Die Prüfung der Aufbewahrung

Sie beginnt an einer Sicherung und an den Orten hinter ihr, nicht an einem Löschkonzept: Löschung wird über Orte geprüft, nicht über Systeme.

Kategorie: Checkliste (mit Karte der Orte). Bezug im Buch: Abschnitt 3.8 (Das Prinzip, Was die Norm sagt, Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 6.1.2, 7.5, 8.1 und 9.1 sowie Maßnahmen A.5.9, A.5.20, A.5.22, A.5.33, A.5.34, A.6.5, A.7.14, A.8.10, A.8.11 und A.8.13 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 28. September 2026.

Haus		**Stand (Datum)**	
Datenart (ein Blatt je Datenart)		**Geprüft von**	

So nutzen Sie diese Vorlage

1. Fragen Sie zuerst nach den Orten, dann nach den Fristen. Wer zuerst über Fristen spricht, führt ein Gespräch über Recht, und es dauert zwei Stunden; wer über Orte spricht, führt ein Gespräch über das Haus, und die Fristen ergeben sich danach fast von selbst.
2. Beginnen Sie bei den Sicherungen und füllen Sie die Karte der Orte aus: für jede Datenart acht Zeilen. Für ein Hotel zählen selten mehr als sechs Datenarten.
3. Verlangen Sie keine Erklärung, sondern eine Suche: Lassen Sie mit Genehmigung der Leitung einen Namen aus einem angeblich gelöschten Jahrgang über alle Systeme, Laufwerke und Postfächer suchen. Das dauert zwanzig Minuten.
4. Fragen Sie auf jede Aussage «es ist gelöscht»: gelöscht wo, und woran sehen wir das? Der Nachweis ist eine Liste der Orte mit dem Datum der letzten Prüfung, kein Bericht über einen Lauf.

Spalte «Im Buch»: verlangt = von Norm oder Recht verlangt, wie der Band es nennt; Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Die Karte der Orte (eine Datenart je Blatt)

Nr.	Ort	Wo genau liegt es, wer hat Zugriff?	Frist (und Grund)	Verantwortlicher	Letzte Prüfung (Datum, Nachweis)
1	Das führende System				
2	Die Sicherungen				
3	Die Altsysteme				
4	Die Exporte				
5	Die Berichte				
6	Die Postfächer				
7	Die Papierablage				
8	Die Geräte der Dienstleister				

Eine Frist ohne Ort ist eine Absicht. Umgesetzt ist die Maßnahme zur Löschung erst, wenn für jede Datenart ein Ort, eine Frist, ein Verantwortlicher und ein Nachweis existieren: Diese vier Angaben sind die kürzeste brauchbare Fassung eines Löschkonzepts.

2 Die Sicherungen zuerst

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
1	Wie lange wird jede Sicherung aufbewahrt? (Tage) Ist die Verzögerung jeder Löschung um diese Dauer aufgeschrieben? _____	Eine Sicherung, die dreißig Tage aufbewahrt wird, verzögert jede Löschung um dreißig Tage; das ist unvermeidbar, zulässig und gehört aufgeschrieben.	**Methode** dieses Bandes.
2	Bleibt irgendeine Sicherung unbegrenzt bestehen? _____	Nicht zulässig ist eine Sicherung, die unbegrenzt bleibt, weil Speicher billig geworden ist. Wer Archiv und Sicherung im selben Speicher hält, hat ein Archiv, das er Sicherung nennt.	**verlangt:** Sicherung von Informationen (A.8.13); Löschung von Informationen (A.8.10).
3	Sind Sicherung und Archiv getrennt? Hat das Archiv eine eigene Frist, einen eigenen Zugriff, ein eigenes Löschdatum? _____	Sicherungen dienen der Wiederherstellung und brauchen Tage oder Wochen, nicht Jahre; Archive dienen der Aufbewahrung.	**Methode** dieses Bandes.
4	Liegen Sicherungen des Hauses noch bei einem früheren Dienstleister? (Dienstleister · Vertragsende) _____	In Rostock hielt der frühere Dienstleister die Sicherungen nach Vertragsende auf eigenem Speicher, in dessen System die Aufbewahrung auf «unbegrenzt» stand; niemand hatte Rückgabe oder Löschung verlangt.	**verlangt:** Vereinbarungen mit Lieferanten samt Überwachung (A.5.20, A.5.22).

3 Die Orte hinter der Sicherung

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
5	Welche Altsysteme laufen noch, physisch oder als virtuelle Maschine? Wer ist ihr Eigentümer? Sind sie am Netz? Wann werden sie entsorgt? _____	Der alte Server in Rostock lag fünf Jahre im Keller, am Netz, ohne Eigentümer: IT und Buchhaltung wiesen die Zuständigkeit einander zu. Ein Gerät ohne Eigentümer ist dasselbe wie eine Tür ohne Schlüsselliste. Maßnahme: trennen und befristen (Kabel ziehen, Zugriff auf zwei Personen, Entsorgungsdatum, monatlich fragen).	**Methode** dieses Bandes.
6	Welche Exporte und Migrationsexporte liegen auf Laufwerken, in Postfächern, auf externen Platten? Hat jede Datei ein Datum und einen Namen? _____	Der Ordner «Altdaten TEMP – nach Prüfung löschen» trug weder Datum noch Namen (vierundzwanzig Dateien, rund hundertzwanzigtausend Datensätze). Exporte gelten als Arbeitsergebnis, nicht als Datenbestand.	**Methode** dieses Bandes.
7	Wie viele Gästedatensätze hält das Haus, genau? (Zahl je System) _____	Die einfachste Kennzahl der Informationssicherheit eines Hotels: in jedem System in einer Minute zu ermitteln, und die einzige, die sagt, wie groß der Schaden im schlimmsten Fall wäre.	**Methode** dieses Bandes.

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
8	Wurde die Namenssuche durchgeführt? Genehmigt von der Leitung, ausgeführt von der IT (nicht vom Auditor), Name aus einem alten Jahrgang ohne laufenden Bezug zum Haus, Ergebnis als Zahl der Fundorte protokolliert, nicht als Datensatz? (Datum · Zahl der Fundorte) _____	So bleibt die Prüfung eine Prüfung und wird nicht selbst zur Verarbeitung. Das Ergebnis ist schneller und deutlicher als jedes Dokument.	**Methode** dieses Bandes.
9	Wurden bei jedem Dienstleisterwechsel die fünf Zeilen beantwortet: Was wird zurückgegeben, in welchem Format, bis wann, was wird gelöscht, wer bestätigt es schriftlich? _____	Der Wechsel eines Dienstleisters ist der gefährlichste Moment im Lebenslauf von Daten. Ohne schriftliche Bestätigung endet der Vertrag, aber die Daten bleiben. Für den Eintritt eines Lieferanten gibt es in den meisten Häusern ein Verfahren, für seinen Austritt keines. Regel: keine Schlussrechnung ohne Löschbestätigung.	**verlangt:** Der Auftragsverarbeiter löscht oder gibt zurück nach Wahl des Verantwortlichen und löscht vorhandene Kopien, soweit keine Pflicht zur Speicherung besteht (Datenschutz-Grundverordnung).
10	Wer löscht in zentral betriebenen Systemen einer Gruppe? Gibt es eine schriftliche Zuordnung? _____	Betreibt die Gruppe das System für fünf Häuser, ist Löschen eine zentrale Handlung mit fünf verantwortlichen Gesellschaften; ohne Zuordnung nimmt jede Seite an, die andere habe es getan.	**Methode** dieses Bandes.

4 Fristen, Nachweis und Kennzahl

Nr.	Frage (Eintrag unter der Frage)	Grund (aus dem Band)	Im Buch
11	Hat jede Datenart eine Frist mit einem Satz Begründung, einen Verantwortlichen, und erinnert ihn einmal im Jahr jemand, ob die Frist noch stimmt? _____	Daraus folgt keine feste Frist, sondern eine Begründungspflicht. Drei Sätze, eine Tabelle.	**verlangt:** Speicherbegrenzung: personenbezogene Daten nur so lange in identifizierbarer Form, wie für die Zwecke erforderlich (Datenschutz-Grundverordnung); Schweiz: Vernichtung oder Anonymisierung nicht mehr benötigter Personendaten.
12	Sind steuerlich relevante Unterlagen von den Gästedaten getrennt, in einem Archiv mit eigener Frist, eigenem Zugriff und eigenem Speicherort, nicht im Verwaltungssystem? _____	Die Rechnung bleibt, das Gästeprofil geht; der Aufenthalt in der Buchhaltung bleibt, die Vorliebe im Notizfeld geht. Wer die Trennung nicht macht, hält zu viel oder löscht zu viel.	**Methode** dieses Bandes.
13	Beginnt die Antwort an Firmenkunden mit dem Zusatz: in welchem System, mit welcher Verzögerung durch Sicherungen, mit welchen Ausnahmen aus steuerlichen Gründen? _____	Der Satz «wir löschen nach drei Jahren» ist fast immer zu kurz; mit Zusatz ist er der Unterschied zwischen einer Auskunft und einer falschen Zusicherung.	**Methode** dieses Bandes.
14	Ist die Zahl der Orte, an denen Gästedaten liegen, als Kennzahl festgelegt, und sinkt sie? (Zahl · Stichtag) _____	Eine der wenigen Kennzahlen dieses Gebiets, die man senken kann und deren Senkung unmittelbar Risiko abbaut.	**verlangt:** Festlegen, was überwacht und gemessen wird (9.1).
15	Besteht der Nachweis in einer Liste der Orte mit Datum der letzten Prüfung (halbe Seite je Datenart)? _____	Für Löschung heißt Nachweis nicht «Bericht über den Lauf», sondern «Nachweis über den Zustand».	**verlangt:** Dokumentierte Information als Nachweis der Ergebnisse von Überwachung und Messung (nach dem Band zu 9.1); Lenkung dokumentierter Information einschließlich Beseitigung (7.5).
16	Führt die Erklärung zur Anwendbarkeit die Löschung als umgesetzt, nur mit Verweis auf die Aufbewahrungsrichtlinie? _____	Eine Richtlinie ist die Absicht; umgesetzt ist die Maßnahme erst mit Ort, Frist, Verantwortlichem und Nachweis je Datenart. Gästedaten sind nicht schon deshalb dokumentierte Information im Sinne der Norm.	**verlangt:** Löschung (A.8.10), Maskierung (A.8.11), Sicherung (A.8.13), Geräte (A.7.14); Verzeichnis A.5.9; rechtliche Anforderungen A.5.33, A.5.34.

Rechtliche Anker laut Band. Steuer- und handelsrechtliche Aufbewahrung: Deutschland zehn Jahre für Bücher und bestimmte Aufzeichnungen, grundsätzlich acht Jahre für Buchungsbelege, grundsätzlich sechs Jahre für weitere Unterlagen (§ 147 Abgabenordnung; Verlängerungstatbestände gesondert prüfen); Österreich sieben Jahre (Bundesabgabenordnung); Schweiz zehn Jahre (Obligationenrecht). Besondere Meldescheine ausländischer Gäste in Deutschland: eigene, kürzere Frist des Melderechts. Die Fristen leben nebeneinander und betreffen verschiedene Datenbestände; alle sind an der geltenden Fassung zu prüfen. Benachrichtigung der Betroffenen: bei voraussichtlich hohem Risiko (Datenschutz-Grundverordnung; Schweiz Artikel 24 Datenschutzgesetz). Rechtsstand des Bandes: 28. September 2026.

Häufige Fehler (aus dem Band)

Nr.	Fehler	Was der Band daraus macht
1	Löschung mit Löschlauf gleichgesetzt	Ein Löschlauf ist eine Handlung in einem System; Löschung ist ein Zustand über alle Orte hinweg.
2	Das Altsystem, das nie abgeschaltet wurde	Kaum ein Haus nach einer Migration ohne einen solchen Server; angeschlossen, weil jemand «noch mal reinschauen» wollte.
3	Der Export für einen guten Zweck	Weihnachtsmailing, Auswertung für den Eigentümer, Tabelle für die Preisverhandlung: Gästedaten ohne Frist, weil sie als Arbeitsergebnis gelten.
4	Migrationsexporte	Jede Systemumstellung erzeugt Kontrolldateien, die danach niemandem mehr gehören; Systemwechsel sind ein Erbe, und Erbschaften werden nicht inventarisiert.
5	Das Vertragsende ohne Rückgabe	Der scheidende Dienstleister hat weder Anlass noch Auftrag noch Vergütung dafür; verlangt es niemand, geschieht es selten.
6	Vertrauen in die Aussage «das ist gelöscht»	Sie stammt fast immer von einer Person, die einen Vorgang ausgeführt hat, nicht von einer, die den Zustand geprüft hat.
7	Die Richtlinie ohne Karte	Sie nannte Fristen für Datenarten, aber keine Orte.
8	Berichte, die nur den Vorgang belegen	Vier Löschberichte erzeugen Zuversicht; ihre Aussagekraft endet an der Systemgrenze.
9	Der Auditumfang	In vier internen Audits war die Löschung anhand von Richtlinie und Berichten geprüft; die Frage «Wo liegen dieselben Daten noch?» wurde nie gestellt.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch das Recht oder die Regelwerke, die für Ihr Haus gelten. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt, dass jemand hingesehen hat, nicht dass der Zustand besteht, den es beschreibt. Sie legt keine Aufbewahrungsfristen fest: Die Norm tut das nicht, das Recht schon, und die Fristen stehen hier nur, wenn Sie sie aus Ihrem Recht eintragen. Ein Löschbericht, eine Namenssuche und eine Liste der Orte belegen den Zustand zu einem Tag, nicht dauerhaft. Rechtsstand des Bandes: 28. September 2026.