Controller	Primary	Verpflichtungen gegenüber betroffenen Personen und Transparenz bei KI-bezogener Verarbeitung
ISO/IEC 27701:2025	Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Primary	Widerspruch, Auskunft, Berichtigung, Löschung, Bearbeitung von Anfragen und Verpflichtungen bei automatisierter Entscheidungsfindung
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5	Controller	Primary	Grenzen für Erhebung, Verarbeitung und Minimierung von KI-Eingaben, Ausgaben und abgeleiteten Daten
ISO/IEC 27701:2025	Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5	Conditional	Supporting	Internationale Übermittlung, Offenlegung und Weiterleitung von Offenlegungsersuchen für

				KI-bezogene personenbezogene Daten
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Processor	Primary	Vereinbarung mit Auftragsverarbeitern, dokumentierte Weisungen, Unterstützung von Kundenpflichten und Aufzeichnungen
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Processor	Supporting	Unterstützung durch Auftragsverarbeiter für Pflichten gegenüber betroffenen Personen, Weiterleitung von Übermittlungen und Umgang mit Offenlegungen
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Schutz von Aufzeichnungen und Protokollierung im Zusammenhang mit KI- bezogener Verarbeitung personenbezogener Daten
GDPR	Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2)	Controller	Primary	Profiling, Fairness, Transparenz, Zweckbindung, Minimierung, Richtigkeit und Rechenschaftspflicht
GDPR	Article 6; Article 9; Article 10	Controller	Primary	Rechtmäßigkeit, Daten besonderer Kategorien und Schutzmaßnahmen für Daten zu strafrechtlichen Verurteilungen oder Straftaten
GDPR	Article 12; Article 13; Article 14; Article 15	Controller	Primary	Transparente Information, Auskunft und aussagekräftige Informationen über automatisierte Entscheidungsfindung
GDPR	Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Primary	Berichtigung, Löschung, Einschränkung, Widerspruch und Rechte bei automatisierter Entscheidungsfindung
GDPR	Article 24; Article 25; Article 26; Article 28; Article	Both	Supporting	Verantwortung des Verantwortlichen, Datenschutz durch

	30; Article 32; Article 35; Article 39			Technikgestaltung und datenschutzfreundliche Voreinstellungen, gemeinsam Verantwortliche, Auftragsverarbeiter, Aufzeichnungen, Sicherheit, DPIA und Aufgaben des DPO
GDPR	Article 44	Conditional	Referenced	Weiterleitung internationaler Übermittlungen für KI-bezogene Verarbeitung personenbezogener Daten
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7	Both	Primary	Grundsätze für Zweck, Erhebung, Minimierung, Nutzung, Aufbewahrung, Offenlegung, Richtigkeit und Qualität
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparenz, Beteiligung betroffener Personen, Rechenschaftspflicht, Informationssicherheit und Einhaltung des Datenschutzes
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2; Clause 6.3	Both	Supporting	Nutzen der PIA, Schwellenwertbestimmung und Vorbereitung der KI-bezogenen Datenschutz-Risikobeurteilung
ISO/IEC 29151:2022	Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10	Both	Supporting	Kontrollen für Zweck, Erhebung, Minimierung, Nutzung, Aufbewahrung, Offenlegung, Richtigkeit und Beteiligung betroffener Personen

1. Geltungsbereich

1.1 Diese Richtlinie legt verbindliche Datenschutzerfordernungen für Verarbeitungstätigkeiten mit künstlicher Intelligenz, Profiling, Scoring, Empfehlungssystemen, Entscheidungsunterstützung und automatisierter Entscheidungsfindung fest, die innerhalb des PIMS-Geltungsbereichs personenbezogene Daten verwenden, ableiten, erzeugen, offenlegen oder anderweitig verarbeiten.

1.2 Diese Richtlinie gilt für:

1.2.1 KI-gestützte Systeme, Anwendungen, Modelle, Dienste, Workflows, Entscheidungsmaschinen, Scoring-Werkzeuge, Empfehlungssysteme, Analysemodelle und Prozesse zur automatisierten Entscheidungsfindung, die personenbezogene Daten verarbeiten;

1.2.2 Profiling, Segmentierung, Klassifizierung, Vorhersage, Inferenz, Personalisierung, Ranking, Berechtigungsprüfung, Betrugserkennung, Risiko-Scoring, Zugangsentscheidungen, beschäftigungsbezogene Beurteilungen, Profiling von Kindern, Marketing-Personalisierung und ähnliche Verarbeitung, bei der personenbezogene Daten beteiligt sind;

1.2.3 KI-bezogene personenbezogene Daten, die für Training, Tests, Validierung, Feinabstimmung, Überwachung, Produktionsinferenz, Ausgabenprüfung, Leistungsmessung, Vorfallsuntersuchung oder Außerbetriebnahme von Modellen verwendet werden;

1.2.4 Kontexte als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter;

1.2.5 KI-bezogene Anbieter, Auftragsverarbeiter, Unterauftragsverarbeiter, Empfänger von Datenweitergaben und internationale Übermittlungswege, die personenbezogene Daten verarbeiten.

1.3 Diese Richtlinie schafft kein vollständiges KI-Governance-Rahmenwerk, kein KI-Managementsystem, kein KI-Inventar, kein Modellinventar, kein Modellrisikoregister, kein Fairness-Register, kein Algorithmusregister, kein KI-Vorfallsregister, kein KI-Gremium, keine Rolle als Modellverantwortlicher, keine Rolle als KI-Systemverantwortlicher, keinen Workflow für Rechtsberatung und kein separates KI-Genehmigungsformular.

1.4 Diese Richtlinie ersetzt nicht:

1.4.1 PII03 für Verarbeitungsinventar, Rechtsgrundlage und ROPA-Verantwortung;

1.4.2 PII04 für die Governance von Datenschutzhinweisen;

1.4.3 PII05 für Einwilligungs- und Präferenzmanagement;

1.4.4 PII06 für den Workflow zu Rechten betroffener Personen;

1.4.5 PII07 für Datenschutz-Risikobeurteilung und DPIA-Methodik;

1.4.6 PII08 für Prüfpunkte zu Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen;

1.4.7 PII09 für Kontrollen zur Erhebung, Nutzung, Offenlegung und Datenweitergabe;

1.4.8 PII10 für die Umsetzung von Aufbewahrung, Löschung und Entsorgung;

1.4.9 PII11 für Kontrollen zur Richtigkeit und Qualität;

1.4.10 PII12 für die Lebenszyklus-Governance von Auftragsverarbeitern, Unterauftragsverarbeitern und Drittparteien;

1.4.11 PII13 für Kontrollen zu internationalen Übermittlungen;

1.4.12 PII14 für Sicherheit und Zugriffskontrolle;

1.4.13 PII15 für die Behandlung von Vorfällen und Verletzungen;

1.4.14 PII18 für Überwachung, Audit und Verbesserung;

- 1.4.15 PII19 für Beschäftigtendatenschutz;
- 1.4.16 PII20 für den Datenschutz von Kindern;
- 1.4.17 PII22 für Marketing-Datenschutz und Cookies.

2. Zweck

- 2.1 Zweck dieser Richtlinie ist sicherzustellen, dass Tätigkeiten mit KI, Profiling und automatisierter Entscheidungsfindung, die personenbezogene Daten betreffen, über das PIMS identifiziert, dokumentiert, risikobeurteilt, transparent, anfechtbar, überwacht und kontrolliert werden, ohne doppelte KI-spezifische Governance-Artefakte zu schaffen.
- 2.2 Diese Richtlinie stellt sicher, dass Datenschutzpflichten für KI-bezogene Verarbeitung personenbezogener Daten über REG02, REG04, REG06, REG07, REG08, REG09, REG10 und REG12 nachgewiesen werden.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

- 3.1.1 KI, Profiling und automatisierte Entscheidungsfindung betreffende Verarbeitung personenbezogener Daten in REG02 zu identifizieren;
- 3.1.2 KI-bezogene Zwecke, Rechtsgrundlagen, Kategorien personenbezogener Daten, Datenquellen, abgeleitete Daten, Ausgaben, Empfänger und Entscheidungsauswirkungen in REG02 zu dokumentieren;
- 3.1.3 Datenschutz-Risiko-Screening und DPIA-Weiterleitung über REG04 auszulösen;
- 3.1.4 sicherzustellen, dass KI-bezogene Datenschutzhinweise und aussagekräftige Informationen in REG07 aufgezeichnet werden;
- 3.1.5 Anfragen zu Rechten, Widerspruch, menschlicher Überprüfung und Anfechtbarkeit über REG06 zu leiten;
- 3.1.6 KI-bezogene Auftragsverarbeiter, Unterauftragsverarbeiter, Anbieter und Vereinbarungen zur Datenweitergabe über REG08 zu kontrollieren;
- 3.1.7 KI-bezogene internationale Übermittlungen über REG09 zu leiten;
- 3.1.8 vermutete KI-bezogene Datenschutzvorfälle, Missbrauch, unbefugte Offenlegung und nachteilige Datenschutzfolgen über REG10 und REG12 zu eskalieren;
- 3.1.9 Überwachung, Ausnahmen, Nichtkonformitäten, Korrekturmaßnahmen und Verbesserungen in REG12 aufzuzeichnen.

4. Richtlinienaussagen

4.1 Identifizierung von KI, Profiling und automatisierter Entscheidungsfindung

- 4.1.1 [Controller] Wenn ein neues oder wesentlich geändertes System, eine Anwendung, ein Modell, ein Workflow, ein Dienst oder ein Geschäftsprozess vorgeschlagen wird, muss der Process Owner / Business Owner feststellen, ob dabei KI, Profiling, Scoring, Empfehlungen, Entscheidungsunterstützung oder automatisierte Entscheidungsfindung unter Einbeziehung personenbezogener Daten verwendet werden, und die Feststellung in REG02 dokumentieren.
- 4.1.2 [Controller] Bevor KI-bezogene Verarbeitung personenbezogener Daten beginnt, muss der Process Owner / Business Owner den Verarbeitungszweck, Kategorien personenbezogener Daten, Kategorien betroffener Personen, Datenquellen, Kategorien abgeleiteter oder daraus gewonnener Daten, Ausgabekategorien, Empfängerkategorien, Rechtsgrundlage und Verknüpfung zur Aufbewahrung in REG02 dokumentieren.
- 4.1.3 [Controller] Bevor Profiling, Scoring, Empfehlungen, Entscheidungsunterstützung oder automatisierte Entscheidungsfindung in der Produktion eingesetzt werden, muss der Process Owner / Business Owner den Entscheidungskontext, die erwarteten Auswirkungen auf

betroffene Personen, die menschliche Beteiligung und den Rechtsweg in REG02 und REG04 dokumentieren.

- 4.1.4 [Joint Controller] Bevor KI-bezogene Verarbeitung personenbezogener Daten mit einem gemeinsam Verantwortlichen durchgeführt wird, muss der Privacy Lead / PIMS Manager die Verantwortung für Zweckbestimmung, Datenschutzhinweis, Rechtebearbeitung, DPIA-Unterstützung, Governance von Auftragsverarbeitern und Vorfalleskalation in REG08 dokumentieren.
- 4.1.5 [Processor] Bevor personenbezogene Daten über einen KI-bezogenen Dienst für einen Kunden verarbeitet werden, muss der Process Owner / Business Owner bestätigen, dass Kundenweisungen, zulässige Zwecke, verbotene Nutzungen, Umgang mit Ausgaben und Unterstützungspflichten in REG08 dokumentiert sind.
- 4.1.6 [Both] Bevor KI-bezogene Verarbeitung personenbezogener Daten aktiviert wird, muss der Privacy Lead / PIMS Manager bestätigen, dass die Verarbeitung mit den anwendbaren kanonischen Nachweisobjekten verknüpft ist und dass kein separates KI-spezifisches Register außerhalb von REG02, REG04, REG06, REG07, REG08, REG09, REG10 oder REG12 erstellt wird.

4.2 Datenschutz-Risikobeurteilung und DPIA-Weiterleitung

- 4.2.1 [Controller] Vor Einführung oder wesentlicher Änderung KI-bezogener Verarbeitung personenbezogener Daten muss der Privacy Lead / PIMS Manager ein Datenschutz-Risiko-Screening abschließen und die DPIA-Entscheidung in REG04 aufzeichnen.
- 4.2.2 [Conditional] Wenn KI-bezogene Verarbeitung Profiling, automatisierte Entscheidungen, groß angelegte Bewertung, Daten besonderer Kategorien, Daten zu Straftaten, schutzbedürftige betroffene Personen, Beschäftigtenbeurteilung, Kinder, Verhaltensüberwachung, Standortdaten, biometrische Daten, Scoring mit hoher Tragweite oder erhebliche Auswirkungen umfasst, muss der Data Protection Officer / Privacy Advisor das Datenschutzrisiko prüfen und die Beratung in REG04 aufzeichnen.
- 4.2.3 [Controller] Vor der Produktivsetzung KI-bezogener Verarbeitung personenbezogener Daten muss der Process Owner / Business Owner Risikobehandlungsmaßnahmen, Status des Restrisikos und Nachweise zur Bereitschaft für die Produktivsetzung in REG04 oder REG12 dokumentieren.
- 4.2.4 [Controller] Bevor personenbezogene Daten für KI-Training, Tests, Validierung, Feinabstimmung, Überwachung oder Modellverbesserung für einen neuen oder wesentlich geänderten Zweck wiederverwendet werden, muss der Process Owner / Business Owner eine Datenschutzprüfung abschließen und die Entscheidung in REG02 und REG04 aufzeichnen.
- 4.2.5 [Conditional] Wenn nach der geplanten Behandlung ein hohes Datenschutz-Restrisiko verbleibt, muss Top Management die Produktionsnutzung genehmigen, ablehnen oder eine weitere Behandlung verlangen und die Entscheidung in REG04 und REG12 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 [All] Vor einer Abweichung von einer KI-bezogenen Datenschutzerfordernung in dieser Richtlinie muss der anfragende Process Owner / Business Owner eine Ausnahmebegründung und Nachweise zu kompensierenden Kontrollen in REG12 einreichen.
- 9.2 [Conditional] Wenn eine Ausnahme Profiling, automatisierte Entscheidungsfindung, menschliche Überprüfung, Anfechtbarkeit, Transparenz, DPIA-Ergebnis, Scoring mit hoher Tragweite, Verarbeitung mit Bezug zu Kindern, Verarbeitung mit Bezug zu Beschäftigten, Beschränkungen für

Auftragsverarbeiter oder internationale Übermittlungen betrifft, muss der Data Protection Officer / Privacy Advisor die Ausnahme prüfen und die Beratung in REG04 oder REG12 aufzeichnen.

9.3 [Conditional] Wenn eine Ausnahme ein hohes Datenschutz-Restrisiko schafft oder aufrechterhält, muss Top Management die Ausnahme genehmigen oder ablehnen und die Entscheidung in REG04 und REG12 aufzeichnen.

9.4 [All] Bevor eine genehmigte KI-bezogene Datenschutzausnahme abläuft, muss der Privacy Lead / PIMS Manager den Status von Abschluss, Verlängerung oder Korrekturmaßnahme prüfen und das Ergebnis in REG12 aufzeichnen.

10. Durchsetzung

10.1 [All] Wenn eine Nichteinhaltung dieser Richtlinie festgestellt wird, muss der Privacy Lead / PIMS Manager die Nichtkonformität und Korrekturmaßnahme in REG12 aufzeichnen.

10.2 [Both] Wenn unbefugte KI-bezogene Verarbeitung personenbezogener Daten, Offenlegung, Zugriff, Modellmissbrauch, ein Fehler bei der Rechtebearbeitung oder eine nachteilige Datenschutzfolge vermutet wird, muss der Incident Response Coordinator die Vorfalleskalation einleiten und Nachweise in REG10 und REG12 aufzeichnen.

10.3 [Both] Wenn ein Auftragsverarbeiter, Unterauftragsverarbeiter, Lieferant oder Empfänger einer Datenweitergabe KI-bezogene Datenschutzpflichten nicht erfüllt, muss der Vendor / Procurement Owner Abhilfe-, Eskalations- oder Beendigungsmaßnahmen in REG08 und REG12 aufzeichnen.

10.4 [All] Wenn wiederholte oder systemische KI-bezogene Datenschutz-Nichtkonformitäten auftreten, muss Top Management das Thema prüfen und die Managementmaßnahme in REG12 aufzeichnen.

11. Überprüfung und Pflege

11.1 [All] Mindestens jährlich muss der Privacy Lead / PIMS Manager diese Richtlinie auf fortdauernde Eignung prüfen und das Prüfergebnis in REG12 aufzeichnen.

11.2 [Conditional] Wenn sich Gesetze, Dienste, Modelle, Datenquellen, Profiling-Praktiken, Logik der automatisierten Entscheidungsfindung, Anbietervereinbarungen, Übermittlungswege oder Datenschutzrisiken wesentlich ändern, muss der Privacy Lead / PIMS Manager betroffene KI-bezogene Datenschutzkontrollen prüfen und das Ergebnis in REG02, REG04 oder REG12 aufzeichnen.

11.3 [Controller] Mindestens jährlich und nach wesentlichen Änderungen der KI-bezogenen User Journey muss der Process Owner / Business Owner Nachweise zu Transparenz, aussagekräftigen Informationen, menschlicher Überprüfung und Rechteweg prüfen und die Prüfung in REG06 und REG07 aufzeichnen.

11.4 [All] Nach Abschluss KI-bezogener Datenschutz-Korrekturmaßnahmen muss der Internal Audit / Compliance Reviewer die Wirksamkeit verifizieren und Verifizierungsnachweise in REG12 aufzeichnen.

12. Zugehörige Richtlinien

12.1 PII01 - Richtlinie zum Datenschutz-Informationsmanagementsystem

12.2 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht

12.3 PII03 - Richtlinie zum Verarbeitungsinventar für personenbezogene Daten und zur Rechtsgrundlage

12.4 PII04 - Richtlinie zu Datenschutzhinweisen und Transparenz

12.5 PII05 - Richtlinie zum Einwilligungs- und Präferenzmanagement

12.6 PII06 - Richtlinie zum Management der Rechte betroffener Personen

12.7 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

- 12.8 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen
- 12.9 PII09 - Richtlinie zur Erhebung, Nutzung, Offenlegung und Datenweitergabe personenbezogener Daten
- 12.10 PII10 - Richtlinie zur Aufbewahrung, Löschung und Entsorgung personenbezogener Daten
- 12.11 PII11 - Richtlinie zur Richtigkeit und Qualität personenbezogener Daten
- 12.12 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Drittparteien
- 12.13 PII13 - Richtlinie zur internationalen Übermittlung personenbezogener Daten
- 12.14 PII14 - Richtlinie zur Sicherheit personenbezogener Daten und Zugriffskontrolle
- 12.15 PII15 - Richtlinie zum Management von Datenschutzvorfällen und Verletzungen des Schutzes personenbezogener Daten
- 12.16 PII17 - Richtlinie zu dokumentierter Information und Nachweismanagement im PIMS
- 12.17 PII18 - Richtlinie zu PIMS-Überwachung, Audit und Verbesserung
- 12.18 PII19 - Beschäftigtendatenschutzrichtlinie
- 12.19 PII20 - Richtlinie zum Datenschutz von Kindern
- 12.20 PII22 - Richtlinie zu Marketing-Datenschutz und Cookies

13. Referenzstandards und Rahmenwerke

- 13.1 ISO/IEC 27701:2025 - Clause 7.5; Clause 8.1. Addressed by clauses [4.1.6; 4.8.1; 6.1; 7.1; 7.5; 11.1].
- 13.2 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.2; 4.6.5; 4.8.2; 6.5; 8.1; 8.2; 8.3; 8.4; 8.5; 10.1; 11.4].
- 13.3 ISO/IEC 27701:2025 - Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.9. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.2.3; 4.2.4; 4.8.1; 7.1; 7.2].
- 13.4 ISO/IEC 27701:2025 - Annex A.1.2.7; Annex A.1.2.8. Addressed by clauses [4.1.4; 4.7.1; 4.7.2; 4.7.3; 5.7; 6.3; 7.6].
- 13.5 ISO/IEC 27701:2025 - Annex A.1.3.2; Annex A.1.3.3; Annex A.1.3.4. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 7.3; 11.3].
- 13.6 ISO/IEC 27701:2025 - Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11. Addressed by clauses [4.1.3; 4.3.2; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4; 11.3].
- 13.7 ISO/IEC 27701:2025 - Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5. Addressed by clauses [4.2.4; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 7.1; 7.5].
- 13.8 ISO/IEC 27701:2025 - Annex A.1.5.2; Annex A.1.5.3; Annex A.1.5.4; Annex A.1.5.5. Addressed by clauses [4.7.3; 4.7.4; 4.7.5; 7.7].
- 13.9 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7. Addressed by clauses [4.1.5; 4.3.5; 4.5.5; 4.7.1; 4.7.2; 5.7; 6.3; 7.6].
- 13.10 ISO/IEC 27701:2025 - Annex A.2.3.2; Annex A.2.5.2; Annex A.2.5.3; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6. Addressed by clauses [4.3.5; 4.5.5; 4.7.1; 4.7.2; 4.7.4; 4.7.5; 7.6; 7.7].
- 13.11 ISO/IEC 27701:2025 - Annex A.3.14; Annex A.3.25. Addressed by clauses [4.4.4; 4.6.1; 4.6.3; 4.8.1; 5.4; 7.5; 7.8; 10.2].
- 13.12 GDPR - Article 4(4); Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(d); Article 5(2). Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.1; 4.4.1; 4.4.2; 4.4.5; 4.8.1; 8.1].
- 13.13 GDPR - Article 6; Article 9; Article 10. Addressed by clauses [4.1.2; 4.2.4; 4.4.3; 4.7.3; 7.1].
- 13.14 GDPR - Article 12; Article 13; Article 14; Article 15. Addressed by clauses [4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.5.2; 4.5.3; 7.3; 11.3].

- 13.15 GDPR - Article 16; Article 17; Article 18; Article 21; Article 22. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 7.4].
- 13.16 GDPR - Article 24; Article 25; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.2.2; 4.2.5; 4.4.4; 4.7.1; 4.8.2; 5.3; 6.2; 6.4; 7.2].
- 13.17 GDPR - Article 44. Addressed by clauses [4.7.4; 7.7; 8.4].
- 13.18 ISO/IEC 29100:2020 - Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.7. Addressed by clauses [4.1.2; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.7.5].
- 13.19 ISO/IEC 29100:2020 - Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12. Addressed by clauses [4.3.1; 4.3.2; 4.5.1; 4.5.2; 4.6.3; 4.8.1; 4.8.2; 8.5; 10.1].
- 13.20 ISO/IEC 29134:2020 - Clause 5.1; Clause 6.2; Clause 6.3. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.6.4; 6.4; 7.2; 9.2].
- 13.21 ISO/IEC 29151:2022 - Annex A.4; Annex A.5; Annex A.7; Annex A.8; Annex A.10. Addressed by clauses [4.3.1; 4.3.2; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.2; 4.5.4; 4.7.5].