DSGVO-Checkliste für KI-Projekte

Diese Checkliste unterstützt Sie dabei, Ihr KI-Projekt datenschutzkonform umzusetzen. Die Datenschutz-Grundverordnung (DSGVO) ist kein Hindernis, sondern ein Qualitätsmerkmal für verantwortungsvolle KI-Nutzung. Mit diesen fünf Punkten stellen Sie sicher, dass Ihr Projekt rechtssicher und transparent ist.

Die 5 DSGVO-Punkte zum Abhaken

☐ 1. EU-Server prüfen

Was ist zu tun?

Klären Sie, wo die Daten Ihres KI-Tools gespeichert und verarbeitet werden. Idealerweise sollten die Server innerhalb der Europäischen Union oder in Ländern mit einem Angemessenheitsbeschluss der EU-Kommission stehen.

Warum ist das wichtig?

Die DSGVO schreibt vor, dass personenbezogene Daten nur in Regionen mit angemessenem Datenschutzniveau übermittelt werden dürfen. Server außerhalb der EU können zusätzliche rechtliche Anforderungen mit sich bringen.

Praxis-Tipp:

Fragen Sie Ihren KI-Anbieter explizit nach dem Standort der Rechenzentren. Achten Sie auf Zertifizierungen wie ISO 27001 oder SOC 2, die zusätzliche Sicherheit bieten.

☐ 2. Auftragsverarbeitungsvertrag (AVV/DPA) abschließen

Was ist zu tun?

Schließen Sie mit Ihrem KI-Anbieter einen Auftragsverarbeitungsvertrag (AVV) ab, auch bekannt als Data Processing Agreement (DPA). Dieser Vertrag regelt, wie der Anbieter mit Ihren Daten umgeht.

Warum ist das wichtig?

Laut Art. 28 DSGVO sind Sie als Unternehmen verpflichtet, mit jedem Dienstleister, der personenbezogene Daten in Ihrem Auftrag verarbeitet, einen AVV abzuschließen. Ohne AVV drohen Bußgelder.

Praxis-Tipp:

Die meisten seriösen KI-Anbieter stellen standardisierte AVV-Vorlagen bereit. Prüfen Sie, ob der Vertrag die wesentlichen Punkte abdeckt: Zweck der Verarbeitung, Art der Daten, Löschfristen, Unterauftragnehmer.

☐ 3. Transparenz gewährleisten

Was ist zu tun?

Informieren Sie Ihre Mitarbeiter, Kunden oder andere betroffene Personen darüber, dass und wie Sie KI-Tools einsetzen. Dies kann über Ihre Datenschutzerklärung, interne Richtlinien oder direkte Kommunikation erfolgen.

Warum ist das wichtig?

Die DSGVO verlangt Transparenz über die Verarbeitung personenbezogener Daten. Betroffene Personen haben das Recht zu erfahren, welche Daten zu welchem Zweck verarbeitet werden.

Praxis-Tipp:

Erstellen Sie eine kurze, verständliche Information über den KI-Einsatz. Beispiel: "Wir nutzen ein KI-gestütztes Tool zur Bearbeitung von Kundenanfragen. Ihre Daten werden ausschließlich zur Beantwortung Ihrer Anfrage verwendet und nicht an Dritte weitergegeben."

☐ 4. Datenarten klassifizieren

Was ist zu tun?

Unterscheiden Sie zwischen verschiedenen Datenarten und passen Sie Ihre Schutzmaßnahmen entsprechend an. Besonders sensible Daten (z.B. Gesundheitsdaten, biometrische Daten) erfordern strengere Sicherheitsvorkehrungen.

Warum ist das wichtig?

Nicht alle Daten sind gleich schützenswert. Die DSGVO unterscheidet zwischen "normalen" personenbezogenen Daten und "besonderen Kategorien" (Art. 9 DSGVO), die einem erhöhten Schutz unterliegen.

Praxis-Tipp:

Erstellen Sie eine einfache Tabelle mit den Datenarten, die Ihr KI-Tool verarbeitet:

Datenart	Beispiel	Schutzniveau	Maßnahmen
Kontaktdaten	Name, E-Mail	Normal	AVV, EU-Server
Vertragsdaten	Rechnungen, Bestellungen	Normal	AVV, EU-Server
Gesundheitsdaten	Diagnosen, Befunde	Besonders sensibel	AVV, EU-Server, Verschlüsselung, Einwilligung

☐ 5. Datenschutzbeauftragten (DSB) einbinden

Was ist zu tun?

Informieren Sie Ihren Datenschutzbeauftragten (falls vorhanden) über das geplante KI-Projekt. Lassen Sie prüfen, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist.

Warum ist das wichtig?

Der Datenschutzbeauftragte ist Ihr interner Experte für DSGVO-Fragen. Bei risikoreichen Verarbeitungen (z.B. automatisierte Entscheidungen, umfangreiche Datenverarbeitung) ist eine DSFA gesetzlich vorgeschrieben.

Praxis-Tipp:

Auch wenn Sie keinen eigenen DSB haben, können Sie externe Datenschutzexperten oder spezialisierte Anwälte konsultieren. Viele IHKs und Wirtschaftsverbände bieten kostengünstige Beratung an.

Mini-Glossar: Die wichtigsten DSGVO-Begriffe

Auftragsverarbeitungsvertrag (AVV) / Data Processing Agreement (DPA)

Ein Vertrag zwischen Ihnen (als Auftraggeber) und einem Dienstleister (als Auftragsverarbeiter), der regelt, wie der Dienstleister mit Ihren Daten umgeht. Der AVV ist nach Art. 28 DSGVO verpflichtend, wenn ein Dienstleister personenbezogene Daten in Ihrem Auftrag verarbeitet.

Beispiel: Sie nutzen ein KI-Tool zur Analyse von Kundenfeedback. Der Anbieter des Tools ist Auftragsverarbeiter und muss mit Ihnen einen AVV abschließen.

EU-Server

Server, die physisch in einem Mitgliedsstaat der Europäischen Union oder in einem Land mit Angemessenheitsbeschluss stehen. Die DSGVO bevorzugt die Verarbeitung personenbezogener Daten innerhalb der EU, um ein hohes Datenschutzniveau zu gewährleisten.

Beispiel: Ein KI-Anbieter betreibt seine Rechenzentren in Frankfurt am Main (Deutschland) – das sind EU-Server.

Einwilligung

Eine freiwillige, informierte und eindeutige Zustimmung der betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten. Die Einwilligung muss jederzeit widerrufbar sein.

Beispiel: Ein Kunde willigt ein, dass seine E-Mail-Adresse für personalisierte KI-gestützte Produktempfehlungen genutzt wird.

Datenschutz-Folgenabschätzung (DSFA)

Eine systematische Bewertung der Risiken, die eine Datenverarbeitung für die Rechte und Freiheiten betroffener Personen mit sich bringt. Eine DSFA ist erforderlich, wenn die Verarbeitung voraussichtlich ein hohes Risiko birgt (z.B. bei automatisierten Entscheidungen mit rechtlicher Wirkung).

> *Beispiel:* Ein KI-System zur automatischen Kreditwürdigkeitsprüfung erfordert eine DSFA, da es weitreichende Auswirkungen auf die betroffenen Personen hat.

> **Datenschutzbeauftragter (DSB)**
>
> Eine Person, die in Ihrem Unternehmen für die Überwachung der Einhaltung der DSGVO zuständig ist. Ein DSB ist verpflichtend, wenn Sie regelmäßig und systematisch personenbezogene Daten in großem Umfang verarbeiten oder besondere Kategorien von Daten verarbeiten.
>
> *Beispiel:* Ein Unternehmen mit 250 Mitarbeitern, das umfangreiche Kundendaten verarbeitet, muss einen DSB bestellen.

Hinweise zur Dokumentation

Die DSGVO verlangt nicht nur die Einhaltung der Datenschutzvorschriften, sondern auch deren **Nachweisbarkeit**. Dokumentieren Sie daher alle relevanten Schritte Ihres KI-Projekts.

Was sollten Sie dokumentieren?

Verzeichnis von Verarbeitungstätigkeiten (VVT): Führen Sie ein Verzeichnis, in dem Sie alle Datenverarbeitungen Ihres Unternehmens auflisten. Für Ihr KI-Projekt sollten folgende Informationen enthalten sein:

- Zweck der Verarbeitung (z.B. "Automatisierte Beantwortung von Kundenanfragen")
- Kategorien betroffener Personen (z.B. "Kunden, Interessenten")
- Kategorien personenbezogener Daten (z.B. "Name, E-Mail-Adresse, Anfrageinhalte")
- Empfänger der Daten (z.B. "KI-Anbieter XY")
- Übermittlung in Drittländer (falls zutreffend)
- Löschfristen (z.B. "Daten werden nach 12 Monaten gelöscht")

Auftragsverarbeitungsvertrag (AVV): Bewahren Sie eine Kopie des unterzeichneten AVV mit Ihrem KI-Anbieter auf. Prüfen Sie regelmäßig, ob der Vertrag noch aktuell ist (z.B. bei Änderungen des Leistungsumfangs).

Datenschutz-Folgenabschätzung (DSFA): Falls erforderlich, dokumentieren Sie die Durchführung und Ergebnisse der DSFA. Halten Sie fest, welche Risiken identifiziert wurden und welche Maßnahmen zur Risikominimierung ergriffen wurden.

Einwilligungen: Wenn Sie Einwilligungen von betroffenen Personen einholen, dokumentieren Sie, wann, wie und wofür die Einwilligung erteilt wurde. Stellen Sie sicher, dass die Einwilligung jederzeit widerrufbar ist.

Schulungen und Sensibilisierung: Dokumentieren Sie, welche Mitarbeiter im Umgang mit dem KI-Tool geschult wurden und welche Datenschutzrichtlinien kommuniziert wurden.

Wie lange sollten Sie Dokumente aufbewahren?

Die DSGVO schreibt keine konkreten Aufbewahrungsfristen vor, aber es gilt: Solange die Datenverarbeitung stattfindet, müssen die Nachweise verfügbar sein. Nach Beendigung der Verarbeitung sollten Sie die Dokumente mindestens drei Jahre aufbewahren, um im Falle einer Prüfung durch die Aufsichtsbehörde Rechenschaft ablegen zu können.

Wo sollten Sie Dokumente aufbewahren?

Bewahren Sie alle DSGVO-relevanten Dokumente an einem zentralen, sicheren Ort auf – idealerweise digital und verschlüsselt. Stellen Sie sicher, dass nur autorisierte Personen (z.B. Geschäftsführung, Datenschutzbeauftragter) Zugriff haben.

Checkliste: Haben Sie alles erledigt?

Nutzen Sie diese Übersicht, um Ihren Fortschritt zu überprüfen:

Nr.	DSGVO-Punkt	Erledigt?	Notizen
1	EU-Server geprüft	☐	Serverstandort: _____
2	AVV/DPA abgeschlossen	☐	Datum: _____
3	Transparenz gewährleistet	☐	Kommunikation erfolgt über: _____
4	Datenarten klassifiziert	☐	Besonders sensible Daten: Ja ☐ / Nein ☐
5	DSB eingebunden	☐	Name DSB: _____

Weiterführende Ressourcen

Offizielle Quellen:

- **Europäische Datenschutz-Grundverordnung (DSGVO):** https://eur-lex.europa.eu/eli/reg/2016/679/oj
- **Bayerisches Landesamt für Datenschutzaufsicht (BayLDA):** https://www.lda.bayern.de
- **Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI):** https://www.bfdi.bund.de

Praxishilfen:

- **IHK-Leitfaden zur DSGVO:** Viele Industrie- und Handelskammern bieten kostenlose Leitfäden und Mustervorlagen an.
- **Datenschutzkonferenz (DSK):** Die DSK veröffentlicht regelmäßig Orientierungshilfen zu aktuellen Datenschutzthemen.

Kontakt und Unterstützung

BDS KI-Akademie Bayern
E-Mail: akademie@bds-bayern.de | Website: https://bds-akademie-bayern.de

DSGVO ist kein Hindernis – sondern ein Qualitätsmerkmal für verantwortungsvolle KI-Nutzung.

Herausgeber: Bund der Selbständigen Bayern e.V. | BDS KI-Akademie Bayern

Stand: November 2025