					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII19					Dokumenttitel: **Datenschutzrichtlinie für Beschäftigte**							
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 7.5; Clause 8.1	Both	Primary	Nachweise zum Datenschutz von Beschäftigten und operative Kontrolle
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Überwachung, Nichtkonformität und Korrekturmaßnahmen
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9	Controller	Primary	HR-Zwecke, Verknüpfung mit der Rechtsgrundlage, DSFA-Auslöser, gemeinsame Verantwortlichkeit und Aufzeichnungen
ISO/IEC 27701:2025	Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7	Both	Supporting	Verträge mit HR-Auftragsverarbeitern, Weisungen, Unterstützung und Aufzeichnungen
ISO/IEC 27701:2025	Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11	Controller	Supporting	Verpflichtungen und Rechte von Beschäftigten sowie Weiterleitung bei automatisierter Entscheidungsfindung
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Erhebung, Verarbeitung, Minimierung und Verknüpfung mit Aufbewahrung
ISO/IEC 27701:2025	Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6	Both	Supporting	Aufzeichnungen zu Offenlegungen und Umgang mit rechtlich bindenden Offenlegungen
ISO/IEC 27701:2025	Annex A.3.14; Annex A.3.25	Both	Supporting	Schutz von HR-Aufzeichnungen und Protokollierungsnachweise
GDPR	Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)	Controller	Primary	Datenschutzgrundsätze für Beschäftigte und Rechenschaftspflicht
GDPR	Article 6; Article 9; Article 10	Controller	Supporting	Rechtmäßigkeit, besondere Kategorien und Daten aus Zuverlässigkeitsüberprüfungen

GDPR	Article 12; Article 13; Article 14	Controller	Primary	Transparenz und Datenschutzhinweise für Beschäftigte
GDPR	Article 15; Article 16; Article 17; Article 18; Article 21; Article 22	Controller	Supporting	Rechte von Beschäftigten und Weiterleitung bei automatisierter Entscheidungsfindung
GDPR	Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39	Both	Supporting	Governance, gemeinsam Verantwortliche, Auftragsverarbeiter, Aufzeichnungen, Sicherheit, DSFA und Beratung
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Controller	Supporting	Zweck, Erhebung, Minimierung, Nutzung, Aufbewahrung und Offenlegung
ISO/IEC 29100:2020	Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12	Both	Supporting	Transparenz, Beteiligung, Rechenschaftspflicht, Sicherheit und Einhaltung
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10	Controller	Supporting	PII-Zweck, Erhebung, Minimierung, Aufbewahrung und Beteiligung der betroffenen Person
ISO/IEC 29151:2022	Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2	Controller	Supporting	PII-schützende Kontrollen im Beschäftigungslebenszyklus
ISO/IEC 29151:2022	Clause 15.1.2; Clause 15.2.2; Clause 15.2.3	Both	Supporting	Bewertung, Überwachung und Änderungskontrolle von HR-Auftragsverarbeitern
ISO/IEC 29134:2020	Clause 5.1; Clause 6.2	Controller	Supporting	Verknüpfung mit Datenschutzrisiken im HR-Bereich und DSFA-Auslösern
ISO/IEC 27002:2022	Controls 5.34; 6.1; 6.2; 6.5; 6.6	Both	Supporting	PII-Schutz und Beschäftigungslebenszyklus der Informationssicherheit
ISO/IEC 27002:2022	Controls 8.15; 8.16	Both	Supporting	Protokollierungs- und Überwachungstätigkeiten

1. Geltungsbereich

1.1 Diese Richtlinie definiert Datenschutzanforderungen für Beschäftigte in Bezug auf Erhebung, Nutzung, Offenlegung, Verknüpfung mit Aufbewahrung, Datenschutzhinweise, Bearbeitung von Rechten, Überwachung, Unterstützung durch Auftragsverarbeiter und Nachweismanagement für personenbezogene Daten von Beschäftigten innerhalb des Privacy Information Management System.

1.2 Für diese Richtlinie umfasst „personenbezogene Daten von Beschäftigten“ PII, die sich auf Beschäftigte, Bewerber, ehemalige Beschäftigte, Auftragnehmer, Zeitarbeitskräfte, Praktikanten, entsandte Beschäftigte und andere am Personalbestand beteiligte Personen bezieht, soweit die Organisation deren PII für Zwecke des Personalbestands, der Rekrutierung, Beschäftigung, Beauftragung, Vergütung, Zusatzleistungen, Sicherheit, Einhaltung, Arbeitsplatzverwaltung oder damit verbundene geschäftliche Zwecke verarbeitet.

1.3 Diese Richtlinie gilt für Kontexte als Verantwortlicher und als gemeinsam Verantwortlicher, in denen die Organisation die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten von Beschäftigten bestimmt.

1.4 Diese Richtlinie gilt auch für Kontexte als Auftragsverarbeiter und Unterauftragsverarbeiter, in denen die Organisation personenbezogene Daten von Beschäftigten im Auftrag eines Kunden, vorgelagerten Auftragsverarbeiters oder anderen Verantwortlichen nach dokumentierten Weisungen verarbeitet.

1.5 Diese Richtlinie deckt Folgendes ab:

1.5.1 Erhebung von Beschäftigtendaten;

1.5.2 HR-Verarbeitungszwecke;

1.5.3 Datenschutzhinweise für Beschäftigte;

1.5.4 Bearbeitung von Rechten von Beschäftigten;

1.5.5 Verknüpfung mit Aufbewahrung;

1.5.6 Beschäftigtenüberwachung;

1.5.7 interne Offenlegung;

1.5.8 Kontrollen für HR-Auftragsverarbeiter, Lohn- und Gehaltsabrechnung, HRIS, Zusatzleistungen, Zuverlässigkeitsüberprüfungen und ausgelagerte HR-Services, soweit anwendbar;

1.5.9 Datenschutzvorfälle mit personenbezogenen Daten von Beschäftigten, Nichtkonformitäten, Korrekturmaßnahmen und Verbesserungsnachweise.

1.6 Diese Richtlinie schafft kein separates HR-Datenschutzregister, Beschäftigten-Datenschutzregister, HR-Verarbeitungsregister, Register für Beschäftigtenüberwachung, Register für Zuverlässigkeitsüberprüfungen, HR-Dienstleisterregister, Register für Rechte von Beschäftigten oder Register für Beschäftigtenvorfälle. Nachweise zur Beschäftigtenverarbeitung werden in REG02, REG04, REG06, REG07, REG08, REG10 und REG12 aufgezeichnet.

1.7 Diese Richtlinie enthält keine arbeitsrechtliche Beratung, keine Beratung zu Arbeitsbeziehungen, keine rechtliche Kommentierung zu Betriebsräten, keine Inhalte zu Disziplinarverfahren, keine Verfahrensinhalte für die Lohn- und Gehaltsabrechnung und keine länderspezifischen Vorlagen für Beschäftigungsdokumente.

1.8 Diese Richtlinie dupliziert nicht:

1.8.1 PIMS-Governance in PII01;

1.8.2 Rollenrechenschaftspflicht in PII02;

1.8.3 Verarbeitungsinventar und Verantwortlichkeit für Rechtsgrundlagen in PII03;

1.8.4 Governance für Inhalte von Datenschutzhinweisen in PII04;

1.8.5 Betrieb von Einwilligung und Präferenzen in PII05;

1.8.6 Workflow für Rechte betroffener Personen in PII06;

1.8.7 Methodik für Datenschutzrisiken und DSFA in PII07;

1.8.8 Gates für Datenschutz durch Technikgestaltung in PII08;

1.8.9 Grundregeln für Erhebung, Nutzung, Offenlegung und Weitergabe in PII09;

1.8.10 Umsetzung von Aufbewahrung, Löschung und Entsorgung in PII10;

1.8.11 Governance für Richtigkeit und Qualität in PII11;

1.8.12 Lebenszyklus-Governance für Auftragsverarbeiter, Unterauftragsverarbeiter und Drittparteien in PII12;

1.8.13 Kontrollen für Instrumente internationaler Übermittlungen in PII13;

1.8.14 Umsetzung von Sicherheit und Zugriffskontrolle in PII14;

1.8.15 Behandlung von Vorfällen und Verletzungen in PII15;

1.8.16 Management von Schulung und Sensibilisierung in PII16;

1.8.17 Lenkung dokumentierter Informationen in PII17;

1.8.18 Governance für PIMS-Überwachung, Audit und Verbesserung in PII18;

1.8.19 Kontrollen für KI und automatisierte Entscheidungsfindung in PII21, sofern diese optionale Richtlinie enthalten ist.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass personenbezogene Daten von Beschäftigten nur für dokumentierte, genehmigte, transparente, verhältnismäßige und rechenschaftspflichtige Zwecke des Personalbestands verarbeitet werden und dass Nachweise zum Datenschutz von Beschäftigten in den kanonischen PIMS-Registern geführt werden, ohne eine separate HR-Datenschutznachweisebene zu schaffen.

2.2 Diese Richtlinie unterstützt eine einheitliche Handhabung der Beschäftigtenverarbeitung, indem Beschäftigtenverarbeitungstätigkeiten mit REG02, Datenschutzhinweise für Beschäftigte mit REG07, Betroffenenanfragen von Beschäftigten mit REG06, HR-Datenschutzrisiken und DSFA-Auslöser mit REG04, HR-Auftragsverarbeiter sowie Anbieter für Lohn- und Gehaltsabrechnung oder HRIS mit REG08, Datenschutzvorfälle mit personenbezogenen Daten von Beschäftigten mit REG10 und Ausnahmen, Nichtkonformitäten, Korrekturmaßnahmen sowie Überwachungsnachweise mit REG12 verknüpft werden.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 Nachweise zum Inventar der Beschäftigtenverarbeitung in REG02 zu führen;

3.1.2 Erhebungsquellen, PII-Kategorien, Zwecke, Systeme, Empfänger und Verknüpfung mit Aufbewahrung für Beschäftigte zu dokumentieren;

3.1.3 Nachweise zu Datenschutzhinweisen für Beschäftigte in REG07 zu führen;

3.1.4 HR-Datenschutzrisiken und DSFA-Auslöser über REG04 zu steuern;

3.1.5 Betroffenenanfragen von Beschäftigten über REG06 zu steuern;

3.1.6 Nachweise zu HR-Auftragsverarbeitern, Lohn- und Gehaltsabrechnung, HRIS, Zusatzleistungen, Zuverlässigkeitsüberprüfungen und ausgelagerten HR-Services in REG08 zu führen;

3.1.7 sicherzustellen, dass Beschäftigtenüberwachung dokumentiert, verhältnismäßig, überprüft und, soweit anwendbar, über REG04 und REG12 eskaliert wird;

3.1.8 vermutete Datenschutzvorfälle mit personenbezogenen Daten von Beschäftigten über REG10 zu steuern;

3.1.9 Ausnahmen, Nichtkonformitäten, Korrekturmaßnahmen und Verbesserungsmaßnahmen zum Datenschutz von Beschäftigten in REG12 aufzuzeichnen;

3.1.10 arbeitsrechtliche Beratung und rechtliche Kommentierung zu Betriebsräten in operativen Klauseln zu vermeiden;

3.1.11 doppelte Register, Rollen, Formulare, Dashboards oder HR-spezifische Nachweisobjekte zu vermeiden.

4. Richtlinienaussagen

4.1 Inventar der Beschäftigtenverarbeitung und HR-Verarbeitungszwecke

4.1.1 [Controller] The Process Owner / Business Owner MUST jede Beschäftigtenverarbeitungstätigkeit in REG02 aufzeichnen, bevor personenbezogene Daten von Beschäftigten erhoben, erzeugt, importiert, genutzt oder offengelegt werden.

4.1.2 [Controller] The Process Owner / Business Owner MUST die PII-Kategorien von Beschäftigten, die Beschäftigtengruppe, die Erhebungsquelle, den Verarbeitungszweck, das System, die interne Empfängerkategorie, die externe Empfängerkategorie und die Verknüpfung mit Aufbewahrung in REG02 dokumentieren, bevor die Verarbeitungstätigkeit genehmigt wird.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUST jede neue oder wesentlich geänderte Beschäftigtenverarbeitungstätigkeit in REG02 prüfen, bevor die Verarbeitungstätigkeit für den Betrieb genehmigt wird.

4.1.4 [Conditional] The Data Protection Officer / Privacy Advisor MUST Datenschutzberatung in REG04 aufzeichnen, bevor Beschäftigtenverarbeitung genehmigt wird, die besondere Kategorien von PII, Daten zu Straftaten, Zuverlässigkeitsüberprüfungen, arbeitsmedizinische Daten, biometrische Daten, Standortdaten, Beschäftigtenüberwachung oder Verarbeitung umfasst, die einen Beschäftigten wesentlich beeinträchtigen kann.

4.1.5 [Processor] The Privacy Lead / PIMS Manager MUST die Kundenweisung, den Servicezweck, die Kategorien personenbezogener Daten von Beschäftigten des Kunden und die Verknüpfung mit der Auftragsverarbeiterrolle in REG08 aufzeichnen, bevor personenbezogene Daten von Beschäftigten des Kunden als ausgelagerter HR-, Lohn- und Gehaltsabrechnungs-, Zusatzleistungs-, HRIS-, Screening- oder Personalunterstützungsservice verarbeitet werden.

4.1.6 [Joint Controller] The Privacy Lead / PIMS Manager MUST die Zuweisung der Verantwortlichkeiten zwischen gemeinsam Verantwortlichen für die Verarbeitung von personenbezogenen Daten von Beschäftigten in REG08 aufzeichnen, bevor die gemeinsame Beschäftigtenverarbeitungstätigkeit beginnt.

4.2 Erhebung von Beschäftigtendaten und Datenschutzhinweise für Beschäftigte

4.2.1 [Controller] The Process Owner / Business Owner MUST die Erhebung von personenbezogenen Daten von Beschäftigten auf die in REG02 dokumentierten Kategorien beschränken, bevor die Erhebung für Rekrutierung, Onboarding, Beschäftigungsverwaltung, Verwaltung von Zusatzleistungen, Lohn- und Gehaltsabrechnung, Screening, Überwachung oder Offboarding beginnt.

4.2.2 [Controller] The Process Owner / Business Owner MUST die Quelle personenbezogener Daten von Beschäftigten, die von Dritten erhoben werden, in REG02 aufzeichnen, bevor die Erhebungsquelle eines Dritten genutzt wird.

4.2.3 [Controller] The Privacy Lead / PIMS Manager MUST einen Datensatz zu Datenschutzhinweisen für Beschäftigte in REG07 führen, bevor personenbezogene Daten von Beschäftigten direkt oder indirekt für einen neuen oder wesentlich geänderten Zweck erhoben werden.

4.2.4 [Controller] The Process Owner / Business Owner MUST bestätigen, dass der aktuelle in REG07 aufgezeichnete Datenschutzhinweis für Beschäftigte verfügbar ist, bevor Erhebung im Rahmen der Rekrutierung, Erhebung im Rahmen des Onboardings, Aktivierung von Überwachung, Anmeldung zu Zusatzleistungen, Zuverlässigkeitsüberprüfung oder eine wesentliche Änderung der Beschäftigtenverarbeitung erfolgt.

4.2.5 [Conditional] The Data Protection Officer / Privacy Advisor MUST den Datensatz zum Datenschutzhinweis für Beschäftigte in REG07 vor Veröffentlichung prüfen, wenn der Hinweis Beschäftigtenüberwachung, Zuverlässigkeitsüberprüfungen, besondere Kategorien von PII, Daten zu Straftaten, automatisierte Entscheidungsfindung oder einen wesentlich geänderten Zweck der Beschäftigtenverarbeitung abdeckt.

4.2.6 [Processor] The Vendor / Procurement Owner MUST Verantwortlichkeiten für beschäftigtenbezogene Erhebungskanäle in REG08 aufzeichnen, bevor ein durch einen Auftragsverarbeiter betriebener HR-, Lohn- und Gehaltsabrechnungs-, HRIS-, Zusatzleistungs-, Screening- oder ausgelagerter HR-Service personenbezogene Daten von Beschäftigten im Auftrag eines Kunden erhebt.

[... 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 MUST einen Ausnahmeantrag in REG12 aufzeichnen, bevor von einer Anforderung dieser Richtlinie abgewichen wird.

9.1.2 [Conditional] The Data Protection Officer / Privacy Advisor MUST Beratung in REG12 aufzeichnen, bevor eine Ausnahme genehmigt wird, die Beschäftigtenüberwachung, Bearbeitung von Rechten von Beschäftigten, Zuverlässigkeitsüberprüfungen, besondere Kategorien von PII, Daten zu Straftaten oder HR-Verarbeitung mit hoher Tragweite betrifft.

9.1.3 [Conditional] Top Management MUST Datenschutz-Ausnahmen für Beschäftigte in REG12 vor Aktivierung genehmigen, wenn die Ausnahme HR-Verarbeitung mit hohem Risiko, Beschäftigtenüberwachung, externe Offenlegung, Abhängigkeit von Auftragsverarbeitern oder ungelöste Korrekturmaßnahmen betrifft.

9.1.4 [All] The Privacy Lead / PIMS Manager MUST jeder Datenschutz-Ausnahme für Beschäftigte in REG12 ein Ablaufdatum von höchstens 90 Tagen zuweisen, bevor die Ausnahme aktiviert wird.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST jede Datenschutz-Ausnahme für Beschäftigte in REG12 innerhalb von fünf Geschäftstagen vor Ablauf prüfen.

9.1.6 [All] The Privacy Lead / PIMS Manager MUST jede abgelaufene Datenschutz-Ausnahme für Beschäftigte in REG12 innerhalb von fünf Geschäftstagen nach Ablauf schließen oder eskalieren.

10. Durchsetzung

10.1.1 [All] The Privacy Lead / PIMS Manager MUST innerhalb von fünf Geschäftstagen eine Nichtkonformität in REG12 aufzeichnen, wenn bei der Verarbeitung personenbezogener Daten von Beschäftigten erforderliche Nachweise in REG02, REG07, REG08, REG04 oder REG06 fehlen.

10.1.2 [Conditional] The Incident Response Coordinator MUST vermuteten unbefugten Zugriff auf personenbezogene Daten von Beschäftigten, Offenlegung, Verlust oder Kompromittierung innerhalb eines Geschäftstags nach Feststellung in REG10 aufzeichnen.

10.1.3 [Controller] The Privacy Lead / PIMS Manager MUST die Genehmigung neuer Beschäftigtenüberwachung in REG12 verhindern, wenn erforderliche Nachweise in REG02, REG04 oder REG07 fehlen.

10.1.4 [Both] The Vendor / Procurement Owner MUST neue Offenlegungen personenbezogener Daten von Beschäftigten gegenüber einem HR-Dienstleister in REG08 aussetzen, wenn erforderliche Nachweise zu Auftragsverarbeiter, Unterauftragsverarbeiter, Weisung oder Unterstützung fehlen.

10.1.5 [All] Top Management MUST wiederholte Nichtkonformitäten beim Datenschutz von Beschäftigten in REG12 prüfen, wenn dieselbe Kategorie innerhalb eines rollierenden Zeitraums von 12 Monaten zwei- oder mehrmals auftritt.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUST Abschlussnachweise in REG12 verifizieren, bevor Auditfeststellungen geschlossen werden, die Verarbeitung von Beschäftigtendaten, Hinweise an Beschäftigte, Beschäftigtenüberwachung, Rechte von Beschäftigten oder HR-Dienstleister betreffen.

11. Prüfung und Pflege

11.1.1 [All] The Privacy Lead / PIMS Manager MUST diese Richtlinie mindestens jährlich in REG12 prüfen.

11.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST diese Richtlinie innerhalb von 30 Tagen nach einer wesentlichen Änderung der Beschäftigtenverarbeitung, Beschäftigtenüberwachung, HR-Systeme, Regelungen zur Lohn- und Gehaltsabrechnung, HRIS-Anbieter, Anbieter von Zusatzleistungen, Anbieter für Zuverlässigkeitsüberprüfungen oder ausgelagerten HR-Services in REG12 prüfen.

11.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST vorgeschlagene wesentliche Änderungen an dieser Richtlinie in REG12 prüfen, bevor Genehmigung durch Top Management erfolgt.

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

11.1.5 [All] The Privacy Lead / PIMS Manager MUST REG02, REG07 oder REG08 innerhalb von 15 Geschäftstagen nach einer genehmigten Richtlinienänderung aktualisieren, wenn diese Datensätze zur Beschäftigtenverarbeitung, Datenschutzhinweise für Beschäftigte oder Nachweise zu HR-Dienstleistern betrifft.

11.1.6 [All] The Internal Audit / Compliance Reviewer MUST Beobachtungen zur Wirksamkeit der Prüfung dieser Richtlinie während des geplanten internen PIMS-Auditzyklus in REG12 aufzeichnen.

12. Zugehörige Richtlinien

12.1 Diese Richtlinie wird durch die folgenden zugehörigen Richtlinien unterstützt:

12.2 PII01 - Privacy Information Management System Policy

12.3 PII02 - Privacy Roles, Responsibilities and Accountability Policy

12.4 PII03 - PII Processing Inventory and Lawful Basis Policy

12.5 PII04 - Privacy Notice and Transparency Policy

12.6 PII05 - Consent and Preference Management Policy

12.7 PII06 - PII Principal Rights Management Policy

12.8 PII07 - Privacy Risk Assessment and DPIA Policy

12.9 PII08 - Privacy by Design and Default Policy

12.10 PII09 - PII Collection, Use, Disclosure and Sharing Policy

12.11 PII10 - PII Retention, Deletion and Disposal Policy

12.12 PII11 - PII Accuracy and Quality Policy

12.13 PII12 - Processor, Subprocessor and Third-Party Privacy Management Policy

12.14 PII13 - International PII Transfer Policy

12.15 PII14 - PII Security and Access Control Policy

12.16 PII15 - PII Incident and Breach Management Policy

12.17 PII16 - Privacy Training, Awareness and Competence Policy

12.18 PII17 - PIMS Documented Information and Evidence Management Policy

12.19 PII18 - PIMS Monitoring, Audit and Improvement Policy

12.20 PII21 - AI and Automated Decision-Making Privacy Policy, where included in the optional add-on release scope

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 7.5; Clause 8.1** - Zugeordnet zu dokumentierten Nachweisen zum Datenschutz von Beschäftigten, operativen Genehmigungsgates, Aufzeichnungen zu HR-Auftragsverarbeitern, Hinweisen an Beschäftigte, Überwachungsaufzeichnungen, Ausnahmebehandlung und Umsetzungsnachweisen. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.3; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.1; 7.1.3].

13.2.2 **Clause 9.1; Clause 10.2** - Zugeordnet zu Datenschutzüberwachung für Beschäftigte, Kennzahlen, Auditnachweisen, Stichproben zur Beschäftigtenüberwachung, Behandlung von Nichtkonformitäten, Korrekturmaßnahmen und Verbesserung. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 4.6.7; 8.1.1; 8.1.4; 8.1.7; 10.1.1; 10.1.5].

13.2.3 **Annex A.1.2.2; Annex A.1.2.3; Annex A.1.2.6; Annex A.1.2.8; Annex A.1.2.9** - Zugeordnet zu Zwecken der Beschäftigtenverarbeitung, Verknüpfung mit Rechtsgrundlagen, Weiterleitung von Datenschutzrisiken und DSFA, Zuweisung zwischen gemeinsam Verantwortlichen und Verarbeitungsaufzeichnungen in REG02 und REG04. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.4; 4.1.6; 4.2.2; 4.6.1; 4.6.2].

13.2.4 **Annex A.1.2.7; Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.6; Annex A.2.2.7** - Zugeordnet zu Verträgen mit HR-Auftragsverarbeitern, dokumentierten Weisungen, Verarbeitung personenbezogener Daten von Beschäftigten des Kunden, Unterstützung durch Auftragsverarbeiter und Auftragsverarbeiteraufzeichnungen in REG08. Addressed by clauses [4.1.5; 4.2.6; 4.4.4; 4.5.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5].

13.2.5 **Annex A.1.3.2; Annex A.1.3.6; Annex A.1.3.7; Annex A.1.3.10; Annex A.1.3.11** - Zugeordnet zur Bearbeitung von Rechten von Beschäftigten, Beratung bei komplexen Rechten und Weiterleitung bei automatisierter Entscheidungsfindung oder Verarbeitung mit hoher Tragweite über REG06 und REG04. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3; Annex A.1.4.5; Annex A.1.4.8; Annex A.1.4.9** - Zugeordnet zur Beschränkung der Erhebung von Beschäftigtendaten, genehmigten internen Nutzung, Minimierung, Verknüpfung mit Aufbewahrung und Weiterleitung von

Aufbewahrungsausnahmen. Addressed by clauses [4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.5; 4.6.1].

13.2.7 **Annex A.1.5.4; Annex A.1.5.5; Annex A.2.5.4; Annex A.2.5.5; Annex A.2.5.6** - Zugeordnet zu externen Offenlegungen personenbezogener Daten von Beschäftigten, Datenweitergabeaufzeichnungen, Autorisierung von Offenlegungen durch Auftragsverarbeiter und Weiterleitung von Vorfällen im Zusammenhang mit Offenlegung. Addressed by clauses [4.3.4; 4.3.5; 4.3.6; 4.7.6].

13.2.8 **Annex A.3.14; Annex A.3.25** - Zugeordnet zum Schutz von Datenschutzaufzeichnungen zu Beschäftigten, Nachweisen zu Protokollen der Beschäftigtenüberwachung und vermutetem Missbrauch oder Kompromittierung von Daten der Beschäftigtenüberwachung. Addressed by clauses [4.6.4; 4.6.6; 4.6.7; 7.1.2].

13.3 GDPR

13.3.1 **Article 5(1)(a); Article 5(1)(b); Article 5(1)(c); Article 5(1)(e); Article 5(2)** - Zugeordnet zu rechtmäßiger, fairer, transparenter, zweckgebundener, minimierter, mit Aufbewahrung verknüpfter und rechenschaftspflichtiger Verarbeitung personenbezogener Daten von Beschäftigten. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.2.3; 4.3.1; 4.3.3; 4.4.1; 4.4.5].

13.3.2 **Article 6; Article 9; Article 10** - Zugeordnet zur Verknüpfung mit Rechtsgrundlagen, Weiterleitung besonderer Kategorien personenbezogener Daten von Beschäftigten, Weiterleitung arbeitsmedizinischer und beschäftigungsbezogener sensibler PII sowie Weiterleitung von Daten zu Straftaten oder Zuverlässigkeitsüberprüfungen. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.2.2; 4.7.3].

13.3.3 **Article 12; Article 13; Article 14** - Zugeordnet zu Transparenz für Beschäftigte, Aufzeichnungen zu Datenschutzhinweisen für Beschäftigte, Auslösern für Hinweise bei direkter und indirekter Erhebung sowie Nachweisen zu Überwachungshinweisen. Addressed by clauses [4.2.3; 4.2.4; 4.2.5; 4.6.5].

13.3.4 **Article 15; Article 16; Article 17; Article 18; Article 21; Article 22** - Zugeordnet zur Weiterleitung von Rechten von Beschäftigten, Nachweisen zu Anfragen, Beratung bei komplexen Anfragen und Weiterleitung bei automatisierter Entscheidungsfindung. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.6.3].

13.3.5 **Article 24; Article 26; Article 28; Article 30; Article 32; Article 35; Article 39** - Zugeordnet zu Governance des Verantwortlichen, Zuweisung zwischen gemeinsam Verantwortlichen, Governance für HR-Auftragsverarbeiter, Verarbeitungsaufzeichnungen, sicherer Handhabung, DSFA-Weiterleitung und Einbindung von Datenschutzberatung. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.3.4; 4.3.5; 4.6.2; 4.6.3; 4.6.6; 4.7.1; 4.7.6].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Zugeordnet zur Zweckfestlegung für Beschäftigte, Beschränkung der Erhebung, Minimierung, Nutzungsbeschränkung, Aufbewahrungsbeschränkung und Offenlegungsbeschränkung. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.4.1; 4.4.2; 4.6.1].

13.4.2 **Clause 5.8; Clause 5.9; Clause 5.10; Clause 5.11; Clause 5.12** - Zugeordnet zu Transparenz, Beteiligung von Beschäftigten, Unterstützung von Rechten von Beschäftigten, Rechenschaftspflicht, Informationssicherheit und Nachweisen zur Einhaltung des Datenschutzes. Addressed by clauses [4.2.3; 4.2.4; 4.5.1; 4.5.2; 4.5.5; 4.6.4; 4.6.6; 4.6.7; 4.7.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.10** - Zugeordnet zu PII-Zweckaufzeichnungen, Erhebungskontrollen, Minimierung, Verknüpfung mit Aufbewahrung,

Offenlegungsbeschränkung und Unterstützung der Beteiligung oder des Zugriffs von Beschäftigten. Addressed by clauses [4.1.1; 4.1.2; 4.2.1; 4.3.1; 4.3.4; 4.4.1; 4.4.2; 4.5.1; 4.5.4].

13.5.2 **Clause 7.1.2; Clause 7.1.3; Clause 7.2.4; Clause 7.3.2** - Zugeordnet zu PII-schützenden Kontrollen im Beschäftigungslebenszyklus, die für Screening, Bedingungen, Verknüpfung mit Durchsetzung bei Datenschutzverletzungen sowie Prüfung der Aufbewahrung bei Beendigung oder Änderung des Beschäftigungsverhältnisses relevant sind. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.5; 10.1.1; 10.1.5].

13.5.3 **Clause 15.1.2; Clause 15.2.2; Clause 15.2.3** - Zugeordnet zur Bewertung von HR-Auftragsverarbeitern, Überwachung von HR-Auftragsverarbeitern, Prüfung von HR-Dienstleistern und Nachweisen zu Serviceänderungen in REG08. Addressed by clauses [4.4.4; 4.7.1; 4.7.2; 4.7.3; 4.7.4; 4.7.5; 4.7.6].

13.6 ISO/IEC 29134:2020

13.6.1 **Clause 5.1; Clause 6.2** - Zugeordnet zu Nutzen von Datenschutz-Folgenabschätzungen und Bestimmung von HR-Datenschutzrisiken oder DSFA-Auslösern für Beschäftigtenüberwachung und HR-Verarbeitung mit hoher Tragweite, ohne die DSFA-Methode zu duplizieren. Addressed by clauses [4.1.4; 4.3.3; 4.6.2; 4.6.3].

13.7 ISO/IEC 27002:2022

13.7.1 Controls 5.34; 6.1; 6.2; 6.5; 6.6 - Zugeordnet zu PII-Schutz, Screening, Beschäftigungsbedingungen, Verantwortlichkeiten nach Beschäftigungsänderungen und Vertraulichkeitserwartungen als PII-unterstützende Kontrollen des Beschäftigungslebenszyklus. Addressed by clauses [4.1.4; 4.2.2; 4.4.2; 4.4.4; 4.7.2; 4.7.3].

13.7.2 Controls 8.15; 8.16 - Zugeordnet zu Protokollen der Beschäftigtenüberwachung, Überwachungstätigkeiten, Beschränkung des Protokollzwecks und Prüfung von Überwachungsnachweisen. Addressed by clauses [4.6.1; 4.6.2; 4.6.4; 4.6.6; 4.6.7].