					Fügen Sie hier den Namen der eingetragenen juristischen Person ein						
Dokumentnummer: PII15					Dokumenttitel: **Richtlinie zum Management von Datenschutzvorfällen und Verletzungen des Schutzes personenbezogener Daten**						
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 / Verordnung	Klausel / Maßnahme / Artikel	Anwendbarkeit	Abdeckungstyp	Kommentar
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	PIMS-Kommunikation und dokumentierte Nachweise zu Verletzungen des Schutzes personenbezogener Daten
ISO/IEC 27701:2025	Clause 8.1; Clause 8.2; Clause 8.3	Both	Supporting	Verknüpfung von operativer Steuerung, Datenschutz-Risikobeurteilung und Risikobehandlung
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Überwachung, Bewertung, Nichtkonformität, Korrekturmaßnahmen und Verbesserung
ISO/IEC 27701:2025	Annex A.3.11	Both	Primary	Planung und Vorbereitung des Vorfallmanagements für die PII-Verarbeitung
ISO/IEC 27701:2025	Annex A.3.12	Both	Primary	Reaktion auf Informationssicherheitsvorfälle mit PII-Bezug
ISO/IEC 27701:2025	Annex A.3.13; Annex A.3.14	Both	Supporting	Gesetzliche, satzungsmäßige, regulatorische und vertragliche Anforderungen sowie Schutz von Aufzeichnungen
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6	Processor	Supporting	Unterstützung von Kundenvereinbarungen des Auftragsverarbeiters und Kundenpflichten
GDPR	Article 5(2); Article 24	Controller	Supporting	Rechenschaftspflicht und Verantwortung des Verantwortlichen
GDPR	Article 26	Joint Controller	Supporting	Koordination der Verantwortlichkeit gemeinsam Verantwortlicher bei Verletzungen des Schutzes personenbezogener Daten
GDPR	Article 28	Both	Supporting	Unterstützung durch Auftragsverarbeiter und vertragliche Pflichten des Auftragsverarbeiters
GDPR	Article 32	Both	Supporting	Sicherheit der Verarbeitung und Fähigkeit zur Erkennung von Verletzungen des

				Schutzes personenbezogener Daten
GDPR	Article 33	Both	Primary	Meldung von Verletzungen des Schutzes personenbezogener Daten und Dokumentation von Verletzungen
GDPR	Article 34	Controller	Primary	Benachrichtigung betroffener Personen über Verletzungen des Schutzes personenbezogener Daten
GDPR	Article 39	Conditional	Supporting	Beratung, Überwachung, Zusammenarbeit und Unterstützung als Kontaktstelle durch den DPO
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Grundsätze der Informationssicherheit und der Einhaltung von Datenschutzanforderungen
ISO/IEC 29151:2022	Clause 16.1.2; Clause 16.1.3	Both	Supporting	Verantwortlichkeiten für die Reaktion auf Datenschutzvorfälle und Ereignismeldung
ISO/IEC 27002:2022	Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28	Both	Supporting	Vorfallplanung, Bewertung, Reaktion, Lessons Learned und Beweissicherung
ISO/IEC 27035-1:2023	Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Supporting	Lebenszyklus des Vorfallmanagementprozesses
ISO/IEC 27035-2:2023	Clause 4; Clause 6; Clause 10; Clause 11; Clause 12	Both	Supporting	Vorfallrichtlinie, Plan, Sensibilisierung, Tests und Lessons Learned
ISO/IEC 27035-3:2020	Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12	Both	Supporting	Erkennung, Benachrichtigung, Triage, Analyse, Reaktion und Meldeprozesse
ISO/IEC 27018:2020	Annex A.10.1	Conditional	Supporting	Erwartungen an Benachrichtigung durch Cloud-Auftragsverarbeiter und Aufzeichnungen zu

				Verletzungen des Schutzes personenbezogener Daten
NIS2 Directive (EU) 2022/2555	Article 23	Conditional	Supporting	Meldung erheblicher Vorfälle, soweit anwendbar
DORA Regulation (EU) 2022/2554	Article 17; Article 18; Article 19	Conditional	Supporting	Management, Klassifizierung und Meldung IKT-bezogener Vorfälle, soweit anwendbar

1. Geltungsbereich

1.1 Diese Richtlinie legt die Anforderungen für die Identifizierung, Meldung, Triage, Bewertung, Eindämmung, Benachrichtigung, Dokumentation, Schließung und Verbesserung im Zusammenhang mit Datenschutzvorfällen und Verletzungen des Schutzes personenbezogener Daten innerhalb des PIMS-Geltungsbereichs fest.

1.2 Diese Richtlinie gilt für:

1.2.1 die Organisation in der Rolle als PII-Verantwortlicher;

1.2.2 die Organisation in der Rolle als gemeinsam Verantwortlicher, wenn eine Koordination der Verantwortlichkeit bei Verletzungen des Schutzes personenbezogener Daten erforderlich ist;

1.2.3 die Organisation in der Rolle als PII-Auftragsverarbeiter;

1.2.4 die Organisation in der Rolle als Unterauftragsverarbeiter;

1.2.5 Systeme, Anwendungen, Services, Prozesse, Lieferanten, Auftragsverarbeiter, Unterauftragsverarbeiter und Dritte, die PII innerhalb des PIMS-Geltungsbereichs verarbeiten, speichern, übermitteln, unterstützen, darauf zugreifen oder anderweitig beeinflussen.

1.3 Diese Richtlinie verwendet REG10 - Register für Datenschutzvorfälle und Verletzungen des Schutzes personenbezogener Daten als primäres Nachweisobjekt für das Management von Datenschutzvorfällen und Verletzungen des Schutzes personenbezogener Daten.

1.4 Diese Richtlinie verwendet unterstützende Nachweisobjekte wie folgt:

1.4.1 REG01 für den PIMS-Geltungsbereich sowie den Kontext anwendbarer interessierter Parteien, gesetzlicher, vertraglicher, branchenspezifischer und kundenbezogener Meldeanforderungen.

1.4.2 REG02 für betroffene Verarbeitungstätigkeiten, PII-Kategorien, Kategorien betroffener Personen, Zwecke und Systeme.

1.4.3 REG03 für die Erklärung zur Anwendbarkeit und Aktualisierungen der Anwendbarkeit von Kontrollen.

1.4.4 REG04 für Verknüpfungen zu Datenschutzrisiken, DPIA und Restrisiken.

1.4.5 REG08 für Nachweise zu Schnittstellen für Vorfälle mit Auftragsverarbeitern, Unterauftragsverarbeitern, Kunden, Lieferanten und Dritten.

1.4.6 REG09 für die Verknüpfung mit internationalen Übermittlungen, wenn ein Vorfall grenzüberschreitende Verarbeitung betrifft.

1.4.7 REG11 für Nachweise zu Schulung, Sensibilisierung und Kompetenz in der Reaktion auf Vorfälle.

1.4.8 REG12 für Nachweise zu Audit, Nichtkonformität, Korrekturmaßnahmen und Verbesserung.

1.5 Diese Richtlinie stützt sich für Spezialkontrollen auf verwandte PIMS-Richtlinien:

1.5.1 PII03 regelt das Verarbeitungsverzeichnis und Aufzeichnungen zu Rechtsgrundlagen.

1.5.2 PII04 regelt Datenschutzhinweise und Transparenzkontrollen außerhalb verletzungsspezifischer Kommunikation.

1.5.3 PII06 regelt Anfragen zu Rechten betroffener Personen, die vor, während oder nach einem Vorfall entstehen.

1.5.4 PII07 regelt die Methodik für Datenschutz-Risikobeurteilung und DPIA.

1.5.5 PII08 regelt Kontrollen für Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen.

1.5.6 PII10 regelt Kontrollen für Aufbewahrung, Löschung und Entsorgung.

1.5.7 PII12 regelt Datenschutzkontrollen für Beziehungen mit Auftragsverarbeitern, Unterauftragsverarbeitern, Lieferanten und Dritten.

1.5.8 PII13 regelt Mechanismen für internationale PII-Übermittlungen und Aufzeichnungen zu Übermittlungsrisiken.

1.5.9 PII14 regelt präventive und aufdeckende PII-Sicherheits- und Zugriffskontrollen.

1.5.10 PII16 regelt Datenschutzschulung, Sensibilisierung und Kompetenz.

1.5.11 PII17 regelt dokumentierte Informationen und Nachweismanagement.

1.5.12 PII18 regelt Überwachung, internes Audit, Managementbewertung, Nichtkonformität, Korrekturmaßnahmen und kontinuierliche Verbesserung.

1.6 Für diese Richtlinie gilt:

1.6.1 „Datenschutzvorfall“ bezeichnet ein vermutetes oder bestätigtes Ereignis, das die Vertraulichkeit, Integrität, Verfügbarkeit, rechtmäßige Verarbeitung oder autorisierte Handhabung von PII beeinträchtigt hat, beeinträchtigt haben kann oder vernünftigerweise beeinträchtigen könnte.

1.6.2 „Verletzung des Schutzes personenbezogener Daten“ bezeichnet einen bestätigten Datenschutzvorfall, der eine unbefugte, rechtswidrige, versehentliche oder unbeabsichtigte Vernichtung, einen Verlust, eine Veränderung, Offenlegung, einen Zugriff, eine Nichtverfügbarkeit oder Kompromittierung von PII umfasst.

1.6.3 „Bewertung der Datenschutzverletzung“ bezeichnet die dokumentierte Bewertung, ob ein Datenschutzvorfall eine Verletzung des Schutzes personenbezogener Daten ist, welche PII und betroffenen Personen betroffen sind, welche Risiken entstehen können, welche Meldungen oder Benachrichtigungen erforderlich sind und welche Abhilfemaßnahmen notwendig sind.

1.6.4 „Kenntnisnahme“ bezeichnet den Zeitpunkt, zu dem die Organisation mit hinreichender Sicherheit davon ausgeht, dass ein Sicherheits- oder Datenschutzvorfall eingetreten ist und PII kompromittiert wurden oder kompromittiert worden sein könnten.

1.6.5 „Datenschutzvorfall mit hoher Tragweite“ bezeichnet einen Datenschutzvorfall, der Verarbeitung mit hohem Risiko, besondere Kategorien oder hochsensible PII, PII in großem Umfang, schutzbedürftige Personen, regulierte Kunden, Auswirkungen in mehreren Rechtsordnungen, wesentliche Kundenauswirkungen, Kompromittierung privilegierter Zugriffe, öffentliche Exponierung, Ransomware, Nichtverfügbarkeit von Services oder erhebliche operative oder reputationsbezogene Auswirkungen umfasst.

1.6.6 „Wesentliche Änderung des Vorfalls“ bezeichnet neue oder geänderte Informationen, die den Vorfallsumfang, den Schweregrad, PII-Kategorien, Auswirkungen auf betroffene Personen, die Meldeentscheidung, Kundenauswirkungen, Ursache, Eindämmung, Wiederherstellung, Korrekturmaßnahmen oder externe Berichtspflichten betreffen.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass Datenschutzvorfälle und Verletzungen des Schutzes personenbezogener Daten einheitlich, unverzüglich, rechtmäßig, sicher und mit auditbereiten Nachweisen behandelt werden.

2.2 Diese Richtlinie unterstützt die Rechenschaftspflicht, indem sie verlangt, dass Datenschutzvorfälle und Verletzungen des Schutzes personenbezogener Daten in REG10 aufgezeichnet und, sofern ausgelöst, mit betroffenen Verarbeitungsaufzeichnungen, Datenschutzrisiken, Beziehungen zu Auftragsverarbeitern und Unterauftragsverarbeitern, Übermittlungsaufzeichnungen, Korrekturmaßnahmen und Schulungsaufzeichnungen verknüpft werden.

2.3 Diese Richtlinie stellt sicher, dass Pflichten von Verantwortlichen, gemeinsam Verantwortlichen, Auftragsverarbeitern und Unterauftragsverarbeitern über getrennte Anwendbarkeitsregeln behandelt werden, während ein integriertes Nachweismodell für Vorfälle und Verletzungen des Schutzes personenbezogener Daten beibehalten wird.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 sicherzustellen, dass vermutete Datenschutzvorfälle unverzüglich gemeldet und aufgezeichnet werden;

3.1.2 sicherzustellen, dass Datenschutzvorfälle anhand einheitlicher Kriterien triagiert und klassifiziert werden;

3.1.3 sicherzustellen, dass Bewertungen der Datenschutzverletzung betroffene PII, betroffene Personen, Systeme, Verarbeitungstätigkeiten, Auftragsverarbeiter, Unterauftragsverarbeiter, Übermittlungen, Risiken und Abhilfemaßnahmen berücksichtigen;

3.1.4 sicherzustellen, dass Entscheidungen über Meldungen durch Verantwortliche und Benachrichtigungen betroffener Personen dokumentiert werden;

3.1.5 sicherzustellen, dass Meldungen von Verletzungen des Schutzes personenbezogener Daten durch Auftragsverarbeiter und Unterauftragsverarbeiter an Kunden oder vorgelagerte Parteien ohne unangemessene Verzögerung und im Einklang mit anwendbaren Vereinbarungen erfolgen;

3.1.6 sicherzustellen, dass Nachweise während der Vorfallsbearbeitung gesichert und geschützt werden;

3.1.7 sicherzustellen, dass Eindämmung, Beseitigung, Wiederherstellung und Validierung über REG10 nachverfolgt werden;

3.1.8 sicherzustellen, dass Auslöser für regulatorische, vertragliche, kundenbezogene und branchenspezifische Meldungen bewertet werden, soweit anwendbar;

3.1.9 sicherzustellen, dass Lessons Learned aus Vorfällen zu Korrekturmaßnahmen und kontinuierlicher Verbesserung führen;

3.1.10 sicherzustellen, dass Vorfalls- und Verletzungsaufzeichnungen für Audit, Managementbewertung, Kundenzusicherung und regulatorische Überprüfung verfügbar sind, soweit anwendbar.

4. Richtlinienaussagen

4.1 Vorfallsbereitschaft und Eingang

4.1.1 [Both] The Privacy Lead / PIMS Manager MUSS Kriterien für die Behandlung von Datenschutzvorfällen und Verletzungen des Schutzes personenbezogener Daten in REG10 mindestens jährlich sowie nach jeder wesentlichen Änderung des PIMS-Geltungsbereichs, des rechtlichen Kontexts, vertraglicher Pflichten oder Verarbeitung mit hohem Risiko pflegen.

4.1.2 [All] The Incident Response Coordinator MUSS jeden gemeldeten oder erkannten vermuteten Datenschutzvorfall innerhalb eines Geschäftstags nach Eingang in REG10 erfassen, oder früher, wenn eine anwendbare Meldefrist oder Kundenberichtspflicht ausgelöst werden kann.

4.1.3 [Both] The System Owner / Application Owner MUSS relevante Systemprotokolle, Warnmeldungen, Zugriffsaufzeichnungen, Konfigurationsnachweise und Wiederherstellungsnachweise mit Verknüpfung zu REG10 sichern, wenn ein vermuteter Vorfall ein System oder eine Anwendung betrifft, die PII verarbeitet.

4.1.4 [Both] The Information Security Lead MUSS die erste technische Triage jedes Sicherheitsereignisses mit PII-Bezug innerhalb von 24 Stunden nach Erkennung abschließen

und den anfänglichen Schweregrad, die betroffenen Assets und den Eindämmungsstatus in REG10 erfassen.

4.2 Klassifizierung und Bewertung der Datenschutzverletzung

4.2.1 [Both] The Incident Response Coordinator MUSS jeden REG10-Eintrag innerhalb von 24 Stunden nach Eingang als Nicht-PII-Ereignis, vermuteten Datenschutzvorfall, bestätigten Datenschutzvorfall oder bestätigte Verletzung des Schutzes personenbezogener Daten klassifizieren oder den REG10-Datensatz mit der Begründung aktualisieren, warum die Klassifizierung noch aussteht.

4.2.2 [Both] The Privacy Lead / PIMS Manager MUSS die betroffene Verarbeitungstätigkeit, PII-Kategorien, Kategorien betroffener Personen, Systeme, Auftragsverarbeiter, Unterauftragsverarbeiter, Übermittlungsorte und Datenschutzrisiken in REG02, REG04, REG08, REG09 und REG10 identifizieren, bevor die Entscheidung über die Meldung einer Verletzung des Schutzes personenbezogener Daten finalisiert wird.

4.2.3 [Controller] The Data Protection Officer / Privacy Advisor MUSS das Risiko für betroffene Personen bei jeder bestätigten oder begründet vermuteten Verletzung des Schutzes personenbezogener Daten bewerten und die Meldeempfehlung, Risikobegründung und Beratung in REG10 erfassen, bevor die Entscheidung über externe Meldung getroffen wird.

4.2.4 [Processor] The Privacy Lead / PIMS Manager MUSS den betroffenen Verantwortlichen oder Kunden und die anwendbaren vertraglichen Meldeanforderungen identifizieren, sobald die Organisation Kenntnis von einer Verletzung des Schutzes personenbezogener Daten erhält, die Kunden-PII betrifft, und MUSS das Ergebnis in REG08 und REG10 erfassen.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUSS die vereinbarte Verantwortlichkeit bei Verletzungen des Schutzes personenbezogener Daten, die führende Kommunikationsverantwortung und die Koordinationsregelung vor jeder externen Meldung oder Benachrichtigung durch einen gemeinsam Verantwortlichen verifizieren und MUSS die Entscheidung in REG08 und REG10 erfassen.

4.2.6 [Conditional] The Privacy Lead / PIMS Manager MUSS für jeden Datenschutzvorfall mit hoher Tragweite anwendbare gesetzliche, branchenspezifische, finanzsektorspezifische, cybersicherheitsbezogene, vertragliche, kundenbezogene und serviceempfängerbezogene Meldeauslöser bewerten und das Ergebnis der Anwendbarkeit in REG01, REG08 und REG10 erfassen.

[... 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 [Both] The Privacy Lead / PIMS Manager MUSS jede Ausnahme von dieser Richtlinie vor Umsetzung in REG12 erfassen oder innerhalb von 24 Stunden nach einer Notfallmaßnahme, wenn eine vorherige Genehmigung nicht möglich war.

9.1.2 [Both] Top Management MUSS jede Ausnahme, die den Zeitpunkt der Meldung einer Verletzung des Schutzes personenbezogener Daten, öffentliche Kommunikation, Kundenverpflichtungen, Beweissicherung oder das Risiko für betroffene Personen wesentlich betrifft, vor Schließung des Vorfalls genehmigen, wobei Genehmigungsnachweise in REG10 und REG12 aufzubewahren sind.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUSS vor Vorfallsschließung Beratung für jede verzögerte Meldung, Nichtmeldeentscheidung oder außergewöhnliche Kommunikationsweise dokumentieren, wobei die Beratung in REG10 aufzubewahren ist.

9.1.4 [Both] The Vendor / Procurement Owner MUSS lieferanten-, auftragsverarbeiter-, unterauftragsverarbeiter- oder kundenbedingte Ausnahmen, die die Vorfallsreaktion betreffen,

innerhalb von fünf Geschäftstagen nach Identifizierung der Ausnahme in REG08 und REG12 erfassen.

10. Durchsetzung

10.1.1 [All] The Process Owner / Business Owner MUSS das Unterlassen der Meldung eines vermuteten Datenschutzvorfalls, der Beweissicherung, der Befolgung zugewiesener Maßnahmen oder der Mitwirkung an der Bewertung der Datenschutzverletzung innerhalb von zwei Geschäftstagen nach Entdeckung an The Privacy Lead / PIMS Manager eskalieren, wobei Nachweise in REG12 aufzubewahren sind.

10.1.2 [Both] The Privacy Lead / PIMS Manager MUSS eine REG12-Nichtkonformität erfassen, wenn eine Verletzung dieser Richtlinie den Vorfallseingang, die Triage, Eindämmung, Meldung, Integrität der Nachweise, Kommunikation oder Korrekturmaßnahmen betrifft.

10.1.3 [Both] The Vendor / Procurement Owner MUSS innerhalb von fünf Geschäftstagen Abhilfemaßnahmen bei Lieferanten oder Auftragsverarbeitern über REG08 und REG12 einleiten, wenn ein Auftragsverarbeiter, Unterauftragsverarbeiter, Lieferant oder anderer Dritter vereinbarte Vorfalls- oder Pflichten bei Verletzungen des Schutzes personenbezogener Daten nicht erfüllt.

10.1.4 [Both] Top Management MUSS wesentliche oder wiederkehrende Nichtkonformitäten im Vorfallmanagement bei der nächsten geplanten Managementbewertung prüfen, wobei Entscheidungen und erforderliche Maßnahmen in REG12 aufzubewahren sind.

11. Überprüfung und Pflege

11.1.1 [Both] The Privacy Lead / PIMS Manager MUSS diese Richtlinie mindestens jährlich überprüfen und das Prüfergebnis, erforderliche Änderungen und den Genehmigungsstatus in REG12 erfassen.

11.1.2 [Both] The Incident Response Coordinator MUSS innerhalb von 30 Kalendertagen nach Schließung jedes Datenschutzvorfalls mit hoher Tragweite oder jeder bestätigten Verletzung des Schutzes personenbezogener Daten eine Überprüfung dieser Richtlinie nach dem Vorfall auslösen, wobei Prüfnachweise in REG10 und REG12 aufzubewahren sind.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUSS diese Richtlinie innerhalb von 30 Kalendertagen nach Kenntnisnahme einer wesentlichen Änderung anwendbarer gesetzlicher, branchenspezifischer, kundenbezogener, vertraglicher, auftragsverarbeiter-, unterauftragsverarbeiter- oder übermittlungsbezogener Anforderungen an Vorfallmeldungen überprüfen, wobei Prüfnachweise in REG01, REG08, REG09 und REG12 aufzubewahren sind.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUSS die Umsetzung dieser Richtlinie mindestens jährlich im Rahmen des PIMS-internen Auditprogramms prüfen, wobei Auditfeststellungen und Korrekturmaßnahmen in REG12 aufzubewahren sind.

11.1.5 [Both] Top Management MUSS Vorfallstrends, erhebliche Verletzungen des Schutzes personenbezogener Daten, Meldeleistung, überfällige Korrekturmaßnahmen und Richtlinienwirksamkeit während der geplanten Managementbewertung prüfen, wobei Ergebnisse in REG12 aufzubewahren sind.

12. Zugehörige Richtlinien

12.1 Diese Richtlinie sollte zusammen gelesen werden mit:

12.1.1 PII01 - Richtlinie zum Datenschutz-Informationsmanagementsystem

12.1.2 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht

12.1.3 PII03 - Richtlinie zum PII-Verarbeitungsverzeichnis und zu Rechtsgrundlagen

12.1.4 PII04 - Richtlinie zu Datenschutzhinweisen und Transparenz

12.1.5 PII06 - Richtlinie zum Management von Rechten betroffener Personen

12.1.6 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

12.1.7 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

12.1.8 PII10 - Richtlinie zur PII-Aufbewahrung, -Löschung und -Entsorgung

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

12.1.10 PII13 - Richtlinie zu internationalen PII-Übermittlungen

12.1.11 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle

12.1.12 PII16 - Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz

12.1.13 PII17 - Richtlinie zum Management dokumentierter Informationen und Nachweise im PIMS

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

13. Referenzstandards und Rahmenwerke

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.7; 4.5.1; 4.5.3; 4.5.4; 5.2.2; 6.2.2; 7.1.1; 7.1.7; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.2.2; 4.3.4; 4.6.3; 6.3.1; 7.1.4; 11.1.2].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.6.1; 4.6.2; 4.6.3; 4.6.4; 6.4.1; 6.5.1; 8.1.1; 8.1.4; 10.1.2; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.2.6; 4.4.1; 5.1.1; 5.4.1; 7.1.1; 7.1.2; 7.1.6].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.4; 4.2.1; 4.2.3; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.5.1; 4.5.4; 6.3.1].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.2.6; 4.4.6; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.6.4; 6.2.2; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.4; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.2; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 4.6.2; 5.2.1; 6.3.1; 8.1.3; 11.1.5].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.1; 4.4.3; 5.3.1; 6.2.2; 11.1.3].

13.10 GDPR - Article 28. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5; 10.1.3].

13.11 GDPR - Article 32. Addressed by clauses [4.1.3; 4.1.4; 4.3.2; 4.3.3; 4.5.2; 4.6.3; 5.5.1; 7.1.4; 8.1.2; 11.1.2].

13.12 GDPR - Article 33. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.4.4; 4.4.5; 4.5.1; 4.5.4; 8.1.3; 9.1.3].

13.13 GDPR - Article 34. Addressed by clauses [4.2.3; 4.2.5; 4.4.2; 4.4.3; 4.4.7; 4.5.4; 8.1.3; 9.1.3].

13.14 GDPR - Article 39. Addressed by clauses [4.2.3; 4.4.2; 5.3.1; 6.2.2; 9.1.3; 11.1.3].

13.15 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.2.2; 4.3.2; 4.3.3; 4.5.3; 4.6.2; 4.6.3; 5.2.2; 6.4.1; 8.1.4; 11.1.4].

13.16 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.3; 4.6.5; 7.1.3; 7.1.6].

13.17 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.5.1; 4.5.2; 4.6.1; 4.6.2; 7.1.2; 7.1.6].

13.18 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.2; 4.6.1; 5.4.1; 7.1.6; 11.1.2].

13.19 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.1; 4.6.1; 4.6.5; 5.1.1; 7.1.1; 7.1.3; 7.1.6; 8.1.6; 11.1.1; 11.1.2].

13.20 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.2; 4.1.4; 4.2.1; 4.3.1; 4.3.2; 4.4.1; 4.4.4; 4.5.1; 5.4.2; 6.1.2; 8.1.2].

13.21 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.4; 4.3.5; 4.4.4; 4.4.5; 4.5.5; 5.8.1; 7.1.5; 8.1.5].

13.22 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.2.6; 4.4.6; 4.4.7; 5.3.1; 6.2.2; 8.1.3; 11.1.3].

13.23 DORA Regulation (EU) 2022/2554 - Article 17; Article 18; Article 19. Addressed by clauses [4.2.1; 4.2.6; 4.4.6; 4.4.7; 5.1.2; 6.2.1; 8.1.3; 11.1.3; 11.1.5].