					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII07					Dokumenttitel: **Richtlinie zur Datenschutz-Risikobeurteilung und DPIA**							
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 / Vorschrift	Klausel / Kontrolle / Artikel	Anwendbarkeit	Abdeckungsart	Kommentar
ISO/IEC 27701:2025	Clause 6.1.1	Both	Primary	PIMS-Risiken und Chancen
ISO/IEC 27701:2025	Clause 6.1.2	Both	Primary	Datenschutz-Risikobeurteilung
ISO/IEC 27701:2025	Clause 6.1.3	Both	Primary	Datenschutz-Risikobehandlung und Verknüpfung mit der SoA
ISO/IEC 27701:2025	Clause 6.3	Both	Supporting	Geplante PIMS-Änderungen und erneute Risikobeurteilung
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Dokumentierte Informationen zu Datenschutzrisiken und DPIA
ISO/IEC 27701:2025	Clause 8.1	Both	Supporting	Operative Planung und Steuerung
ISO/IEC 27701:2025	Clause 8.2	Both	Primary	Operative Datenschutz-Risikobeurteilung
ISO/IEC 27701:2025	Clause 8.3	Both	Primary	Operative Datenschutz-Risikobehandlung
ISO/IEC 27701:2025	Clause 9.1	Both	Supporting	Überwachung und Messung von Datenschutzrisiken
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Managementbewertung von Datenschutzrisiken
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Risikobezogene Nichtkonformität und Korrekturmaßnahme
ISO/IEC 27701:2025	Annex A.1.2.6	Controller	Primary	Datenschutz-Folgenabschätzung
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Supporting	Verarbeitungsaufzeichnungen zur Unterstützung der Risikobeurteilung
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Supporting	Kundenvereinbarung des Auftragsverarbeiters und Unterstützung bei der DPIA
ISO/IEC 27701:2025	Annex A.2.2.6	Processor	Supporting	Informationen des Auftragsverarbeiters zur Unterstützung der Einhaltung durch Kunden
GDPR	Article 5(2)	Controller	Supporting	Nachweise der Rechenschaftspflicht

GDPR	Article 24	Controller	Supporting	Verantwortung des Verantwortlichen und Maßnahmen
GDPR	Article 25	Controller	Supporting	Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
GDPR	Article 28	Both	Supporting	Unterstützung und Weisungen für Auftragsverarbeiter
GDPR	Article 30	Both	Supporting	Verarbeitungsaufzeichnungen zur Unterstützung der DPIA
GDPR	Article 32	Both	Supporting	Sicherheitsrisiko und Schutzmaßnahmen
GDPR	Article 35	Controller	Primary	Datenschutz-Folgenabschätzung
GDPR	Article 36	Controller	Primary	Vorherige Konsultation
GDPR	Article 39	Conditional	Supporting	Beratung und Überwachung durch den DPO, soweit anwendbar
ISO/IEC 29100:2020	Clause 4.7; Clause 5.11; Clause 5.12	Both	Supporting	Datenschutzkontrollen, Informationssicherheit und Einhaltung des Datenschutzes
ISO/IEC 29134:2020	Clause 1; Clause 5.1; Clause 6.2; Clause 6.3	Both	Primary	Umfang, Nutzen, Auslöser und Vorbereitung einer PIA
ISO/IEC 29151:2022	Clause 4.1; Clause 4.2	Both	Supporting	PII-Schutzprogramm und Identifizierung von Anforderungen
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7	Both	Supporting	Integration des organisatorischen Datenschutz-Risikomanagements

1. Geltungsbereich

1.1 Diese Richtlinie definiert die Anforderungen an die Datenschutz-Risikobeurteilung, das DPIA-Screening, die Durchführung einer vollständigen DPIA, die Risikobehandlung, die Restrisikoakzeptanz, die Konsultation, die Überprüfung und das Nachweismanagement für die PII-Verarbeitung innerhalb des PIMS-Geltungsbereichs.

1.2 Diese Richtlinie gilt für:

1.2.1 neue und wesentlich geänderte PII-Verarbeitungstätigkeiten;

1.2.2 Verarbeitungskontexte als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter;

1.2.3 Systeme, Anwendungen, Services, Geschäftsprozesse, Lieferanten, Auftragsverarbeiter, Unterauftragsverarbeiter, internationale Übermittlungen und Datenfreigabevereinbarungen, die die PII-Verarbeitung betreffen;

1.2.4 Nachweise zu Datenschutzrisiken und DPIA, die in REG04 geführt werden, sowie unterstützende Nachweise, die in REG02, REG03, REG08, REG09, REG10, REG11 und REG12 geführt werden.

1.3 Diese Richtlinie ersetzt nicht Kontrollen zum Verarbeitungsinventar, Kontrollen zu Datenschutzhinweisen, Kontrollen zu Einwilligungen, Kontrollen zu Rechten betroffener Personen, Kontrollen zu Datenschutz durch Technikgestaltung, Lieferantenkontrollen, Kontrollen zu internationalen Übermittlungen, PII-Sicherheitskontrollen, Vorfallkontrollen, Kontrollen zu dokumentierten Informationen oder Kontrollen zu Überwachung, Audit und Verbesserung. Diese Anforderungen sind in den in Abschnitt 12 aufgeführten zugehörigen Richtlinien festgelegt.

1.4 Für diese Richtlinie bezeichnet Datenschutz-Risikobeurteilung die dokumentierte Identifizierung, Analyse, Bewertung, Behandlung, Überprüfung und Überwachung potenzieller nachteiliger Auswirkungen auf den Datenschutz, die sich aus der PII-Verarbeitung ergeben.

1.5 Für diese Richtlinie bezeichnet DPIA eine dokumentierte Bewertung, die für Verarbeitungen durch Verantwortliche verwendet wird, die voraussichtlich zu einem hohen Risiko für betroffene Personen führen, und die Erforderlichkeit und Verhältnismäßigkeit der Verarbeitung, Risiken, Schutzmaßnahmen, Restrisiken, Konsultationsbedarf und Genehmigungsbedingungen bewertet.

1.6 Für diese Richtlinie bezeichnet hohes Datenschutz-Restrisiko ein Datenschutzrisiko, das nach vorgeschlagener oder umgesetzter Risikobehandlung über dem genehmigten Akzeptanzschwellenwert verbleibt.

1.7 Für diese Richtlinie bezeichnet eine wesentliche Änderung jede Änderung, die den PIMS-Geltungsbereich, den Verarbeitungszweck, die Rechtsgrundlage, PII-Kategorien, Kategorien betroffener Personen, den Verarbeitungsumfang, die Verarbeitungstechnologie, Überwachung oder Profiling, automatisierte Entscheidungsfindung, schutzbedürftige betroffene Personen, Empfänger, Auftragsverarbeiter, Unterauftragsverarbeiter, internationale Übermittlungen, Aufbewahrung, Sicherheitskontrollen, das Risikoprofil, Kundenweisungen oder den Geltungsbereich der Zertifizierung betrifft.

2. Zweck

2.1 Zweck dieser Richtlinie ist sicherzustellen, dass Datenschutzrisiken und DPIA-Pflichten identifiziert, beurteilt, behandelt, genehmigt, überprüft und nachgewiesen werden, bevor die PII-Verarbeitung ein inakzeptables Risiko für betroffene Personen oder für das PIMS schafft.

2.2 Diese Richtlinie ermöglicht der Organisation, risikobasierte Datenschutz-Governance, Rechenschaftspflicht des Verantwortlichen bei DPIA, Unterstützung durch Auftragsverarbeiter bei DPIA, dokumentierte Risikobehandlung, Genehmigung von Restrisiken, Entscheidungsfindung zur vorherigen Konsultation und kontinuierliche Verbesserung von Datenschutzkontrollen nachzuweisen.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

3.1.1 verbindliche Auslöser für das Datenschutz-Risiko-Screening festzulegen;

3.1.2 festzulegen, wann eine vollständige DPIA erforderlich ist;

3.1.3 sicherzustellen, dass DPIA-Entscheidungen des Verantwortlichen dokumentiert und überprüfbar sind;

3.1.4 sicherzustellen, dass Unterstützung durch Auftragsverarbeiter und Unterauftragsverarbeiter bei DPIA dokumentiert wird, soweit dies durch Kundenweisung oder Vereinbarung erforderlich ist;

3.1.5 sicherzustellen, dass Datenschutzrisiken beurteilt werden, bevor neue oder wesentlich geänderte PII-Verarbeitung erfolgt;

3.1.6 sicherzustellen, dass Datenschutz-Risikobehandlungen zugewiesen, umgesetzt und verifiziert werden;

3.1.7 sicherzustellen, dass hohe Datenschutz-Restrisiken eskaliert und genehmigt werden, bevor die Verarbeitung beginnt oder fortgesetzt wird;

3.1.8 sicherzustellen, dass Entscheidungen zur vorherigen Konsultation dokumentiert werden, wenn ein hohes Restrisiko verbleibt;

3.1.9 sicherzustellen, dass Nachweise zu Datenschutzrisiken und DPIA in REG04 geführt und mit zugehörigen Nachweisobjekten verknüpft werden;

3.1.10 die Erstellung separater DPIA-, Risiko- oder Konsultationsregister außerhalb von REG04 zu vermeiden.

4. Richtlinienaussagen

4.1 Datenschutz-Risiko-Screening

4.1.1 [Both] Der Process Owner / Business Owner MUSS das Datenschutz-Risiko-Screening in REG04 einleiten, bevor eine neue oder wesentlich geänderte PII-Verarbeitung, die in REG02 aufgezeichnet ist, beginnt.

4.1.2 [Both] Der Privacy Lead / PIMS Manager MUSS die Kriterien für das Datenschutz-Risiko-Screening in REG04 vor dem erstmaligen PIMS-Betrieb und danach jährlich pflegen.

4.1.3 [Controller] Der Process Owner / Business Owner MUSS das DPIA-Screening in REG04 abschließen, bevor eine Verarbeitung durch den Verantwortlichen beginnt, die die Kriterien für das Datenschutz-Risiko-Screening erfüllt.

4.1.4 [Processor] Der Vendor / Procurement Owner MUSS Anforderungen des Kunden an die Unterstützung bei der DPIA in REG08 erfassen, bevor die Verarbeitung durch den Auftragsverarbeiter beginnt, wenn die Kundenvereinbarung oder dokumentierte Weisung Unterstützung bei der DPIA verlangt.

4.1.5 [Both] Der System Owner / Application Owner MUSS Nachweise zu Systemdesign, Zugriff, Sicherheit, Protokollierung und Datenflüssen in REG04 bereitstellen, bevor die Datenschutz-Risikobeurteilung für neue oder wesentlich geänderte Systeme, die PII verarbeiten, genehmigt wird.

4.1.6 [Both] Der Privacy Lead / PIMS Manager MUSS das Screening-Ergebnis und die Begründung der Entscheidung zur vollständigen DPIA in REG04 erfassen, bevor die Verarbeitungstätigkeit fortgesetzt wird.

4.2 DPIA-Auslöser und Feststellung der Erforderlichkeit

4.2.1 [Controller] Der Privacy Lead / PIMS Manager MUSS eine vollständige DPIA in REG04 verlangen, bevor eine Verarbeitung durch den Verantwortlichen beginnt, die voraussichtlich zu einem hohen Risiko führt.

4.2.2 [Controller] Der Process Owner / Business Owner MUSS Verarbeitungen mit großem Umfang, systematischer Überwachung, Profiling, automatisierten Entscheidungen, besonderen Kategorien von PII, Daten zu strafrechtlichen Verurteilungen oder Straftaten, schutzbedürftigen betroffenen Personen, innovativer Technologie oder wesentlich geänderter Verarbeitung an den Privacy Lead / PIMS Manager in REG04 verweisen, bevor die Verarbeitung beginnt.

4.2.3 [Controller] Der Data Protection Officer / Privacy Advisor MUSS Beratung in REG04 erfassen, bevor die Entscheidung über die Erforderlichkeit einer vollständigen DPIA für eine Hochrisiko-Verarbeitung durch den Verantwortlichen genehmigt wird.

4.2.4 [Both] Der Process Owner / Business Owner MUSS das Datenschutzrisiko in REG04 erneut screenen, bevor PII für einen neuen Zweck verwendet, ein neuer Empfänger hinzugefügt, ein neuer Auftragsverarbeiter oder Unterauftragsverarbeiter eingeführt, die Systemarchitektur geändert oder eine neue internationale Übermittlung begonnen wird.

4.2.5 [Processor] Der Privacy Lead / PIMS Manager MUSS innerhalb von 10 Geschäftstagen nach Eingang einer Kundenanfrage zur DPIA-Unterstützung in REG08 dokumentieren, ob Unterstützung durch den Auftragsverarbeiter bei der DPIA erforderlich ist.

4.2.6 [Subprocessor] Der Vendor / Procurement Owner MUSS vorgelagerte Anforderungen an die DPIA-Unterstützung in REG08 dokumentieren, bevor die Unterauftragsverarbeitung beginnt, wenn die vorgelagerte Kunden- oder Auftragsverarbeitervereinbarung eine solche Unterstützung verlangt.

[... 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 zu Datenschutzrisiken und DPIA

9.1.1 [All] Der Process Owner / Business Owner MUSS jede Ausnahme von dieser Richtlinie in REG12 beantragen, bevor die Abweichung eintritt.

9.1.2 [All] Der Privacy Lead / PIMS Manager MUSS die Auswirkungen jeder beantragten Ausnahme auf Datenschutz, Recht, Zertifizierung, Betrieb und betroffene Personen innerhalb von 10 Geschäftstagen nach Antragstellung in REG04 oder REG12 bewerten.

9.1.3 [All] Der Data Protection Officer / Privacy Advisor MUSS Beratung in REG12 erfassen, bevor eine Ausnahme genehmigt wird, die Hochrisiko-Verarbeitung, Abschluss einer vollständigen DPIA, vorherige Konsultation, hohes Datenschutz-Restrisiko oder Kundenunterstützung bei DPIA betrifft.

9.1.4 [All] Top Management MUSS Ausnahmen zu Datenschutzrisiken oder DPIA, die Hochrisiko-Verarbeitung, den Geltungsbereich der Zertifizierung, vorherige Konsultation oder ungelöste hohe Datenschutz-Restrisiken betreffen, in REG12 genehmigen, bevor die Ausnahme wirksam wird.

9.1.5 [All] Der Privacy Lead / PIMS Manager MUSS für jede genehmigte Ausnahme zu Datenschutzrisiken oder DPIA vor der Genehmigung ein Ablaufdatum in REG12 festlegen, das 90 Tage nicht überschreitet.

9.1.6 [All] Der Process Owner / Business Owner MUSS jede Ausnahme zu Datenschutzrisiken oder DPIA innerhalb von fünf Geschäftstagen nach Ablauf in REG12 schließen oder erneut beurteilen.

10. Durchsetzung

10.1 Durchsetzung zu Datenschutzrisiken und DPIA

10.1.1 [All] Der Privacy Lead / PIMS Manager MUSS fehlende, unrichtige, unvollständige, überfällige oder nicht genehmigte REG04-Nachweise zu Datenschutzrisiken oder DPIA innerhalb von fünf Geschäftstagen nach Identifizierung als Nichtkonformität in REG12 erfassen.

10.1.2 [Controller] Der Process Owner / Business Owner MUSS neue Hochrisiko-Verarbeitung durch den Verantwortlichen aussetzen, wenn erforderliche REG04-Nachweise zur DPIA-Genehmigung vor dem Start fehlen.

10.1.3 [Both] Der System Owner / Application Owner MUSS die Produktivsetzung von Systemen, die PII verarbeiten, blockieren, wenn erforderliche REG04-Nachweise zur Risikobehandlung vor der Genehmigung der Produktivsetzung fehlen.

10.1.4 [Both] Der Vendor / Procurement Owner MUSS das Onboarding von Lieferanten, Auftragsverarbeitern, Unterauftragsverarbeitern oder Datenfreigaben blockieren, wenn erforderliche REG04-Nachweise zu Datenschutzrisiken oder DPIA-Unterstützung vor der Genehmigung der Vereinbarung fehlen.

10.1.5 [All] Top Management MUSS ungelöste wesentliche Nichtkonformitäten zu Datenschutzrisiken oder DPIA in REG12 während der Managementbewertung überprüfen.

10.1.6 [All] Der Privacy Lead / PIMS Manager MUSS wiederholt versäumte REG04-Fristen für Screening, DPIA-Überprüfung oder Risikobehandlung innerhalb von fünf Geschäftstagen nach dem zweiten Auftreten in einem Zeitraum von 12 Monaten in REG12 an Top Management eskalieren.

10.1.7 [All] Der Internal Audit / Compliance Reviewer MUSS die Wirksamkeit von Korrekturmaßnahmen für Nichtkonformitäten zu Datenschutzrisiken und DPIA in REG12 beim nächsten geplanten Audit oder innerhalb von 60 Tagen nach Abschluss verifizieren, je nachdem, was früher eintritt.

11. Überprüfung und Pflege

11.1 Richtlinienüberprüfung und -pflege

11.1.1 [All] Der Privacy Lead / PIMS Manager MUSS diese Richtlinie jährlich und innerhalb von 30 Tagen nach wesentlichen Änderungen an Anforderungen zu Datenschutzrisiken, DPIA, vorheriger Konsultation, Unterstützung durch Auftragsverarbeiter oder Zertifizierung in REG12 überprüfen.

11.1.2 [All] Der Privacy Lead / PIMS Manager MUSS REG04-Screening-Kriterien, DPIA-Auslösekriterien, Risikoeinstufungskriterien und Kriterien für die Restrisikoakzeptanz jährlich in REG12 überprüfen.

11.1.3 [All] Der Data Protection Officer / Privacy Advisor MUSS datenschutzrelevante Änderungen an dieser Richtlinie in REG12 vor der Genehmigung überprüfen.

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

11.1.5 [All] Der Privacy Lead / PIMS Manager MUSS REG03 und REG04 innerhalb von 15 Geschäftstagen nach genehmigten Richtlinienänderungen aktualisieren, die die Anwendbarkeit von Kontrollen, Risikokriterien oder DPIA-Screening-Anforderungen ändern.

11.1.6 [All] Der Privacy Lead / PIMS Manager MUSS die Kommunikation genehmigter Änderungen an dieser Richtlinie innerhalb von 30 Tagen nach Veröffentlichung in REG11 erfassen.

12. Zugehörige Richtlinien

12.1 Diese Richtlinie wird durch die folgenden zugehörigen Richtlinien unterstützt:

12.2 PII01 - Richtlinie zum Datenschutz-Informationsmanagementsystem

12.3 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht

12.4 PII03 - Richtlinie zum PII-Verarbeitungsinventar und zur Rechtsgrundlage

12.5 PII04 - Richtlinie zu Datenschutzhinweisen und Transparenz

12.6 PII05 - Richtlinie zum Einwilligungs- und Präferenzmanagement

12.7 PII06 - Richtlinie zum Management der Rechte betroffener Personen

12.8 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

12.9 PII09 - Richtlinie zur Erhebung, Nutzung, Offenlegung und Weitergabe von PII

12.10 PII10 - Richtlinie zur Aufbewahrung, Löschung und Entsorgung von PII

12.11 PII11 - Richtlinie zur Richtigkeit und Qualität von PII

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

12.13 PII13 - Richtlinie zu internationalen PII-Übermittlungen

12.14 PII14 - Richtlinie zur PII-Sicherheit und Zugriffskontrolle

12.15 PII15 - Richtlinie zum Management von PII-Vorfällen und Datenschutzverletzungen

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

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

13. Referenzstandards und Rahmenwerke

13.1 Diese Richtlinie ist den folgenden Standards und Vorschriften zugeordnet. Die Zuordnung erläutert, wie die Richtlinie die zitierten Anforderungen unterstützt, und identifiziert die internen Klauseln, die diese umsetzen oder unterstützen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 6.1.1** - Zugeordnet zur Identifizierung und Planung von Maßnahmen für Datenschutzrisiken und Chancen unter Verwendung von Screening-Kriterien, Risikoschwellenwerten, Eskalation und Eingaben für die Managementbewertung. Addressed by clauses [4.1.2; 4.4.5; 4.5.6; 6.1.1; 6.1.2; 8.1.2].

13.2.2 **Clause 6.1.2** - Zugeordnet zur Durchführung von Datenschutz-Risiko-Screening, Datenschutz-Risikobeurteilung, Risikoeinstufung, erneuter Beurteilung und Bewertung von DPIA-Auslösern, bevor neue oder wesentlich geänderte Verarbeitung fortgesetzt wird. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.1.6; 4.2.1; 4.2.4; 4.3.1; 4.3.7; 4.6.1].

13.2.3 **Clause 6.1.3** - Zugeordnet zur Planung der Datenschutz-Risikobehandlung, Aktualisierung der Anwendbarkeit von Kontrollen, Umsetzung von Behandlungsmaßnahmen, Restrisikoakzeptanz und Verknüpfung mit der SoA. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 11.1.5].

13.2.4 **Clause 6.3** - Zugeordnet zu geplanten PIMS- und Verarbeitungsänderungen, die eine erneute Datenschutz-Risikobeurteilung und DPIA-Überprüfung auslösen. Addressed by clauses [4.2.4; 4.6.1; 11.1.1].

13.2.5 **Clause 7.5** - Zugeordnet zu gelenkten dokumentierten Informationen für Datenschutz-Risiko-Screening, DPIA-Nachweise, Risikobehandlung, Restrisikoakzeptanz, Entscheidungen zur vorherigen Konsultation, Ausnahmen, Nichtkonformitäten und Nachweise zur Richtlinienüberprüfung. Addressed by clauses [4.1.6; 4.3.7; 4.4.1; 4.5.1; 5.1.2; 7.1.1; 9.1.1; 10.1.1; 11.1.1].

13.2.6 **Clause 8.1** - Zugeordnet zum Betrieb von Kontrollen für Datenschutzrisiken und DPIA vor Produktivsetzung, Onboarding, Verarbeitungsgenehmigung, Abschluss der Behandlung und Verknüpfung mit Korrekturmaßnahmen. Addressed by clauses [4.1.1; 4.1.5; 7.1.2; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 7.1.7; 7.1.8].

13.2.7 **Clause 8.2** - Zugeordnet zur operativen Datenschutz-Risikobeurteilung für neue, geänderte, systembezogene, lieferantenbezogene, übermittlungsbezogene und vorfallgetriebene Verarbeitungsänderungen. Addressed by clauses [4.1.1; 4.2.4; 4.3.1; 4.3.5; 4.5.5; 4.6.1].

13.2.8 **Clause 8.3** - Zugeordnet zur operativen Datenschutz-Risikobehandlung, Zuweisung von Behandlungsmaßnahmen, Umsetzung von Behandlungsmaßnahmen, Eskalation überfälliger Behandlungen und Verifizierung der Wirksamkeit. Addressed by clauses [4.4.1; 4.4.3; 4.4.4; 4.4.6; 4.4.7; 8.1.3; 10.1.7].

13.2.9 **Clause 9.1** - Zugeordnet zur Überwachung und Messung von Screening-Abdeckung, DPIA-Status, offenen Risiken, überfälligen Behandlungsmaßnahmen, Lieferantenmaßnahmen, Sicherheitsbehandlungsmaßnahmen, Maßnahmen zur erneuten Beurteilung nach Vorfällen und Audit-Feststellungen. Addressed by clauses [4.6.3; 4.6.4; 4.6.5; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 8.1.8].

13.2.10 **Clause 9.3** - Zugeordnet zur Managementbewertung hoher Datenschutz-Restrisiken, überfälliger Behandlungsmaßnahmen, des Status vollständiger DPIAs, von Entscheidungen zur vorherigen Konsultation und wesentlicher Datenschutzrisiko-Ausnahmen. Addressed by clauses [4.6.6; 6.1.1; 6.1.2; 6.1.3; 10.1.5].

13.2.11 **Clause 10.2** - Zugeordnet zu Nichtkonformitäten und Ausnahmen im Zusammenhang mit Datenschutzrisiken und DPIA, Eröffnung von Korrekturmaßnahmen, Eskalation und Verifizierung der Wirksamkeit. Addressed by clauses [4.4.6; 9.1.1; 9.1.2; 9.1.4; 9.1.6; 10.1.1; 10.1.5; 10.1.6; 10.1.7].

13.2.12 **Annex A.1.2.6** - Zugeordnet zur Bewertung des Bedarfs an und gegebenenfalls Umsetzung einer Datenschutz-Folgenabschätzung für neue oder geänderte Verarbeitung durch Verantwortliche. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.2.13 **Annex A.1.2.9** - Zugeordnet zu Verarbeitungsaufzeichnungen, die Eingaben für Datenschutzrisiko- und DPIA-Bewertungen unterstützen, einschließlich Zweck, Kategorien, Systeme, Empfänger, Übermittlungen und Lieferanten. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.2.14 **Annex A.2.2.2** - Zugeordnet zu Kundenvereinbarungen des Auftragsverarbeiters und Verpflichtungen zur Kundenunterstützung bei DPIA. Addressed by clauses [4.1.4; 4.2.5; 4.5.4; 5.1.7; 7.1.6].

13.2.15 **Annex A.2.2.6** - Zugeordnet zur Bereitstellung von Informationen durch den Auftragsverarbeiter, die für die Einhaltung durch den Kunden erforderlich sind, einschließlich DPIA-Unterstützung und Nachweisen zur Kundenunterstützung. Addressed by clauses [4.2.5; 4.2.6; 4.5.4; 8.1.5].

13.3 GDPR

13.3.1 **Article 5(2)** - Zugeordnet zu Nachweisen der Rechenschaftspflicht für DPIA-Screening, Entscheidungen zu vollständigen DPIAs, Risikobehandlung, Restrisikoakzeptanz, Entscheidungen zur vorherigen Konsultation, Ausnahmen, Audit-Feststellungen und Korrekturmaßnahmen. Addressed by clauses [4.1.6; 4.3.7; 4.4.5; 4.5.1; 4.6.4; 10.1.1; 10.1.7].

13.3.2 **Article 24** - Zugeordnet zur Verantwortung des Verantwortlichen für angemessene Datenschutzrisikomaßnahmen, Überprüfung hoher Restrisiken, Genehmigung durch Top Management und Richtlinienpflege. Addressed by clauses [4.4.5; 4.5.3; 6.1.2; 10.1.5; 11.1.4].

13.3.3 **Article 25** - Zugeordnet zu Nachweisen für Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen, die in der Risikobeurteilung und vor Genehmigung der Produktivsetzung verwendet werden. Addressed by clauses [4.1.5; 4.3.4; 7.1.5].

13.3.4 **Article 28** - Zugeordnet zu DPIA-Unterstützung durch Auftragsverarbeiter und Unterauftragsverarbeiter, Umgang mit Kundenweisungen und Nachweisen zur Lieferantenrisikobehandlung. Addressed by clauses [4.1.4; 4.2.5; 4.2.6; 4.4.4; 4.5.4; 7.1.6; 8.1.5].

13.3.5 **Article 30** - Zugeordnet zu Verarbeitungsaufzeichnungen, die Eingaben für Datenschutz-Risikobeurteilungen und DPIA unterstützen. Addressed by clauses [4.3.1; 6.1.4; 8.1.1].

13.3.6 **Article 32** - Zugeordnet zu Eingaben zu PII-Sicherheitsrisiken, Auswahl von Schutzmaßnahmen, Sicherheitsrisikobehandlung und Aktualisierung des Status von Sicherheitskontrollen. Addressed by clauses [4.1.5; 4.3.3; 4.4.2; 8.1.6].

13.3.7 **Article 35** - Zugeordnet zu DPIA-Screening, Feststellung der Erforderlichkeit einer vollständigen DPIA, DPIA-Inhalten, Beratung durch den DPO, Überprüfung und Blockierung von Hochrisiko-Verarbeitung ohne erforderliche DPIA-Genehmigung. Addressed by clauses [4.1.3; 4.2.1; 4.2.2; 4.2.3; 4.3.2; 4.3.6; 4.5.1; 4.6.2; 7.1.4; 10.1.2].

13.3.8 **Article 36** - Zugeordnet zur Entscheidungsfindung über vorherige Konsultation, Beratung durch den DPO, Genehmigung durch Top Management und Maßnahmen zur Fortsetzung, Aussetzung, Neugestaltung oder Konsultation, wenn ein hohes Restrisiko verbleibt. Addressed by clauses [4.5.1; 4.5.2; 4.5.3; 6.1.2].

13.3.9 **Article 39** - Zugeordnet zu Beratung und Überwachung durch Data Protection Officer / Privacy Advisor, soweit anwendbar, für DPIA-Entscheidungen, Hochrisiko-Verarbeitung, vorherige Konsultation und Richtlinienänderungen. Addressed by clauses [4.2.3; 4.3.6; 4.5.2; 5.1.3; 6.1.3; 9.1.3; 11.1.3].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.7; Clause 5.11; Clause 5.12** - Zugeordnet zur Identifizierung von Datenschutzkontrollen, Sicherheitsvorkehrungen, Einhaltung des Datenschutzes, Nachweisen zu Datenschutzrisiken, Überwachung und Überprüfung. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.7; 4.6.3; 4.6.5; 8.1.6; 10.1.7].

13.5 ISO/IEC 29134:2020

13.5.1 **Clause 1; Clause 5.1; Clause 6.2; Clause 6.3** - Zugeordnet zum Umfang des PIA-Prozesses, Nutzen, Auslöserbestimmung, Vorbereitung, Bewertungseingaben, Stakeholder-Nachweisen und zur in REG04 geführten DPIA-Berichtsstruktur. Addressed by clauses [4.1.1; 4.1.3; 4.1.6; 4.2.1; 4.3.1; 4.3.2; 4.3.7; 7.1.1].

13.6 ISO/IEC 29151:2022

13.6.1 **Clause 4.1; Clause 4.2** - Zugeordnet zu Anforderungen an das PII-Schutzprogramm, Identifizierung von PII-Schutzanforderungen, risikobasierter Kontrollauswahl und Verknüpfung mit Datenschutz-Risikobehandlung. Addressed by clauses [4.3.3; 4.4.1; 4.4.2; 4.4.3; 4.4.4; 6.1.5].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 6.4; Clause 6.5; Clause 6.6; Clause 6.7** - Zugeordnet zu organisatorischen Grundsätzen für Datenschutzrisiken, Führung, Integration,

Risikobeurteilung, Risikobehandlung, Überwachung und Überprüfung sowie Aufzeichnung und Berichterstattung. Addressed by clauses [4.1.2; 4.3.1; 4.3.7; 4.4.1; 4.4.5; 4.6.3; 4.6.4; 5.1.1; 6.1.1; 6.1.2; 8.1.1; 8.1.3].