

				Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: PII10				Dokumenttitel: Richtlinie zur Aufbewahrung, Löschung und Entsorgung von PII							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025		Dokumentverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges

Änderungshistorie				
Änderungsnummer	Änderungsdatum	Änderungen	Geprüft von	Prozessverantwortlicher

Genehmigungen			
Name	Position	Datum	Unterschrift

Rechtlicher Hinweis (Urheberrecht und Nutzungsbeschränkungen)
(C) 2025 Clarysec LLC. All rights reserved.

Dieses Dokument ist geistiges Eigentum der Clarysec LLC. Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Genehmigung für kommerzielle oder Implementierungszwecke kopiert, wiederverwendet, verbreitet oder verändert werden.

Die unbefugte Nutzung ist streng untersagt und kann rechtliche Schritte nach sich ziehen.

Für Lizenzierungsanfragen kontaktieren Sie bitte: info@clarysec.com

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	Dokumentierte Aufbewahrungsnachweise und operative Steuerung
ISO/IEC 27701:2025	Clause 9.1; Clause 10.2	Both	Supporting	Überwachung, Nichtkonformität und Korrekturmaßnahmen
ISO/IEC 27701:2025	Annex A.1.2.8; Annex A.1.2.9	Controller / Joint Controller	Supporting	Gemeinsame Verantwortung und Verarbeitungsaufzeichnungen
ISO/IEC 27701:2025	Annex A.1.3.7; Annex A.1.3.8	Controller	Supporting	Unterstützung bei der Durchführung der Löschung
ISO/IEC 27701:2025	Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9	Controller	Primary	Aufbewahrung, Löschung und Entsorgung
ISO/IEC 27701:2025	Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7	Processor	Supporting	Kundenweisungen und Aufzeichnungen des Auftragsverarbeiters
ISO/IEC 27701:2025	Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3	Processor	Primary	Löschunterstützung und Entsorgungsfähigkeit
ISO/IEC 27701:2025	Annex A.3.20; Annex A.3.21; Annex A.3.24	Both	Supporting	Entsorgung von Medien und Umgang mit Backups
GDPR	Article 5(1)(e); Article 5(2)	Controller	Primary	Speicherbegrenzung und Rechenschaftspflicht
GDPR	Article 17	Controller	Supporting	Unterstützung bei der Durchführung der Löschung
GDPR	Article 24	Controller	Supporting	Maßnahmen des Verantwortlichen
GDPR	Article 26	Joint Controller	Supporting	Zuweisung gemeinsamer Verantwortung
GDPR	Article 28	Processor	Supporting	Löschung und Rückgabe durch Auftragsverarbeiter
GDPR	Article 30	Both	Supporting	Verarbeitungsaufzeichnungen
GDPR	Article 32	Both	Supporting	Sichere Verarbeitung und Unterstützung der Entsorgung

ISO/IEC 29100:2020	Clause 5.5; Clause 5.6; Clause 5.10	Both	Supporting	Minimierung, Aufbewahrungsbegrenzung und Rechenschaftspflicht
ISO/IEC 29151:2022	Annex A.7; Annex A.7.2	Both	Supporting	Aufbewahrungs- und Löschkontrollen für temporäre Dateien
ISO/IEC 27555:2025	Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8	Both	Primary	Löschrahmenwerk und Dokumentation
ISO/IEC 27555:2025	Clause 7.2; Clause 7.3; Clause 8.3	Controller	Primary	Löschfristen und Löschrregeln
ISO/IEC 27555:2025	Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7	Both	Primary	Umsetzung und Ausnahmen
ISO/IEC 27555:2025	Clause 10.1; Clause 10.2; Clause 10.3	Both	Primary	Verantwortlichkeiten und Umsetzungsgovernance
ISO/IEC 27557:2022	Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1	Both	Supporting	Integration von Datenschutzrisiken
ISO/IEC 27002:2022	Control 7.14; Control 8.10	Both	Supporting	Sichere Entsorgung und Löschung von Informationen

1. Geltungsbereich

- 1.1 Diese Richtlinie legt die Anforderungen der Organisation an die Festlegung, Überprüfung, Durchführung und Nachweisführung für Aufbewahrung, Löschung, Anonymisierung, De-Identifizierung, Rückgabe, Übermittlung und Entsorgung von PII fest.
- 1.2 Diese Richtlinie gilt für PII, die in Kontexten als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter und Unterauftragsverarbeiter verarbeitet wird, einschließlich PII in Produktivsystemen, Archiven, Backup-Kopien, Replikaten, Protokollen, Staging-Umgebungen, temporären Dateien, Papieraufzeichnungen und Speichermedien.
- 1.3 Diese Richtlinie gilt für Aufbewahrungs- und Löschpflichten, die sich aus genehmigten Verarbeitungszwecken, Aufzeichnungen zu Rechtsgrundlagen, Weisungen des Verantwortlichen, vertraglichen Anforderungen, Ergebnissen zur Löschung bei betroffenen Personen, Servicebeendigung, Entsorgung von Speichermedien und Feststellungen der PIMS-Überwachung ergeben.
- 1.4 Diese Richtlinie definiert nicht die Auswahl der Rechtsgrundlage, den Inhalt von Datenschutzhinweisen, die vollständige Bearbeitung der Rechte betroffener Personen, die Governance des Lebenszyklus von Auftragsverarbeitern, Mechanismen für internationale Übermittlungen, die Architektur von Sicherheitskontrollen, den Workflow zur Reaktion auf Vorfälle oder die PIMS-Auditmethodik. Diese Kontrollen werden in zugehörigen Richtlinien behandelt.
- 1.5 Für diese Richtlinie bezeichnet eine wesentliche Änderung jede Änderung des Verarbeitungszwecks, der PII-Kategorie, der Kategorie betroffener Personen, des Systemspeicherorts, des Aufbewahrungsgesetzes oder -vertrags, der Kundenweisung, der Backup-Architektur, des Archivierungsansatzes, des Entsorgungsverfahrens, der Vereinbarung mit Auftragsverarbeiter oder Unterauftragsverarbeiter, des Lösch-Workflows oder des PIMS-Geltungsbereichs der Zertifizierung, die sich auf Aufbewahrung, Löschung oder Entsorgung auswirkt.

2. Zweck

- 2.1 Zweck dieser Richtlinie ist es sicherzustellen, dass PII nur für genehmigte Zwecke und Zeiträume aufbewahrt, gelöscht oder anderweitig entsorgt wird, wenn sie nicht mehr erforderlich ist, und durch auditbereite Nachweise gestützt wird.
- 2.2 Diese Richtlinie ermöglicht es der Organisation, Speicherbegrenzung, rechenschaftspflichtige Aufbewahrungsgovernance, kontrollierte Durchführung von Löschungen, sichere Entsorgung, Ausrichtung an Kundenweisungen für Auftragsverarbeiter, Ausnahmesteuerung und kontinuierliche Verbesserung nachzuweisen, ohne ein separates Löschregister zu schaffen.

3. Ziele

3.1 Die Ziele dieser Richtlinie sind:

- 3.1.1 die Verantwortlichkeit für Aufbewahrungsregeln und die erforderlichen Aufbewahrungsmetadaten festzulegen;
- 3.1.2 sicherzustellen, dass Aufbewahrungsregeln im PII Processing Inventory / ROPA erfasst werden;
- 3.1.3 sicherzustellen, dass Löschmaßnahmen von Auftragsverarbeitern und Unterauftragsverarbeitern auf Kundenweisung oder Vertrag beruhen;
- 3.1.4 sicherzustellen, dass abgelaufene PII mit genehmigten Verfahren gelöscht, zurückgegeben, übermittelt, anonymisiert, de-identifiziert oder entsorgt wird;
- 3.1.5 zwischen Produktivsystemen, Archiven, Backups, Replikaten, Protokollen, Staging-Bereichen und temporären Dateien zu unterscheiden;

- 3.1.6 sicherzustellen, dass Lösch- und Entsorgungsnachweise in kanonischen PIMS-Nachweisobjekten aufbewahrt werden;
- 3.1.7 sicherzustellen, dass Aufbewahrungsausnahmen zeitlich begrenzt, genehmigt und überprüft werden;
- 3.1.8 die Überwachung von Aufbewahrung und Löschung mit Nichtkonformität, Korrekturmaßnahmen und Verbesserung zu integrieren.

4. Richtlinienaussagen

4.1 Zuweisung von Aufbewahrungsregeln

- 4.1.1 [Controller] The Process Owner / Business Owner MUST vor Beginn der Verarbeitungstätigkeit jeder Verarbeitungstätigkeit als Verantwortlicher in REG02 eine dokumentierte Aufbewahrungsregel zuweisen.
- 4.1.2 [Joint Controller] The Process Owner / Business Owner MUST vor Beginn oder Änderung der gemeinsamen Verarbeitung die Zuweisung der Aufbewahrungs- und Löschverantwortung gemeinsam Verantwortlicher in REG02 und REG08 erfassen.
- 4.1.3 [Processor] The Vendor / Procurement Owner MUST vor Beginn oder Änderung der Verarbeitung durch den Auftragsverarbeiter Kundenweisungen zur Aufbewahrung, Rückgabe, Übermittlung oder Löschung für Auftragsverarbeitungstätigkeiten in REG08 erfassen.
- 4.1.4 [Subprocessor] The Vendor / Procurement Owner MUST vor dem Onboarding eines Unterauftragsverarbeiters oder einer Änderung der Weisung Anforderungen zur Weitergabe von Aufbewahrungs-, Rückgabe-, Übermittlungs- oder Löschpflichten an Unterauftragsverarbeiter in REG08 erfassen.
- 4.1.5 [Both] The Privacy Lead / PIMS Manager MUST vor Genehmigung der Regel verifizieren, dass jede genehmigte Aufbewahrungsregel in REG02 den Aufbewahrungszeitraum, den Startauslöser, den Verantwortlichen, die Begründung, die endgültige Behandlung und das nächste Überprüfungsdatum enthält.
- 4.1.6 [Both] The Data Protection Officer / Privacy Advisor MUST vor Genehmigung jeder Aufbewahrungsregel, die einen rechtlichen Konflikt, eine risikoreiche Verarbeitung, besondere Kategorien von PII oder eine Aufbewahrung über den ursprünglichen Verarbeitungszweck hinaus betrifft, Beratung in REG02 oder REG12 erfassen.

4.2 Überprüfung und Begrenzung der Aufbewahrung

- 4.2.1 [Both] The Process Owner / Business Owner MUST zugewiesene Aufbewahrungsregeln in REG02 mindestens jährlich und innerhalb von 30 Tagen nach einer wesentlichen Änderung überprüfen.
- 4.2.2 [Both] The Privacy Lead / PIMS Manager MUST neue oder geänderte Aufbewahrungsregeln in REG02 innerhalb von 10 Geschäftstagen nach Einreichung genehmigen oder ablehnen.
- 4.2.3 [Both] The System Owner / Application Owner MUST vor der Produktivsetzung und während jeder jährlichen Aufbewahrungsüberprüfung die technische oder manuelle Durchsetzungsmethode für jede Aufbewahrungsregel in REG02 bestätigen.
- 4.2.4 [Controller] The Process Owner / Business Owner MUST die aktive Nutzung von PII, die nur aus rechtlichen, vertraglichen, Audit- oder Streitfallgründen aufbewahrt wird, in REG02 innerhalb von fünf Geschäftstagen nach Feststellung der Einschränkungsbefugnis beschränken.
- 4.2.5 [Both] The Privacy Lead / PIMS Manager MUST ungelöste Risiken aus übermäßiger Aufbewahrung oder überfällige Aufbewahrungsüberprüfungen in REG12 innerhalb von fünf Geschäftstagen nach Feststellung erfassen.

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

9. Ausnahmen

- 9.1.1 [All] The Process Owner / Business Owner MUST jeden Antrag auf Aufbewahrung von PII über die genehmigte REG02-Aufbewahrungsregel hinaus in REG12 einreichen, bevor die Ausnahme aktiv wird.
- 9.1.2 [All] The Privacy Lead / PIMS Manager MUST Anträge auf Aufbewahrungsausnahmen in REG12 genehmigen oder ablehnen, bevor die Ausnahme aktiv wird.
- 9.1.3 [All] The Data Protection Officer / Privacy Advisor MUST vor Genehmigung jeder Ausnahme, die einen rechtlichen Konflikt, eine Ablehnung der Löschung, risikoreiche PII, externe Weitergabe oder Auswirkungen auf die Zertifizierung betrifft, Beratung in REG12 erfassen.
- 9.1.4 [All] Top Management MUST Aufbewahrungsausnahmen, die 90 Tage überschreiten, risikoreiche Verarbeitung betreffen oder externe Vertrauensbildung betreffen, in REG12 genehmigen, bevor die Ausnahme aktiv wird.
- 9.1.5 [All] The Privacy Lead / PIMS Manager MUST für jede genehmigte Ausnahme zu Aufbewahrung, Löschung oder Entsorgung in REG12 einen Verantwortlichen, ein Ablaufdatum, eine kompensierende Kontrolle und eine Überprüfungshäufigkeit zuweisen.
- 9.1.6 [All] The Privacy Lead / PIMS Manager MUST jede offene Ausnahme in REG12 mindestens monatlich bis zum Abschluss überprüfen.
- 9.1.7 [All] The Process Owner / Business Owner MUST jede Ausnahme in REG12 vor dem Ablaufdatum der Ausnahme schließen oder erneuern.

10. Durchsetzung

- 10.1.1 [All] The Privacy Lead / PIMS Manager MUST innerhalb von fünf Geschäftstagen nach Feststellung fehlender Aufbewahrungsmetadaten, überfälliger Aufbewahrungsüberprüfung, nicht unterstützter Aufbewahrung, versäumter endgültiger Behandlungsmaßnahme oder fehlender Nachweise eine Nichtkonformität in REG12 erfassen.
- 10.1.2 [All] The System Owner / Application Owner MUST die neue produktive Nutzung einer Verarbeitungstätigkeit in REG12 aussetzen, wenn erforderliche technische Aufbewahrungskontrollen vor der Produktivsetzung fehlen.
- 10.1.3 [All] The Process Owner / Business Owner MUST die nicht genehmigte aktive Nutzung von PII, die nur aus rechtlichen, vertraglichen, Audit- oder Streitfallgründen aufbewahrt wird, innerhalb von fünf Geschäftstagen beenden und die Maßnahme in REG02 oder REG12 erfassen.
- 10.1.4 [Processor] The Vendor / Procurement Owner MUST überfällige durch Kunden angewiesene endgültige Behandlungsmaßnahmen in REG08 und REG12 innerhalb von fünf Geschäftstagen nach Versäumen der vertraglichen Frist eskalieren.
- 10.1.5 [Subprocessor] The Vendor / Procurement Owner MUST fehlende Nachweise zur endgültigen Behandlung durch Unterauftragsverarbeiter in REG08 und REG12 innerhalb von fünf Geschäftstagen nach Versäumen der vertraglichen Nachweisfrist eskalieren.
- 10.1.6 [All] The Internal Audit / Compliance Reviewer MUST die Wirksamkeit von Korrekturmaßnahmen für Nichtkonformitäten bei Aufbewahrung, Löschung und Entsorgung in REG12 beim nächsten geplanten Audit oder innerhalb von 60 Tagen nach Abschluss verifizieren, je nachdem, was früher eintritt.

10.1.7 [Conditional] The Incident Response Coordinator MUST die REG10-Bearbeitung einleiten, wenn eine Nichtkonformität bei Aufbewahrung, Löschung oder Entsorgung auf einen vermuteten PII-Vorfall hinweist.

11. Überprüfung und Pflege

11.1.1 [All] The Privacy Lead / PIMS Manager MUST diese Richtlinie jährlich überprüfen und das Überprüfungsergebnis in REG12 erfassen.

11.1.2 [All] The Privacy Lead / PIMS Manager MUST diese Richtlinie innerhalb von 30 Tagen nach einer wesentlichen Änderung des Aufbewahrungsrechts, des Verarbeitungszwecks, der Weisung des Auftragsverarbeiters, der Systemarchitektur, der Backup-Architektur, des Archivierungsansatzes, des Lösch-Workflows, des Entsorgungsprozesses oder der PIMS-Zertifizierungsanforderungen überprüfen.

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

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

11.1.5 [All] The Privacy Lead / PIMS Manager MUST die Kommunikation genehmigter Richtlinienänderungen in REG11 innerhalb von 30 Tagen nach Veröffentlichung erfassen.

12. Zugehörige Richtlinien

- 12.1 Diese Richtlinie wird durch die folgenden zugehörigen Richtlinien unterstützt:
- 12.2 PII01 - Richtlinie für das Datenschutz-Informationssystem
- 12.3 PII02 - Richtlinie zu Datenschutzrollen, Verantwortlichkeiten und Rechenschaftspflicht
- 12.4 PII03 - Richtlinie zum PII-Verarbeitungsinventar und zu Rechtsgrundlagen
- 12.5 PII04 - Richtlinie zu Datenschutzhinweisen und Transparenz
- 12.6 PII06 - Richtlinie zum Management der Rechte betroffener Personen
- 12.7 PII08 - Richtlinie zu Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- 12.8 PII09 - Richtlinie zur Erhebung, Nutzung, Offenlegung und Weitergabe von PII
- 12.9 PII12 - Richtlinie zum Datenschutzmanagement für Auftragsverarbeiter, Unterauftragsverarbeiter und Dritte
- 12.10 PII14 - Richtlinie zur PII-Sicherheit und Zugriffskontrolle
- 12.11 PII15 - Richtlinie zum Management von PII-Vorfällen und Datenschutzverletzungen
- 12.12 PII17 - Richtlinie zum Management dokumentierter Informationen und Nachweise im PIMS
- 12.13 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 genannten Anforderungen unterstützt, und identifiziert die internen Klauseln, die sie umsetzen oder unterstützen.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 7.5; Clause 8.1** - Zugeordnet zu dokumentierten Aufbewahrungsnachweisen, operativer Planung, Aufbewahrungsmetadaten, Umsetzungsnachweisen und Aufzeichnungen zur Durchführung des Lebenszyklus. Addressed by clauses [4.1.5; 4.2.3; 4.3.5; 4.4.1; 7.1.1; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.2.2 **Clause 9.1; Clause 10.2** - Zugeordnet zu Überwachung, Kennzahlen, Überprüfung überfälliger Maßnahmen, Nichtkonformität und Korrekturmaßnahmen für Kontrollen zu

- Aufbewahrung, Löschung und Entsorgung. Addressed by clauses [4.2.5; 6.1.1; 6.1.2; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 8.1.7; 10.1.1; 10.1.6].
- 13.2.3 **Annex A.1.2.8; Annex A.1.2.9** - Zugeordnet zu Nachweisen der Verantwortung gemeinsam Verantwortlicher und Verarbeitungsaufzeichnungen des Verantwortlichen, die Aufbewahrungs- und endgültige Behandlungsmetadaten enthalten. Addressed by clauses [4.1.1; 4.1.2; 4.1.5; 4.2.1; 6.1.4; 7.1.2].
- 13.2.4 **Annex A.1.3.7; Annex A.1.3.8** - Zugeordnet zur Unterstützung der Durchführung von Löschungen, zur Weiterleitung der Löschbewertung und zur Verknüpfung von Nachweisen Dritter, wenn Löschungsergebnisse Maßnahmen erfordern. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].
- 13.2.5 **Annex A.1.4.6; Annex A.1.4.7; Annex A.1.4.8; Annex A.1.4.9** - Zugeordnet zur Löschung oder De-Identifizierung am Ende der Verarbeitung, zum Umgang mit temporären Dateien, zur Aufbewahrungsbegrenzung und zu dokumentierten Kontrollen der endgültigen Behandlung. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.2.4; 4.3.1; 4.3.5; 4.3.6; 4.4.2; 4.4.5; 4.5.1; 4.5.2; 4.5.3].
- 13.2.6 **Annex A.2.2.2; Annex A.2.2.3; Annex A.2.2.7** - Zugeordnet zu Kundenvereinbarungen von Auftragsverarbeitern, dokumentierten Kundenzwecken und Verarbeitungsaufzeichnungen des Auftragsverarbeiters. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7].
- 13.2.7 **Annex A.2.3.2; Annex A.2.4.2; Annex A.2.4.3** - Zugeordnet zur Unterstützung von Kundenpflichten durch Auftragsverarbeiter, zum Umgang mit temporären Dateien und zur Fähigkeit zur Rückgabe, Übermittlung oder endgültigen Behandlung. Addressed by clauses [4.3.3; 4.3.4; 4.4.3; 4.4.4; 4.4.5; 6.1.5; 7.1.7; 10.1.4; 10.1.5].
- 13.2.8 **Annex A.3.20; Annex A.3.21; Annex A.3.24** - Zugeordnet zum Lebenszyklusmanagement von Speichermedien, zu Prüfungen vor Wiederverwendung oder Freigabe von Geräten und zum Umgang mit Backups für PII. Addressed by clauses [4.3.6; 4.3.7; 4.4.1; 4.4.3; 4.4.4; 4.4.6; 5.1.4].
- 13.3 GDPR**
- 13.3.1 **Article 5(1)(e); Article 5(2)** - Zugeordnet zu Speicherbegrenzung, Rechenschaftspflicht für Aufbewahrung, genehmigten Aufbewahrungsmetadaten, Nachweisen und Überprüfung. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 4.2.4; 4.3.1; 4.3.5; 6.1.1; 8.1.1; 8.1.2; 10.1.1].
- 13.3.2 **Article 17** - Zugeordnet zur Weiterleitung genehmigter Löschungsergebnisse, zu Durchführungsnachweisen und zur Vorfalleskalation, wenn Fehler bei Löschkontrollen auf einen vermuteten PII-Vorfall hinweisen. Addressed by clauses [4.3.2; 4.3.5; 7.1.8; 10.1.7].
- 13.3.3 **Article 24** - Zugeordnet zur Governance des Verantwortlichen, zu Rechenschaftsmaßnahmen, Überprüfungen, Ausnahmen, Korrekturmaßnahmen und Richtlinienpflege. Addressed by clauses [4.1.6; 6.1.2; 6.1.3; 9.1.2; 9.1.3; 9.1.4; 11.1.1; 11.1.2; 11.1.4].
- 13.3.4 **Article 26** - Zugeordnet zur Zuweisung der Aufbewahrungs- und Löschverantwortung gemeinsam Verantwortlicher. Addressed by clauses [4.1.2; 6.1.4].
- 13.3.5 **Article 28** - Zugeordnet zur Ausrichtung an Weisungen für Auftragsverarbeiter und Unterauftragsverarbeiter, Rückgabe, Übermittlung, endgültige Behandlung, Nachweisen und Eskalation. Addressed by clauses [4.1.3; 4.1.4; 4.3.3; 4.3.4; 6.1.5; 6.1.6; 7.1.7; 10.1.4; 10.1.5].
- 13.3.6 **Article 30** - Zugeordnet zu Aufbewahrungs- und endgültigen Behandlungsmetadaten in Verarbeitungsaufzeichnungen für Tätigkeiten als Verantwortlicher und Auftragsverarbeiter. Addressed by clauses [4.1.1; 4.1.3; 4.1.5; 4.2.1; 4.4.1; 7.1.2].

13.3.7 **Article 32** - Zugeordnet zum sicheren operativen Umgang mit aufbewahrten PII, technischer Durchsetzung, Kontrolle von Speichermedien, Umgang mit Backups und Vorfalleskalation. Addressed by clauses [4.2.3; 4.3.6; 4.4.3; 4.4.4; 4.4.6; 7.1.3; 7.1.4; 7.1.8].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 5.5; Clause 5.6; Clause 5.10** - Zugeordnet zu Datenminimierung, Nutzungs- und Aufbewahrungsbegrenzung, endgültiger Behandlung, wenn nicht mehr erforderlich, Beschränkung aufbewahrter PII und Nachweisen der Rechenschaftspflicht. Addressed by clauses [4.1.5; 4.2.1; 4.2.4; 4.3.1; 4.4.2; 4.5.1; 4.5.2; 6.1.1; 8.1.1; 10.1.1].

13.5 ISO/IEC 29151:2022

13.5.1 **Annex A.7; Annex A.7.2** - Zugeordnet zu zeitlich begrenzter Aufbewahrung, endgültiger Behandlung, automatisierter oder manueller Durchsetzung und Umgang mit temporären Dateien. Addressed by clauses [4.2.3; 4.3.1; 4.4.5; 7.1.3; 7.1.4; 7.1.5; 7.1.6].

13.6 ISO/IEC 27555:2025

13.6.1 **Clause 5.1; Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6; Clause 5.8** - Zugeordnet zur Governance des Löschrasterwerks, PII-Gruppierung, Aufbewahrungs- und Löschraster, Unterscheidung von Archiven und Backups, Struktur von Löschrasterregeln und Anforderungen an dokumentierte Verfahren. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.3; 4.4.1; 4.4.2; 4.4.3; 7.1.1; 7.1.2].

13.6.2 **Clause 7.2; Clause 7.3; Clause 8.3** - Zugeordnet zur Festlegung regelmäßiger Löschraster, Identifizierung standardmäßiger Löschraster und Zuordnung von Löschrasterregeln zu PII-Verarbeitungstätigkeiten. Addressed by clauses [4.1.1; 4.1.5; 4.2.1; 4.2.2; 7.1.1; 7.1.2].

13.6.3 **Clause 9.1; Clause 9.2; Clause 9.3; Clause 9.4; Clause 9.5; Clause 9.6; Clause 9.7** - Zugeordnet zu Umsetzungsanforderungen für Systeme, manuelle Prozesse, organisationsweite Aspekte, Auftragsverarbeiter, Umgang mit Wiederherstellung und Ausnahmemanagement. Addressed by clauses [4.3.1; 4.3.3; 4.3.4; 4.4.1; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 7.1.3; 7.1.4; 7.1.5; 7.1.6; 9.1.1; 9.1.5; 9.1.6].

13.6.4 **Clause 10.1; Clause 10.2; Clause 10.3** - Zugeordnet zu Rollenzuweisung, Dokumentation, operativer Verankerung, Audit und Umsetzungsgovernance für Aufbewahrung, Löschraster und Entsorgung. Addressed by clauses [5.1.2; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.9; 6.1.7; 7.1.3; 7.1.4; 11.1.1; 11.1.2].

13.7 ISO/IEC 27557:2022

13.7.1 **Clause 4; Clause 5.2; Clause 5.3; Clause 5.4.1** - Zugeordnet zu risikobasierter Datenschutz-Governance, Bewusstsein der Leitung, Integration von Datenschutzrisiken in das PIMS und aufbewahrungsbezogenem Risikokontext. Addressed by clauses [4.1.6; 4.2.5; 4.5.4; 6.1.2; 6.1.3; 9.1.3; 9.1.4].

13.8 ISO/IEC 27002:2022

13.8.1 Control 7.14; Control 8.10 - Zugeordnet zur Löschraster von Informationen, zum kontrollierten Abschluss des Lebenszyklus, zur Freigabe von Speichermedien und zu Nachweisen der endgültigen Behandlung. Addressed by clauses [4.3.1; 4.3.5; 4.3.6; 4.3.7; 4.4.4; 4.4.5; 7.1.3; 7.1.4; 10.1.2].