					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P14S					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	Deckt Risikobehandlung, operative Kontrollen und Aufbewahrungsanforderungen ab
ISO/IEC 27002:2022	Maßnahme 5	Leitlinien für Aufbewahrungsfristen und sichere Vernichtungsmethoden
NIST SP 800-53 Rev. 5	AU-11, MP-6, SI-12	Aufbewahrung von Audit-Protokollen, Bereinigung von Medien, Grenzen und Durchsetzung der Datenaufbewahrung
EU NIS2	Artikel 21(2)(a)	Eine dem Risiko angemessene Richtlinie für das Lebenszyklusmanagement ist erforderlich
EU DORA	Artikel 5(1)	IKT-Risikomanagement: Datenverfügbarkeit und Datenlöschung
COBIT 2019	BAI03.04, DSS01	Kontrollen über den Informationslebenszyklus, sichere Entsorgung
DSGVO	Artikel 5(1)(e), 17	Daten nicht länger als erforderlich aufbewahren; Recht auf Löschung

1. Zweck

1.1 Zweck dieser Richtlinie ist es, verbindliche Vorgaben für die Aufbewahrung und sichere Entsorgung von Informationen in einer SME-Umgebung festzulegen. Sie stellt sicher, dass Aufzeichnungen nur so lange aufbewahrt werden, wie dies gesetzlich, aufgrund vertraglicher Verpflichtungen oder aus geschäftlicher Notwendigkeit erforderlich ist, und anschließend sicher vernichtet werden.

1.2 Diese Richtlinie dient dazu, Informationsrisiken zu reduzieren, rechtliche Risiken zu steuern und die Speicherung redundanter oder veralteter Daten zu begrenzen. Sie unterstützt die Einhaltung von ISO/IEC 27001 und Datenschutzrahmenwerken wie der DSGVO, indem sie die unbefugte Aufbewahrung personenbezogener oder sensibler Informationen minimiert.

1.3 Ein strukturiertes Rahmenwerk für Aufbewahrung und Entsorgung senkt Betriebskosten, verbessert die Systemleistung und erhöht die Audit-Fähigkeit. Für SMEs mit begrenzten IT-Kapazitäten bietet es einen praktikablen Ansatz, digitale und physische Informationswerte verantwortungsvoll zu verwalten.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für:

2.1.1 alle Aufzeichnungen, Dateien, Protokolle, Kommunikationsinhalte und Datenbestände, die von der Organisation erstellt, erhoben, verarbeitet oder gespeichert werden,

2.1.2 alle Mitarbeitenden und Auftragnehmer sowie externe Dienstleister, die Daten der Organisation verarbeiten,

2.1.3 alle Datenformate (z. B. Papier, elektronisch, Bild, Audio oder Protokoll) und alle Speichermedien (z. B. lokale Laufwerke, Cloud-Dienste, E-Mail-Server, Backups).

2.2 Der Geltungsbereich umfasst:

2.2.1 Geschäftsdokumente (z. B. Rechnungen, Verträge, Projektberichte),

2.2.2 Betriebsaufzeichnungen (z. B. Protokolle, Zugriffshistorie, Backup-Snapshots),

2.2.3 personenbezogene Daten (z. B. Personalakten, Kundenkommunikation, Support-Aufzeichnungen),

2.2.4 intern, extern oder in hybriden Systemen gehostete Daten,

2.2.5 archivierte Daten und Backup-Daten, unabhängig davon, ob sie aktiv oder inaktiv sind.

2.3 Alle Phasen des Datenlebenszyklus fallen in den Geltungsbereich – von der Erstellung bis zur autorisierten Entsorgung.

3. Ziele

3.1 Einheitliche Aufbewahrungsregeln auf Grundlage rechtlicher, operativer und regulatorischer Kriterien festlegen.

3.2 Die vorzeitige Löschung kritischer Aufzeichnungen verhindern und unnötige Datenbestände beseitigen.

3.3 Sicherstellen, dass Daten sicher und irreversibel entsorgt werden, sobald keine Aufbewahrung mehr erforderlich ist.

3.4 Die Verantwortlichkeit für die Durchsetzung von Aufbewahrungs- und Löschentscheidungen unter den personellen Rahmenbedingungen einer SME festlegen.

3.5 Auditfähige Dokumentation bereitstellen, um die gebotene Sorgfalt nach ISO 27001, DSGVO, NIS2 und anderen Rahmenwerken nachzuweisen.

3.6 Einen sicheren Umgang mit Daten über ihren gesamten Lebenszyklus fördern, ohne für nicht spezialisierte Mitarbeitende unnötige technische Hürden zu schaffen.

4. Rollen und Verantwortlichkeiten

4.1 Geschäftsführung (GM)

4.1.1 genehmigt diese Richtlinie und trägt die Gesamtverantwortung dafür.

4.1.2 stellt sicher, dass Verfahren zur Aufbewahrung und Entsorgung im Einklang mit rechtlichen und geschäftlichen Risiken umgesetzt werden.

4.1.3 genehmigt erforderlichenfalls Ausnahmen sowie Legal Holds und Löschsperren.

4.1.4 veranlasst Richtlinienüberprüfungen und genehmigt Aktualisierungen auf Grundlage geschäftlicher oder regulatorischer Änderungen.

4.2 Benannter Dateneigentümer

4.2.1 wird je Datenkategorie zugewiesen (z. B. Finanzen, Personal, Kundenaufzeichnungen).

4.2.2 klassifiziert Aufzeichnungen und legt auf Grundlage der Richtlinie sowie rechtlicher Vorgaben angemessene Aufbewahrungsfristen fest.

4.2.3 genehmigt die Löschung, sobald die Aufbewahrungsanforderungen erfüllt sind.

4.2.4 unterstützt interne Audits durch die Bereitstellung von Kontext zur Aufbewahrungslogik und zu Entsorgungsvorgängen.

[... 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 muss mindestens einmal jährlich oder bei Eintreten eines der folgenden Ereignisse überprüft werden:

9.1.1 Änderungen geltender Rechtsvorschriften (z. B. Datenschutz, Finanzberichterstattung)

9.1.2 Einführung neuer Systeme oder Prozesse, die sich auf den Datenlebenszyklus auswirken

9.1.3 Auditfeststellungen oder Vorfälle, die Lücken in den Aufbewahrungspraktiken aufdecken

9.2 Bei Überprüfungen ist sicherzustellen, dass das Aufbewahrungsverzeichnis vollständig bleibt und alle wesentlichen Aufzeichnungskategorien abbildet.

9.3 Aktualisierungen dieser Richtlinie müssen durch die Geschäftsführung genehmigt und an betroffene Mitarbeitende kommuniziert werden. Die jeweils aktuelle Version muss zugänglich und versionskontrolliert sein.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 P2S – Richtlinie zu Governance-Rollen und Verantwortlichkeiten: Definiert Richtlinienverantwortung und Befugnisse für Ausnahmen.

10.2 P13S – Richtlinie zur Datenklassifizierung und Kennzeichnung: Legt fest, wie Aufbewahrungsregeln mit der Datenklassifizierung abgestimmt werden.

10.3 P12S – Richtlinie zum Asset-Management: Regelt Speichermedien, die Daten enthalten, welche Aufbewahrungs- oder Entsorgungsanforderungen unterliegen.

10.4 P17S – Richtlinie zu Datenschutz und Privatsphäre: Stellt Datenminimierung sicher und unterstützt die rechtmäßige Informationsverarbeitung nach der DSGVO.

10.5 P30S – Incident-Response-Richtlinie: Wird aktiviert, wenn Fehler bei Entsorgung oder Aufbewahrung zu einer möglichen Datenexposition führen.

11. Referenzstandards und Rahmenwerke

11.1 ISO/IEC 27001

11.1.1 Klausel 6.1.3: Verlangt die Behandlung informationsbezogener Risiken, einschließlich Aufbewahrungsrisiken.

11.1.2 Klausel 8.1: Definiert operative Kontrollen über den Lebenszyklus.

11.2 ISO/IEC 27002

11.2.1 Maßnahme 5.33: Leitlinien für die Festlegung von Aufbewahrungsfristen und sicheren Vernichtungsmethoden.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-11: Verlangt die Aufbewahrung von Audit-Protokollen.

11.3.2 MP-6: Definiert Verfahren zur Bereinigung von Medien.

11.3.3 SI-12: Behandelt Grenzen und Durchsetzung der Datenaufbewahrung.

11.4 DSGVO

11.4.1 Artikel 5(1)(e): Daten dürfen nicht länger als erforderlich aufbewahrt werden.

11.4.2 Artikel 17: Das Recht auf Löschung gilt, wenn Daten nicht mehr rechtmäßig aufbewahrt werden.

11.5 EU NIS2

11.5.1 Artikel 21(2)(a): Verlangt dem Risiko angemessene organisatorische Richtlinien, einschließlich Lebenszyklusmanagement.

11.6 EU DORA

11.6.1 Artikel 5(1): IKT-Risikomanagement umfasst Datenverfügbarkeit und Datenlöschung.

11.7 COBIT 2019

11.7.1 BAI03.04: Kontrollen für den Informationslebenszyklus sind erforderlich.

11.7.2 DSS01.06: Sichere Entsorgungsverfahren als Teil des Schutzes von Informationswerten.