

WERKSTATT-CHECK: DATENSCHUTZ UND INFORMATIONSSICHERHEIT

Leitfaden für die Geschäftsführung · so läuft der Termin und so stellen Sie sich darauf ein

Beim Termin gehen wir gemeinsam mit Ihnen einen Fragebogen durch und sehen uns anschließend den Betrieb an. Am Ende wissen Sie, was bei Ihnen mit Kunden- und Beschäftigendaten schon gut läuft, was noch fehlt und was zuerst angepackt wird. Dieser Leitfaden zeigt, wie der Termin abläuft und wie Sie sich mit wenig Aufwand darauf einstellen.

1 · WURUM ES GEHT

Datenschutz schützt die Menschen

Kunden, Beschäftigte, Bewerber: Es geht darum, wie mit ihren Daten umgegangen wird. Vom Kennzeichen im Auftrag über die Krankmeldung bis zur Bewerbung.

Informationssicherheit schützt den Betrieb

Rechner, Zugänge, Datensicherung, Ablauf bei einem Ausfall. Sie entscheidet darüber, wie lange Sie arbeiten können, wenn morgen früh ein System nicht startet.

Beides gehört zusammen, weil in einer Werkstatt dieselben Daten über dieselben Geräte laufen. Der Check ist eine **Bestandsaufnahme**. Er ist keine Prüfung durch eine Behörde und keine Rechtsberatung.

2 · SO LÄUFT DER TERMIN AB

Der Fragebogen hat fünf Seiten und zwölf Abschnitte. Wir gehen ihn in vier Teilen durch. Die Dauer richtet sich nach der Größe des Betriebs; Rainer Orthober nennt sie bei der Terminabsprache.

Teil	Was besprochen wird	Abschnitte
Gespräch am Tisch	Betrieb und Verantwortlichkeiten, Datenwege im Alltag, Verarbeitung und Aufbewahrung, Dienstleister und Verträge	1 bis 4 (Seite 1 und 2)
Rundgang	Annahme, Büro, Werkstatt, Lager und IT: Zugänge, Geräte, Arbeitsplätze, Datensicherung und sichere Kommunikation	5 und 6 (Seite 3)
Organisation	Dokumentation, Unterweisung, Datenpannen, Notbetrieb und, falls vorhanden, Kameras	7 bis 9 (Seite 4)
Abschluss	Anforderungen Ihrer Kunden, NIS-2, Maßnahmenplan mit Prioritäten, nächster Schritt	10 bis 12 (Seite 5)

3 · WER DABEI SEIN SOLLTE

Wer	Wofür
Geschäftsführung	Betrieb, Zuständigkeiten, Entscheidungen, Maßnahmenplan
Wer die IT betreut , intern oder extern	Programme, Fernzugriff, Datensicherung, Zugänge. Ist die IT-Betreuung extern, genügt es, wenn sie für Rückfragen erreichbar ist.
Büro, Buchhaltung, Personal	Wege der Daten bei Auftrag, Rechnung, Lohn und Zeiterfassung
Werkstattleitung	Rundgang: Fotos, Aufträge, Schlüssel, Ausdrücke, Zutritt

4 · WAS SIE BEREITLEGEN KÖNNEN

Nichts davon ist Pflicht für den Termin. Was nicht da ist, wird im Maßnahmenplan festgehalten und gehört dann zu den ersten Schritten.

- ☐ Zahl der Beschäftigten: gesamt, Büro, Werkstatt
- ☐ Wer täglich am Rechner oder Tablet mit Kunden- oder Beschäftigendaten arbeitet
- ☐ Programme und Dienstleister: Werkstattsoftware, IT-Betreuung, Lohnbüro, Steuerberatung, Website, E-Mail und Cloud
- ☐ Verträge mit diesen Dienstleistern, soweit vorhanden

- ☐ Verzeichnis der Verarbeitungstätigkeiten, falls vorhanden
- ☐ Datenschutzhinweise: Website, Aushang, Beschäftigte, Bewerber
- ☐ Nachweise zu Unterweisung, Löschregeln und Notfallplan, falls vorhanden
- ☐ Anfragen, Fragebögen oder Klauseln von Kunden, Versicherern, Autohäusern oder Portalen
- ☐ Datum der letzten Rücksicherung; bei Kameras: Bereiche und Speicherdauer

Ein „unklar“ ist ein gültiger Eintrag. Im Fragebogen steht U für unklar oder ungeprüft. Es zählt nicht als erfüllt, bleibt aber auch kein Makel: Es zeigt, wo als Nächstes nachgesehen wird.

5 · WAS WIR NICHT AUFNEHMEN

- **Keine Kundennamen und keine Kennzeichen.** Wir arbeiten mit Rollen und Anzahlen, etwa „Werkstattleiter“ oder „zwei im Büro“.
- **Keine Kennwörter und keine Zugangsdaten.** Bitte zeigen Sie uns keine, und lassen Sie sich auch keine von uns geben.
- **Keine Gesundheitsdetails.** Bei Personal und Krankmeldungen interessiert nur, wer Zugriff hat und ob die Daten getrennt geschützt sind, nicht der Inhalt.

6 · SO LESEN SIE DEN FRAGEBOGEN

Status	Bedeutung
J	ja, erfüllt
N	nein, fehlt
U	unklar oder ungeprüft
E	entfällt, mit Begründung

Nachweis	Bedeutung
A	Auskunft
S	Sichtprüfung beim Rundgang
D	Dokument liegt vor

Priorität	Bedeutung
P1	unverzüglich, akutes Risiko
P2	zeitnah beheben
P3	planmäßig verbessern

Ein Dokument gilt nur dann als vorhanden, wenn sein Inhalt geeignet und aktuell ist. Gesetzliche oder vertragliche Fristen gehen bei den Prioritäten vor.

7 · WAS SIE DAVON HABEN

- **Ein klares Bild an einem Tag.** Wo steht der Betrieb, was läuft schon richtig, was ist offen.
- **Eine Liste mit nächsten Schritten.** Auf der letzten Seite des Bogens stehen Befund, Maßnahme, Priorität, Zuständigkeit und Termin, und die Sofortmaßnahmen werden am Termin gemeinsam vereinbart.
- **Antworten für Ihre Kunden.** Wenn ein Großkunde, ein Versicherer oder ein Portal nach Nachweisen zu IT-Sicherheit und Datenschutz fragt, haben Sie eine Grundlage, auf der Sie antworten können.
- **Ein Ausgangspunkt für die jährliche Wiederholung.** Ein ausgefüllter Bogen lässt sich im nächsten Jahr leicht fortschreiben.

8 · DIE WICHTIGSTEN BEGRIFFE IN EINEM SATZ

Begriff	Was gemeint ist
Verzeichnis der Verarbeitungstätigkeiten	Die Übersicht, welche Daten Sie wofür verarbeiten, wo sie liegen, wer Zugriff hat und wann sie gelöscht werden.
Technische und organisatorische Maßnahmen	Alles, womit Sie Daten schützen: eigene Zugänge, Updates, Sicherung, abschließbare Archive, vertrauliche Entsorgung.
Auftragsverarbeitung (AV-Vertrag)	Der Vertrag mit einem Dienstleister, der in Ihrem Auftrag Daten verarbeitet, etwa Werkstattsoftware im Hosting, IT-Betreuung mit Fernwartung oder das Lohnbüro.
Datenschutzbeauftragter	Pflicht, wenn in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§ 38 Abs. 1 Satz 1 BDSG). Unabhängig von der Zahl, wenn eine Datenschutz-Folgenabschätzung nötig ist.
Datenschutz-Folgenabschätzung	Eine Bewertung vorab, wenn eine Verarbeitung voraussichtlich ein hohes Risiko mit sich bringt. Bei Videoüberwachung ist zu prüfen, ob sie nötig ist.
Datenpanne	Daten gehen verloren, gelangen an Unbefugte oder werden verändert. Die Meldung an die Aufsicht erfolgt grundsätzlich unverzüglich und möglichst binnen 72 Stunden ab Bekanntwerden, sofern nicht voraussichtlich kein Risiko besteht.
NIS-2	EU-Regelung zur IT-Sicherheit. Direkt betroffen sind nur Einrichtungen bestimmter Arten und Größen (§ 28 BSIG). Fragen kommen oft trotzdem, weil Großkunden die Sicherheit ihrer Lieferanten nachweisen müssen (§ 30 Abs. 2 Satz 2 Nr. 4 BSIG). Ob das auf Ihren Betrieb zutrifft, klären wir im Abschnitt 10.

9 · VERTRAULICHKEIT UND GRENZEN

Der ausgefüllte Bogen enthält Betriebsinterna und wird vertraulich behandelt. Er dient der Auswertung dieses Termins. Der Check ist eine stichprobenbasierte Bestandsaufnahme: Er bestätigt keine vollständige Rechtskonformität, und was nicht geprüft wurde, wird im Bogen ausdrücklich so vermerkt.

Fragen vorab? Horos Consulting & Vermittlung GmbH · orthober@horos-consulting.de