VORLAGE ZU ABSCHNITT 3.4 DES BANDES 5B

Die Rechtsprüfung ohne Jurist

Die Fragen, die ein interner Auditor stellen darf, und die Grenze, an der er aufhört: geprüft wird der Weg, auf dem eine Pflicht erkannt, zugeordnet und beantwortet wird.

Kategorie: Prüfliste (mit Anwendung in Schritten und häufigen Fehlern). Bezug im Buch: Abschnitt 3.4 (Das Prinzip, Der Rahmen in Deutschland, Österreich und der Schweiz); Norm: Klauseln 4.2, 5.3, 6.1.3, 7.4, 8.1 und 9.2 sowie Maßnahmen A.5.2, A.5.31, A.5.34 und A.6.8 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 28. September 2026.

Haus / Standort		**Ausgefüllt von**	
Datum		**Land (DE / AT / CH)**	

So nutzen Sie diese Vorlage

1. Nehmen Sie drei Pflichten, die das Haus selbst in seiner Liste führt, und verfolgen Sie für jede dieselben vier Fragen (Teil 1). Sie befreien den Auditor von der Frage «ist das erlaubt» und führen auf die Frage «wie würde es hier ablaufen».
2. Halten Sie die Antworten in der Tabelle mit vier Spalten fest: Pflicht, auslösendes Ereignis, Frist, Nachweis (Teil 2). Ob die Frist einen Monat, unverzüglich oder «so rasch als möglich» heißt, entscheidet nicht der Auditor; dass in der Spalte «Nachweis» etwas steht, sehr wohl.
3. Bleiben Sie auf der Seite der Grenze, die Teil 3 zieht: Der Auditor stellt keinen Gesetzesverstoß fest, sondern dass eine Pflicht des Hauses keinen Weg, keine Frist und keinen Nachweis hat.

Spalte «Im Buch»: verlangt = von der Norm oder vom Recht verlangt, wie das Buch es in eigenen Worten wiedergibt (Klausel oder Quelle in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Die vier Fragen je Pflicht

Frage	Grund (aus dem Band)	Im Buch
Wie erfährt das Haus davon, dass die Pflicht ausgelöst wurde?	Rechtspflichten sind in einem Betrieb keine Dokumente, sondern Ereignisse mit Uhren daran; ein Ersuchen kommt überall an, am Tresen, am Telefon, als Antwort auf einen Newsletter.	verlangt (7.4)
Wer bearbeitet sie?	Eine bestellte Datenschutzbeauftragte, deren Adresse an der Rezeption niemand kennt, ist zugewiesen, aber nicht bekannt gemacht.	verlangt (5.3; A.5.2)
Welche Frist gilt?	Die Frist beginnt mit dem Eingang im Unternehmen, nicht bei der zuständigen Person; ein Ersuchen im Sammelpostfach läuft.	verlangt (Recht des Landes); Frage: Methode
Wo steht, dass sie erfüllt wurde?	Eine Pflicht ohne Empfangsstelle im Haus ist eine Pflicht, die das Haus erst erfährt, wenn sie verletzt ist; «Erledigt» ist ein Ordner und kein Nachweis.	Methode dieses Bandes

Pflicht (aus der Liste des Hauses)	Wie erfährt das Haus davon?	Wer bearbeitet sie?	Frist	Wo steht, dass sie erfüllt wurde?
1				
2				
3				

2 Pflicht, auslösendes Ereignis, Frist, Nachweis

Pflicht	Auslösendes Ereignis	Frist	Nachweis

Eine Feststellung zu einer Rechtspflicht nennt das auslösende Ereignis, nicht den Paragrafen; der Paragraf gehört in die Anlage, das Ereignis in den Satz (Methode dieses Bandes).

3 Fragen, die ein Auditor stellen darf, und die Grenze

Frage	Antwort	Grund (aus dem Band)	Im Buch
Zeig mir, was passiert, wenn jemand auf den Newsletter antwortet.		Die Frage, die nach zwanzig Minuten gefunden hätte, was die Prüfung der Dokumente nicht fand; sie stand auf keiner Liste, weil Listen aus Maßnahmen gebaut sind und nicht aus Ereignissen.	Methode dieses Bandes
Woran erkennt man bei uns ein Ersuchen? Steht es auf einer Karte am Arbeitsplatz mit Gästekontakt?		Die Merkmale sind sprachlich, nicht juristisch: «keine Werbung mehr», «bitte löschen», «welche Daten haben Sie über mich», «das stimmt nicht», «ich widerspreche»; weitere Wendungen des Hauses: _____.	Methode dieses Bandes

Frage	Antwort	Grund (aus dem Band)	Im Buch
Hat die Eingangsadresse einen Namen, eine Stellvertretung, eine tägliche Sichtung und eine Liste (Eingang, Art, Frist, Bearbeiter, Abschluss)?		Verantwortung verdünnt sich mit der Zahl der Zugriffsberechtigten; wer die Erkennung an eine Person bindet, die «so etwas immer sieht», hat Glück, keinen Prozess.	Methode dieses Bandes
Wie viele Ersuchen erwartet das Haus im Jahr, und wie viele wurden erkannt?		Ein Haus mit achttausend Adressen und null Ersuchen hat sie nicht erhalten, sondern nicht erkannt: Die Null ist ein Alarm.	Methode dieses Bandes
Wo endet die Löschung auf Ersuchen, und wo beginnt die gesetzliche Aufbewahrung?		Rechnungen, Meldescheine und steuerlich relevante Unterlagen bleiben; gelöscht wird, was darüber hinaus gehalten wird: Profile, Präferenzen, Marketingadressen, Notizfelder.	verlangt (Recht des Landes); Frage: Methode
Gibt es eine schriftlich genehmigte Testanfrage, ihre Laufzeit und die Stelle, an der sie liegen blieb?		Der Test wird vorher genehmigt und hinterher offengelegt; er prüft den Weg, nicht die Person, und berichtet nie personenbezogen.	Methode dieses Bandes

Der Auditor darf feststellen	Der Auditor stellt nicht fest
Dass eine Pflicht, die das Haus selbst in seiner Liste führt, keinen Weg, keine Frist und keinen Nachweis hat.	Dass das Haus gegen das Gesetz verstoßen hat; das steht ihm nicht zu.
Dass eine Frist gelaufen ist: eine Beobachtung mit Datum.	Dass die Frist versäumt wurde: das ist eine rechtliche Würdigung.
Dass die Liste in den letzten zwölf Monaten nicht gegen eine äußere Quelle geprüft wurde.	Ob die Auslegung einer Bestimmung richtig ist; Auslegung ist Sache der Juristen, Prozess Sache des Managementsystems.

Formulierung, die sich bewährt hat: Eingang am dritten Februar, keine Antwort dokumentiert bis zum Berichtsdatum, kein Verfahren zur Erkennung vorhanden. Der Bericht unterscheidet «dokumentiert», «beobachtet» und «geprüft am Vorgang» (Methode dieses Bandes; Klausel 9.2: verlangt, dass das Audit prüft, ob das System die eigenen Anforderungen der Organisation erfüllt, einschließlich der Liste der rechtlichen Verpflichtungen).

4 Recht, auf das der Auditor trifft (Rechtsstand: 28. September 2026)

Gegenstand	Deutschland	Österreich	Schweiz
Rechte der betroffenen Person und Antwortfrist	DSGVO: Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch; Antwort unverzüglich, in jedem Fall innerhalb eines Monats nach Eingang (Art. 12); Verlängerung um höchstens zwei weitere Monate nur, soweit erforderlich, mit Mitteilung der Gründe binnen eines Monats	wie Deutschland (DSGVO); Datenschutzbehörde zuständig	revDSG: Auskunfts- und Löschungsansprüche; Frist für das einzelne Begehren gesondert zu bestimmen; ob die DSGVO daneben anwendbar ist, ist gesondert zu prüfen
Widerspruch gegen Direktwerbung	Ohne Abwägung; wirkt sofort; Wettbewerbsrecht für E-Mail-Werbung; Aufsichtsbehörden der Länder	Ohne Abwägung; TKG 2021: unerbetene Nachrichten ohne Einwilligung unzulässig, enge Ausnahme für Bestandskunden mit einfacher Abmeldemöglichkeit; Widerspruch per Antwort ist wirksam	Lauterkeitsrecht für Massenwerbung; Fristen und Rechtsfolgen nicht identisch mit den europäischen

5 Anwendung in Schritten

Schritt	Was zu tun ist (Operative Synthese des Abschnitts)	Erledigt
1 Sofort	Marketing-, Reservierungs- und Empfangspostfach der letzten zwölf Monate nach den Wendungen der Karte durchsuchen und zählen, wie viele Ersuchen unerkannt liegen.	☐
2 Planen	Eine Eingangsadresse mit Namen und Stellvertretung einrichten, die Karte mit den Wendungen an jeden Arbeitsplatz mit Gästekontakt hängen, eine Liste mit fünf Spalten führen.	☐
3 Überwachen	Einmal jährlich eine genehmigte Testanfrage stellen und die Laufzeit messen; die Zahl der erkannten Ersuchen und die mittlere Bearbeitungsdauer in die Managementbewertung nehmen.	☐
4 Berichten	Jede Feststellung nennt das auslösende Ereignis, nicht den Paragrafen.	☐

6 Häufige Fehler

Fehler (wie der Band ihn nennt)	Was der Band dagegen zeigt
Pflicht und Dokument werden gleichgesetzt: Die Löschfristentabelle sagt nichts darüber, was bei einem Löschverlangen geschieht.	Das sind zwei verschiedene Pflichten mit verschiedenen Fristen.
Die Pflichten sind nach Abteilungen geordnet; Gäste unterscheiden nicht zwischen Abteilungen.	An jeder Schnittstelle liegt eine Lücke; die Zahl der Schnittstellen ist in einem Hotel größer als in fast jedem Betrieb dieser Größe.
Niemand weiß, woran man ein Ersuchen erkennt.	Eine Karte mit den Wendungen neben dem Bildschirm und einer Adresse darunter ist die wirksamste Maßnahme des Abschnitts.
Das gemeinsame Postfach: niemand zuständig, alles gilt als gelesen, «Erledigt» ist ein Ordner.	Dem Postfach einen Namen geben: eine Person, eine Stellvertretung, eine tägliche Sichtung, eine Liste.
Das Newsletter-Werkzeug kennt nur den Abmeldelink; wer per Antwort schreibt, existiert für das Werkzeug nicht.	Werkzeuge verwalten, was erkannt wurde; sie ersetzen die Erkennung nicht.
Die bestellte externe Beauftragte sieht in vierzehn Monaten kein Ersuchen.	Eine Funktion ohne Zulauf ist keine Funktion; erkennen kann nur das Haus.
Der Auditor prüft, was das System beschreibt, nicht was es nicht beschreibt.	Rechtspflichten gelten unabhängig davon, ob ein Verfahren für sie existiert.
Die Schulung fragt die Meldefrist ab, nicht den Auslöser.	Schulungen, die Wissen abfragen statt Handlungen zu proben, erzeugen Menschen, die die Frist kennen und den Auslöser nicht.

Fehler (wie der Band ihn nennt)	Was der Band dagegen zeigt
Die Maßnahme zum Schutz personenbezogener Daten gilt als umgesetzt, weil Datenschutzerklärung und Verträge existieren.	Beide Belege betreffen die Außendarstellung und die Lieferkette, nicht die Bearbeitung eingehender Ersuchen.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und keine juristische Würdigung: Sie sagt nicht, ob ein Haus das Gesetz erfüllt, und der Auditor, der sie benutzt, stellt das auch nicht fest. Sie ersetzt weder die ISO/IEC 27001 noch das Recht, das für Ihr Haus gilt; Fristen und Zuständigkeiten sind an der geltenden Fassung zu prüfen. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt einen Weg, nicht dass eine Pflicht erfüllt wurde. Rechtsstand des Bandes: 28. September 2026.