Anlage: Technische und organisatorische Maßnahmen für KI-Systeme v1.0
Anlage 2 zur Dienstvereinbarung über den Einsatz KI-gestützter Systeme

Anlage zur Dienstvereinbarung über den Einsatz KI-gestützter Systeme

Fassung	v1.0 vom 16. September 2026
Geltungsbereich	katholische und evangelische Einrichtungen, siehe Teil A
Rechtsstand der zitierten Vorschriften	am 1. September 2026 an der Primärquelle geprüft, siehe Teil E
Verfasser	Nils Peters, kirchliche-ki.de
Verwendung	frei verwendbar, anpassbar und weitergebbar, mit Quellenangabe

Hinweis zur Rechtsdienstleistung. Diese Anlage ist ein Formularwerk für typische Sachverhaltskonstellationen und ersetzt keine Prüfung des Einzelfalls. Sie enthält keine rechtliche Würdigung für eine bestimmte Einrichtung. Die Anpassung an die konkrete Einrichtung, die rechtliche Bewertung und die Freigabe des Textes gehören zur oder zum betrieblichen Datenschutzbeauftragten beziehungsweise zur anwaltlichen Beratung der Einrichtung.

Teil A: Anwendungshinweise

Wozu diese Anlage dient

Die Muster-Dienstvereinbarung über den Einsatz KI-gestützter Systeme führt in ihrer Anlage 1 unter Abschnitt 10 den Punkt „Sicherheitsmaßnahmen" auf und beschreibt ihn in zwei Zeilen: Authentifizierung, Trennung der Nutzerbereiche, Verschlüsselung, Sicherung, Löschverfahren. Das ist als Gliederungspunkt richtig und als Arbeitsgrundlage zu wenig. Wer eine Dienstvereinbarung unterschreibt, in der dieser Punkt aus zwei Zeilen besteht, hat die Maßnahmen nicht vereinbart, sondern nur ihre Überschriften.

Diese Anlage füllt diesen einen Abschnitt aus. Sie ist als **Anlage 2** zur Dienstvereinbarung gedacht und tritt neben die Systembeschreibung, ohne sie zu ersetzen. Anlage 1 beschreibt, **was** das System verarbeitet. Anlage 2 beschreibt, **womit** diese Verarbeitung gesichert wird und **woran** sich das überprüfen lässt.

Warum eine allgemeine Maßnahmenliste hier nicht genügt

Jede Einrichtung, die Datenschutz ernst betreibt, hat bereits eine Liste technischer und organisatorischer Maßnahmen. Diese Listen sind nicht falsch, sie greifen bei einem KI-gestützten System aber an drei Stellen ins Leere.

Erstens verlässt die Verarbeitung mit jedem einzelnen Aufruf das Haus. Bei einer Fachanwendung im eigenen Rechenzentrum ist die Frage nach dem Übertragungsweg einmal zu beantworten. Bei einem System mit externer Modellanbindung ist jeder Eingabevorgang eine Übermittlung an eine oder mehrere externe Stellen, und was dabei übermittelt wird, entscheidet nicht die Nutzerin, sondern die Software: Sie stellt selbständig einen Kontext zusammen, lädt Dokumente nach und ruft Zusatzdienste auf. Die Frage „an welche Stellen wird übermittelt" lässt sich deshalb nicht aus der Produktbeschreibung beantworten, sondern nur aus der laufenden Installation.

Zweitens entsteht mit dem durchsuchbaren Index eine neue Datensammlung. Wer Akten, Protokolle und Postfächer für ein KI-System erschließt, erzeugt einen Bestand, in dem Daten nebeneinanderliegen, die vorher in getrennten Verfahren lagen. Für den katholischen Rechtskreis ist das ausdrücklich geregelt: Bei der Einordnung in eine Datenschutzklasse ist „auch der Zusammenhang mit anderen gespeicherten Daten" zu berücksichtigen (§ 9 Abs. 2 KDG-DVO). Ein Index über mehrere Bestände kann damit in einer höheren Klasse landen als jeder einzelne Bestand für sich.

Drittens sind die Voreinstellungen des Anbieters Teil der Maßnahme. Ob ein Dienst Eingaben speichert, wie lange er sie aufbewahrt und wer darauf zugreifen kann, hängt bei den meisten Angeboten nicht vom Vertrag ab, sondern von einer Einstellung im Konto und vom gewählten technischen Zugang. Beide Rechtskreise verlangen ausdrücklich, dass durch **Voreinstellung** nur die erforderlichen Daten verarbeitet werden, und nennen dabei die Speicherfrist und die Zugänglichkeit beim Namen (§ 27 Abs. 2 KDG; § 28 Abs. 2 DSG-EKD). Eine Maßnahme, die nur im Vertrag steht und nicht in der Einstellung, erfüllt diese Anforderung nicht.

Der Unterschied zwischen den Rechtskreisen

Die Maßnahmen sind in beiden Kirchen dieselben. Ihre Herleitung ist es nicht, und daraus folgt ein praktischer Unterschied, der die Reihenfolge der Arbeit bestimmt.

Katholisch: die Maßnahmen stehen im Recht. Die KDG-DVO benennt in § 6 Abs. 2 elf Maßnahmenbereiche, ordnet Daten über § 9 in drei Datenschutzklassen ein und hängt an jede Klasse in §§ 11 bis 13 feste Mindestmaßnahmen. Dazu kommen Sondervorschriften, die für ein KI-System unmittelbar einschlägig sind: § 18 zur Nutzung von Cloud-Diensten, § 19 zu autorisierten Programmen und § 22 zu externen Zugriffen. Eine Anlage lässt sich hier gegen einen Katalog abgleichen. Wer keine Einordnung vornimmt, bekommt sie kraft Gesetzes: Dann gilt automatisch Klasse III, sofern nicht die Voraussetzungen des § 14 vorliegen (§ 9 Abs. 5 KDG-DVO). Für Daten des Beicht- und des Seelsorgegeheimnisses kennt § 14 eine Stufe oberhalb der drei Klassen; diese Anlage setzt voraus, dass solche Daten nach der Dienstvereinbarung ohnehin nicht in das System gelangen.

Evangelisch: die Maßnahmen stehen im eigenen Konzept. § 27 Abs. 6 DSG-EKD verpflichtet zur IT-Sicherheit und verweist für das Nähere auf eine Rechtsverordnung. Diese Verordnung, die ITSVO-EKD, nennt keine einzelne Maßnahme. Sie verlangt stattdessen ein **IT-Sicherheitskonzept**, das fortgeschrieben wird, sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik orientiert und den Schutzbedarf der Daten berücksichtigt (§ 1 Abs. 2 und 3 ITSVO-EKD). Diese Anlage ersetzt ein solches Konzept nicht. Sie ist der KI-spezifische Baustein darin.

Aus dieser Delegation folgt aber nicht, dass der evangelische Strang die schwächeren Pflichten hätte. Bei der Auftragsverarbeitung ist er sogar strenger im Zeitpunkt: § 30 Abs. 3 Sätze 3 und 4 DSG-EKD verlangt, sich **vor Beginn der Datenverarbeitung** und sodann regelmäßig von den Maßnahmen des Auftragsverarbeiters zu überzeugen und das Ergebnis zu dokumentieren.

Zwei Vorschriften der ITSVO-EKD haben dabei mehr Gewicht, als ihre Kürze vermuten lässt. § 2 Abs. 1 Nr. 3 macht zur Mindestvoraussetzung für den Einsatz von IT, dass „die Systeme vor ihrem Einsatz getestet wurden". Und § 3 verlangt, die Beauftragten für den Datenschutz „bei der Entscheidung zur Auswahl" **frühzeitig** zu beteiligen. Wer ein KI-System erst nach Vertragsschluss vorlegt, hat damit nicht nur eine Prüfung versäumt, sondern eine Vorschrift verletzt, und zwar unabhängig davon, wie das Ergebnis der Prüfung ausgefallen wäre.

So wird die Anlage benutzt

Teil B enthält 25 Prüfpositionen in sechs Blöcken. Jede Position nennt die Maßnahme, ihre Bedeutung im KI-Zusammenhang, den Nachweis und die Fundstelle in beiden Rechtskreisen. Am Ende jeder Position steht ein Feld für das Ergebnis.

Drei Regeln für das Ausfüllen:

1. **Nur ausfüllen, was in der laufenden Installation überprüft wurde.** Eine Angabe aus dem Angebot des Anbieters ist kein Nachweis. Für den katholischen Bereich steht das im Verordnungstext: Der Verantwortliche hat sich vom Schutzniveau des Auftragsverarbeiters „in geeigneter Weise, insbesondere durch persönliche Überprüfung oder Vorlage von Nachweisen" zu überzeugen (§ 9 Abs. 7 KDG-DVO).
2. **„Nicht erfüllt" ist ein zulässiges Ergebnis, „nicht geprüft" ist keines.** Eine offen ausgewiesene Lücke lässt sich abwägen, überwachen und beheben. Eine stillschweigend übergangene Position taucht erst im Schadensfall wieder auf.
3. **Die Anlage hat ein Datum und einen Bezug auf eine Version.** Ein Modellwechsel, ein neuer Unterauftragsverarbeiter oder eine geänderte Voreinstellung machen einzelne Antworten ungültig. Ohne Datum lässt sich nicht sagen, welche.

Einbau in eine bestehende Dienstvereinbarung

Die Muster-Dienstvereinbarung erklärt in § 1 Abs. 4 die Anlage 1 zum Bestandteil der Vereinbarung. Wer diese Anlage aufnehmen will, erweitert die Vorschrift und ergänzt in Abschnitt 10 der Anlage 1 einen Verweis. Vorschlag für den Wortlaut:

> *§ 1 Abs. 4:* „Anlage 1 und Anlage 2 sind Bestandteil dieser Dienstvereinbarung."
>
> *Anlage 1, Abschnitt 10:* „Die technischen und organisatorischen Maßnahmen sind in Anlage 2 im Einzelnen ausgewiesen und nachgewiesen."

Wer die Anlage ohne Dienstvereinbarung nutzt, etwa als Fragenkatalog gegenüber einem Anbieter oder als Prüfraster der oder des betrieblichen Datenschutzbeauftragten, kann Teil B unverändert verwenden. Der Bezug auf die Dienstvereinbarung ist dann gegenstandslos, die Prüffragen sind es nicht.

Was diese Anlage nicht leistet

Sie ist **kein IT-Sicherheitskonzept** und ersetzt im evangelischen Bereich nicht das von § 1 Abs. 2 ITSVO-EKD geforderte Konzept. Sie ist **keine Risikoanalyse** im Sinne des § 10 KDG-DVO und **keine Datenschutz-Folgenabschätzung**. Sie behandelt **nicht** die allgemeine Grundabsicherung der Einrichtung, also Gebäude, Netz, Endgeräte, Sicherungskonzept und Notfallvorsorge; diese Themen sind vorausgesetzt und in den einschlägigen Werken besser behandelt, als es hier möglich wäre. Und sie trifft **keine Aussage über einzelne Produkte**.

Teil B: Prüfraster

Block 1: Zugang, Berechtigung, Trennung

1.1 Anmeldung und Mehr-Faktor-Authentifizierung

Maßnahme. Der Zugang zum System ist nur nach Authentifizierung nach dem Stand der Technik möglich. Bei Zugriffen außerhalb gesicherter Netze ist ein zweiter Faktor vorzusehen.

Im KI-System. Der Zugang zu einem KI-System ist regelmäßig ein Zugang zu allem, was für das System erschlossen wurde. Wer die Zugangsdaten einer einzigen Person besitzt, kann den gesamten Index in natürlicher Sprache befragen und muss dazu weder Ordnerstrukturen noch Berechtigungen kennen. Das hebt die Bedeutung des Anmeldeverfahrens gegenüber einer gewöhnlichen Fachanwendung deutlich an. Zugänge über Schnittstellen (technische Konten für andere Programme) sind gesondert zu betrachten, weil sie den zweiten Faktor typischerweise nicht kennen.

Nachweis. Anmeldeverfahren in der laufenden Installation vorführen lassen, einschließlich des Verhaltens bei Zugriff aus einem fremden Netz. Liste aller technischen Konten mit ihrem jeweiligen Verfahren.

Fundstelle. § 11 Abs. 2 lit. b KDG-DVO (Mehr-Faktor-Authentifizierung ausdrücklich bei Zugriffen außerhalb gesicherter Netze), § 6 Abs. 2 lit. b KDG-DVO; § 27 Abs. 1 DSG-EKD in Verbindung mit § 1 ITSVO-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

1.2 Abgestufte Rechteverwaltung, Trennung von Anwendung und Administration

Maßnahme. Anwender- und Administrationsrechte sind getrennt. Es besteht eine abgestufte Rechteverwaltung.

Im KI-System. Zu prüfen ist, ob die Administration des KI-Systems inhaltlichen Zugriff auf Verläufe, Eingaben und Index hat, und ob dieser Zugriff abschaltbar ist. Ist er es nicht, ist das offen auszuweisen. Eine Dienstvereinbarung, die einen Administrationszugriff ausschließt, obwohl er technisch besteht, ist an dieser Stelle angreifbar.

Nachweis. Rollenübersicht mit den technisch bestehenden Zugriffsmöglichkeiten je Rolle, nicht mit den vorgesehenen. Stichprobe: Kann ein Administratorkonto einen fremden Verlauf öffnen?

Fundstelle. § 6 Abs. 2 lit. j KDG-DVO; korrespondiert mit § 9 der Muster-Dienstvereinbarung und Abschnitt 7 der Anlage 1. Evangelisch: § 27 Abs. 1 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

1.3 Zugriffskontrolle bei der Suche im Bestand

Maßnahme. Berechtigte dürfen ausschließlich auf die ihrer Zuständigkeit unterliegenden personenbezogenen Daten zugreifen können.

Im KI-System. Dies ist die Position, an der KI-Einführungen am häufigsten scheitern, und sie ist die technisch anspruchsvollste dieser Anlage. Die Berechtigungen des Quellsystems gelten für den Suchbestand des KI-Systems nicht automatisch weiter. Wird ein Bestand für die Suche aufbereitet, entsteht daraus eine eigene Datenhaltung, und ob diese die Rechte des Ursprungs kennt, ist eine Eigenschaft der Software und keine Selbstverständlichkeit. Die praktische Folge ist gravierend: Eine Antwort kann Inhalte aus Dokumenten enthalten, die die fragende Person selbst nicht öffnen dürfte, ohne dass ihr das erkennbar wird.

Nachweis. Prüfung mit zwei Konten unterschiedlicher Berechtigung an demselben Bestand: Wird ein Dokument, das Konto B nicht öffnen darf, in einer Antwort an Konto B inhaltlich wiedergegeben oder als Fundstelle genannt? Zusätzlich: Wie schnell wirkt ein Entzug von Rechten im Suchbestand?

Fundstelle. § 6 Abs. 2 lit. c KDG-DVO; § 27 Abs. 1 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

1.4 Trennungsgebot und Mandantentrennung

Maßnahme. Zu unterschiedlichen Zwecken erhobene Daten werden getrennt verarbeitet. Bei geteilter Infrastruktur ist die Trennung von den Daten anderer Kunden sicherzustellen.

Im KI-System. Zwei Ebenen. Innerhalb der Einrichtung: Werden Bestände unterschiedlicher Zwecke, etwa Personalakten und Klientendokumentation, in einem gemeinsamen Suchbestand zusammengeführt? Nach außen: Die gemeinsame Nutzung einer Cloud-Infrastruktur durch mehrere Kunden ist im katholischen Recht ausdrücklich als erhöhtes Risiko benannt und deshalb vor der Nutzung zu bewerten.

Nachweis. Angabe, ob die Instanz dediziert oder geteilt betrieben wird, und auf welcher Ebene die Trennung erfolgt (eigene Datenhaltung, eigener Schlüssel, nur logische Trennung). Abgleich mit Abschnitt 1 der Anlage 1.

Fundstelle. § 6 Abs. 2 lit. i KDG-DVO, § 18 Abs. 2 lit. f KDG-DVO; § 27 Abs. 1 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

Block 2: Was das System selbst speichert

2.1 Verlauf und Kontextspeicher

Maßnahme. Für jeden Speicherort ist Datenart, Speicherdauer, Löschmechanismus und Zugriffsberechtigung festgelegt.

Im KI-System. Neben dem sichtbaren Gesprächsverlauf führen viele Systeme einen Kontextspeicher, aus dem sich spätere Antworten speisen, sowie eine Sammlung von Nutzungspräferenzen. Diese Bestände sind für die Nutzerin nicht sichtbar und werden bei der Beschreibung des Systems regelmäßig übersehen. Sie sind trotzdem personenbezogene Daten und müssen in Abschnitt 5 der Anlage 1 auftauchen.

Nachweis. Vollständige Aufstellung der Speicherorte aus der Systemdokumentation, gegen die tatsächlich vorhandenen Datenbestände der Installation abgeglichen. Testfrage nach einem Inhalt, der zwei Sitzungen zurückliegt: Wird er beantwortet, existiert ein Kontextspeicher.

Fundstelle. § 27 Abs. 2 KDG (Voreinstellung, ausdrücklich für Speicherfrist und Zugänglichkeit), § 5 Abs. 1 KDG-DVO; § 28 Abs. 2 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

2.2 Der durchsuchbare Bestand als eigene Datensammlung

Maßnahme. Der aufbereitete Suchbestand ist als eigener Datenbestand erfasst, eingeordnet und gesichert.

Im KI-System. Der Suchbestand ist keine Kopie der Quelle, sondern eine Umformung: Texte werden zerlegt, in eine numerische Darstellung überführt und zusammen mit Auszügen im Klartext abgelegt. Aus dieser Darstellung lassen sich Inhalte in erheblichem Umfang zurückgewinnen. Der Bestand ist deshalb wie der Quellbestand zu schützen und für die Einordnung gesondert zu bewerten, unter

Berücksichtigung des Zusammenhangs mit den anderen dort liegenden Daten.

Nachweis. Ort und Verschlüsselung des Suchbestands, Angabe der Klasse mit Begründung, und die Frage, wer auf den Bestand unmittelbar zugreifen kann, also unter Umgehung der Oberfläche.

Fundstelle. § 9 Abs. 1 und 2 KDG-DVO (Einordnung unter Berücksichtigung des Zusammenhangs), § 9 Abs. 5 KDG-DVO (ohne Einordnung gilt Klasse III), § 6 Abs. 2 lit. c KDG-DVO; § 27 Abs. 1 DSG-EKD in Verbindung mit § 1 Abs. 3 ITSVO-EKD (Schutzbedarf).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

2.3 Zwischenspeicher, Fehlerprotokolle, Absturzberichte

Maßnahme. Auch Datenbestände, die nicht beabsichtigt sind, aber technisch anfallen, sind erfasst und begrenzt.

Im KI-System. Zwischenspeicher beschleunigen wiederholte Anfragen und enthalten dazu die Anfrage im Klartext. Fehler- und Absturzberichte enthalten regelmäßig den Inhalt, bei dem der Fehler auftrat. Beides entsteht ohne Zutun der Anwenderin, überlebt häufig das Löschen des Verlaufs und wird bei Auskunftsersuchen übersehen. Wird die Fehlerbehandlung von einem externen Dienst übernommen, ist dieser Teil der Verarbeitungskette.

Nachweis. Auflistung aller Protokoll- und Zwischenspeicherpfade mit Aufbewahrungsdauer. Probe: einen Fehler auslösen und prüfen, welcher Inhalt im Protokoll landet und wohin dieses Protokoll geht.

Fundstelle. § 27 Abs. 2 Satz 2 KDG (die Pflicht zur Voreinstellung gilt für Menge, Umfang der Verarbeitung, Speicherfrist und Zugänglichkeit), § 29 Abs. 2 KDG für einen externen Dienst der Fehlerbehandlung; § 28 Abs. 2 Satz 2 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

2.4 Eingabekontrolle und ihre Grenze zur Leistungskontrolle

Maßnahme. Es ist grundsätzlich sicherzustellen, dass nachträglich feststellbar ist, ob und von wem personenbezogene Daten verarbeitet worden sind. Im katholischen Bereich umfasst diese Eingabekontrolle unbeschadet gesetzlicher Aufbewahrungsfristen mindestens sechs Monate.

Im KI-System. Diese Position wirkt auf den ersten Blick wie ein Widerspruch zur Dienstvereinbarung, die eine Verhaltens- und Leistungskontrolle ausschließt. Sie ist keiner. Die Eingabekontrolle dient dem Nachweis, dass eine Verarbeitung stattgefunden hat, und ist im katholischen Bereich grundsätzlich vorgeschrieben. Die Leistungskontrolle wertet dieselben Daten zur Bewertung einer Person aus und ist untersagt. Getrennt werden beide nicht durch die Menge der Protokolle, sondern durch die Zweckbindung, die abschließende Auswertungsliste und die Beschränkung des Zugriffs. Wer protokolliert, ohne diese drei Punkte zu regeln, erfüllt eine Pflicht und verletzt zugleich eine andere.

Nachweis. Nachweis der sechsmonatigen Protokollierung, zusammen mit dem abschließenden Verzeichnis der zulässigen Auswertungen, der Mindestgruppengröße für Aggregate und der Liste der Zugriffsberechtigten. Abgleich mit Abschnitt 5 und 6 der Anlage 1.

Fundstelle. § 6 Abs. 2 lit. f KDG-DVO (Eingabekontrolle, mindestens sechs Monate); für die Gegenseite § 36 Abs. 1 Nr. 9 MAVO beziehungsweise § 40 Buchstabe k MVG-EKD. Evangelisch für die Protokollierung: § 27 Abs. 1 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

Block 3: Was der Anbieter speichert

3.1 Aufbewahrung beim Modellbetreiber und die maßgebliche Voreinstellung

Maßnahme. Die Speicherfrist beim Auftragsverarbeiter ist bekannt, vertraglich festgelegt und durch die tatsächliche Einstellung des Zugangs abgesichert.

Im KI-System. Ob Eingaben beim Modellbetreiber gespeichert werden, hängt bei den meisten Angeboten nicht vom Hauptvertrag ab, sondern vom gewählten technischen Zugang und von einer Einstellung im Konto. Derselbe Anbieter kann über den einen Zugang ohne Speicherung und über den anderen mit dreißigtägiger Aufbewahrung arbeiten. Beide Rechtskreise verlangen ausdrücklich Maßnahmen, die durch **Voreinstellung** die Speicherfrist begrenzen. Der maßgebliche Nachweis ist deshalb die Einstellung, nicht die Vertragsklausel.

Nachweis. Angabe des verwendeten Zugangs und Abzug der Kontoeinstellung zur Aufbewahrung, mit Datum. Schriftliche Bestätigung des Anbieters über Dauer, Ort und Zugriffsberechtigte.

Fundstelle. § 27 Abs. 2 KDG (Voreinstellung, ausdrücklich für Speicherfrist und Zugänglichkeit), § 29 Abs. 3 und 4 KDG; § 28 Abs. 2 DSG-EKD, § 30 Abs. 3 Satz 2 Nr. 1 DSG-EKD (Dauer des Auftrags).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

3.2 Aufbewahrung zur Missbrauchserkennung

Maßnahme. Eine Aufbewahrung zu Sicherheits- oder Missbrauchszwecken beim Anbieter ist erfasst, begrenzt und in der Anlage 1 ausgewiesen.

Im KI-System. Dies ist die am häufigsten übersehene Verarbeitung. Zahlreiche Anbieter bewahren Ein- und Ausgaben für einen festen Zeitraum auf, um missbräuchliche Nutzung zu erkennen, und tun das **unabhängig** von einem vereinbarten Trainingsausschluss. In diesem Zeitraum können Beschäftigte des Anbieters unter definierten Voraussetzungen auf die Inhalte zugreifen. Wer den Trainingsausschluss für die Antwort auf die Frage nach der Speicherung hält, hat diese Verarbeitung nicht erfasst.

Nachweis. Schriftliche Auskunft über Dauer, Speicherort, Zugriffsberechtigte und Zugriffsvoraussetzungen. Prüfung, ob für den gewählten Zugang eine Vereinbarung ohne Aufbewahrung verfügbar ist, und falls ja, ob sie in Anspruch genommen wurde.

Fundstelle. § 29 Abs. 3 lit. b und Abs. 4 lit. a KDG (Verarbeitung nur auf dokumentierte Weisung, Dauer der Verarbeitung), § 9 Abs. 7 KDG-DVO; § 30 Abs. 3 Satz 2 Nr. 9 DSG-EKD (Umfang der vorbehaltenen Weisungsbefugnis).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

3.3 Trainingsausschluss, einschließlich der Zusatzdienste

Maßnahme. Daten der Einrichtung werden nicht zum Training oder zur Weiterentwicklung von Modellen verwendet. Der Ausschluss gilt gegenüber allen Stellen der Verarbeitungskette.

Im KI-System. Der Ausschluss wird üblicherweise für das Hauptmodell vereinbart und für die Zusatzdienste vergessen. Spracherkennung, Dokumentenkonvertierung, Übersetzung und Websuche sind eigene Verarbeitungen bei möglicherweise eigenen Anbietern mit eigenen Bedingungen. Ein Trainingsausschluss, der nur für das Hauptmodell gilt, ist unvollständig.

Nachweis. Vertragliche Grundlage je Stelle der Kette, nicht nur für den Hauptanbieter. Abgleich mit Abschnitt 8 der Anlage 1. Zusätzlich die Frage, was bei Rückmeldungen der Nutzenden geschieht, etwa bei einer Bewertung einer Antwort: Diese Rückmeldungen sind bei einigen Anbietern vom Trainingsausschluss ausgenommen.

Fundstelle. § 29 Abs. 2, 4 und 5 KDG (Unterauftragsverarbeiter, gleiche Pflichten); § 30 DSG-EKD. Korrespondiert mit § 11 der Muster-Dienstvereinbarung.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

3.4 Nachweis des Schutzniveaus beim Auftragsverarbeiter

Maßnahme. Der Verantwortliche hat sich vom Schutzniveau des Auftragsverarbeiters zu überzeugen und dessen Maßnahmen regelmäßig zu überprüfen.

Im KI-System. Beide Rechtskreise sind hier ungewöhnlich deutlich, und der evangelische setzt den Zeitpunkt sogar früher an: Die beauftragende Stelle hat sich **vor Beginn der Datenverarbeitung** und sodann regelmäßig von der Einhaltung der Maßnahmen zu überzeugen, und das Ergebnis ist zu dokumentieren. Der katholische Rechtskreis benennt dafür die beiden zulässigen Wege: persönliche Überprüfung oder Vorlage von Nachweisen. Eine Zusicherung im Angebot ist keines von beidem. Die Überprüfung ist mindestens alle zwei Jahre zu wiederholen und zu dokumentieren; bei Vorlage eines anerkannten Zertifikats des Auftragsverarbeiters kann sie entfallen. Für ein KI-System ist dabei zu beachten, dass ein Zertifikat sich regelmäßig auf den Betrieb des Rechenzentrums bezieht und nicht auf die Frage, was das Modell mit den Eingaben tut.

Nachweis. Prüfbericht oder Zertifikat mit Datum und Geltungsbereich, dazu die Feststellung, welche Teile der Verarbeitungskette der Nachweis abdeckt und welche nicht.

Fundstelle. § 9 Abs. 7 KDG-DVO, § 15 Abs. 5 KDG-DVO (zwei Jahre, Dokumentation, Verzicht bei Zertifikat nach § 29 Abs. 6 KDG); § 30 Abs. 3 Satz 3 und 4 DSG-EKD (Überzeugung vor Beginn der Verarbeitung und sodann regelmäßig, Dokumentation des Ergebnisses).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

Block 4: Übertragung, Weitergabe, Nebendienste

4.1 Verschlüsselung der Übertragung

Maßnahme. Die Übermittlung außerhalb eines geschlossenen und gesicherten Netzwerks erfolgt verschlüsselt, auch über automatisierte Schnittstellen.

Im KI-System. Unstrittig und in aller Regel erfüllt, weil die Anbindung ohnehin über gesicherte Verbindungen läuft. Die Position bleibt trotzdem im Raster, weil sie für die Schnittstellen zwischen den Bestandteilen der eigenen Installation oft nicht geprüft wird: zwischen Oberfläche und Suchbestand, zwischen Suchbestand und Modellanbindung.

Nachweis. Angabe je Verbindung innerhalb der Installation, nicht nur für die Verbindung zum Anbieter.

Fundstelle. § 12 Abs. 2 lit. e KDG-DVO, § 6 Abs. 2 lit. d KDG-DVO, § 26 Abs. 1 lit. a KDG; § 27 Abs. 1 Nr. 1 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

4.2 Weitergabekontrolle: an welche Stellen tatsächlich übermittelt wird

Maßnahme. Es muss überprüft und festgestellt werden können, an welche Stellen eine Übermittlung personenbezogener Daten erfolgt.

Im KI-System. Dies ist die Position, an der sich Papier und Wirklichkeit am deutlichsten unterscheiden, und sie ist zugleich die am einfachsten zu prüfende. Ein KI-System ruft im Betrieb regelmäßig mehr Gegenstellen auf, als seine Dokumentation nennt: Aktualisierungs- und Lizenzprüfungen, Nutzungsstatistik, Fehlerübermittlung, nachgeladene Schriften und Symbole, Vorschaudienste für Verweise. Nicht jeder dieser Aufrufe überträgt personenbezogene Daten, aber welche es tun, lässt sich nicht vermuten, sondern nur messen.

Nachweis. Aufzeichnung der ausgehenden Verbindungen der Installation über einen definierten Zeitraum im Normalbetrieb, Abgleich der aufgetretenen Gegenstellen mit der Kette aus Abschnitt 8 der Anlage 1. Jede Gegenstelle, die dort nicht steht, ist zu klären oder zu unterbinden.

Fundstelle. § 6 Abs. 2 lit. e KDG-DVO (Weitergabekontrolle, Protokollierungspflicht bei Weitergabe außerhalb der vorgesehenen Datenübertragung); § 27 Abs. 1 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

4.3 Zusatzdienste und die Vollständigkeit der Kette

Maßnahme. Alle an der Verarbeitung beteiligten Stellen sind vertraglich gebunden und genehmigt.

Im KI-System. Zusatzdienste springen nur bei bestimmten Funktionen an und fehlen deshalb in der Kette: Spracherkennung beim Diktat, Texterkennung beim Einlesen eines Scans, Dokumentenkonvertierung beim Anhängen einer Datei, Websuche bei einer aktuellen Frage. Auch das Modell, das Dokumente für den Suchbestand aufbereitet, ist eine eigene Stelle. Jede von ihnen bedarf im katholischen Bereich einer gesonderten oder allgemeinen Genehmigung, und bei allgemeiner Genehmigung ist der Anbieter verpflichtet, über jede beabsichtigte Änderung zu informieren.

Nachweis. Funktionsweise Punkt für Punkt durchgehen und je Funktion feststellen, welche Stelle beteiligt ist. Nachweis der Genehmigungsart und, bei allgemeiner Genehmigung, des Verfahrens, mit dem der Anbieter Änderungen mitteilt.

Fundstelle. § 29 Abs. 2 KDG (gesonderte oder allgemeine Genehmigung, Informationspflicht, Einspruchsrecht), § 29 Abs. 5 KDG; § 30 Abs. 3 Satz 2 Nr. 6 DSG-EKD (Bedingungen von Unterauftragsverhältnissen).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

4.4 Externe Zugriffe, Fernwartung, Kopierschutz

Maßnahme. Zugriffe Externer erfolgen nur aufgrund vertraglicher Vereinbarung, sind befristet oder werden unverzüglich deaktiviert, und es ist nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der Datenbestände gefertigt werden können. Fernwartung darf nur nach aktiver Einleitung durch den Auftraggeber erfolgen und ist zu protokollieren.

Im KI-System. Bei einem betreuten Betrieb hat der Dienstleister regelmäßig Zugang zur Installation und damit zum Suchbestand. Der Verordnungstext verlangt hier ausdrücklich mehr als eine Vertragsklausel, nämlich zusätzlich eine technische Absicherung, soweit möglich. Das ist die Norm, auf die sich die Aussage stützt, dass eine Zusicherung allein nicht genügt.

Nachweis. Liste der externen Zugänge mit Befristung, Verfahren für die Einleitung einer Fernwartung, Protokolle der letzten Wartungsvorgänge.

Fundstelle. § 22 Abs. 1 bis 5 KDG-DVO; § 27 Abs. 1 DSG-EKD in Verbindung mit § 1 ITSVO-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

Block 5: Löschung, Sicherung, Beendigung

5.1 Löschung wirkt an allen Speicherorten

Maßnahme. Eine Löschung erfasst alle Orte, an denen der Inhalt vorliegt.

Im KI-System. Ein gelöschter Verlauf verschwindet aus der Oberfläche. Ob er auch aus dem Suchbestand, dem Zwischenspeicher, den Fehlerprotokollen, der Datensicherung und der Aufbewahrung beim Anbieter verschwindet, sind fünf getrennte Fragen mit fünf getrennten Antworten. Diese Position ist zugleich die Voraussetzung dafür, ein Auskunfts- oder Löschersuchen vollständig beantworten zu können.

Nachweis. Löschvorgang durchführen und danach denselben Inhalt über die Suche, über die Protokolle und über eine Wiederherstellung aus der Sicherung aufzurufen versuchen. Für den Anbieter die schriftliche Bestätigung der Löschfrist.

Fundstelle. § 17 und § 19 KDG (Auskunftsrecht, Recht auf Löschung), § 29 Abs. 4 lit. g KDG (Löschung oder Rückgabe nach Abschluss der Leistung); § 30 Abs. 3 Satz 2 Nr. 4 und Nr. 10 DSG-EKD (Löschung, Löschung beim Auftragsverarbeiter nach Beendigung des Auftrags).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

5.2 Datensicherung und die Rückkehr gelöschter Inhalte

Maßnahme. Es besteht ein Datensicherungskonzept. Sicherungskopien sind vor unbefugtem Zugriff geschützt.

Im KI-System. Die Datensicherung ist Pflicht und steht in einem bekannten Spannungsverhältnis zur Löschung: Ein aus dem laufenden System gelöschter Inhalt bleibt in der Sicherung, bis deren Aufbewahrungsfrist abläuft. Das ist zulässig, muss aber beschrieben sein, weil sonst eine Wiederherstellung gelöschte Bestände zurückholt. Für den Suchbestand kommt hinzu, dass nach einer Wiederherstellung Bestand und Berechtigungen auseinanderlaufen können.

Nachweis. Aufbewahrungsfristen der Sicherung, Verfahren nach einer Wiederherstellung, insbesondere für die erneute Anwendung zwischenzeitlicher Löschungen und Rechteänderungen.

Fundstelle. § 16 Abs. 1 und 2 KDG-DVO, § 11 Abs. 2 lit. c KDG-DVO, § 26 Abs. 1 lit. c KDG; § 27 Abs. 1 Nr. 3 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

5.3 Exit-Strategie

Maßnahme. Vor der Nutzung eines Cloud-Dienstes ist in Abhängigkeit von der Risikoanalyse eine Exit-Strategie zu definieren.

Im KI-System. Zu klären ist, welche Bestände in welchem Format exportierbar sind, was **nicht** exportierbar ist, wie und wann gelöscht wird und wie die Löschung nachgewiesen wird. Der Suchbestand ist dabei gesondert zu betrachten: Er ist beim Anbieter in einer Form abgelegt, die sich häufig nicht exportieren lässt, und muss nach einem Wechsel neu aufgebaut werden.

Nachweis. Exportprobe mit einem echten Bestand, nicht mit einem Testdatensatz, und die Feststellung dessen, was dabei fehlt.

Fundstelle. § 18 Abs. 3 KDG-DVO, § 18 Abs. 2 lit. c und d KDG-DVO (Portabilität, Abhängigkeit), § 29 Abs. 4 lit. g KDG; § 30 Abs. 3 Satz 2

Nr. 10 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

5.4 Verschlüsselung bei erhöhter Schutzklasse und langfristige Lesbarkeit

Maßnahme. Daten der höchsten Schutzklasse werden auf mobilen Geräten und Datenträgern nur verschlüsselt gespeichert. Die langfristige Lesbarkeit ist sicherzustellen, einschließlich der Verfügbarkeit der Schlüssel.

Im KI-System. Praktisch bedeutsam für lokale Zwischenstände auf Endgeräten, etwa bei einer Anwendung mit Offline-Fähigkeit oder bei einem lokalen Zwischenspeicher, und für die Schlüsselverwaltung des Suchbestands. Ein verschlüsselter Bestand, dessen Schlüssel nur im laufenden Dienst existiert, ist nach einem Zwischenfall nicht wiederherstellbar.

Nachweis. Angabe der lokal abgelegten Bestände und ihrer Verschlüsselung, Verortung der Schlüssel im Datensicherungskonzept.

Fundstelle. § 13 Abs. 2 lit. a und b KDG-DVO, § 16 Abs. 1 KDG-DVO; § 27 Abs. 1 Nr. 1 und 3 DSG-EKD.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

Block 6: Betrieb, Änderung, Nachweis

6.1 Nur autorisierte Programme

Maßnahme. Auf dienstlichen IT-Systemen dürfen ausschließlich vom Verantwortlichen autorisierte Programme und Kommunikationstechnologien verwendet werden.

Im KI-System. Diese Vorschrift ist kurz und in ihrer Wirkung weitreichend. Nach ihrem Wortlaut erfasst sie nicht nur Programme, sondern auch Kommunikationstechnologien, und damit nach naheliegendem Verständnis auch einen im Browser genutzten Dienst. Die Nutzung eines nicht freigegebenen KI-Dienstes wäre danach im katholischen Bereich bereits als solche unzulässig, unabhängig davon, ob dabei personenbezogene Daten eingegeben wurden. Wer dieser Lesart nicht folgt, kommt über den Datenschutz zum selben Ergebnis, sobald das erste Dokument eingefügt wird. Wer ein freigegebenes System einführt, sollte deshalb im selben Zug regeln, wie mit den nicht freigegebenen umgegangen wird. Eine Freigabe ohne diese Regelung verlagert das Problem nur.

Nachweis. Verzeichnis der autorisierten Programme mit Datum der Freigabe. Feststellung, wie die Nutzung nicht autorisierter Dienste erkannt oder unterbunden wird.

Fundstelle. § 19 KDG-DVO; evangelisch § 2 Abs. 1 ITSVO-EKD (Anforderungsprofil, Dokumentation, Test vor Einsatz).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

6.2 Bewertung des Dienstes vor der Nutzung

Maßnahme. Primär sind bereits geprüfte und freigegebene Cloud-Dienste zu nutzen. Vor der Nutzung anderer Dienste ist anhand benannter Aspekte zu prüfen, ob die Sicherheitsanforderungen erfüllt sind.

Im KI-System. Die KDG-DVO benennt neun Risikoaspekte, von denen mehrere auf einen KI-Dienst unmittelbar zutreffen: die gemeinsame Nutzung der Infrastruktur durch mehrere Kunden, die Unkenntnis über den Speicherort, die Abhängigkeit vom Anbieter mangels Wechselmöglichkeit, die mangelnde Portabilität und der unbefugte Zugriff durch Administrationspersonal des Anbieters. Diese Aspekte sind vor der Nutzung zu bewerten, nicht im laufenden Betrieb.

Nachweis. Dokumentierte Bewertung entlang der neun Aspekte des § 18 Abs. 2 KDG-DVO mit Datum, evangelisch die entsprechende Feststellung im IT-Sicherheitskonzept.

Fundstelle. § 18 Abs. 1 und 2 KDG-DVO; § 1 Abs. 2 und 3 ITSVO-EKD, § 3 ITSVO-EKD (frühzeitige Beteiligung der Datenschutzbeauftragten bei der Auswahl).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

6.3 Modellwechsel und Versionsbindung

Maßnahme. Eine Änderung des Systems löst die Anpassung der Anlagen und die Beteiligung der Mitarbeitervertretung aus.

Im KI-System. Ein Modellwechsel ist keine Aktualisierung im gewohnten Sinn. Er kann den Verarbeitungsort, den Betreiber, die Aufbewahrung und das Verhalten des Systems gleichzeitig verändern, und er geschieht bei vielen Angeboten ohne Zutun der Einrichtung, sobald der Anbieter eine Version zurückzieht. Zu klären ist deshalb, ob eine feste Version vereinbart werden kann, mit welcher Frist ein Wechsel angekündigt wird und was in der Zwischenzeit gilt.

Nachweis. Vertragliche Regelung zur Versionsbindung und zur Ankündigungsfrist, dazu die Liste der derzeit freigegebenen Modelle mit Betreiber und Verarbeitungsort. Abgleich mit Abschnitt 9 der Anlage 1.

Fundstelle. § 29 Abs. 2 KDG (Änderung bei Unterauftragsverarbeitern, Einspruchsrecht); korrespondiert mit § 14 der Muster-Dienstvereinbarung. Evangelisch: § 2 Abs. 1 Nr. 3 ITSVO-EKD (Test vor Einsatz, auch nach einem Wechsel).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

6.4 Wirksamkeitsprüfung und Dokumentation

Maßnahme. Die getroffenen Maßnahmen sind regelmäßig, mindestens alle zwei Jahre, auf ihre Wirksamkeit zu überprüfen. Die Überprüfung ist zu dokumentieren.

Im KI-System. Der Zwei-Jahres-Takt der Verordnung ist bei einem KI-System die Untergrenze und nicht der passende Rhythmus. Ein Modellwechsel, ein neuer Zusatzdienst oder eine geänderte Voreinstellung beim Anbieter machen einzelne Positionen dieser Anlage sofort ungültig. Sinnvoll ist deshalb, die Wiederholung an ein Ereignis zu binden und nicht nur an eine Frist.

Nachweis. Datum der letzten Prüfung, Name der prüfenden Stelle, Ergebnis je Position, Liste der Ereignisse, die eine Wiederholung auslösen.

Fundstelle. § 7 Abs. 1 und 3 KDG-DVO (mindestens alle zwei Jahre, Dokumentation), § 7 Abs. 2 KDG-DVO (Zertifikat mit Orientierung an BSI-Veröffentlichungen oder vergleichbaren Regelungen, insbesondere ISO/IEC 27001, als Nachweis zulässig), § 26 Abs. 1 lit. d KDG; § 27 Abs. 1 Nr. 4 DSG-EKD, § 1 Abs. 2 ITSVO-EKD (kontinuierliche Fortschreibung).

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

6.5 Test vor Einsatz und frühzeitige Beteiligung

Maßnahme. Das System ist vor seinem Einsatz zu testen. Die Datenschutzbeauftragten sind bei der Auswahl frühzeitig zu beteiligen.

Im KI-System. Diese Position stammt aus dem evangelischen Recht und ist dort ausdrücklich als Mindestvoraussetzung formuliert. Für den katholischen Bereich folgt Vergleichbares aus der Pflicht, die Maßnahmen vor Beginn der Verarbeitung zu treffen, und aus der Anhörung der oder des betrieblichen Datenschutzbeauftragten bei der Einordnung. Ein Test vor Einsatz meint bei einem KI-System nicht den Funktionstest, sondern die Prüfung der Positionen dieser Anlage an der eingerichteten Installation. Der praktische Wert liegt im Zeitpunkt: Nach Vertragsschluss sind die meisten Feststellungen dieser Anlage nicht mehr verhandelbar.

Nachweis. Datum der Beteiligung der Datenschutzbeauftragten im Verhältnis zum Datum des Vertragsschlusses. Testbericht vor Inbetriebnahme.

Fundstelle. § 2 Abs. 1 Nr. 3 ITSVO-EKD, § 3 ITSVO-EKD, § 30 Abs. 3 Satz 3 DSG-EKD; katholisch § 5 Abs. 2 KDG-DVO (Verarbeitung erst nach Treffen der erforderlichen Maßnahmen), § 9 Abs. 3 Satz 2 KDG-DVO.

Ergebnis. ☐ erfüllt ☐ nicht erfüllt ☐ nicht anwendbar · Bemerkung: _____

Teil C: Abschluss der Prüfung

System und Version	
Stand der Installation am	
Geprüft durch	
Beteiligt: betriebliche Datenschutzbeauftragte	
Datum	
Nicht erfüllte Positionen	
Vereinbarte Behandlung dieser Positionen	
Nächste Überprüfung spätestens am	

Nicht erfüllte Positionen sind kein Grund, die Prüfung zu verwerfen. Sie sind der Grund, aus dem eine Prüfung stattfindet. Maßgeblich ist, dass zu jeder offenen Position eine Entscheidung festgehalten wird: beheben, befristet hinnehmen, oder den Einsatz auf die Fälle beschränken, in denen die Lücke nicht wirkt.

Teil D: Was bei der Prüfung erfahrungsgemäß schiefgeht

1. **Die Liste des Anbieters wird übernommen.** Anbieter liefern auf Anfrage eine Aufstellung ihrer Maßnahmen. Diese Aufstellung beschreibt den Betrieb des Rechenzentrums und beantwortet die Fragen dieser Anlage überwiegend nicht. Sie ist ein Beleg für Block 3, nicht für die Blöcke 1, 2 und 4.
2. **Der Suchbestand wird als Teil der Quelle behandelt.** Er ist ein eigener Bestand mit eigener Einordnung, eigener Berechtigung und eigenem Löschverfahren. Wer ihn nicht gesondert erfasst, hat die Hälfte der Verarbeitung nicht beschrieben.
3. **Die Prüfung findet nach Vertragsschluss statt.** Dann ist sie eine Bestandsaufnahme und keine Auswahlentscheidung. Im evangelischen Bereich verstößt das zusätzlich gegen § 3 ITSVO-EKD.
4. **Der Trainingsausschluss wird für die Antwort auf alle Speicherfragen gehalten.** Er sagt nichts über die Aufbewahrung zur Missbrauchserkennung, nichts über Zwischenspeicher und nichts über die Zusatzdienste.
5. **Die Protokollierung wird entweder ganz vermieden oder ganz freigegeben.** Beides ist falsch. Die Eingabekontrolle ist Pflicht, die Leistungskontrolle ist untersagt, und getrennt werden sie durch Zweckbindung, abschließende Auswertungsliste und Zugriffsbeschränkung.
6. **Eine erfüllte Position wird nicht datiert.** Nach dem nächsten Modellwechsel weiß niemand, welche Antworten noch gelten.

Teil E: Grenze dieser Anlage und Quellen

Grenze

Diese Anlage ist an den Vorschriften geprüft, nicht an einem Produkt. Sie sagt, welche Fragen zu stellen sind und woran sich die Antwort überprüfen lässt. Sie sagt nicht, welches System diese Antworten gibt.

Drei Einschränkungen sind offen zu benennen. **Erstens** setzt die Prüfung der Positionen 1.3, 2.3 und 4.2 einen Zugang zur laufenden Installation voraus, den nicht jede Einrichtung hat; wo der Betrieb vollständig beim Anbieter liegt, bleibt nur die schriftliche Auskunft, und das ist ein schwächerer Nachweis. **Zweitens** ist die MAVO diözesanes Recht, und die Paragrafenangaben zur Mitbestimmung können in einzelnen Diözesen abweichen; die Angaben in dieser Anlage folgen der Rahmenordnung. **Drittens** hat die KDG-DVO durch den Beschluss der Vollversammlung des Verbandes der Diözesen Deutschlands vom 24. November 2025 Änderungen erfahren, deren Übernahme in das jeweilige Diözesanrecht zu prüfen ist; maßgeblich ist die im Amtsblatt des eigenen Bistums veröffentlichte Fassung.

Quellen

Alle Vorschriften wurden am 1. September 2026 an der jeweiligen Primärquelle geprüft.

- **Gesetz über den Kirchlichen Datenschutz (KDG)** , Lesefassung des Verbandes der Diözesen Deutschlands, veröffentlicht durch das Sekretariat der Deutschen Bischofskonferenz. Herangezogen: § 17 (Auskunftsrecht), § 19 (Recht auf Löschung), § 26 (Technische und organisatorische Maßnahmen), § 27 (Technikgestaltung und Voreinstellungen), § 29 (Verarbeitung personenbezogener Daten im Auftrag). https://www.dbk.de/fileadmin/redaktion/diverse_downloads/VDD/2025_KDG_neu_Lesefassung.pdf
- **Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO)** , in der Fassung des Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 19. November 2018, geändert durch Beschluss vom 24. November 2025. Herangezogen: §§ 5, 6, 7, 9, 10, 11, 12, 13, 15, 16, 18, 19, 22. https://www.katholisches-datenschutzzentrum.de/wp-content/uploads/2025/12/kdg-dvo-dbk-beschlussfassung-nov-2025.pdf
- **Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (EKD-Datenschutzgesetz, DSG-EKD)** , in der Fassung der Bekanntmachung vom 15. Januar 2025 (ABl. EKD 2025 S. 1 Nr. 1), berichtigt am 20. Februar 2025 (ABl. EKD 2025 S. 42 Nr. 7). Herangezogen: § 27 (Technische und organisatorische Maßnahmen, IT-Sicherheit), § 28 (Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen), § 30 (Verarbeitung von personenbezogenen Daten im Auftrag). https://www.kirchenrecht-ekhn.de/pdf/57715.pdf
- **Verordnung zur Sicherheit der Informationstechnik (IT-Sicherheitsverordnung, ITSVO-EKD)** vom 29. Mai 2015 (ABl. EKD 2015 S. 146). Herangezogen: § 1 (IT-Sicherheit), § 2 (Einsatz von IT), § 3 (Beteiligung), § 5 (IT-Sicherheitsbeauftragte). https://www.kirchenrecht-ekvw.de/pdf/33288.pdf
- **Muster-Dienstvereinbarung über den Einsatz KI-gestützter Systeme**, katholische Fassung (MAVO / KDG) und evangelische Fassung (MVG-EKD / DSG-EKD), kirchliche-ki.de. https://kirchliche-ki.de/muster-dienstvereinbarung-ki-katholisch/ und https://kirchliche-ki.de/muster-dienstvereinbarung-ki/