

Anlage zur „DigiAssist“ Leistungsbeschreibung

Datenschutz und Compliance

Der Auftragnehmer gewährleistet die Einhaltung sämtlicher geltender Datenschutz-, Compliance- und Informationssicherheitsanforderungen, insbesondere der Datenschutz-Grundverordnung (DSGVO), des Datenschutzgesetzes der Evangelischen Kirche in Deutschland (DSG-EKD) sowie aller einschlägigen Vorgaben des Auftraggebers. Er stellt sicher, dass die eingesetzten Mitarbeitenden regelmäßig zu den aktuellen Anforderungen des Datenschutzes geschult und zur Einhaltung der entsprechenden Bestimmungen verpflichtet werden.

Personenbezogene Daten dürfen ausschließlich im für die Leistungserbringung erforderlichen Umfang verarbeitet werden. Hierbei sind angemessene technische und organisatorische Maßnahmen zum Schutz der Daten vor unbefugtem Zugriff, Verlust, Manipulation oder Missbrauch umzusetzen. Vor der Inbetriebnahme der Lösung sind sämtliche erforderlichen Nachweise und Unterlagen bereitzustellen, insbesondere Auftragsverarbeitungsverträge (AVV), die Beschreibung der technischen und organisatorischen Maßnahmen (TOMs), Datenschutz- und Löschkonzepte, Informationen zu Datenverarbeitungsprozessen und Speicherorten sowie gegebenenfalls Nachweise zu den eingesetzten KI-Komponenten.

Im Rahmen der Service- und Supportleistungen stellt der Auftragnehmer sicher, dass die Integrität der gespeicherten Daten gewahrt bleibt und das Risiko von Manipulationen durch geeignete technische und organisatorische Maßnahmen weitestgehend ausgeschlossen wird.

Alle eingesetzten KI-Komponenten müssen die Anforderungen der DSGVO sowie die Vorgaben des EU AI Act erfüllen. Die Datenhoheit verbleibt jederzeit beim Auftraggeber.

Personenbezogene Daten sind nach dem Grundsatz der Datenminimierung zu verarbeiten und, soweit technisch und fachlich möglich, zu pseudonymisieren oder zu anonymisieren.

Darüber hinaus stellt der Auftragnehmer sicher, dass KI-gestützte Empfehlungen und Ergebnisse nachvollziehbar erläutert werden können, Entscheidungs- und Verarbeitungsprozesse transparent dokumentiert sind sowie geeignete Auditierungs- und Protokollierungsfunktionen zur Verfügung stehen. Der Einsatz unzulässiger oder verbotener KI-Anwendungen ist ausgeschlossen. Zudem ist ein angemessenes Rollen- und Berechtigungskonzept umzusetzen, das den kontrollierten und sicheren Zugriff auf Daten, Funktionen und Systeme gewährleistet.

KI

Soweit Bestandteile der angebotenen Lösung Verfahren der Künstlichen Intelligenz verwenden, hat der Auftragnehmer die Anforderungen der geltenden europäischen KI-Verordnung (EU AI Act) zu berücksichtigen. Hierzu sind mindestens folgende Nachweise vorzulegen:

- Dokumentation, ob und in welchem Umfang KI-Komponenten eingesetzt werden;
- Risikoeinstufung des eingesetzten KI-Systems gemäß den Vorgaben der KI-Verordnung;
- Beschreibung der vorgesehenen Schutzmaßnahmen und Nutzungsbedingungen;
- Informationen über Trainingsdaten, Transparenzanforderungen und menschliche Kontrollmöglichkeiten, soweit gesetzlich erforderlich.

Liegt bereits eine Risikobewertung des Herstellers oder Anbieters vor, ist diese dem Auftraggeber unaufgefordert zur Verfügung zu stellen.

Der Auftraggeber behält sich vor, auf Grundlage der vorgelegten Risikoeinstufung zusätzliche organisatorische oder technische Maßnahmen festzulegen.

(Datum und Unterschrift)

Die Eigenerklärung wurde unterzeichnet von:

(Vorname, Name der natürlichen Person: Textform)