

Checkliste: Datenschutz beim Ticketsystem

Die Liste ersetzt keine Rechtsberatung und keinen Datenschutzbeauftragten. Sie ersetzt das ungute Gefühl beim Lesen von Anbieter-Websites durch achtzehn konkrete Fragen. Zu jeder steht, woran man die Antwort erkennt. Die Punkte zur Auftragsverarbeitung folgen Art. 28 Abs. 3 DSGVO, der vorschreibt, was ein solcher Vertrag enthalten muss.

Wo die Daten liegen

☐ **Serverstandort benannt**

Der Anbieter nennt Land und möglichst Rechenzentrum. „Cloud“ ist kein Ort. Erkennbar: Datenschutzerklärung, Sicherheitsseite, AVV-Anlage.

☐ **Anhänge und Sicherungen am selben Ort**

Oft liegen Dateien und Backups bei einem anderen Dienst als die Datenbank. Nachfragen, wo genau.

☐ **Kein Drittlandtransfer ohne Grundlage**

Liegen Daten außerhalb der EU, braucht es Standardvertragsklauseln oder einen Angemessenheitsbeschluss – und eine Bewertung, ob das reicht.

☐ **Anbieter selbst in der EU oder mit EU-Vertreter**

Ein Hersteller außerhalb der EU muss nach Art. 27 DSGVO einen Vertreter benennen. Steht im Impressum oder in der Datenschutzerklärung.

Der Auftragsverarbeitungsvertrag (Art. 28 DSGVO)

☐ **AVV wird angeboten, ohne Verhandlung**

Zum Herunterladen oder per Klick abschließbar. Wer erst nach einem AVV fragen muss, sollte hellhörig werden.

☐ **Gegenstand, Dauer, Art und Zweck beschrieben**

Was verarbeitet wird, wie lange, wozu. Pflichtinhalt nach Art. 28 Abs. 3.

- ☐ **Verarbeitung nur auf Weisung**
Der Anbieter verarbeitet nur, was du ihm aufträgst – und nicht für eigene Zwecke, etwa zum Training von Modellen.

- ☐ **Vertraulichkeit der Beschäftigten**
Mitarbeitende des Anbieters sind zur Vertraulichkeit verpflichtet. Ein Satz, der im Vertrag stehen muss.

- ☐ **Technische und organisatorische Maßnahmen beschrieben**
Verschlüsselung, Zugriffsschutz, Protokollierung, Sicherungen. Als Anlage zum AVV, konkret, nicht als Werbetext.

- ☐ **Unterauftragnehmer aufgelistet**
Hosting, E-Mail-Versand, KI-Dienst, Support-Tool. Jeder einzeln, mit Sitz. Änderungen müssen angekündigt werden und ein Widerspruchsrecht haben.

- ☐ **Unterstützung bei Betroffenenrechten**
Auskunft, Berichtigung, Löschung: Der Anbieter muss helfen, wenn eine betroffene Person ihre Rechte ausübt.

- ☐ **Meldung von Datenschutzverletzungen**
Unverzüglich, mit Frist. Du hast selbst 72 Stunden zur Meldung an die Aufsichtsbehörde – der Anbieter darf davon nicht die Hälfte verbrauchen.

- ☐ **Löschung oder Rückgabe bei Vertragsende**
Alle Daten, inklusive Sicherungen, nach einer benannten Frist. Und ein Export vorher, in einem lesbaren Format.

- ☐ **Nachweise und Prüfrecht**
Der Anbieter legt Nachweise vor (Zertifikate, Berichte) und lässt Prüfungen zu. Ohne das ist jede Zusage ungeprüft.

Im laufenden Betrieb

- ☐ **KI-Funktionen: wohin gehen die Inhalte?**
Wird Ticketinhalt an einen externen KI-Dienst geschickt? In welches Land? Wird er zum Training verwendet? Das gehört in die Liste der Unterauftragnehmer – oder die KI läuft beim Anbieter selbst.

- ☐ **Löschkonzept vorhanden**
Vorgänge, Kontakte und Anhänge lassen sich nach Frist löschen – restlos, nicht nur „archiviert“. Manuell und möglichst automatisch.



Zugriff nach Rolle und Bereich

Nicht jede Person sieht alles. Teams oder Bereiche mit getrennter Sicht, Zwei-Faktor-Anmeldung, Protokoll der Zugriffe.



Kundenportal und Formulare geprüft

Wo Kundinnen selbst Daten eingeben: Verschlüsselte Übertragung, Datenschutzhinweis am Formular, keine unnötigen Pflichtfelder.
