					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII08					Dokumenttitel: **Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen**							
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 6.1.2; Clause 6.1.3	Both	Supporting	Verknüpfung von Datenschutz-Risikobeurteilung und Datenschutz-Risikobehandlung
ISO/IEC 27701:2025	Clause 6.3; Clause 8.1	Both	Primary	Geplante Änderungen und operative Steuerung
ISO/IEC 27701:2025	Clause 7.5	Both	Supporting	Dokumentierte Nachweise zur Datenschutzgestaltung
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Überwachung und Korrekturmaßnahmen
ISO/IEC 27701:2025	Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9	Controller	Supporting	Zwecke, PIA-Auslöser und Aufzeichnungen
ISO/IEC 27701:2025	Annex A.1.4.2; Annex A.1.4.3	Controller	Primary	Beschränkung von Erhebung und Verarbeitung
ISO/IEC 27701:2025	Annex A.1.4.4; Annex A.1.4.5	Controller	Supporting	Ziele für Richtigkeit und Minimierung
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7	Controller	Supporting	Gestaltung von De-Identifizierung, Löschung und temporären Dateien
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7	Processor	Supporting	Kundenvereinbarung, Unterstützung und Aufzeichnungen des Auftragsverarbeiters
ISO/IEC 27701:2025	Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4	Processor	Supporting	Gestaltungsmöglichkeiten des Auftragsverarbeiters
ISO/IEC 27701:2025	Annex A.3.27; Annex A.3.29	Both	Supporting	Entwicklungslebenszyklus und technische Gestaltungsgrundsätze
GDPR	Article 5(1)(b); Article 5(1)(c); Article 5(2)	Controller	Supporting	Zweckbindung, Minimierung und Rechenschaftspflicht
GDPR	Article 24	Controller	Supporting	Maßnahmen des Verantwortlichen
GDPR	Article 25	Controller	Primary	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

GDPR	Article 28	Both	Supporting	Weisungen und Unterstützung durch Auftragsverarbeiter
GDPR	Article 30	Both	Supporting	Aufzeichnungen zu Verarbeitungstätigkeiten
GDPR	Article 35	Controller	Supporting	Verknüpfung mit DPIA-Auslösern
ISO/IEC 29100:2020	Clause 4.7	Both	Supporting	Datenschutzkontrollen durch Gestaltung
ISO/IEC 29100:2020	Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6	Both	Primary	Zweck, Erhebung, Minimierung und Nutzungsbeschränkung
ISO/IEC 29100:2020	Clause 5.7; Clause 5.10; Clause 5.12	Both	Supporting	Richtigkeit, Rechenschaftspflicht und Einhaltung
ISO/IEC 29151:2022	Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8	Both	Primary	PII-Schutzgrundsätze und Kontrollen

1. Geltungsbereich

1.1 Diese Richtlinie legt Anforderungen fest, um Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen in neue und geänderte PII-Verarbeitungstätigkeiten, Projekte, Produkte, Dienste, Systeme, Anwendungen, Integrationen, Beschaffungsaktivitäten und Änderungen von Geschäftsprozessen innerhalb des PIMS-Geltungsbereichs einzubetten.

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

1.3 Pflichten von Auftragsverarbeitern und Unterauftragsverarbeitern gelten, wenn die Organisation Verarbeitungen im Auftrag eines Kunden, Verantwortlichen oder vorgelagerten Auftragsverarbeiters nach dokumentierten Weisungen gestaltet, konfiguriert, ändert oder betreibt.

1.4 Diese Richtlinie umfasst Folgendes:

1.4.1 Datenschutzanforderungen bei Projektinitiierung;

1.4.2 Gestaltungsmaßnahmen für Zweck, Datenminimierung und Voreinstellungen;

1.4.3 Prüfung der Datenschutzgestaltung vor der Produktivsetzung;

1.4.4 durch Änderungen ausgelöste Prüfung der Datenschutzgestaltung;

1.4.5 beschaffungsbezogene Prüfungen des Datenschutzes durch Technikgestaltung;

1.4.6 Verknüpfung mit Datenschutzrisiko, DPIA-Screening und Nachweisen zu Korrekturmaßnahmen.

1.5 Diese Richtlinie ersetzt nicht Folgendes:

1.5.1 PII03 für Verzeichnis der Verarbeitungstätigkeiten, Zwecke, Rechtsgrundlage und ROPA-Aufzeichnungen;

1.5.2 PII04 für Inhalte und Veröffentlichung von Datenschutzhinweisen;

1.5.3 PII05 für Einwilligungs- und Präferenzkontrollen;

1.5.4 PII06 für die Bearbeitung von Rechten betroffener Personen;

1.5.5 PII07 für Datenschutz-Risikobeurteilung und DPIA-Methodik;

1.5.6 PII09 für Kontrollen zu Erhebung, Nutzung, Offenlegung und Weitergabe;

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

1.5.8 PII11 für den Betrieb von Richtigkeits- und Qualitätsmaßnahmen;

1.5.9 PII12 für die Lebenszyklus-Governance von Auftragsverarbeitern, Unterauftragsverarbeitern und Dritten;

1.5.10 PII13 für Mechanismen zur internationalen Übermittlung;

1.5.11 PII14 für PII-Sicherheit und Betrieb der Zugriffskontrolle;

1.5.12 PII18 für PIMS-weite Überwachung, Audit, Korrekturmaßnahmen und Verbesserungs-Governance.

2. Zweck

2.1 Zweck dieser Richtlinie ist es sicherzustellen, dass Datenschutzanforderungen identifiziert, umgesetzt und nachgewiesen werden, bevor die PII-Verarbeitung beginnt oder sich wesentlich ändert, und dass Systeme und Prozesse standardmäßig so konfiguriert sind, dass PII-Erhebung, Nutzung, Exposition, Aufbewahrungsabhängigkeit, Offenlegungsabhängigkeit und Identifizierbarkeit auf das für den dokumentierten Zweck erforderliche Maß beschränkt werden.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 Datenschutzanforderungen in Entscheidungen zu Projektinitiierung, Gestaltung, Beschaffung, Änderung und Produktivsetzung einzubetten;

3.1.2 sicherzustellen, dass Gestaltungen der PII-Verarbeitung mit dokumentierten Zwecken und REG02-Verarbeitungsaufzeichnungen verknüpft sind;

3.1.3 Datenminimierung und datenschutzfreundliche Voreinstellungen umzusetzen, bevor die Verarbeitung beginnt;

3.1.4 sicherzustellen, dass Datenschutzrisiko- und DPIA-Screening ausgelöst werden, ohne die PII07-Methodik zu duplizieren;

3.1.5 sicherzustellen, dass Anforderungen an Beschaffung und Auftragsverarbeitergestaltung aufgezeichnet werden, ohne die PII12-Lebenszyklus-Governance zu duplizieren;

3.1.6 sicherzustellen, dass ungelöste Gestaltungsprobleme über REG12 eskaliert werden;

3.1.7 auditbereite Gestaltungsnachweise in REG02, REG04, REG08 und REG12 zu pflegen.

4. Richtlinienaussagen

4.1 Projektinitiierung und Datenschutzanforderungen

4.1.1 [Both] The Process Owner / Business Owner MUSS einen Eintrag zur Datenschutzgestaltung in REG04 erfassen, bevor ein Projekt, Produkt, Dienst, System, eine Anwendung, Integration oder Änderung eines Geschäftsprozesses initiiert wird, der bzw. die PII betrifft.

4.1.2 [Both] The Process Owner / Business Owner MUSS jeden Eintrag zur Datenschutzgestaltung in REG04 mit einer bestehenden oder im Entwurf befindlichen REG02-Verarbeitungstätigkeit verknüpfen, bevor funktionale Anforderungen genehmigt werden.

4.1.3 [Controller] The Privacy Lead / PIMS Manager MUSS Anforderungen des Verantwortlichen an Datenschutz durch Technikgestaltung in REG04 erfassen, bevor die funktionale Gestaltung des Verantwortlichen genehmigt wird.

4.1.4 [Processor] The Vendor / Procurement Owner MUSS Kundenweisungen zur Datenschutzgestaltung und vertragliche Gestaltungsbeschränkungen in REG08 erfassen, bevor die Gestaltung eines Auftragsverarbeiterdienstes oder eine wesentliche Dienständerung genehmigt wird.

4.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUSS eine Beratung in REG04 erfassen, bevor ein risikoreiches, neuartiges, sensibles, automatisiertes, groß angelegtes oder wesentlich geändertes PII-Design genehmigt wird.

4.1.6 [Both] The Information Security Lead MUSS Abhängigkeiten von PII-Sicherheitskontrollen, die die Datenschutzgestaltung unterstützen, in REG04 erfassen, bevor die Architektur genehmigt wird.

4.2 Datenminimierung und Gestaltung datenschutzfreundlicher Voreinstellungen

4.2.1 [Controller] The Process Owner / Business Owner MUSS die mindestens erforderlichen PII-Kategorien, Kategorien betroffener Personen, Quellen und Zwecke in REG02 und REG04 dokumentieren, bevor die Gestaltung der Erhebung oder des Imports genehmigt wird.

4.2.2 [Both] The System Owner / Application Owner MUSS standardmäßige Verarbeitungseinstellungen auf die für den dokumentierten Zweck mindestens erforderliche PII-Erhebung und -Verarbeitung konfigurieren und Nachweise in REG04 erfassen, bevor die Produktivsetzung erfolgt.

4.2.3 [Controller] The Process Owner / Business Owner MUSS optionale PII-Felder, optionale Verarbeitungsoptionen und standardmäßig deaktivierte Einstellungen in REG02 und REG04 dokumentieren, bevor Benutzeroberfläche, Formular oder Workflow genehmigt werden.

4.2.4 [Both] The System Owner / Application Owner MUSS standardmäßige Einstellungen zur Datenschutzexposition für Ansichten, Berichte, Exporte, Schnittstellen und automatisierte Workflows in REG04 dokumentieren, bevor die Produktivsetzung erfolgt.

4.2.5 [Both] The Process Owner / Business Owner MUSS die Machbarkeit von De-Identifizierung, Pseudonymisierung, Aggregation oder nicht identifizierbarer Verarbeitung in REG04 dokumentieren, bevor identifizierbare PII für Tests, Analysen, Berichterstattung oder sekundäre operative Nutzung genehmigt werden.

4.2.6 [Both] The System Owner / Application Owner MUSS den Umgang mit temporären PII-Artefakten, einschließlich temporärer Dateien, Caches, Protokolle oder Staging-Aufzeichnungen, in REG04 dokumentieren, bevor die Produktivsetzung erfolgt.

4.2.7 [Both] The Process Owner / Business Owner MUSS Gestaltungsanforderungen, die PII10, PII11, PII13 oder PII14 zugeordnet sind, innerhalb von fünf Geschäftstagen nach Identifizierung der Abhängigkeit an den Nachweispfad der zugehörigen Richtlinie in REG04 weiterleiten.

[... 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 Ausnahmen der Datenschutzgestaltung

9.1.1 [Both] The Process Owner / Business Owner MUSS eine Ausnahme der Datenschutzgestaltung in REG12 beantragen, bevor eine Gestaltung oder Änderung genehmigt wird, die eine anwendbare Anforderung an die Datenschutzgestaltung nicht erfüllen kann.

9.1.2 [Both] The Privacy Lead / PIMS Manager MUSS Auswirkung, kompensierende Kontrollen und Ablauf jeder Ausnahme der Datenschutzgestaltung innerhalb von fünf Geschäftstagen nach Antragstellung in REG12 bewerten.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUSS vor Genehmigung einer Ausnahme der Datenschutzgestaltung, die risikoreiche, sensible, automatisierte, groß angelegte, strittige oder rechtlich wesentliche Verarbeitung betrifft, eine Beratung in REG12 erfassen.

9.1.4 [All] Top Management MUSS eine Ausnahme der Datenschutzgestaltung, die Verarbeitung mit hoher Auswirkung, den Geltungsbereich der Zertifizierung, ungelöste wesentliche Risiken oder rechtliche Verpflichtungen betrifft, in REG12 genehmigen, bevor die Ausnahme wirksam wird.

9.1.5 [Both] The Privacy Lead / PIMS Manager MUSS vor Genehmigung für jede genehmigte Ausnahme der Datenschutzgestaltung in REG12 ein Ablaufdatum festlegen, das 90 Tage nicht überschreitet.

9.1.6 [Both] The Privacy Lead / PIMS Manager MUSS jede Ausnahme der Datenschutzgestaltung innerhalb von fünf Geschäftstagen nach Ablauf in REG12 schließen oder erneut bewerten.

10. Durchsetzung

10.1 Durchsetzung und Behandlung von Nichtkonformitäten

10.1.1 [Both] The Privacy Lead / PIMS Manager MUSS eine fehlende Prüfung der Datenschutzgestaltung, fehlende Minimierungsnachweise, ungelöstes Versagen von Voreinstellungen oder nicht autorisierte Produktivsetzung innerhalb von fünf Geschäftstagen nach Identifizierung als Nichtkonformität in REG12 erfassen.

10.1.2 [Both] The System Owner / Application Owner MUSS die Produktivsetzung eines PII-verarbeitenden Systems verhindern, wenn die REG04-Prüfung der Datenschutzgestaltung unvollständig ist, und die Entscheidung vor der Produktivsetzung in REG12 erfassen.

10.1.3 [Both] The Vendor / Procurement Owner MUSS Lieferanten-Onboarding oder Vertragsunterzeichnung verhindern, wenn erforderliche REG08-Nachweise zur Datenschutzgestaltung fehlen, und die Entscheidung vor Onboarding oder Unterzeichnung in REG12 erfassen.

10.1.4 [Both] The Process Owner / Business Owner MUSS die Nutzung einer neuen oder geänderten Gestaltung der PII-Verarbeitung aussetzen, bis REG04-Prüfung, REG02-Aktualisierungen und erforderliche REG12-Ausnahmen abgeschlossen sind.

10.1.5 [All] Top Management MUSS innerhalb von 10 Geschäftstagen eine Korrekturmaßnahme in REG12 für wiederholtes, andauerndes oder schwerwiegendes Versagen der Datenschutzgestaltung verlangen.

10.1.6 [All] The Internal Audit / Compliance Reviewer MUSS die Wirksamkeit von Korrekturmaßnahmen für Nichtkonformitäten der Datenschutzgestaltung in REG12 beim nächsten geplanten PIMS-Audit oder innerhalb von 60 Tagen nach Abschluss verifizieren, je nachdem, was zuerst eintritt.

11. Überprüfung und Pflege

11.1 Überprüfung von Richtlinie und Gestaltungskontrollen

11.1.1 [All] The Privacy Lead / PIMS Manager MUSS diese Richtlinie jährlich und innerhalb von 30 Tagen nach wesentlichen Änderungen in Recht, Verarbeitung, Technologie, Geltungsbereich der Zertifizierung oder PIMS-Kontrollen in REG12 überprüfen.

11.1.2 [Both] The Process Owner / Business Owner MUSS aktive REG02-Verarbeitungstätigkeiten jährlich und innerhalb von 30 Tagen nach wesentlicher Änderung der Verarbeitung auf Änderungen von Abhängigkeiten der Datenschutzgestaltung überprüfen.

11.1.3 [Both] The System Owner / Application Owner MUSS Nachweise zu datenschutzfreundlichen Voreinstellungen in REG04 jährlich und innerhalb von 30 Tagen nach wesentlicher Systemänderung überprüfen.

11.1.4 [Both] The Vendor / Procurement Owner MUSS Pflichten zur Datenschutzgestaltung von Lieferanten, Auftragsverarbeitern, Unterauftragsverarbeitern und Dritten in REG08 vor Verlängerung und innerhalb von 30 Tagen nach wesentlicher Änderung der Geschäftsbeziehung überprüfen.

11.1.5 [Conditional] The Data Protection Officer / Privacy Advisor MUSS die Datenschutz-Auswirkungen wesentlicher Richtlinienänderungen in REG12 vor Genehmigung überprüfen.

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

12. Zugehörige Richtlinien

12.1 PII01 - Richtlinie zum Datenschutz-Informationsmanagementsystem

12.2 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht

12.3 PII03 - Richtlinie zum PII-Verzeichnis der Verarbeitungstätigkeiten und zur Rechtsgrundlage

12.4 PII04 - Richtlinie zu Datenschutzhinweis und Transparenz

12.5 PII05 - Richtlinie zum Einwilligungs- und Präferenzmanagement

12.6 PII06 - Richtlinie zum Management von Rechten betroffener Personen

12.7 PII07 - Richtlinie zur Datenschutz-Risikobeurteilung und DPIA

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

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

12.10 PII11 - Richtlinie zu PII-Richtigkeit und Qualität

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

12.12 PII13 - Richtlinie zur internationalen PII-Übermittlung

12.13 PII14 - Richtlinie zu PII-Sicherheit und Zugriffskontrolle

12.14 PII17 - Richtlinie zu dokumentierter Information und Nachweismanagement im PIMS

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

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 6.1.2; Clause 6.1.3** - Zugeordnet zu Datenschutzrisiko-Screening, Verknüpfung von Behandlungsmaßnahmen, Analyse von Gestaltungsabhängigkeiten, Eskalation und Korrekturmaßnahmen, ohne die vollständige Methodik für Datenschutzrisiko und DPIA zu duplizieren. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.5; 5.1.3; 7.1.7].

13.2.2 **Clause 6.3; Clause 8.1** - Zugeordnet zu geplanten Datenschutzänderungen, Projektinitiierung, operativer Prüfung der Datenschutzgestaltung, Kontrolle der Produktivsetzung und Prüfung wesentlicher Änderungen. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.3.3; 4.3.5; 4.5.1; 4.5.3; 4.5.4; 4.5.6; 7.1.2; 7.1.5; 10.1.2].

13.2.3 **Clause 7.5** - Zugeordnet zu dokumentierten Nachweisen der Datenschutzgestaltung, die in REG02, REG04, REG08 und REG12 aufbewahrt werden. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 5.1.2; 5.1.5; 5.1.6; 5.1.7; 7.1.1; 7.1.3; 7.1.4].

13.2.4 **Clause 9.1; Clause 10.2** - Zugeordnet zu Kennzahlen zur Datenschutzgestaltung, Stichprobenprüfung von Nachweisen, Erfassung von Nichtkonformitäten, Korrekturmaßnahmen und Verifizierung der Wirksamkeit. Addressed by clauses [4.3.6; 4.4.5; 4.5.5; 6.1.1; 6.1.2; 6.1.4; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 10.1.1; 10.1.5; 10.1.6].

13.2.5 **Annex A.1.2.2; Annex A.1.2.6; Annex A.1.2.9** - Zugeordnet zur Dokumentation von Verarbeitungszwecken, Verarbeitungsaufzeichnungen, Verknüpfung der Datenschutzgestaltung und Auslösern für Datenschutzrisiko- oder DPIA-Screening bei Verarbeitung durch Verantwortliche. Addressed by clauses [4.1.2; 4.2.1; 4.3.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.2.6 **Annex A.1.4.2; Annex A.1.4.3** - Zugeordnet zur Beschränkung von PII-Erhebung und -Verarbeitung durch zweckbezogene Mindestdatenanforderungen, standardmäßig deaktivierte optionale Verarbeitung und minimale Standardverarbeitungseinstellungen. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.5.4; 7.1.5; 11.1.3].

13.2.7 **Annex A.1.4.4; Annex A.1.4.5** - Zugeordnet zur Weiterleitung von Richtigkeitsabhängigkeiten, Minimierungszielen, Machbarkeit der De-Identifizierung und Gestaltungsnachweisen zur Minimierung identifizierbarer PII. Addressed by clauses [4.2.5; 4.2.7; 4.3.2; 4.5.2; 7.1.3; 11.1.2].

13.2.8 **Annex A.1.4.6; Annex A.1.4.7** - Zugeordnet zur Identifizierung von De-Identifizierung, Löschabhängigkeit, temporären PII-Artefakten und Weiterleitung an Lebenszykluskontrollen in der Gestaltungsphase, ohne die Umsetzung von Aufbewahrung oder Entsorgung zu duplizieren. Addressed by clauses [4.2.5; 4.2.6; 4.2.7; 4.3.3; 4.5.4; 7.1.5; 11.1.3].

13.2.9 **Annex A.2.2.2; Annex A.2.2.6; Annex A.2.2.7** - Zugeordnet zu Kundenweisungen an Auftragsverarbeiter, Kundenunterstützungsinformationen, Gestaltungsaufzeichnungen des Auftragsverarbeiters und kundenautorisierten Änderungen der Dienstgestaltung. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.6; 5.1.7; 7.1.4; 11.1.4].

13.2.10 **Annex A.2.4.2; Annex A.2.4.3; Annex A.2.4.4** - Zugeordnet zu Gestaltungsmöglichkeiten des Auftragsverarbeiters für temporäre Dateien, Rückgabe- oder Entsorgungsabhängigkeiten und Abhängigkeiten von Übertragungskontrollen, die als Gestaltungsnachweis aufgezeichnet werden, ohne operative Lösch- oder Sicherheitskontrollverfahren zu duplizieren. Addressed by clauses [4.2.6; 4.2.7; 4.4.3; 4.4.4; 4.4.6; 7.1.4; 7.1.6; 11.1.4].

13.2.11 **Annex A.3.27; Annex A.3.29** - Zugeordnet zu Datenschutzanforderungen im Entwicklungslebenszyklus, technischen Gestaltungsgrundsätzen, PII-Schutzprüfpunkten und Nachweisen zu datenschutzfreundlichen Voreinstellungen. Addressed by clauses [4.1.6; 4.3.3; 4.3.4; 4.4.4; 4.5.1; 4.5.4; 5.1.4; 5.1.6; 7.1.5; 7.1.6; 10.1.2; 11.1.3].

13.3 GDPR

13.3.1 **Article 5(1)(b); Article 5(1)(c); Article 5(2)** - Zugeordnet zu Zweckbindung, Mindestgestaltung für PII, Verknüpfung mit Verarbeitungsaufzeichnungen, standardmäßiger Minimierung, Nachweisen und Rechenschaftspflicht. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.4.2; 4.5.2; 5.1.5; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Zugeordnet zu Maßnahmen des Verantwortlichen, Governance-Prüfung, Genehmigung von Ausnahmen, Korrekturmaßnahmen und Richtlinienpflege für die Umsetzung von Datenschutz durch Technikgestaltung. Addressed by clauses [4.1.3; 4.5.6; 5.1.1; 6.1.2; 9.1.2; 9.1.4; 10.1.5; 11.1.6].

13.3.3 **Article 25** - Zugeordnet zu Projektinitiierung, Datenschutzanforderungen in der Gestaltungsphase, datenschutzfreundlichen Voreinstellungen, Minimierung, Beschaffungsprüfungen zur Gestaltung, Prüfung vor Produktivsetzung und durch Änderungen ausgelöster Prüfung. Addressed by clauses [4.1.1; 4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.3.5; 4.4.1; 4.5.1; 4.5.3; 4.5.4; 10.1.2].

13.3.4 **Article 28** - Zugeordnet zu Weisungen an Auftragsverarbeiter, Unterstützung der Gestaltung durch Auftragsverarbeiter, Nachweisen zur Datenschutzgestaltung von Lieferanten und kundenautorisierten Gestaltungsänderungen. Addressed by clauses [4.1.4; 4.4.1; 4.4.3; 4.4.5; 4.4.6; 5.1.7; 7.1.4; 10.1.3; 11.1.4].

13.3.5 **Article 30** - Zugeordnet zur Verknüpfung mit Verarbeitungsaufzeichnungen, REG02-Aktualisierungen, Gestaltungsabhängigkeiten von Verarbeitungstätigkeiten und Nachweisen zu Verarbeitungsaufzeichnungen. Addressed by clauses [4.1.2; 4.2.1; 4.4.2; 4.5.2; 5.1.5; 7.1.3; 11.1.2].

13.3.6 **Article 35** - Zugeordnet zu Auslösern für Datenschutzrisiko- und DPIA-Screening in der Gestaltungsphase, Beratung bei hohem Risiko und nachgelagerten Prüfungen, ohne die DPIA-Methodik zu duplizieren. Addressed by clauses [4.1.5; 4.3.1; 4.3.6; 5.1.3; 6.1.3; 9.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7** - Zugeordnet zur Identifizierung von Datenschutzkontrollen in der Gestaltungsphase, Verknüpfung mit Datenschutzrisiken und Gestaltungsnachweisen für die Kontrollumsetzung. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.3.1; 4.3.2; 4.3.3; 4.3.5; 4.5.1].

13.4.2 **Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6** - Zugeordnet zu Zweckbestimmung, Erhebungsbeschränkung, Datenminimierung, beschränkter Nutzung und standardmäßigen Verarbeitungseinstellungen. Addressed by clauses [4.1.2; 4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.4.2; 4.5.2].

13.4.3 **Clause 5.7; Clause 5.10; Clause 5.12** - Zugeordnet zur Weiterleitung von Richtigkeitsabhängigkeiten, Nachweisen zur Rechenschaftspflicht, Überwachung der Datenschutzgestaltung, Audit und Korrekturmaßnahmen. Addressed by clauses [4.2.7; 4.3.6; 4.5.5; 6.1.1; 6.1.4; 8.1.1; 8.1.2; 10.1.1; 10.1.6].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.3; Annex A.4; Annex A.5; Annex A.7; Annex A.8** - Zugeordnet zu Zwecklegitimität, Erhebungsbeschränkung, Datenminimierung, Nutzungs- und Offenlegungsbeschränkung, Aufbewahrungsabhängigkeit, Umgang mit temporären Dateien und Gestaltungskontrollen für Richtigkeitsabhängigkeiten. Addressed by clauses [4.2.1; 4.2.2; 4.2.3; 4.2.4; 4.2.5; 4.2.6; 4.2.7; 4.4.2; 4.5.2; 4.5.4; 7.1.3; 7.1.5].