CHECKLISTE · MAI 2026

DSGVO und KI

Praxis-Checkliste für rechtssicheren KI-Einsatz.
Mit Mustertexten und Verarbeitungsverzeichnis.

Einleitung

KI verarbeitet Daten. Sobald diese Daten Personen zuzuordnen sind, gilt die DSGVO in vollem Umfang. Anders als oft behauptet ist das kein Hindernis für KI-Einsatz, sondern ein klarer Rahmen, der für alle gleich gilt.

Diese Checkliste fasst die wichtigsten Pflichten zusammen und liefert Mustertexte für die häufigsten Fälle. Sie richtet sich an Datenschutzbeauftragte, IT-Verantwortliche und Geschäftsführungen, die KI rechtssicher einführen wollen.

> **Hinweis:** Diese Checkliste ist eine Praxishilfe, kein Ersatz für eine individuelle Datenschutz-Folgenabschätzung. Im Zweifel den eigenen Datenschutzbeauftragten oder einen Rechtsanwalt einschalten.

1. Sieben Prüffragen vor jedem KI-Einsatz

Frage 1 · Werden personenbezogene Daten verarbeitet?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierbare Person beziehen. Name, Adresse, IP-Adresse, Inhalte einer Bürgermail, eines Bewerbungsschreibens, eines Beschwerdebriefs. Wenn Sie diese Frage mit Ja beantworten, gilt die DSGVO.

Frage 2 · Welche Rechtsgrundlage?

Jede Verarbeitung braucht eine Rechtsgrundlage nach Art. 6 DSGVO. In der Verwaltung typisch: gesetzliche Aufgabe (lit. e). In Unternehmen typisch: Vertrag (lit. b) oder berechtigtes Interesse (lit. f). Bei besonderen Kategorien wie Gesundheitsdaten gelten zusätzliche Schranken nach Art. 9 DSGVO.

Frage 3 · Wo werden die Daten verarbeitet?

Die Verarbeitung in EU oder EWR ist unproblematisch. Verarbeitung außerhalb erfordert Angemessenheitsbeschluss oder Standardvertragsklauseln. US-Anbieter sind nach Schrems II problematisch, auch wenn das EU-US Data Privacy Framework wieder Erleichterung gebracht hat. Sicherer: EU-Anbieter wählen.

Frage 4 · Liegt ein Auftragsverarbeitungsvertrag vor?

Sobald ein externer Dienstleister Daten verarbeitet, braucht es einen AVV nach Art. 28 DSGVO. Die meisten KI-Anbieter bieten standardisierte AVV an, oft auf der Website verlinkt. Vor Vertragsschluss prüfen, ob alle Pflichtbestandteile enthalten sind.

Frage 5 · Werden Daten zum Modelltraining genutzt?

Bei kostenlosen Diensten oft Ja, bei Business-Lizenzen oft Nein. Vertraglich sicherstellen: Eingaben dürfen nicht für das Training fremder Modelle verwendet werden. Sonst landen Bürger- oder Kundendaten potenziell in Modellen, die von Dritten genutzt werden.

Frage 6 · Welche Speicherdauer?

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für den Zweck erforderlich ist. Bei KI-Anbietern oft Standard: 30 Tage Logs, dann automatische Löschung. Vertraglich prüfen, individuell anpassen falls nötig.

Frage 7 · Sind Betroffene informiert?

Datenschutzhinweise auf Website und in Formularen müssen den KI-Einsatz nennen. Bei automatisierten Entscheidungen mit Rechtswirkung gilt zusätzlich Art. 22 DSGVO: klare Information, Recht auf menschliche Überprüfung, Anspruch auf Erklärung.

2. Die häufigsten Stolperfallen

Sensible Daten in der Cloud-KI

Beispiel: Die Personalabteilung nutzt einen KI-Dienst zur Vorqualifikation von Bewerbungen. Bewerbungsunterlagen enthalten oft Gesundheitsdaten, Religionszugehörigkeit, Familienstand. Hier reicht die normale Rechtsgrundlage nicht aus, es greift Art. 9 DSGVO. Lösung: Anonymisierung vor der Verarbeitung oder explizite Einwilligung.

Schatten-IT

Mitarbeitende kopieren Inhalte aus internen Systemen in die kostenlose Variante eines bekannten Chatbots. Damit landen Daten potenziell auf Servern in den USA, ohne AVV, mit Trainingseinschluss. Klare Regelung: nur freigegebene KI-Tools verwenden, das Verbot in der IT-Richtlinie verankern, regelmäßig schulen.

Bewerber-KI ohne Information

Wenn Bewerbungen durch KI vorgefiltert werden, muss das im Bewerbungsprozess transparent sein. Nicht: erst nach der Absage erwähnen. Datenschutzhinweis im Bewerbungsformular, Hinweis auf das Recht auf menschliche Überprüfung.

3. Mustertexte für Datenschutzhinweise

Allgemeiner Hinweis auf KI-Einsatz

> *„Wir setzen KI-gestützte Systeme ein, um [Zweck einsetzen]. Dabei werden Ihre personenbezogenen Daten [welche Kategorien] auf Servern innerhalb der EU verarbeitet. Anbieter ist [Anbieter], mit dem ein Vertrag zur Auftragsverarbeitung besteht. Eine Nutzung Ihrer Daten zum Training der Modelle findet nicht statt."*

Hinweis auf automatisierte Entscheidung (Art. 22 DSGVO)

> *„Im Rahmen [des Verfahrens] kann eine automatisierte Entscheidung einschließlich Profiling erfolgen. Sie haben das Recht, eine ausschließlich menschliche Überprüfung dieser Entscheidung zu verlangen, Ihren Standpunkt darzulegen und die Entscheidung anzufechten. Wenden Sie sich dazu an [Kontakt]."*

Hinweis auf KI-generierte Inhalte (Transparenzpflicht)

> *„Dieser Inhalt wurde mit Unterstützung Künstlicher Intelligenz erstellt. Inhaltliche Verantwortung trägt [verantwortliche Person oder Stelle]."*

4. Verarbeitungsverzeichnis: Was muss rein?

Ein KI-System ist eine Verarbeitungstätigkeit nach Art. 30 DSGVO und gehört damit ins Verarbeitungsverzeichnis. Die folgenden Punkte sind Pflicht.

- **Bezeichnung der Verarbeitung:** Eindeutiger Name (zum Beispiel „KI-gestützte Bürgeranfragen-Klassifikation").
- **Verantwortlicher:** Wer trägt die Verantwortung im Sinne der DSGVO?
- **Zweck der Verarbeitung:** Wozu dient die Verarbeitung konkret?
- **Kategorien betroffener Personen:** Bürger, Kunden, Mitarbeiter, Bewerber.
- **Kategorien personenbezogener Daten:** Name, Adresse, Mailinhalt, IP, etc.
- **Empfänger:** Welche Anbieter erhalten die Daten?
- **Drittlandtransfer:** Findet ein solcher statt? Wenn ja, mit welcher Grundlage?
- **Löschfristen:** Nach wie vielen Tagen werden Daten gelöscht?
- **Technische und organisatorische Maßnahmen:** Verschlüsselung, Zugriffsbeschränkung, Protokollierung, AVV.

5. Datenschutz-Folgenabschätzung: Wann nötig?

Eine Datenschutz-Folgenabschätzung (DSFA) ist nach Art. 35 DSGVO immer dann Pflicht, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen bewirkt. Das gilt bei KI fast immer, wenn folgende Faktoren zusammenkommen.

- Verarbeitung großer Datenmengen.
- Verwendung neuer Technologien.
- Profiling oder automatisierte Entscheidung.
- Bewertung persönlicher Aspekte (Bewerbung, Bonität, Gesundheit).
- Systematische Überwachung öffentlich zugänglicher Bereiche.

In der Praxis: Bei den meisten produktiven KI-Anwendungen mit personenbezogenen Daten ist eine DSFA sinnvoll, auch wenn sie nicht zwingend ist. Sie schafft Klarheit und ist bei Beanstandungen ein wichtiger Nachweis.

Kernbotschaft.

DSGVO und KI sind keine Gegensätze. Mit klaren Prozessen, sauberen Verträgen und vorgedachten Mustertexten ist datenschutzkonformer KI-Einsatz Routine. Wer beim ersten Projekt sauber arbeitet, hat das Fundament für alle weiteren.

Über den Autor

Thomas Peter Finger ist KI-Stratege aus Grevesmühlen. Er berät Politik, Verwaltung und Mittelstand bei der praktischen Einführung von KI. Hauptberuflich Referent für Kommunikation im Wahlkreisbüro einer Bundestagsabgeordneten, ehrenamtlich engagiert in CDU und kommunaler Selbstverwaltung.

Kontakt: kontakt@thomas-finger.com · +49 174 949 64 32 · thomas-finger.com