

## 1. Zweckprüfung und Risikoeinstufung

Klären, zu welchem Zweck personenbezogene Daten verarbeitet bzw. das KI-Tool eingesetzt wird.

---

Prüfen, ob dieser Zweck datenschutzrechtlich (DSGVO) und nach der KI-Verordnung (KI-VO) jeweils zulässig ist.

## 2. Dokumentation und KI-Klassifizierung

Klassifizierung und Dokumentation des KI-Tools nach der KI-VO (z. B. verbotenes System, Hochrisiko-System).

---

Dokumentation nach der DSGVO (insb. Art. 30, 32 DSGVO).

## 3. Vertragliche Absicherung

Überprüfung des Auftragsvertrags gemäß Art. 28 DSGVO. Sicherstellung der Zweckgebundenheit der Verarbeitung durch den Dienstleister, insb. in Bezug auf eine Nutzung von Daten zum KI-Training.

---

Überprüfung der Lizenz- und urheberrechtlichen Regelungen (i.d.R. im Dienstleistungsvertrag/ Service-Level-Agreement) zum Schutz des geistigen Eigentums und der Geschäftsgeheimnisse.

## 4. Transparenz wahren

Mitarbeitende und Betroffene informieren, wann und wie KI-Tools eingesetzt werden und welche personenbezogenen Daten betroffen sind (gemäß Art. 13 DSGVO und Art. 50 KI-VO).

## 5. Schulung und Richtlinien

Interne Richtlinien zur Nutzung von KI-Tools festlegen bzw. (regelmäßig) updaten.

---

Mitarbeitende regelmäßig zum Datenschutz (Art. 32 DSGVO) und dem verantwortungsvollen Umgang mit KI-Tools (Art. 4 KI-VO) schulen.

## 6. Überwachung und regelmäßige Evaluation

Regelmäßige Evaluation des rechtmäßigen Einsatzes von KI-Tools und Sicherstellung der Einhaltung der DSGVO.

---

Aktive Überwachung bei Hochrisiko-Systemen durch Risk-Management nach KI-VO sicherstellen.