					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII16					Dokumenttitel: **Richtlinie zu Datenschutzschulung, Sensibilisierung und Kompetenz**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard / Regulation	Clause / Control / Article	Applicability	Coverage Type	Comment
ISO/IEC 27701:2025	Clause 7.2; Clause 7.3	Both	Primary	Kompetenz und Sensibilisierung
ISO/IEC 27701:2025	Clause 7.4; Clause 7.5	Both	Supporting	Kommunikation und dokumentierte Nachweise
ISO/IEC 27701:2025	Clause 8.1; Clause 9.1; Clause 10.2	Both	Supporting	Operative Steuerung, Messung und Verbesserung
ISO/IEC 27701:2025	Annex A.3.17	Both	Primary	Sensibilisierung, Ausbildung und Schulung zur Verarbeitung von PII
GDPR	Article 5(2); Article 24; Article 28; Article 32; Article 39	Both	Supporting	Rechenschaftspflicht, Governance für Auftragsverarbeiter, Sicherheit und Aufgaben des DPO
ISO/IEC 27001:2022	Clause 7.2; Clause 7.3; Annex A control 6.3	Both	Supporting	Kompetenz, Sensibilisierung und Schulung
ISO/IEC 27002:2022	Control 6.3	Both	Supporting	Leitlinien zu Sensibilisierung, Ausbildung und Schulung
ISO/IEC 29100:2020	Clause 5.11; Clause 5.12	Both	Supporting	Informationssicherheit und Einhaltung datenschutzbezogener Anforderungen

1. Geltungsbereich

1.1 Diese Richtlinie legt die Anforderungen der Organisation an Datenschutzschulung, Sensibilisierung und Kompetenz innerhalb des Privacy Information Management System fest.

1.2 Diese Richtlinie gilt für Personal, Auftragnehmer, Zeitarbeitskräfte, relevante Dritte, Auftragsverarbeiter, Unterauftragsverarbeiter und andere interessierte Parteien, deren Arbeit die Verarbeitung von PII, die PIMS-Leistung, Rechte betroffener Personen, Datenschutzrisiken, Informationssicherheit im Zusammenhang mit PII, Weisungen an Auftragsverarbeiter, Datenschutzvorfälle, dokumentierte Informationen oder Nachweise der Einhaltung beeinflussen kann.

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

1.4 Diese Richtlinie umfasst:

1.4.1 Identifizierung der Schulungszielgruppen für Datenschutzschulungen;

1.4.2 Onboarding-Schulung;

1.4.3 jährliche Auffrischungsschulung;

1.4.4 rollenbasierte und ereignisgesteuerte Schulung;

1.4.5 Nachweise über den Schulungsabschluss;

1.4.6 Eskalation bei Nichtabschluss;

1.4.7 Überprüfung der Schulungswirksamkeit;

1.4.8 Nachweise zur Sicherstellung von Schulungen bei Auftragsverarbeitern, Unterauftragsverarbeitern und Dritten.

1.5 Diese Richtlinie erstellt keine separate Schulungsmatrix, kein Schulungs-Dashboard, kein Personalregister, kein Kompetenzregister, kein Disziplinarregister und kein Kundenschulungsregister. Schulungszuweisungen, Abschlüsse, Erinnerungen, Kompetenznachweise und Sensibilisierungsnachweise werden in REG11 aufgezeichnet; Ausnahmen, Eskalationen, Nichtkonformitäten, Korrekturmaßnahmen und Überprüfungsnachweise werden in REG12 aufgezeichnet. Nachweise zur Sicherstellung von Schulungen bei Auftragsverarbeitern, Unterauftragsverarbeitern und Dritten werden, soweit relevant, in REG08 aufgezeichnet.

1.6 Diese Richtlinie dupliziert nicht:

1.6.1 die Zuweisung von Rollenverantwortlichkeiten in PII02;

1.6.2 Anforderungen an das Verzeichnis der Verarbeitungstätigkeiten und die Rechtsgrundlage in PII03;

1.6.3 Methodik für Datenschutzrisiken und DPIA in PII07;

1.6.4 Gates für Datenschutz durch Technikgestaltung in PII08;

1.6.5 Governance des Lebenszyklus von Auftragsverarbeitern in PII12;

1.6.6 Betrieb der PII-Sicherheit und Zugriffskontrolle in PII14;

1.6.7 Workflow für Datenschutzvorfälle und Verletzungen des Schutzes personenbezogener Daten in PII15;

1.6.8 Governance dokumentierter Informationen in PII17;

1.6.9 Governance für Überwachung, internes Audit und Verbesserung in PII18.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass Personen, deren Arbeit die Verarbeitung von PII beeinflusst, ihre Datenschutzverantwortlichkeiten verstehen, angemessene Schulungen nach

einem festgelegten Turnus absolvieren, rollenrelevante Kompetenz aufrechterhalten und auditierbare Nachweise über Schulung, Sensibilisierung und Eskalation erzeugen.

2.2 Diese Richtlinie unterstützt eine konsistente PIMS-Umsetzung, indem REG11 als primäres Nachweisobjekt für Schulung und Sensibilisierung sowie REG08, REG10 und REG12 als unterstützende Nachweisobjekte verwendet werden.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 Schulungszielgruppen für Datenschutzschulungen zu definieren;

3.1.2 Anforderungen an Onboarding-Schulungen zu definieren;

3.1.3 Anforderungen an jährliche Auffrischungsschulungen zu definieren;

3.1.4 Anforderungen an rollenbasierte Datenschutzschulungen zu definieren;

3.1.5 Abschlussnachweise in REG11 aufzuzeichnen;

3.1.6 Nichtabschlüsse über REG12 zu eskalieren;

3.1.7 Nachweise zur Sicherstellung von Schulungen bei Auftragsverarbeitern, Unterauftragsverarbeitern und Dritten, soweit relevant, in REG08 zu pflegen;

3.1.8 die Schulungswirksamkeit zu überprüfen, ohne übermäßige Kennzahlen oder doppelte Register zu erstellen;

3.1.9 sicherzustellen, dass Schulungsinhalte weiterhin an aktuellen PIMS-Richtlinien und wesentlichen Datenschutzverpflichtungen ausgerichtet bleiben.

4. Richtlinienaussagen

4.1 Schulungszielgruppe und Zuweisung

4.1.1 [All] The Privacy Lead / PIMS Manager MUSS PIMS-Schulungszielgruppen in REG11 definieren, bevor jeder jährliche Schulungszyklus beginnt.

4.1.2 [All] The Process Owner / Business Owner MUSS Personal, dessen Aufgaben die Verarbeitung von PII umfassen, in REG11 identifizieren, bevor Onboarding, Rollenzuweisung oder eine wesentliche Änderung von Aufgaben erfolgt.

4.1.3 [Conditional] The System Owner / Application Owner MUSS Benutzer, die Schulungen zu PII-Systemen, privilegiertem Zugriff oder administrativem Datenschutz benötigen, in REG11 identifizieren, bevor der Zugriff aktiviert oder wesentlich geändert wird.

4.1.4 [Joint Controller] The Privacy Lead / PIMS Manager MUSS die Zuweisung der Schulungsverantwortung für gemeinsam Verantwortliche in REG11 oder REG08 aufzeichnen, bevor die gemeinsame Verarbeitungstätigkeit beginnt oder wesentlich geändert wird.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUSS erweiterte Datenschutzschulungsbedarfe in REG11 identifizieren, bevor Schulungen Rollen zugewiesen werden, die risikoreiche Verarbeitung, besondere Kategorien von PII, Rechte betroffener Personen, DPIAs, internationale Übermittlungen oder Bewertungen von Datenschutzverletzungen bearbeiten.

4.1.6 [All] The Privacy Lead / PIMS Manager MUSS die zugewiesene Schulungszielgruppe, den Schulungstyp, das erforderliche Abschlussdatum und den Nachweisverantwortlichen in REG11 aufzeichnen, bevor jeder jährliche Schulungszyklus beginnt.

4.2 Onboarding und Turnus jährlicher Schulungen

4.2.1 [All] The Privacy Lead / PIMS Manager MUSS Basisschulungen zur Datenschutzsensibilisierung in REG11 innerhalb von 10 Geschäftstagen nach dem Onboarding für Personal mit Zugriff auf PII oder PIMS-Verantwortlichkeiten zuweisen.

4.2.2 [All] The Process Owner / Business Owner MUSS sicherstellen, dass zugewiesenes Personal die Onboarding-Datenschutzschulung in REG11 abschließt, bevor unbeaufsichtigter Zugriff auf PII genehmigt wird oder innerhalb von 30 Tagen nach dem Onboarding, je nachdem, was zuerst eintritt.

4.2.3 [All] The Privacy Lead / PIMS Manager MUSS jährliche Datenschutz-Auffrischungsschulungen in REG11 mindestens einmal alle 12 Monate zuweisen.

4.2.4 [All] The Process Owner / Business Owner MUSS den Status des Abschlusses der jährlichen Auffrischungsschulung für zugewiesenes Personal in REG11 bis zum veröffentlichten jährlichen Fälligkeitstermin bestätigen.

4.2.5 [Conditional] The Privacy Lead / PIMS Manager MUSS gezielte Auffrischungsschulungen in REG11 innerhalb von 30 Tagen nach einer wesentlichen Änderung einer Datenschutzrichtlinie, einer wesentlichen Änderung eines PIMS-Prozesses, einer Audit-Feststellung, wiederholtem Schulungsversagen oder einer relevanten Erkenntnis aus einem Datenschutzvorfall zuweisen.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Ausnahmen

9.1.1 [All] The Process Owner / Business Owner MUSS einen Antrag auf Ausnahme von Datenschutzschulungen in REG12 aufzeichnen, bevor eine erforderliche Abschlussfrist verlängert wird.

9.1.2 [All] The Privacy Lead / PIMS Manager MUSS Anträge auf Ausnahme von Datenschutzschulungen in REG12 genehmigen oder ablehnen, bevor die Ausnahme aktiv wird.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUSS zu Schulungsausnahmen in REG12 vor Genehmigung beraten, wenn die Ausnahme risikoreiche Verarbeitung, besondere Kategorien von PII, Bearbeitung von Rechten, Vorfallbearbeitung, internationale Übermittlungen oder Zertifizierungsnachweise betrifft.

9.1.4 [Conditional] Top Management MUSS Datenschutzschulungsausnahmen in REG12 vor Aktivierung genehmigen, wenn die Ausnahme wiederholten Nichtabschluss, privilegierten PII-Zugriff, PII-Verarbeitung mit hoher Tragweite oder Nachweise gegenüber Aufsichtsbehörden betrifft.

9.1.5 [All] The Privacy Lead / PIMS Manager MUSS Ausnahmenverantwortlichen, Ablaufdatum, kompensierende Maßnahme und Überprüfungsdatum in REG12 definieren, bevor eine Datenschutzschulungsausnahme genehmigt wird.

9.1.6 [All] The Process Owner / Business Owner MUSS genehmigte Datenschutzschulungsausnahmen in REG12 vor dem Ablaufdatum der Ausnahme schließen oder verlängern.

10. Durchsetzung

10.1.1 [All] The Privacy Lead / PIMS Manager MUSS eine Schulungsnichtkonformität in REG12 innerhalb von fünf Geschäftstagen aufzeichnen, wenn Nachweise verpflichtender Datenschutzschulungen fehlen, unvollständig, überfällig oder nicht auf REG11 rückführbar sind.

10.1.2 [All] The Process Owner / Business Owner MUSS sicherstellen, dass überfällige verpflichtende Datenschutzschulungen in REG11 oder REG12 innerhalb von 10 Geschäftstagen nach Aufzeichnung des überfälligen Status abgeschlossen oder eskaliert werden.

10.1.3 [Conditional] The System Owner / Application Owner MUSS neuen PII-Zugriff mit hoher Tragweite in REG12 einschränken, wenn erforderliche Onboarding- oder rollenbasierte Datenschutzschulungen nach Eskalation weiterhin nicht abgeschlossen sind.

10.1.4 [Processor] The Vendor / Procurement Owner MUSS fehlende Sicherstellungsnachweise zu Schulungen von Auftragsverarbeitern, Unterauftragsverarbeitern oder externen Arbeitskräften in REG08 und REG12 innerhalb von fünf Geschäftstagen nach Identifizierung eskalieren.

10.1.5 [Conditional] The Incident Response Coordinator MUSS schulungsbezogene Durchsetzungsmaßnahmen innerhalb eines Geschäftstags mit REG10 verknüpfen, wenn das Schulungsversagen zu einem vermuteten oder bestätigten Datenschutzvorfall beigetragen hat.

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

11. Überprüfung und Pflege

11.1.1 [All] The Privacy Lead / PIMS Manager MUSS diese Richtlinie und die Schulungsinhalte mindestens jährlich überprüfen und das Überprüfungsergebnis in REG11 oder REG12 aufzeichnen.

11.1.2 [All] The Privacy Lead / PIMS Manager MUSS diese Richtlinie innerhalb von 30 Tagen nach einer wesentlichen Änderung des PIMS-Geltungsbereichs, des Datenschutzrechts, der Verarbeitungstätigkeiten, des Rollenmodells, der Erkenntnisse aus Vorfällen, der Audit-Feststellungen oder der Ergebnisse zur Schulungswirksamkeit überprüfen.

11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUSS datenschutzrelevante Richtlinienänderungen in REG12 vor Genehmigung überprüfen.

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

11.1.5 [All] The Privacy Lead / PIMS Manager MUSS Schulungsinhalte und Nachweise zur Zuweisung in REG11 innerhalb von 30 Tagen nach einer genehmigten wesentlichen Richtlinienänderung aktualisieren.

12. Zugehörige Richtlinien

12.1 Diese Richtlinie sollte zusammen gelesen werden mit:

12.2 PII01 - Richtlinie zum Privacy Information Management System;

12.3 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht;

12.4 PII03 - Richtlinie zum PII-Verarbeitungsverzeichnis 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 von PII;

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

12.12 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Dritte;

12.13 PII13 - Richtlinie zur internationalen Übermittlung von PII;

12.14 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle;

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

12.16 PII17 - Richtlinie zum Management dokumentierter PIMS-Informationen und Nachweise;

12.17 PII18 - Richtlinie zu PIMS-Überwachung, Audit und Verbesserung.

13. Referenzstandards und Rahmenwerke

13.1 ISO/IEC 27701:2025 - Clause 7.2; Clause 7.3; Clause 7.4. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 7.1.1; 7.1.2; 7.1.3; 11.1.1; 11.1.5].

13.2 ISO/IEC 27701:2025 - Clause 7.5; Clause 9.1; Clause 10.2. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.1; 4.6.4; 4.6.5; 6.1.1; 6.1.2; 6.1.3; 6.1.5; 7.1.7; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 9.1.1; 9.1.2; 9.1.5; 10.1.1; 10.1.2; 10.1.6; 11.1.1; 11.1.2; 11.1.4].

13.3 ISO/IEC 27701:2025 - Annex A.3.17. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.2; 4.6.3; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 11.1.5].

13.4 GDPR - Article 5(2); Article 24; Article 28; Article 32; Article 39. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.2.2; 4.2.3; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.4.4; 4.5.3; 4.5.4; 4.5.5; 5.1.1; 5.1.3; 5.1.7; 6.1.2; 6.1.3; 6.1.4; 7.1.4; 7.1.5; 9.1.3; 9.1.4; 10.1.3; 10.1.4; 10.1.5; 11.1.3].

13.5 ISO/IEC 27001:2022 - Clause 7.2; Clause 7.3; Annex A control 6.3. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 4.2.1; 4.2.3; 4.3.1; 4.3.5; 4.4.1; 4.4.3; 4.5.1; 4.5.2; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 6.1.1; 7.1.1; 7.1.2; 8.1.1; 8.1.2; 8.1.3; 11.1.1].

13.6 ISO/IEC 27002:2022 - Control 6.3. Addressed by clauses [4.1.6; 4.2.1; 4.2.3; 4.2.5; 4.3.1; 4.3.5; 4.3.6; 4.4.1; 4.4.3; 4.5.5; 4.6.1; 4.6.4; 5.1.2; 5.1.4; 5.1.8; 7.1.1; 7.1.2; 7.1.6; 8.1.5; 10.1.2].

13.7 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.5; 4.2.5; 4.3.2; 4.3.3; 4.3.4; 4.3.5; 4.3.6; 4.4.1; 4.5.5; 4.6.4; 4.6.5; 5.1.3; 6.1.2; 6.1.3; 6.1.5; 8.1.5; 9.1.3; 10.1.1; 10.1.6; 11.1.2].