Die ersten zweiundsiebzig Stunden

Die fünf Fragen, die schnell entscheiden, was eine Nachricht ist, und die drei Verbote der ersten Stunde: vorher vorbereitet, nicht unter Druck erfunden.

Kategorie: Arbeitsblatt. Bezug im Buch: Abschnitt 2.11 (Leitfrage, Tabellen 1, 2, 4 und 5); Norm: Maßnahmen A 5.24, 5.25, 5.26, 5.27, 5.28, 5.5, 5.6, 6.8 und 8.8 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Buches. Rechtsstand des Bandes: 27. September 2026.

Haus / Standort		**Ausgefüllt von**	
Gültig ab		**Zuletzt auf Papier geübt**	

So nutzen Sie diese Vorlage

1. Schreiben Sie auf, was an einem Freitag um fünf geschieht, wenn an der allgemeinen Adresse eine E-Mail eintrifft, in der jemand schreibt, er könne die Buchungen Ihrer Gäste einsehen: wer sie liest, wann, wer entscheidet, ob sie stimmt, und wer entscheidet, ob Behörde und Gäste informiert werden müssen (2.11, Leitfrage). Beginnen die Antworten am Montag, kann die Uhr drei Tage gelaufen sein.
2. Teil 1 benennt, wer zu jeder Stunde entscheidet, mit Vertretung. Teil 2 und 3 hat der diensthabende Manager in der ersten Stunde in der Hand; Teil 4 bis 6 halten Uhr, Zeitplan und Fristen fest. Der Plan wird einmal im Jahr auf Papier geübt.

1 Wer entscheidet, wer spricht, wohin die Warnungen gehen

Rolle	Name und Erreichbarkeit	Vertretung und Erreichbarkeit
Erster Entscheider zu jeder Stunde (diensthabender Manager)		
Direktion, mit benannter Vertretung darüber		
Datenschutzbeauftragter (wird sofort gerufen, wenn es um personenbezogene Daten gehen könnte)		
IT-Dienstleister		
Sprecher für das Haus (Gäste, Presse, Behörden; alle anderen benutzen die Worte, die sie erhalten)		
Adresse, an der Warnungen ankommen und die auch am Wochenende gelesen wird		
Datenschutzbehörde (Meldeformular vorher bekannt)		
Computer-Notfallteam (DE: BSI; AT: CERT.at; CH: Bundesamt für Cybersicherheit)		

verlangt: Rollen und Verantwortlichkeiten festgelegt und bekannt gemacht (A 5.24); Kontakt zu Behörden und Fachgruppen (A 5.5, 5.6); rechtzeitige Meldung durch das Personal (A 6.8); eine Adresse für Information über Schwachstellen (A 8.8). **Methode** dieses Bandes: der diensthabende Manager als erster Entscheider.

2 Die fünf Fragen der ersten Stunde

Nr.	Frage	Grund (aus dem Band)	Antwort (ja / nein / Notiz)	Im Buch
1	**Betrifft es personenbezogene Daten von Gästen oder Personal?**	Davon hängt ab, ob der Datenschutzbeauftragte sofort gerufen wird und ob die Frist des Datenschutzrechts läuft.		**Methode** dieses Bandes. Verlangt: Ereignisse beurteilen und entscheiden, ob sie Vorfälle sind (A 5.25).
2	**Lässt sich feststellen, ob es stimmt, und wie schnell?**	Eine kurze Reihe von Fragen hätte binnen einer Stunde festgestellt, dass die Bildschirmfotos echt waren und sich die Lücke in drei Minuten nachvollziehen ließ.		**Methode** dieses Bandes (A 5.25).
3	**Woher können die Daten kommen, auch von Dienstleistern?**	Die Daten lagen auch in der Buchungsstrecke einer Agentur, die in keinem Register stand; die ersten Stunden gingen mit der Suche am falschen Ort verloren.		**Methode** dieses Bandes (A 5.25).
4	**Dauert es an?**	In den drei Tagen zwischen Eingang und Antwort liefen die fremden Abfragen weiter.		**Methode** dieses Bandes (A 5.25).
5	**Wer außerhalb des Hauses muss es erfahren, und bis wann?**	Die Fristen kommen aus dem Recht und aus Verträgen; der Plan führt sie zusammen, damit die Person, die in der ersten Stunde entscheidet, alle kennt.		**Methode** dieses Bandes (A 5.25).

Nicht verlangt ist ein förmliches Klassifizierungsschema für Vorfälle.

3 Die drei Verbote der ersten Stunde

Verbot	Was es heißt	Im Buch
☐ **nicht weiterleiten**	außer an die im Plan Genannten. Die E-Mail vierzehnmal weiterzuleiten verteilte fünf Bildschirmfotos mit Daten wirklicher Gäste auf vierzehn Postfächer.	**verlangt:** Beweise ermitteln, sammeln und sichern (A 5.28). **Methode** dieses Bandes: die drei Verbote.
☐ **nicht dem Absender antworten**	außer nach dem Plan. Die Antwort an einen Melder ist ein Dank, eine Bitte um die Einzelheiten und eine Zusage, wann er wieder hört; eine Drohung vertreibt den einzigen Menschen, der helfen wollte.	**Methode** dieses Bandes (A 5.28, A 8.8).
☐ **nichts löschen und nichts abschalten**	bevor der IT-Dienstleister sagt, wie Spuren gesichert werden. Das Original der Nachricht wird behalten.	**verlangt:** Beweise sichern (A 5.28).

4 Die Uhr

Die Frist von zweiundsiebzig Stunden läuft ab dem Zeitpunkt, zu dem der Verantwortliche Kenntnis von der Verletzung erlangt. Kenntnis heißt hinreichende Gewissheit; eine kurze erste Prüfung ist zulässig, aber sie muss sofort beginnen. Eine feste Zeitspanne dafür gibt es nicht: Eingang, Prüfung, Grad der Gewissheit und die Gründe einer Verzögerung sind festzuhalten (2.11, Rahmen).

Eingang der Nachricht (Datum, Uhrzeit)		**Beginn der Prüfung (Datum, Uhrzeit)**	
Grad der Gewissheit erreicht (Zeitpunkt)		**Gründe einer Verzögerung**	
Meldung an die Behörde (Datum, Uhrzeit)		**Benachrichtigung der Gäste (Datum, Uhrzeit)**	

Rechtsstand des Bandes: 27. September 2026. Dokumentationspflicht: jede Verletzung, auch die nicht gemeldete (Art. 33 Abs. 5 DSGVO, DE/AT); CH: Dokumentationspflicht nach der Verordnung zum DSG.

5 Der Zeitplan: erste Stunde, erster Tag, zweiundsiebzig Stunden

Zeitraum	Was geschieht, wer tut es	Erledigt (Datum, Uhrzeit)
Erste Stunde		
Erster Tag		
Zweiundsiebzig Stunden		

verlangt: auf Vorfälle nach dokumentierten Verfahren reagieren (A 5.26); aus Vorfällen lernen, mit festgehaltenen Änderungen (A 5.27). **Methode** dieses Bandes: der Zeitplan für diese drei Zeiträume, auf zwei Seiten; ausführliche Handbücher für jede Art von Vorfall sind nicht verlangt.

6 Wer was wem wann meldet (Tabelle 5)

Pflicht	Deutschland	Österreich	Schweiz
Datenschutz: Meldung an die Behörde	binnen 72 Stunden ab Kenntnis, außer bei voraussichtlich keinem Risiko; schrittweise möglich (Art. 33 DSGVO)	ebenso, an die Datenschutzbehörde	so rasch als möglich an den EDÖB, wenn voraussichtlich ein hohes Risiko besteht (revDSG Art. 24)
Datenschutz: Benachrichtigung der Gäste	unverzüglich bei voraussichtlich hohem Risiko (Art. 34 DSGVO)	ebenso	wenn zu ihrem Schutz nötig oder vom EDÖB verlangt
Dienstleister gegenüber dem Hotel	unverzüglich (Art. 33 Abs. 2 DSGVO)	ebenso	so rasch als möglich (revDSG Art. 24 Abs. 3)
Cybersicherheit: erhebliche Vorfälle	24 Stunden Frühwarnung, 72 Stunden Meldung, ein Monat Abschlussbericht, nur für erfasste Einrichtungen; das Hotel ist es nicht	ebenso nach dem NISG 2026 ab 1. Oktober 2026; ein Hotel ist allein aufgrund der Beherbergung in der Regel nicht erfasst	24 Stunden an das Bundesamt für Cybersicherheit, nur für kritische Infrastrukturen; das Hotel ist keine

Ein Haus, das sich mit der falschen Frist beschäftigt, verpasst leicht die richtige. Ist ein Dienstleister des Hauses erfasst, läuft neben der Frist des Hauses auch dessen eigene; beide sollten voneinander wissen.

Was diese Vorlage nicht ist

Dieses Blatt ersetzt weder die Norm noch eine Rechtsberatung, keinen Plan für Vorfälle des Hauses und kein Urteil einer Zertifizierungsstelle oder Datenschutzbehörde. Ein ausgefülltes Blatt ist kein Nachweis, dass das Haus auf einen Vorfall vorbereitet ist: Es hält fest, wer entscheidet und wie die Uhr zu führen ist; ob eine Meldung rechtzeitig ist, bleibt eine Frage des Einzelfalls. Die Rechtshinweise geben den Stand des Bandes wieder (Rechtsstand des Bandes: 27. September 2026); verbindlich ist die jeweils gültige Fassung von Gesetz und Norm.