

DSGVO-Checkliste für KI-Tools im KMU

Sieben Prüfpunkte von Serverstandort bis Löschfristen – in ca. 60 Minuten pro Tool durchgehen

Hinweis: Diese Checkliste ist eine allgemeine Orientierung und keine Rechtsberatung. Sie hilft, die richtigen Fragen an Anbieter zu stellen – sie ersetzt weder die Prüfung des konkreten Vertrags noch fachkundigen Rat im Zweifelsfall.

Die 9-Punkte-Checkliste

- 1 **Serverstandort und Rechenzentrum dokumentiert** – Firmensitz und tatsächlicher Verarbeitungsort getrennt notieren, beide können abweichen.
- 2 **Firmensitz des Anbieters geprüft** – steht meist in der Datenschutzerklärung unter "Datenverarbeitung" oder "Hosting".
- 3 **AVV angefragt und unterschrieben vorliegend** – Tool erst produktiv nutzen, wenn der AVV unterschrieben zurück ist.
- 4 **Drittlandtransfer eingeordnet (ja/nein)** – auch Support-/Wartungszugriffe aus Drittländern zählen, nicht nur der Rechenzentrumsstandort.
- 5 **Cloud-Act-Risiko bei US-Anbietern geprüft** – auch bei EU-Serverstandort möglich, wenn der Mutterkonzern US-amerikanisch ist.
- 6 **Rechtsgrundlage (SCCs oder DPF) dokumentiert** – SCCs und DPF sind nicht austauschbar, nur eine davon ist vertraglich vereinbart.
- 7 **KI-Training-Opt-out für alle Teamzugänge aktiviert** – nicht nur für den eigenen Account, auch für weitere Teammitglieder mit eigenem Zugang.
- 8 **TOMs des Anbieters eingesehen und bewertet** – konkrete Maßnahmen (Verschlüsselung, Zugriffskontrollen) einfordern, nicht mit "wir nehmen Datenschutz ernst" zufriedengeben.
- 9 **Löschfristen geklärt und Datenminimierung umgesetzt** – nicht stillschweigend auf Standardeinstellungen verlassen, nur wirklich nötige Daten eingeben.

Häufigste Fehler

- 10 Serverstandort nur anhand des Firmensitzes einschätzen statt anhand des tatsächlichen Rechenzentrums.
- 11 Tool produktiv nutzen, bevor der AVV unterschrieben zurück ist.
- 12 Sich mit pauschalen Sicherheitsversprechen statt konkreten TOM-Angaben zufriedengeben.