					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P14					Dokumenttitel: **Richtlinie zur Datenaufbewahrung und -entsorgung**							
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/Artikel	Kommentar
ISO/IEC 27001:2022	Klauseln 6.1.3, 8.1	
ISO/IEC 27002:2022	Maßnahmen 5.10, 5.12, 5.30, 5	
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12, PL-2	
EU-DSGVO	Artikel 5(1)(e), 17, 32	
EU-NIS2	Artikel 21(2)(a-e)	
EU-DORA	Artikel 5, 9	
COBIT 2019	DSS01, DSS05, MEA	

1. Zweck

1.1 Zweck dieser Richtlinie ist es, die organisatorischen Anforderungen an die Datenaufbewahrung und die sichere Entsorgung über alle Phasen des Lebenszyklus von Informationswerten hinweg festzulegen. Sie stellt die Einhaltung anwendbarer gesetzlicher, regulatorischer und vertraglicher Verpflichtungen sicher und verhindert die unnötige oder risikobehaftete Anhäufung von Daten.

1.2 Diese Richtlinie unterstützt die Umsetzung von ISO/IEC 27001:2022, indem sie die Steuerung der Dauer der Datenspeicherung und irreversible Entsorgungsverfahren sicherstellt. Sie ermöglicht eine nachvollziehbare Dokumentation von Aufzeichnungen, setzt an der Sensitivität der Klassifizierung ausgerichtete Aufbewahrungsfristen durch und gewährleistet Auditfähigkeit für interne und externe Audits, behördliche Prüfungen und Beweissicherungsverfahren.

1.3 Darüber hinaus dient sie dazu, die Vertraulichkeit, Integrität und Verfügbarkeit (CIA) von Daten zu wahren und zugleich Geschäftsrisiken, betriebliche Ineffizienzen sowie die Exposition gegenüber Datenschutzverstößen infolge unsachgemäßer Datenaufbewahrung oder Vernichtung zu minimieren.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle physischen und digitalen Informationswerte, die sich im Eigentum der Organisation befinden, von ihr verarbeitet oder aufbewahrt werden, einschließlich solcher, die unter der Kontrolle von Dritten, Tochtergesellschaften oder Outsourcing-Partnern stehen.

2.2 Der Geltungsbereich umfasst unter anderem:

2.2.1 Dokumente, Dateien und Aufzeichnungen (digital und papierbasiert)

2.2.2 Datenbanken und Archive

2.2.3 E-Mails und Protokolle von Sofortnachrichten

2.2.4 Backups, Systemprotokolle und Audit-Trails

2.2.5 Quellcode, Anwendungsdaten und in der Cloud gehostete Werte

2.2.6 Wechseldatenträger und Altgeräte mit Datenbeständen

2.3 Die Richtlinie regelt sowohl operative Aufzeichnungen als auch regulierte Datenbestände (z. B. finanzbezogene, rechtliche, HR-bezogene, kundenbezogene und auditrelevante Inhalte), unabhängig von Speicherort oder System.

2.4 Sie gilt für alle Organisationsbereiche sowie für Mitarbeitende, Auftragnehmer und Lieferanten, die an der Erstellung, Speicherung, Verwaltung oder Entsorgung von Daten beteiligt sind.

3. Ziele

3.1 Sicherzustellen, dass Daten nur so lange aufbewahrt werden, wie dies rechtlich, vertraglich oder betrieblich erforderlich ist, und sicher entsorgt werden, sobald sie nicht mehr benötigt werden.

3.2 Die vorzeitige, unbefugte oder versehentliche Löschung von Aufzeichnungen zu verhindern, die für laufende Betriebsabläufe, die Compliance, Gerichtsverfahren oder Audit-Zwecke erforderlich sind.

3.3 Konsistente Datenaufbewahrungspläne auf der Grundlage von Informationsklassifizierung, Asset-Typ, anwendbaren Rechtsvorschriften und Risikoexposition festzulegen und durchzusetzen.

3.4 Die Privatsphäre und Vertraulichkeit von Daten während ihrer Aufbewahrungsfrist und zum Zeitpunkt der Entsorgung zu schützen, einschließlich der Erfüllung der Rechte betroffener Personen (z. B. Löschung nach Artikel 17 DSGVO).

3.5 Sicherzustellen, dass alle Methoden zur Datenentsorgung irreversibel, angemessen dokumentiert und mit anerkannten Standards wie NIST SP 800-88 konform sind.

3.6 Betriebliche Ineffizienzen, Kostenmehraufwand und rechtliche Exposition infolge überlanger Aufbewahrung oder nicht nachverfolgbarer Altdaten zu minimieren.

3.7 Die Ziele zur Aufrechterhaltung des Geschäftsbetriebs und zur Notfallwiederherstellung durch integrierte Governance der Backup-Aufbewahrung und belastbare Datenarchivierungspraktiken zu unterstützen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsleitung

4.1.1 Genehmigt diese Richtlinie und stellt eine angemessene Finanzierung, Ressourcenausstattung sowie die Integration in das unternehmensweite Risikomanagement und in Compliance-Programme sicher.

4.1.2 Trägt die Gesamtverantwortung für die gesetzliche und regulatorische Compliance im Zusammenhang mit Datenaufbewahrung und sicherer Entsorgung.

4.2 Chief Information Security Officer (CISO)

4.2.1 Ist für diese Richtlinie verantwortlich und zuständig für die Festlegung und Überprüfung der Governance für Aufbewahrung und Entsorgung im Einklang mit dem Informationssicherheits-Managementsystem (ISMS).

4.2.2 Stellt sicher, dass klassifizierungsbasierte Anforderungen an Aufbewahrung und Entsorgung in den Geschäftsbereichen und technischen Systemen umgesetzt werden.

4.2.3 Überwacht die Einhaltung dieser Richtlinie und veranlasst erforderlichenfalls Korrekturmaßnahmen.

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

9. Anforderungen an Überprüfung und Aktualisierung

9.1 Diese Richtlinie ist jährlich oder bei Eintritt einer der folgenden Bedingungen zu überprüfen:

9.1.1 Änderungen an anwendbaren Gesetzen oder Vorschriften, die die Datenaufbewahrung betreffen (z. B. Aktualisierungen der DSGVO, Steuervorschriften, DORA)

9.1.2 Überarbeitungen des Klassifizierungsrahmens oder von Geschäftsprozessen mit Auswirkungen auf die Phasen des Datenlebenszyklus

9.1.3 Einführung neuer IT-Systeme, Archivierungsplattformen oder Technologien zur Entsorgung von Datenträgern

9.1.4 Feststellungen aus internen Audits oder regulatorische Empfehlungen, die Lücken in den Praktiken zur Aufbewahrung oder Entsorgung aufzeigen

9.2 Die Überprüfung wird durch den CISO und den Datenschutzbeauftragten (DSB) geleitet, unter Einbindung von Rechtsabteilung, Compliance, IT und Geschäftsbereichen.

9.3 Der Master-Datenaufbewahrungsplan (MDRS) und das Entsorgungsregister sind parallel zu überprüfen, um sicherzustellen, dass:

9.3.1 die Pläne korrekt bleiben und den betrieblichen, rechtlichen und regulatorischen Anforderungen entsprechen,

9.3.2 die Entsorgungsdokumentation vollständig und auditierbar ist,

9.3.3 Aufzeichnungen zu Legal Hold und Löschsperren validiert und, soweit angemessen, aufgehoben werden.

9.4 Jede Aktualisierung dieser Richtlinie muss:

9.4.1 formal versioniert werden und im ISMS-Dokumentenregister aufbewahrt werden,

9.4.2 eine Versionshistorie und eine Begründung der Änderung enthalten,

9.4.3 durch die Geschäftsleitung genehmigt werden,

9.4.4 den relevanten Mitarbeitenden zusammen mit aktualisierten Schulungs- oder Leitmaterialien mitgeteilt werden.

9.5 Bei wesentlichen Änderungen der Richtlinie müssen betroffene Mitarbeitende innerhalb von 30 Tagen nach Veröffentlichung eine gezielte Nachschulung absolvieren, um die fortlaufende Einhaltung sicherzustellen.

9.6 Zugehörige Richtlinien und Verknüpfungen

10. Zugehörige Richtlinien und Verknüpfungen

10.1.1 P4 - Richtlinie zur Zugriffskontrolle: Stellt sicher, dass nur autorisierte Personen während der Aufbewahrungsfrist auf Daten zugreifen und dass abgelaufene Daten bis zur Entsorgung eingeschränkt bleiben.

10.1.2 P12 - Asset-Management-Richtlinie: Legt fest, welche Assets Daten enthalten, die planmäßig entsorgt werden müssen, und verfolgt deren Lebenszyklus von der Beschaffung bis zur Vernichtung.

10.1.3 P13 - Richtlinie zur Datenklassifizierung und Kennzeichnung: Steuert Klassifizierungsentscheidungen, die unmittelbar beeinflussen, wie lange Daten aufbewahrt werden und welche Entsorgungsmethode erforderlich ist.

10.1.4 P15 - Richtlinie für Backup und Wiederherstellung: Legt Aufbewahrungsfristen und Entsorgungsverfahren für Backup-Medien und replizierte Datenbestände fest.

10.1.5 P18 - Richtlinie zu kryptografischen Kontrollen: Unterstützt die kryptografische Löschung zur Entsorgung und setzt Verschlüsselung bei der Datenspeicherung bis zur Vernichtung durch.

10.1.6 P30 - Incident-Response-Richtlinie (P30): Wird aktiviert, wenn unsachgemäße Entsorgung zu potenziellem Datenverlust, einer Sicherheitsverletzung oder einem regulatorischen Verstoß führt.

10.2 Jede verknüpfte Richtlinie trägt zur Durchsetzung eines kohärenten Governance-Modells für Daten über Klassifizierung, Lebenszyklussteuerung, Zugriff und Auditfähigkeit hinweg bei.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an weltweit anerkannten Standards und regulatorischen Rahmenwerken ausgerichtet, die sichere, konforme und effiziente Praktiken für den Datenlebenszyklus festlegen.

11.2 ISO/IEC 27001:

11.2.1 Klausel 6.1.3 - Risikobehandlungsplan: Unterstützt die Minderung von Risiken im Zusammenhang mit überlanger Aufbewahrung, Datenschutzverletzungen oder Entsorgungsfehlern.

11.2.2 Klausel 8.1 - Operative Planung und Steuerung: Legt Lebenszykluskontrollen fest, die Speicherung, Archivierung und Vernichtung regeln.

11.3 ISO/IEC 27002:2022 - Maßnahmen 5.10, 5.12, 5.30, 5: Bieten praktische Leitlinien für zulässige Datennutzung, die Begründung von Aufbewahrung, kontrollierte Löschung und belastbare Aufzeichnungsführung im Einklang mit der Risikotoleranz der Organisation.

11.4 NIST SP 800-53 Rev. 5:

11.4.1 AU-11 - Aufbewahrung von Audit-Aufzeichnungen: Stellt eine ausreichende Speicherung von Audit-Protokollen und Compliance-Nachweisen sicher.

11.4.2 MP-6 - Medienbereinigung: Verlangt sichere, dokumentierte Vernichtungsmethoden für physische und elektronische Medien.

11.4.3 SI-12 - Informationshandhabung: Erzwingt einen angemessenen Umgang mit Daten im Einklang mit Kontrollen zur Aufbewahrung und Entsorgung.

11.4.4 PL-2 - System-Sicherheits- und Datenschutzplan: Verlangt systemspezifische Dokumentation zum Umgang mit dem Datenlebenszyklus und Regelungen zur sicheren Entsorgung.

11.5 EU-DSGVO (2016/679):

11.5.1 Artikel 5(1)(e) - Datenminimierung und Speicherbegrenzung: Verlangt, dass Daten nicht länger als erforderlich aufbewahrt werden.

11.5.2 Artikel 17 - Recht auf Löschung ("Recht auf Vergessenwerden"): Verlangt die zeitnahe und dauerhafte Löschung personenbezogener Daten auf berechtigten Antrag.

11.5.3 Artikel 32 - Sicherheit der Verarbeitung: Verstärkt den Schutz von Daten während der Aufbewahrung und verlangt die sichere Vernichtung abgelaufener Aufzeichnungen.

11.6 EU-NIS2-Richtlinie (2022/2555):

11.6.1 Artikel 21(2)(a-e): Verlangt, dass Einrichtungen Richtlinien und technische Maßnahmen für eine sichere Datenverarbeitung einführen, einschließlich Speicherbegrenzungen und Entsorgungsmethoden.

11.7 EU-DORA (2022/2554):

11.7.1 Artikel 5 - Governance und Kontrolle: Verlangt ein strukturiertes IKT-Risikomanagement einschließlich des sicheren Umgangs mit dem Informationslebenszyklus.

11.7.2 Artikel 9 - Rahmenwerk für das Management von IKT-Risiken: Verlangt Richtlinien für Datenaufbewahrung, Vernichtung und gesetzliche bzw. regulatorische Compliance digitaler Betriebsabläufe.

11.8 COBIT 2019:

11.8.1 DSS01 - Gesteuerte Betriebsabläufe: Unterstützt die Nachverfolgung von Aufbewahrungsfristen und Konsistenz über Datensysteme hinweg.

11.8.2 DSS05 - Sicherheitsdienste verwalten: Stellt den Schutz gespeicherter und archivierter Daten bis zu ihrer sicheren Entsorgung sicher.

11.8.3 MEA03 - Überwachen, Evaluieren und Beurteilen der Compliance: Ermöglicht die Auditierung der Durchsetzung von Aufbewahrungsfristen, Löschverfahren und regulatorischer Erfüllung.