DSGVO-konforme KI-Tools gibt es nicht

Es kommt immer auf den konkreten Einsatz an

Die datenschutzrechtliche Bewertung hängt am Anwendungsfall, nicht am Tool. Rechtsanwalt Stefan Humer: Die DSGVO ist **technologieneutral** und gilt für KI genauso wie für andere automatisierte Datenverarbeitungen. Es geht um Kontrollverlust über eingegebene Daten.

DREI PRÜFPUNKTE, AUS DENEN SICH ALLES ERGIBT

WELCHE DATEN?
Sollen personenbezogene oder sensible Daten verarbeitet werden?

WAS PASSIERT DAMIT?
Werden sie gespeichert, weitergegeben, zum Training genutzt?

WELCHER SCHUTZ?
Einstellungen, vertragliche Absicherung, technische Maßnahmen.

Schon die Eingabe personenbezogener Daten ist eine Datenverarbeitung im Sinn der DSGVO, unabhängig davon, ob der Anbieter sie speichert.

WAS WERBEVERSPRECHEN NICHT LEISTEN

„DSGVO-konform“, „EU-gehostet“, „Made in Germany“.
Ein Anbieter kann technische und organisatorische Maßnahmen setzen, nimmt dem nutzenden Unternehmen die datenschutzrechtliche Verantwortung aber nicht ab.

„US-Tools sind automatisch verboten.“
Maßgeblich ist, ob und unter welchen Voraussetzungen Daten in Drittländer gehen. Werden sie ausschließlich in Europa verarbeitet, entfallen die zusätzlichen Prüfpflichten zum Drittstaatentransfer.

„Ein Toolwechsel löst das Problem.“
Das Risiko wandert nur zum nächsten Anbieter, solange das Unternehmen nicht selbst definiert, wofür und in welchem Rahmen ein Tool eingesetzt werden darf.

ANWENDUNGSFÄLLE

- **Marketing, allgemein.** Ideensammlung und Texterstellung sind meist unbedenklich.
- **Marketing mit echten Daten.** Kundendaten, Kampagneninfos, Geschäftsgeheimnisse: heikel.
- **Kundenservice.** Namen, Mailadressen, Bestellnummern, Vertragsdaten brauchen Rechtfertigungsgrund und saubere Ausgestaltung. Ausgeschlossen ist es aber nicht.
- **Lokal gehostete Modelle.** Entschärfen bestimmte Themen, sind aber auch eine strategische Ressourcenfrage.

WAS KMU KONKRET TUN

1. **Kein Komplettverbot.** Sonst weichen Mitarbeiter auf private Tools aus, Shadow AI, und das Unternehmen haftet in aller Regel dennoch.
2. **Genaue interne Vorgaben.** Welches Tool für welchen Anwendungsfall auf welche Art.
3. Guardrails setzen.
4. **Regelmäßig überprüfen.** Auch technisch abgesichert, als Teil einer KI-Governance.

DIE PRÜFFRAGEN VOR DEM EINSATZ

1. Personenbezogene oder sensible Daten im Spiel?
2. Liegt eine Rechtsgrundlage vor?
3. Wo wird verarbeitet und gespeichert?
4. Wie wird der Einsatz transparent gemacht?
5. Werden Eingaben zum Training verwendet?

1. Braucht es einen Auftragsverarbeitervertrag?
2. Welche Subdienstleister sind eingebunden?
3. Können Daten gelöscht werden?
4. Protokollierung und Zugriffskontrollen vorhanden?
5. Passt das Tool zum konkreten Anwendungsfall?

MERKSÄTZE

Werden KI-Tools mit E-Mail oder CRM verbunden, drohen bei großem Zugriff Bußgelder, Schadenersatz und der Verlust des Geschäftsgeheimnisschutzes. Agentische KI verschärft das.

Wichtiger als der Wechsel des Tools sind klare interne Richtlinien, wer welches Tool wofür einsetzen darf.