VORLAGE ZU ABSCHNITT 4.12 DES BANDES 5B

Prüfung fremder Zertifikate

Eine Seite für den Einkauf: sieben Fragen an das Zertifikat eines Anbieters, bevor der Vertrag unterschrieben wird, und was in den Vertrag gehört.

Kategorie: Prüfliste. Bezug im Buch: Abschnitt 4.12 (Banken, Versicherer und das Zertifikat als Nachweis); Norm: Klausel 8.1 sowie Maßnahmen des Anhangs A (Fassung 2022) zu Lieferantenbeziehungen der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 28. September 2026.

Anbieter		**Ausgefüllt von**	
Eingekaufte Leistung		**Datum**	
Ausstellende Stelle		**Gültig bis**	

So nutzen Sie diese Vorlage

1. Prüfen Sie das Zertifikat des Anbieters vor der Beauftragung, mit demselben Blick, mit dem das Haus selbst geprüft wird. Die Prüfung ist Teil der Steuerung extern bereitgestellter Prozesse (8.1) und nicht Einkaufssache.
2. Beantworten Sie die Fragen in dieser Reihenfolge; die letzte ist die unbequemste und die aufschlussreichste. Tragen Sie in «Antwort» ein, was Sie gesehen haben, nicht, was der Anbieter zusagt.

1 Das Zertifikat in sieben Schritten

Frage	Antwort	Grund (aus dem Band)	Im Buch
Steht die ausstellende Stelle im Verzeichnis einer nationalen Akkreditierungsstelle? ☐ ja ☐ nein		Das Haus verlangt von sich selbst eine Zertifizierung und prüft deshalb die seines Dienstleisters mindestens so weit, wie es selbst geprüft wurde.	Methode (Anker: 8.1)
Ist das Zertifikat in der öffentlichen Datenbank abrufbar und gültig? ☐ ja ☐ nein Fehlt es dort: bei der Stelle und bei der Akkreditierungsstelle nachfragen.		Ein Fehlen ist ein Anlass nachzufragen, kein Beweis einer Fälschung.	Methode dieses Bandes
Nennt der Geltungsbereich die Leistung, die wir einkaufen: Betrieb, nicht nur Entwicklung? ☐ ja ☐ nein Wörtlicher Geltungsbereich:		«Entwicklung der Plattform» heißt: Geprüft wurde, wie Software entsteht, nicht, wie Gästedaten verarbeitet, gespeichert und gesichert werden.	Methode dieses Bandes
Nennt der Anhang den Standort, an dem unsere Daten verarbeitet werden? ☐ ja ☐ nein		Im Fall lagen die Produktivdaten an keinem der beiden im Anhang genannten Standorte, sondern bei einem Unterauftragnehmer.	Methode dieses Bandes
Wer sind die Unterauftragnehmer, und in welchen Ländern sitzen sie?		Ein Zertifikat sagt nichts über die Kette hinter dem Anbieter; sie steht im Vertrag, im Verzeichnis der Unterauftragnehmer und in der Vereinbarung zur Auftragsverarbeitung, wenn jemand danach gefragt hat.	Methode dieses Bandes
Wann läuft es ab (Datum), und wer schickt uns das Nachfolgezertifikat unaufgefordert?		Im Fall war das Zertifikat bei Vertragsunterzeichnung sieben Wochen vor Ablauf, und das Nachfolgezertifikat hatte niemand angefordert.	Methode dieses Bandes
Was ergab das letzte Überwachungsaudit? Vertraglich absicherbar: Zusage einer Zusammenfassung oder einer Bestätigung der Stelle über den Fortbestand.		Die letzte Frage ist die unbequemste und die aufschlussreichste.	Methode dieses Bandes

2 Was in den Vertrag gehört

Vereinbart?	Inhalt der Vereinbarung (Regel 2 des Abschnitts)	Fundstelle im Vertrag
☐ ja ☐ nein	Verzeichnis der Unterauftragnehmer mit Zustimmungsvorbehalt	
☐ ja ☐ nein	Orte der Verarbeitung	
☐ ja ☐ nein	Meldefristen bei Vorfällen	
☐ ja ☐ nein	Prüfrecht	
☐ ja ☐ nein	Rückgabe und Löschung bei Vertragsende	
☐ ja ☐ nein	Verfügbarkeit und Wiederanlauf	

Ein zertifizierter Anbieter mit schlechtem Vertrag ist schlechter als ein nicht zertifizierter mit gutem. Deckt das Zertifikat eines jungen Anbieters nur die Entwicklung, ist er kein schlechter Anbieter: Seine Betriebsrisiken regelt das Haus im Vertrag, statt sie einer Urkunde zu überlassen. Die sieben Fragen dienen nicht dem Ausschluss, sondern der Kenntnis dessen, was man kauft. Methode dieses Bandes; Anker: Anhang A (2022), Lieferantenbeziehungen und Lieferkette.

3 Häufiger Fehler

Das Zertifikat wird in zehn Sekunden «geprüft»: Jemand sieht, dass es eines gibt. Der Geltungsbereich nennt nur die Entwicklung.	Dieselbe Firma, derselbe Name, dasselbe Zeichen, aber eine andere Aussage als der gekaufte Betrieb. Im Einkauf fühlt sich ein Haus als Kunde und damit als der, der beruhigt werden soll. Gegenüber einem Anbieter, der Gästedaten verarbeitet, bleibt es gegenüber den Gästen verantwortlich und ist insoweit selbst die prüfende Stelle.

Recht laut Buch (Rechtsstand des Bandes: 28. September 2026.): Ein Auftragsverarbeiter darf einen weiteren nur mit Genehmigung einsetzen; die Verarbeitung außerhalb des Europäischen Wirtschaftsraums braucht eine eigene Grundlage; verantwortlich gegenüber dem Gast bleibt in jedem Fall das Haus. Ein Zertifikat ändert daran nichts. Schweiz: vergleichbare Lage nach dem revidierten Datenschutzgesetz.

Was diese Vorlage nicht ist

Diese Vorlage ist kein Rechtsrat und ersetzt weder die ISO/IEC 27001 noch den Vertrag mit dem Anbieter, die Vereinbarung zur Auftragsverarbeitung oder die Auskunft der ausstellenden Stelle. Sie empfiehlt keinen Anbieter und keine Zertifizierungsstelle. Ein ausgefülltes Blatt ist kein Nachweis: Es zeigt, dass jemand das Zertifikat gelesen hat, nicht, dass der Anbieter hält, was es beschreibt.