

Datenschutz-Schnellcheck: 12 Punkte, die bei jeder Prüfung drankommen

Die Pflichtunterlagen der DSGVO – und woran es im Mittelstand meistens hakt.

Wenn die Aufsichtsbehörde schreibt, liegt der Fragebogen meistens innerhalb weniger Wochen auf dem Tisch. Wer die folgenden zwölf Punkte beisammen hat, kann gelassen antworten. Diese Liste ist nach Häufigkeit der Beanstandungen sortiert.

Die Pflichtunterlagen

- ☐ **Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO)**
Der mit Abstand häufigste Mangel. Muss aktuell sein, nicht nur vorhanden.
- ☐ **Auftragsverarbeitungsverträge mit allen Dienstleistern (Art. 28)**
Betrifft auch Lohnbüro, Cloud-Anbieter, IT-Dienstleister und Werbeagentur.
- ☐ **Technische und organisatorische Maßnahmen, schriftlich (Art. 32)**
Nicht abschreiben – die Maßnahmen müssen zu Ihrer tatsächlichen Technik passen.
- ☐ **Löschkonzept mit Fristen je Datenkategorie**
Aufbewahrungspflichten und Löschpflichten gegeneinander abgewogen und dokumentiert.
- ☐ **Datenschutzerklärung auf der Website, aktuell**
Muss zu den tatsächlich eingebundenen Diensten passen, inklusive Cookie-Einwilligung.
- ☐ **Benennung und Meldung des Datenschutzbeauftragten**
Pflicht ab 20 Personen, die ständig mit automatisierter Verarbeitung befasst sind. Die Meldung erfolgt einzeln bei der Aufsicht, nicht gesammelt.

Die Nachweise

- ☐ **Mitarbeiterschulung mit Teilnahmenachweis**
Einmal beim Eintritt reicht nicht. Jährlich ist die gängige Praxis.
- ☐ **Verpflichtung auf das Datengeheimnis**
Unterschrieben, abgelegt, bei neuen Beschäftigten Teil des Onboardings.
- ☐ **Prozess für Betroffenenanfragen**
Auskunft binnen eines Monats – wer übernimmt das, wenn die Anfrage am Freitag kommt?
- ☐ **Meldeweg für Datenpannen, 72-Stunden-Frist (Art. 33)**
Inklusive Telefonnummer, die auch abends jemand abnimmt.
- ☐ **Einwilligungen, wo erforderlich – widerrufbar und dokumentiert**
Besonders bei Newsletter, Fotos und Bewerberpools.
- ☐ **Datenschutz-Folgenabschätzung, wo nötig (Art. 35)**
Bei Videoüberwachung, Bewerbermanagement mit KI, umfangreichen Gesundheitsdaten.

Der Zusammenhang, den viele unterschätzen

Datenschutz und IT-Sicherheit lassen sich nicht trennen. Ein Löschkonzept ist wertlos, wenn das Backup die Daten weitere zehn Jahre vorhält. Genau deshalb schreiben bei uns CMD und BES Systemhaus solche Konzepte gemeinsam – eines beschreibt, das andere baut.