Das Register der Schlüssel

Jeder Lieferant, der das Haus von außen erreichen kann, was er erreicht und wie viele Stunden er hat, es Ihnen zu sagen.

Kategorie: Arbeitsblatt. Bezug im Buch: Abschnitt 1.12 (Leitfrage, Tabellen 1, 2, 4 und 5; als Register auch in der Excel-Datei zu Abschnitt 1.12); Norm: Klauseln 4.3 und 8.1 sowie Maßnahmen A 5.19 bis 5.23 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 27. September 2026.

Haus		**Geführt von (benannte Person)**	
Stand (Datum)		**Zahl der Lieferanten gesamt**	

So nutzen Sie diese Vorlage

1. Schreiben Sie in Teil 1 jedes Unternehmen auf, das die Systeme oder die Information Ihres Hauses von außerhalb erreichen kann, gleich welche Abteilung den Vertrag hält: auch die, die Türschlösser, Aufzüge, Kameras, Gebäudeleittechnik und das Fernsehsystem der Zimmer warten.
2. Notieren Sie daneben die Zahl, die sein Vertrag ihm gibt, um Ihnen einen Einbruch auf seiner Seite zu melden, mit der Einheit (Stunden oder Tage). Ist die Spalte leer, erfahren Sie es so, wie die meisten Hotels es erfahren: von jemand anderem.
3. Stellen Sie die Fragen aus Teil 2 vor der Wahl, verlangen Sie die Klauseln aus Teil 3 vor der Unterschrift und bei jeder Verlängerung. Das ausführliche Register mit allen Spalten ist die Excel-Datei zu Abschnitt 1.12.

Spalte «Im Buch»: verlangt = von der Norm verlangt, wie der Band sie in eigenen Worten wiedergibt (Klausel oder Maßnahme in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Das Register: eine Zeile je Schlüssel

Die meisten Häuser führen zwei Listen, die IT-Liste (Verwaltungssystem, Channel Manager, Zahlungen, Leitung) und die Liste der Wartungsfirmen (Aufzüge, Schlösser, Pool, Heizung, Kameras). Die Liste der Schlüssel fragt, wer von außen in welche Systeme gelangt; sie gehört keiner der beiden Abteilungen und wird deshalb von niemandem geführt. **verlangt:** extern bereitgestellte Dienste gesteuert (8.1), Nachweis: eine Liste aller Lieferanten, die Systeme oder Information erreichen. **Methode:** eine benannte Person, die sie führt.

Nr.	Lieferant	Was er erreicht	Zugang (ständig · auf Anforderung)	Frist zur Meldung (Zahl · Stunden/Tage)	Wer im Haus die Meldung erhält
Bsp.	Firma, die die elektronischen Schlösser installiert und betreut	Schlossserver: Zimmernummern, Gültigkeitszeiten der Karten, bei einem Teil die Namen der Gäste; kann eine Karte für jedes Zimmer erzeugen	ständig (Fernwartung)	keine Klausel	niemand benannt: allgemeine E-Mail an eine Adresse, die niemand las

Erste Zeile: **Beispiel aus Abschnitt 1.12** (Montreux, Wartungsvertrag der Haustechnik, zwölf Jahre alt, elfmal per Rechnung verlängert). Das Beispiel ist Illustration; Ihre Zeilen beginnen darunter.

2 Bei der Wahl: die Fragen an den Lieferanten

Nr.	Frage	Grund (aus dem Band)	Im Buch	Antwort
1	Wie erreicht der Lieferant das System nach der Installation: ständig oder nur auf Anforderung, wenn das Haus den Zugang öffnet, ihn protokolliert und danach schließt?	Ein Zugang, der immer offen ist, ist ein Zugang, den das Haus nicht steuert.	**verlangt:** Risiken aus der Nutzung der Produkte und Dienste von Lieferanten gesteuert (A 5.19). **Methode:** der Zugang auf Anforderung.	
2	Wie ist der Zugang geschützt, wer kann ihn sonst noch benutzen, und sind die Zugangsdaten für jeden Kunden getrennt?	Der Lieferant benutzte bei allen Kunden dieselben Zugangsdaten; das konnte das Haus nur durch Fragen erfahren, nicht durch einen Blick auf seine eigenen Systeme.	**verlangt:** Anforderungen mit jedem Lieferanten festgelegt und vereinbart, nach Art der Beziehung (A 5.20).	
3	Von wem hängt der Lieferant ab: Fernwartungsprogramm, Server, übernehmende Gruppe?	Jedes Glied der Kette konnte den Schlossserver betreffen, und das Haus kannte keines.	**verlangt:** Risiken der Lieferkette für Informations- und Kommunikationstechnik gesteuert (A 5.21). **Methode:** nicht bis ins vierte Glied.	

Nr.	Frage	Grund (aus dem Band)	Im Buch	Antwort
4	Was tut der Lieferant, wenn der Zugang gestohlen wird oder seine Systeme kompromittiert sind, und wie bald unterrichtet er das Haus, wen?	Der Lieferant hatte seine Kunden mit einer allgemeinen E-Mail unterrichtet, an eine Adresse, die niemand las.	**verlangt:** Anforderungen zu Meldung vereinbart (A 5.20). **Methode:** Frist in Stunden und benannte Funktion im Wortlaut.	
5	Wo liegen die Daten bei gehosteten Systemen, und wie werden sie am Vertragsende zurückgegeben oder gelöscht?	Der Schlossvertrag hatte keine Klausel zu Protokollen oder zur Rückgabe und Löschung von Daten am Vertragsende.	**verlangt:** Erwerb, Nutzung, Verwaltung und Beendigung von Cloud-Diensten (A 5.23).	

3 Bei der Unterschrift und bei jeder Verlängerung: die Klauseln

Klausel	Grund (aus dem Band)	Im Buch	☐
Wie der Zugang geschützt und gesteuert wird, mit getrennten Zugangsdaten je Kunde	Der Wartungsvertrag war für Geräte geschrieben, die früher mechanisch waren; er sagte nichts über Fernzugang.	**verlangt:** A 5.20. Wortlaut: Methode.	☐
Meldefrist für einen Vorfall, der das Haus betrifft, und die benannte Funktion im Haus, die ihn erhält	Ohne diese beiden Sätze kann ein Lieferant seine gesetzliche Pflicht erfüllen und das Haus trotzdem erst beim Abendessen davon erfahren.	**verlangt:** A 5.20. Frist und Funktion im Vertrag: Methode.	☐
Welche Unterauftragnehmer beteiligt sind, und wie Änderungen an ihnen mitgeteilt werden	Der Lieferant war übernommen worden, hatte sein Fernwartungsprogramm zweimal gewechselt und seine Server verlegt, ohne dass jemand fragte.	**verlangt:** A 5.20, 5.21, 5.22 (Änderungen gesteuert).	☐
Welche Protokolle geführt werden	Der Schlossserver bewahrte sein Protokoll nur vierzehn Tage auf; ob etwas geschehen war, ließ sich nicht mehr sagen.	**verlangt:** A 5.20.	☐
Rückgabe und Löschung von Daten am Vertragsende; Datenstandort bei gehosteten Systemen	Diese Klauseln kosten nichts, wenn der Lieferant den Auftrag will; danach sind sie fast nicht zu bekommen.	**verlangt:** A 5.23.	☐

Verlängerung per Rechnung ist eine zweite Gelegenheit, dieselben Klauseln nachzuholen. Jährliche Überprüfung jedes wichtigen Lieferanten, und ein Anlass, wenn ein Lieferant sich ändert (**verlangt** · A 5.22): Datum der letzten Überprüfung je Zeile im Register in Excel. Ein Einzelhaus kann kein weltweites Softwareunternehmen prüfen: Es kann die Bedingungen lesen, die Fragen stellen, die sie nicht beantworten, Lieferanten mit guten Antworten vorziehen und für die übrigen das angenommene Risiko festhalten (**Methode**).

4 Was das Recht zu Lieferant und Meldung sagt

Ebene	Deutschland	Österreich	Schweiz
Meldung des Lieferanten an das Haus	unverzüglich nach Bekanntwerden einer Verletzung (Art. 33 Abs. 2 DSGVO)	ebenso	so rasch als möglich (revDSG Art. 24 Abs. 3)
Meldung des Hauses	an die Aufsicht unverzüglich und möglichst binnen 72 Stunden ab Kenntnis, außer bei voraussichtlich unwahrscheinlichem Risiko; an die Gäste unverzüglich bei voraussichtlich hohem Risiko	ebenso, an die Datenschutzbehörde	an den Eidgenössischen Datenschutzbeauftragten bei voraussichtlich hohem Risiko; an die Gäste, wenn zu ihrem Schutz erforderlich
Lieferant, der im Auftrag Personendaten bearbeitet	Auftragsverarbeitung mit schriftlichem Vertrag; Unterauftragnehmer nur mit Genehmigung (Art. 28 DSGVO)	ebenso	Auftragsbearbeitung; Unterauftrag nur mit vorheriger Genehmigung (revDSG)

Das Gesetz nennt keine Frist in Tagen und keinen Empfänger: beides gehört in den Vertrag. Hersteller vernetzter Produkte im Anwendungsbereich des Cyber Resilience Act müssen seit 11. September 2026 schwerwiegende Vorfälle und aktiv ausgenutzte Schwachstellen melden; das hilft dem Haus nur, wenn es weiß, welche Produkte es von welchen Herstellern besitzt, und jemand die Mitteilungen liest. Für die Schweiz gilt der Act nicht allgemein; bei Produkten, die auch auf dem Unionsmarkt bereitgestellt werden, ist mittelbarer Nutzen am Modell und im Vertrag zu prüfen. Wo Lieferanten selbst gesetzlichen Sicherheitspflichten unterliegen, ersetzen diese die eigenen Anforderungen des Hauses nicht.

Was diese Vorlage nicht ist

Dieses Blatt ersetzt weder die Norm noch eine Rechtsberatung oder einen Vertragsentwurf und ist kein Nachweis: Ein ausgefülltes Register belegt weder, dass ein Lieferant sicher ist, noch, dass eine Klausel vereinbart wurde; das tut nur der unterschriebene Vertrag. Wie lange ein Lieferant zur Meldung hat, bestimmt der Vertrag; das Gesetz nennt hier keine Zahl. Die Fragen, die Klauseln in dieser Form und die Spalte «Eintrag» sind Methode dieses Bandes, keine Anforderung; verlangt ist, was mit einer Klausel oder Maßnahme der Norm gekennzeichnet ist. Die Angaben zum Recht geben den Stand des Bandes wieder (Rechtsstand des Bandes: 27. September 2026).