Arbeitshilfe 2: Checkliste für Datenschutzverantwortliche – KI-Systeme einführen

Prüfpunkt	✔
Schritt 1: Einsatzbereich und Datenarten definieren	
Welche KI-Systeme werden genutzt (externe Anbieter/eigene Modelle)?	◯
Wurden der Hersteller und das Tool auf Datenschutz und Risiken geprüft?	◯
Werden personenbezogene Daten verarbeitet – und wenn ja, in welchem Umfang (z. B. Kundendaten, Beschäftigtendaten)?	◯
Schritt 2: Rechtsgrundlage und Zweckbindung klären	
Liegt eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch oder mit KI vor (z. B. Vertragserfüllung, berechtigtes Interesse)?	◯
Ist der Einsatz der KI auf den definierten Zweck beschränkt?	◯
Schritt 3: Datenminimierung und Vorverarbeitung umsetzen	
Werden Daten vor der Nutzung bereinigt, pseudonymisiert oder anonymisiert?	◯
Werden überflüssige oder doppelte Datensätze vor dem Training/der Nutzung entfernt?	◯
Schritt 4: Rollen und Verantwortlichkeiten dokumentieren	
Ist klar geregelt, ob der KI-Anbieter als Auftragsverarbeiter oder eigener Verantwortlicher handelt?	◯
Sind entsprechende Verträge (AVV) oder Vereinbarungen geschlossen?	◯
Schritt 5: Technische und organisatorische Schutzmaßnahmen prüfen	
Gibt es Schutzmechanismen gegen Memorisation und ungewollte Datenausgaben (z. B. Filter, Prompt-/Output-Restriktionen)?	◯
Werden Zugriffe protokolliert und überwacht (Audit Logging)?	◯
Zugriff auf KI-Systeme ist durch Zwei-Faktor-Authentifizierung abgesichert.	◯
Sicherheitskopien von Modellen, Einstellungen und Trainingsdaten sind vorhanden.	◯
KI-Ausgaben werden stichprobenartig überprüft (technisch oder durch Personen).	◯
Schritt 6: Vorbereitung auf Sicherheitsvorfälle	
Ist geprüft, wie bei Sicherheitsvorfällen mit dem KI-System reagiert wird (Notfallplan, Abschaltung möglich)?	◯
Ist dokumentiert, wo Daten gespeichert werden (in Deutschland, EU oder außerhalb)?	◯
Schritt 7: Umgang mit Betroffenenrechten definieren	
Ist dokumentiert, wie Auskunfts-, Lösch- oder Berichtigungsanfragen im Kontext von KI behandelt werden?	◯
Können Ausgaben unterdrückt oder Daten für zukünftige Trainings ausgeschlossen werden, wenn erforderlich?	◯

Arbeitshilfe 2: Checkliste für Datenschutzverantwortliche – KI-Systeme einführen	
Schritt 8: Transparenz- und Informationspflichten erfüllen	
Werden Mitarbeiter geschult (welche Daten erlaubt sind, wie Ergebnisse zu prüfen sind)?	◯
Werden Kunden oder Betroffene informiert, falls KI in Kommunikations- oder Entscheidungsprozessen eingesetzt wird?	◯
Schritt 9: Testphase und Grenzen des Systems	
KI-System wurde vor dem Einsatz getestet (Probephase mit definierten Erfolgskriterien).	◯
Typische Fehler des KI-Systems sind bekannt (z. B. falsche/erfundene Antworten).	◯
Es gibt Prozesse zur fachlichen Prüfung von KI-Ergebnissen vor Verwendung.	◯
Schritt 10: Governance und kontinuierliche Überwachung etablieren	
Gibt es einen klar definierten KI-Prozess im Datenschutzmanagement (z. B. als Bestandteil der TOMs oder DSFA)?	◯
Werden neue Risiken regelmäßig bewertet (z. B. durch technische Weiterentwicklung oder geänderte Nutzung)?	◯
Schritt 11: Richtlinien und Schulung	
Ist eine KI-Nutzungsrichtlinie erstellt, die festlegt, was erlaubt und was verboten ist?	◯
Wurden alle Mitarbeiter zum sicheren Umgang mit KI-Systemen geschult?	◯
Werden regelmäßige Auffrischungsschulungen durchgeführt?	◯
Ist klar kommuniziert, wer bei Fragen Ansprechpartner ist?	◯