

Patientendaten und KI

Datenschutz, Speicherung und Grenzen der Kontrolle bei externen KI-Diensten

Überarbeitete Fassung, Stand 01.10.2026

Allgemeine Information, keine Rechtsberatung. Die datenschutzrechtliche, berufsrechtliche, medizinproduktrechtliche und organisatorische Bewertung eines konkreten Einsatzes sollte mit Datenschutzbeauftragten, Rechtsberatung, Informationssicherheit und – soweit einschlägig – der zuständigen ärztlichen Leitung abgestimmt werden.

1. Kurzfassung

Kernaussagen

- Gesundheitsdaten sind besonders geschützte personenbezogene Daten im Sinn von Art. 9 DSGVO. Ihre Verarbeitung mit KI ist nicht grundsätzlich verboten. Sie setzt jedoch voraus, dass die gesamte Verarbeitungskette – von der Eingabe über Übertragung, Verarbeitung, Sicherheitsmechanismen und Speicherung bis zur Löschung – rechtlich zulässig, technisch abgesichert und nachvollziehbar gestaltet ist.
- Anonymisierung ist kontextabhängig. Das bloße Entfernen eines Namens genügt regelmäßig nicht. Alter, seltene Erkrankungen, Behandlungsverläufe, Zeitangaben, Ortsbezüge, Bilder und Freitext können eine Re-Identifizierung ermöglichen. Pseudonymisierung ist keine Anonymisierung.
- Ob pseudonymisierte Daten für einen bestimmten Empfänger noch personenbezogen sind, hängt davon ab, ob dieser Empfänger die betroffene Person mit vernünftigerweise einsetzbaren Mitteln identifizieren kann. Für den ursprünglichen Verantwortlichen können dieselben Daten weiterhin personenbezogen bleiben.
- „Kein Training“ bedeutet nicht „keine Speicherung“. Davon getrennt zu beurteilen sind insbesondere Logs, Sicherheits- und Missbrauchsüberwachung, Application State, Backups, Supportzugriffe, technische Kopien, Evaluationen sowie gesetzliche Aufbewahrungs- und Herausgabepflichten.
- Bei externen Enterprise- oder API-Diensten kann die Speicherung durch Verträge, zugelassene Endpunkte und technische Einstellungen erheblich reduziert werden. Eine uneingeschränkte, in jeder Ausnahmesituation geltende und vom Anwender selbst überprüfbare Null-Speicherung lässt sich jedoch nicht allein aus einem Prompt, einer Chat-Löschung oder einer ZDR-Einstellung ableiten.
- Prompts und lokale Einstellungen können das Verhalten des Modells sowie die eigene Anwendung beeinflussen. Sie steuern jedoch nicht automatisch die Sicherheits-, Logging-, Speicher-, Support- oder Zugriffssysteme eines externen Anbieters.
- Die höchste technische und organisatorische Kontrolle besteht bei einer selbst betriebenen Infrastruktur. Das bedeutet jedoch zugleich vollständige eigene Verantwortung für Informationssicherheit, Patchmanagement, Zugriffsrechte, Monitoring, Backups, Löschung und Nachweisbarkeit.

2. Ausgangspunkt

Gesundheitsdaten gehören zu den besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO. Dazu können nicht nur Diagnosen, Befunde und Arztbriefe zählen, sondern auch Angaben zu Symptomen, Behandlungen, Medikamenten, Behinderungen, psychischen Zuständen, genetischen Informationen oder Gesundheitsrisiken.

Der Begriff „Patientendaten“ ist weiter als „Gesundheitsdaten“. Patientendaten können außerdem Identifikationsdaten, Kontaktdaten, Termin- und Abrechnungsdaten, Kommunikationsinhalte, Bilder, Dokumentmetadaten und technische Nutzungsdaten umfassen. Auch Kombinationen an sich unscheinbarer Angaben können einen Personenbezug herstellen.

Entscheidend ist daher nicht allein, ob eine KI verwendet wird. Maßgeblich ist, ob für die konkrete Verarbeitung insbesondere folgende Anforderungen erfüllt sind:

- eine tragfähige Rechtsgrundlage nach Art. 6 DSGVO und bei Gesundheitsdaten zusätzlich eine Ausnahme nach Art. 9 Abs. 2 DSGVO
- Zweckbindung und Datenminimierung
- Transparenz und Erfüllung der Informationspflichten
- technische und organisatorische Maßnahmen
- kontrollierte Zugriffsrechte
- nachvollziehbare Speicher- und Löschkonzepte
- geregelte Unterauftragsverhältnisse
- Prüfung möglicher Drittlandtransfers
- Dokumentation der Verarbeitung und gegebenenfalls Datenschutz-Folgenabschätzung

Datenschutzrechtliche Zulässigkeit ersetzt keine Prüfung weiterer Anforderungen. Je nach Funktionsumfang können zusätzlich insbesondere ärztliches Berufsrecht, Schweigepflichten, Sozialrecht, Qualitätsmanagement, Medizinprodukterecht und die europäische KI-Regulierung relevant sein.

3. Anonymisierung und Pseudonymisierung

Echte Anonymisierung

Echte Anonymisierung kann die datenschutzrechtliche Lage wesentlich vereinfachen. Sind Daten tatsächlich anonym, fehlt der Personenbezug; die DSGVO findet auf diese anonymen Informationen grundsätzlich keine Anwendung.

Bei Patientendaten sind die Hürden jedoch hoch. Eine Person kann auch ohne Name oder Geburtsdatum identifizierbar oder zumindest wiedererkennbar sein. Relevante Merkmale können etwa sein:

- ungewöhnliche Kombinationen von Alter, Geschlecht und Wohnort
- seltene Erkrankungen oder außergewöhnliche Behandlungsverläufe
- konkrete Zeitangaben
- Klinik-, Praxis- oder Stationsbezüge
- präzise Angaben zu Operationen, Medikamenten oder Komplikationen
- Freitextpassagen aus Arztbriefen oder Verlaufsdokumentationen
- Bilddaten, DICOM-Metadaten oder andere eingebettete Identifikatoren

Anonymisierung ist deshalb kein einmaliger Löschvorgang einzelner Identifikatoren. Sie erfordert eine risikobasierte Bewertung der Re-Identifizierbarkeit im jeweiligen Kontext.

Pseudonymisierung ist keine Anonymisierung

Pseudonymisierung bedeutet, dass direkte Identifikatoren durch Kennungen ersetzt oder von den übrigen Daten getrennt werden. Die Zuordnung kann jedoch über einen Schlüssel, Zusatzwissen oder die Kombination mehrerer Merkmale weiterhin möglich sein. Pseudonymisierung ist eine wichtige Schutzmaßnahme. Sie reduziert Risiken, beseitigt aber den Personenbezug nicht zwingend.

Zur Rechtsprechung des EuGH

- Nach der Rechtsprechung des EuGH kommt es darauf an, ob eine Identifizierung mit Mitteln möglich ist, die vernünftigerweise eingesetzt werden können. Daten sind nicht allein deshalb personenbezogen, weil irgendeine beliebige Person theoretisch eine Zuordnung herstellen könnte.

- Im Urteil vom 4. September 2025 in der Rechtssache C-413/23 P hat der EuGH hervorgehoben, dass die Einordnung pseudonymisierter Daten aus Sicht des jeweiligen Empfängers zu prüfen ist. Kann ein Empfänger die betroffene Person nicht mit vernünftigerweise einsetzbaren Mitteln identifizieren, können die Daten für diesen Empfänger anonym sein. Für den ursprünglichen Verantwortlichen können dieselben Daten weiterhin personenbezogen bleiben.
- Für Gesundheitsdaten ist Art. 9 DSGVO weit auszulegen. Der besondere Schutz kann auch dann eingreifen, wenn Gesundheitsinformationen nicht ausdrücklich genannt werden, sich aber aus anderen Daten ableiten lassen.

Folgerungen

- Die datenschutzrechtliche Bewertung ist akteurs- und kontextbezogen. Derselbe Datensatz kann für einen Akteur personenbezogen und für einen anderen Akteur anonym sein.
- Wer Daten pseudonymisiert und anschließend übermittelt, verarbeitet regelmäßig weiterhin personenbezogene Daten. Es sind daher insbesondere Rechtsgrundlage, Transparenz, Zweckbindung, Auftragsverarbeitung und Sicherheitsmaßnahmen zu prüfen.
- Auch die Anonymisierung selbst ist eine Verarbeitung personenbezogener Daten, solange der Personenbezug noch besteht.
- Bei medizinischem Freitext, Befunden, Bildern, seltenen Diagnosen und komplexen Behandlungsverläufen ist eine belastbare Anonymisierung besonders anspruchsvoll.
- Der Europäische Datenschutzausschuss hat im Juli 2026 den Entwurf der Guidelines 02/2026 on Anonymisation veröffentlicht. Die öffentliche Konsultation läuft bis zum 30.10.2026. Der Entwurf ist daher zu berücksichtigen, aber nicht als endgültige abgeschlossene aufsichtsbehördliche Position auszugeben.

4. Identifizierbare Gesundheitsdaten in einer kontrollierten KI

Personenbezogene Gesundheitsdaten müssen nicht zwingend vor jeder KI-Verarbeitung anonymisiert werden. Sie können unter geeigneten Voraussetzungen in einer kontrollierten medizinischen oder organisatorischen KI-Umgebung verarbeitet werden.

Vor einem Einsatz sind insbesondere folgende Punkte zu prüfen:

- Rechtsgrundlage nach Art. 6 DSGVO und zusätzlich eine Ausnahme für besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 2 DSGVO. Im Versorgungskontext kann insbesondere Art. 9 Abs. 2 Buchst. h in Verbindung mit Art. 9 Abs. 3 DSGVO relevant sein. Ergänzend können nationale Regelungen, etwa § 22 BDSG, zu beachten sein.
- Rollenverteilung der Beteiligten: Verantwortlicher, gemeinsamer Verantwortlicher, Auftragsverarbeiter, Unterauftragsverarbeiter sowie mögliche eigenständig Verantwortliche.
- Auftragsverarbeitungsvertrag nach Art. 28 DSGVO, soweit der Anbieter tatsächlich als Auftragsverarbeiter tätig wird.
- Technische und organisatorische Maßnahmen nach Art. 32 DSGVO, etwa Verschlüsselung, Zugriffskontrolle, Berechtigungskonzepte, Protokollierung, Mandantentrennung und sichere Schlüsselverwaltung.
- Datenschutz-Folgenabschätzung nach Art. 35 DSGVO, sofern eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten betroffener Personen zur Folge hat.
- Ärztliche Schweigepflicht nach § 203 StGB sowie berufsrechtliche Verschwiegenheitspflichten. Ein Auftragsverarbeitungsvertrag allein beantwortet nicht abschließend, ob ein externer Dienstleister unter den Voraussetzungen der Schweigepflicht zulässig eingebunden wird.
- Speicherorte, Datenübermittlungen in Drittländer, Garantien nach Kapitel V DSGVO, Unterauftragnehmer, menschliche Supportzugriffe, Löschfristen, Backupzyklen und Berechtigungskonzepte.

- Medizinproduktrechtliche und regulatorische Einordnung. Je nach Zweckbestimmung und Funktion kann eine KI-Anwendung als Medizinprodukt oder als reguliertes KI-System einzuordnen sein.

5. Training ist nicht dasselbe wie Speicherung

Die Aussage „Kundendaten werden nicht zum Training verwendet“ beantwortet nur eine Teilfrage. Sie kann bedeuten, dass Eingaben und Ausgaben nicht zur Verbesserung oder zum Training allgemeiner Modelle verwendet werden.

Davon klar zu trennen sind unter anderem:

- Speicherung von Eingaben und Ausgaben für den sichtbaren Chat oder die Anwendung
- technische Verarbeitungsprotokolle
- Abuse- und Safety-Monitoring
- Sicherheitsklassifikation
- Rate-Limiting und Betrugserkennung
- Fehleranalyse und Debugging
- Caching und Application State
- Supportzugriffe
- Sicherungskopien und Disaster-Recovery-Systeme
- gesetzliche Aufbewahrungs-, Auskunfts- oder Herausgabepflichten

Die Aussage „kein Training“ ist daher kein Nachweis dafür, dass Daten nicht gespeichert, nicht protokolliert, nicht in Sicherheitsprozessen verarbeitet oder nicht durch Unterauftragnehmer verarbeitet werden.

6. Speicherung durch Sicherheits- und Betriebsprozesse

Moderne KI-Dienste bestehen nicht nur aus einem Sprachmodell. Zwischen Eingabe und Ausgabe können zahlreiche technische Systeme arbeiten, beispielsweise:

- Authentifizierung und Berechtigungsprüfung
- Inhaltsklassifizierung
- Missbrauchs- und Betrugserkennung
- Sicherheitsfilter
- Rate-Limiting
- Anomalieerkennung
- Protokollierung
- technische Fehleranalyse
- Qualitäts- und Stabilitätsüberwachung
- Eskalations- und Prüfprozesse
- Backup- und Wiederherstellungssysteme

Diese Verarbeitungsschritte können eigene Datenbestände erzeugen. Sie sind technisch und organisatorisch nicht zwingend identisch mit der sichtbaren Chatansicht oder einer vom Nutzer ausgelösten Löschfunktion.

Für die Datenschutzbewertung sind mindestens vier Ebenen zu unterscheiden:

- Sichtbare Nutzerdaten: Chatverläufe, hochgeladene Dateien, Projekthinhalte oder sonstige im Benutzerkonto sichtbare Daten.

- Operative Daten: Logs, Fehlerdaten, Zugriffsdaten, Sicherheitsdaten, technische Metadaten, Rate-Limit-Informationen und Anwendungsstatus.
- Sicherungs- und Archivsysteme: Backups, Replikationen, Wiederherstellungsdaten und Archivsysteme.
- Drittkomponenten: Externe Integrationen, Hosting-Dienste, Monitoring-Werkzeuge, Datenbanken, Vektorspeicher, E-Mail- oder Ticketing-Systeme sowie gegebenenfalls angebundene KI- oder MCP-Dienste.

Eine Löschung im Benutzerkonto betrifft unmittelbar vor allem die erste Ebene. Die übrigen Ebenen können eigenen Löschfristen, Sicherheitsanforderungen und technischen Wiederherstellungsprozessen unterliegen.

Automatische Sicherheitsklassifikationen sind nicht fehlerfrei. Medizinische Fachbegriffe, Beschreibungen psychischer Krisen, Gewaltfolgen, Missbrauch, Suizidalität oder Medikamentenrisiken können automatisiert als sicherheitsrelevant klassifiziert werden, obwohl die Eingabe medizinisch oder fachlich begründet ist. Die Klassifikation ist selbst ein Verarbeitungsvorgang und keine Garantie dafür, dass kein menschlicher Zugriff, keine Protokollierung oder keine nachgelagerte Prüfung stattfindet.

7. Differenzierung nach Dienstetyp

Die datenschutzrechtliche und technische Bewertung hängt wesentlich vom konkreten Produkt, dem Vertrag, den eingesetzten Endpunkten und den aktivierten Einstellungen ab. Die folgende Übersicht dient nur als Orientierung. Sie ist keine allgemeine Freigabe für bestimmte Produkte oder Anbieter.

Dienstetyp	Training	Speicherung und Ausnahmen	Kontrolle des Anwenders
Verbraucherprodukt, etwa privates Chatkonto	Abhängig von Produkt, Kontoart und Einstellungen	Chat-, Datei- und Nutzungsdaten können nach den jeweils geltenden Produktbedingungen verarbeitet und gespeichert werden. Löschfristen, Sicherheitsausnahmen, Backups und Datenverwendung müssen konkret geprüft werden.	Gering. Für identifizierbare Patientendaten regelmäßig ungeeignet, insbesondere ohne geeignete vertragliche Grundlage und kontrollierte Organisationsumgebung.
Business- oder Enterprise-Produkt	Häufig nach Anbieterangabe kein Training mit Kundendaten	Mögliche Administrationskontrollen für Aufbewahrung; Sicherheits-, Support-, Rechts- und Backup-Ausnahmen müssen konkret geprüft werden.	Mittel. Verträge, Datenverarbeitungsvereinbarungen, Speicherorte, Unterauftragnehmer und konkrete Produktfunktionen sind entscheidend.
Standard-API	Häufig nach Anbieterangabe kein Training mit Kundendaten	Eingaben und Ausgaben können in Abuse-Monitoring-Logs, technischen Logs oder anderem Application State verarbeitet werden; Aufbewahrung und Ausnahmen hängen vom Anbieter und Endpunkt ab.	Mittel. Eigene Datenflüsse und Schnittstellen sind gestaltbar; Anbieterprozesse und Drittkomponenten müssen geprüft werden.
API mit Modified Abuse Monitoring	Kein Training nach Maßgabe des Vertrags beziehungsweise Produkts	Inhalte können aus regulären Abuse-Monitoring-Logs ausgenommen sein; Umfang, Voraussetzungen, Endpunkte und Ausnahmen sind konkret zu prüfen.	Mittel bis hoch. Keine Gleichsetzung mit umfassender Null-Speicherung.
API mit Zero Data Retention	Kein Training nach Maßgabe des Vertrags beziehungsweise Produkts	Bei geeigneten und freigegebenen Endpunkten können Kundendaten von regulären Abuse-Monitoring-Logs ausgenommen sein. Nicht ZDR-fähige Endpunkte oder Funktionen können Application State speichern. Sicherheits- und Rechtsausnahmen sind gesondert zu prüfen.	Hoch innerhalb eines externen Dienstes, aber abhängig von Freigabe, Endpunkten, Integrationen, Vertragslage und aktivierter Konfiguration.
Eigener Betrieb eines lokalen Modells	Nur nach eigener Entscheidung	Logs, Telemetrie, Caches, Backups, Sicherungskopien und Löschung liegen in der eigenen Infrastruktur und müssen selbst gestaltet werden.	Höchste technische Gestaltungsmöglichkeit, zugleich vollständige Verantwortung für IT-Sicherheit, Betrieb, Updates, Zugriffsschutz, Backup und Löschkonzept.

Für die OpenAI-API unterscheidet die aktuelle Dokumentation unter anderem zwischen regulären Abuse-Monitoring-Logs, Modified Abuse Monitoring, Zero Data Retention und Application State. Welche Daten tatsächlich gespeichert werden können, hängt insbesondere von dem verwendeten Endpunkt, der Freigabe und den eingesetzten Funktionen ab.

Anbieterbedingungen und technische Produkteigenschaften können sich ändern. Maßgeblich sind deshalb stets die zum Zeitpunkt der Verarbeitung geltenden Vertragsunterlagen, Datenverarbeitungsvereinbarungen, Produktdokumentationen und technischen Konfigurationen.

8. Kernbefund: keine allein durch den Anwender verifizierbare Null-Speicherung bei externen Diensten

Bei externen Diensten kann die Speicherung von Kundendaten durch geeignete Verträge, datensparsame Architektur, freigegebene ZDR- oder MAM-Konfigurationen und die Beschränkung auf geeignete Endpunkte erheblich reduziert werden.

Daraus folgt jedoch nicht automatisch eine uneingeschränkte, in jeder Situation geltende Null-Speicherung. Zu unterscheiden sind insbesondere:

- reguläre Produktdaten und Chat- beziehungsweise Anwendungsdaten
- Abuse-Monitoring-Logs
- Application State
- operative und technische Metadaten
- Sicherheits- und Missbrauchsprozesse
- Backups und Wiederherstellungsdaten
- gesetzliche Pflichten oder behördliche Anordnungen
- Datenflüsse bei Unterauftragnehmern oder Drittintegrationen

Bei den hier betrachteten OpenAI-Unterlagen sind für bestimmte Konstellationen gesonderte Regelungen zu Abuse-Monitoring, ZDR, Modified Abuse Monitoring und Application State vorgesehen. Die konkrete Anwendung hängt jedoch von den verwendeten Endpunkten, der Freigabe und der jeweiligen Vertragskonstellation ab.

Deshalb sollte nicht behauptet werden, externe Dienste speicherten zwangsläufig jeden Inhalt dauerhaft. Ebenso wenig sollte aus einer ZDR- oder MAM-Einstellung gefolgert werden, dass unter keinen Umständen eine weitere technische Verarbeitung oder Speicherung stattfinden könne.

Die sachgerechte Kernaussage lautet:

Eine weitgehende Speicherreduzierung kann bei externen Diensten technisch und vertraglich möglich sein. Ob für eine konkrete Verarbeitung tatsächlich keine Kundendaten in bestimmten Logs oder Speichern verarbeitet werden, muss für den jeweiligen Anbieter, Vertrag, Endpunkt und Datenfluss nachweisbar geprüft werden. Eine vollständige Kontrolle über jede technische Komponente lässt sich nicht allein durch Prompting, eine sichtbare Löschung oder eine Benutzereinstellung herstellen.

Eine lokal betriebene Lösung kann innerhalb der eigenen Infrastruktur ein höheres Maß an Kontrolle erreichen. Auch dort entsteht jedoch nicht automatisch vollständige Sicherheit: Betriebssystem-, Netzwerk-, Monitoring-, Backup- oder Administrationsprozesse können ihrerseits Daten verarbeiten und speichern.

9. Grenzen von Prompts und Anwenderkontrolle

Ein Prompt kann das Verhalten eines Modells beeinflussen. Er kann beispielsweise anweisen:

- nur erforderliche Angaben zu verwenden
- keine personenbezogenen Details zu wiederholen

- keine zusätzlichen Informationen zu erfinden
- sensible Eingaben zurückzuweisen
- Ergebnisse sachlich und strukturiert auszugeben
- bei Unsicherheit auf menschliche Prüfung hinzuweisen

Ein Prompt kann jedoch nicht verlässlich:

- Sicherheitsarchitekturen des Anbieters abschalten
- Abuse-Monitoring deaktivieren
- Protokollierungs- oder Speichermechanismen steuern
- Zugriffsrechte beim Anbieter ändern
- Unterauftragnehmer ausschließen
- Backupzyklen beeinflussen
- Drittlandtransfers verhindern
- garantieren, dass eine Eingabe ausschließlich durch das Modell verarbeitet wird
- garantieren, dass ein Upload sofort und vollständig aus allen technischen Systemen gelöscht wird

Ein einzelner Anwender kontrolliert vor allem die eigene Eingabe, die Arbeitsanweisung, die Auswahl des Dienstes und die Nutzung des Ergebnisses.

Eine Organisation mit eigener IT- und Entwicklungskompetenz kann zusätzlich eigene Datenflüsse, Vorverarbeitung, Pseudonymisierung, Filter, Berechtigungskonzepte, Freigaben, Speicherfristen, Audit-Protokolle und Schnittstellen gestalten. Die Prozesse eines externen Anbieters bleiben davon jedoch grundsätzlich getrennt und müssen eigenständig geprüft werden.

10. Grenzen einer selbst entwickelten Anbindung

Eine selbst entwickelte Anwendung, die einen externen KI-Dienst über eine API einbindet, bietet mehr Gestaltungsfreiheit als die Nutzung eines allgemeinen Chatprodukts. Sie ermöglicht beispielsweise:

- Eingabefilter und Datenminimierung
- Entfernung direkter Identifikatoren
- Pseudonymisierung vor der Übermittlung
- mandantenbezogene Zugriffskontrolle
- eigene Protokollierung und Löschkonzepte
- Endpunktbeschränkungen
- fachliche Freigabeschritte
- Begrenzung von Uploadformaten
- Trennung medizinischer Primärdaten von KI-Arbeitsdaten

Die entscheidende Grenze liegt jedoch in der fehlenden End-to-End-Kontrolle hinter dem Modell. Bei Gesundheitsdaten muss nachvollziehbar sein:

- welche Daten wohin übertragen werden
- welche Systeme die Daten verarbeiten
- welche Endpunkte und Modellfunktionen verwendet werden
- welche Sicherheitsprüfungen stattfinden
- ob und welche Logs, Caches oder Application-State-Daten entstehen
- welche Backups oder Replikationen bestehen

- welche Unterauftragnehmer beteiligt sind
- ob Daten in Drittländer gelangen
- unter welchen Umständen menschlicher Zugriff möglich ist
- wie lange Daten gespeichert werden
- wie Löschung technisch und organisatorisch nachgewiesen wird

Eine eigene Anwendung kann die Risiken wesentlich reduzieren. Sie ersetzt aber nicht die Prüfung des externen Dienstes, seiner Vertragsbedingungen und seiner technischen Datenverarbeitung.

11. Geeignete Systemarchitektur

Eine tragfähige Architektur für KI-Anwendungen mit Gesundheitsbezug kombiniert mehrere Schutzebenen:

- Datenminimierung: Es werden nur die für die konkrete Aufgabe erforderlichen Informationen verarbeitet.
- Vorverarbeitung: Direkte Identifikatoren wie Name, Geburtsdatum, Adresse, Aktenzeichen, Telefonnummer oder E-Mail-Adresse werden nach Möglichkeit vor der KI-Übermittlung entfernt oder ersetzt.
- Trennung von Zuordnungsschlüssel und Arbeitsdaten: Ein möglicher Schlüssel zur Re-Identifizierung bleibt in einer getrennten, kontrollierten Umgebung.
- Zugriffskontrolle: Rollen, Berechtigungen, Multifaktor-Authentifizierung und nachvollziehbare Administratorrechte werden klar geregelt.
- Kontrollierte Schnittstellen: Es werden nur freigegebene Endpunkte, Datenformate und Integrationen verwendet.
- Eigene Sicherheitsprüfung: Die Organisation überprüft Ein- und Ausgaben auf sensible Inhalte, Fehlübermittlungen und unzulässige Datenflüsse.
- Nachweisbare Speicherung und Löschung: Es bestehen dokumentierte Speicherfristen, Löschroutinen, Backupkonzepte und Kontrollen ihrer Umsetzung.
- Fachliche Kontrolle: KI-Ergebnisse werden vor einer medizinisch, rechtlich oder organisatorisch erheblichen Verwendung durch qualifizierte Personen geprüft.
- Keine unkontrollierte Autonomie: Die KI sollte keine Entscheidungen mit erheblichen Auswirkungen auf Patienten eigenständig treffen und keine Informationen autonom weitergeben, sofern hierfür nicht eine gesonderte rechtliche, technische und organisatorische Grundlage besteht.

Ein vereinfachtes Datenflussmodell lautet:

Eingabe → Vorverarbeitung und Datenminimierung → Zugriffskontrolle → sichere Übertragung → KI-Endpunkt → Sicherheits- und Betriebsprozesse → Ergebnis → fachliche Prüfung → dokumentierte Weiterverwendung oder Löschung

Jede Stufe kann eigene Daten, Metadaten, Logs oder Kopien erzeugen. Eine Datenschutzbewertung muss deshalb den gesamten Ablauf erfassen, nicht nur die Modellantwort.

12. Prüffragen an einen KI-Anbieter

- Welche Kategorien von Daten werden verarbeitet, und welche Daten dürfen nach dem vorgesehenen Einsatz überhaupt übermittelt werden?
- Welche Datenflüsse bestehen vom Upload bis zur Löschung? Welche Systeme, Regionen, Hosting-Standorte und Unterauftragnehmer sind beteiligt?
- Wer ist Modellanbieter, Hosting-Anbieter, Sicherheitsdienstleister und gegebenenfalls Betreiber weiterer integrierter Komponenten?

- Werden Eingaben, Ausgaben oder Dateien zum Training oder zur Modellverbesserung verwendet? Unter welchen Voraussetzungen und mit welchen Opt-out- oder Vertragseinstellungen?
- Welche Logs entstehen? Werden Prompts, Antworten, Dateien, Metadaten, Fehlerdaten oder Sicherheitsbewertungen gespeichert?
- Welche Endpunkte sind ZDR-fähig, welche nicht? Können einzelne Endpunkte, Funktionen oder Werkzeuge Application State speichern?
- Welche Voraussetzungen gelten für Zero Data Retention oder Modified Abuse Monitoring? Sind diese Funktionen für die konkrete Organisation, das konkrete Projekt und den konkreten Endpunkt tatsächlich freigegeben und aktiviert?
- Welche Backups, Replikationen, Archive und Wiederherstellungssysteme bestehen? Welche Löschfristen gelten dort?
- Wie funktionieren Safety-, Abuse- und Fraud-Monitoring? Wann werden Inhalte automatisiert klassifiziert, wann ist eine menschliche Prüfung oder ein Supportzugriff möglich?
- Welche Sicherheits-, Rechts- oder Behördenausnahmen gelten für Löschfristen und Datenzugriffe? Besteht eine Benachrichtigungspflicht oder ein Benachrichtigungsvorbehalt?
- Gibt es Drittlandtransfers? Falls ja: Auf welcher Grundlage erfolgen sie, und welche zusätzlichen Schutzmaßnahmen bestehen?
- Liegt ein Auftragsverarbeitungsvertrag vor? Sind Zweck, Weisungsbindung, Unterauftragnehmer, technische Maßnahmen, Speicherorte und Löschpflichten hinreichend konkret geregelt?
- Ist die ärztliche Schweigepflicht einschließlich der Anforderungen an mitwirkende Personen und vertraglich verpflichtete Dienstleister berücksichtigt?
- Ist eine Datenschutz-Folgenabschätzung erforderlich oder bereits durchgeführt worden?
- Ist die Anwendung medizinprodukterechtlich, berufsrechtlich oder nach sonstigem Gesundheitsrecht gesondert zu bewerten?

13. Schlussfazit

Die zentrale Frage bei KI-Einsätzen mit Patientendaten lautet nicht allein, ob ein Modell trainiert wird. Entscheidend ist die gesamte Verarbeitungskette rund um das Modell.

Dazu gehören insbesondere:

- die Art und Sensibilität der Eingabedaten
- die Möglichkeit einer Re-Identifizierung
- die Rechtsgrundlage
- die Rolle der Beteiligten
- die technische Architektur
- die verwendeten Endpunkte
- Sicherheits- und Abuse-Prozesse
- Logs, Application State, Backups und technische Metadaten
- Unterauftragnehmer und Drittlandtransfers
- Speicher- und Löschfristen
- menschliche Zugriffs- und Prüfmöglichkeiten
- fachliche Kontrolle über die Verwendung der Ergebnisse

Für identifizierbare Patientendaten bedeutet dies: Weder Laien noch Fachpersonen können bei einem externen Dienst allein durch Prompts, lokale Einstellungen oder das Löschen eines Chats vollständige Kontrolle über sämtliche technischen Verarbeitungsschritte, Sicherheitsdaten, Logs, Caches und Backups

herstellen.

Externe Dienste können durch Datenminimierung, geeignete Verträge, datenschutzgerechte Architektur, freigegebene Endpunkte, technische Kontrollen und fachliche Prüfung sinnvoll eingesetzt werden. Eine solche Gestaltung muss jedoch konkret nachgewiesen werden.

Die höchste Kontrollmöglichkeit besteht dort, wo Infrastruktur, Datenflüsse, Zugriffsrechte, Speicherprozesse und Löschung selbst technisch und organisatorisch beherrscht werden. Sie geht jedoch mit eigener umfassender Verantwortung für Datenschutz, Informationssicherheit und Betrieb einher.

Quellen und Prüfstand

Geprüft und berücksichtigt wurden insbesondere:

- OpenAI Platform-Dokumentation zu Datenkontrollen, Abuse-Monitoring, Modified Abuse Monitoring, Zero Data Retention und Application State. Die Dokumentation weist darauf hin, dass Aufbewahrung und Speicherverhalten von den jeweils verwendeten Funktionen und Endpunkten abhängen können.
- EuGH, Urteil vom 04.09.2025, C-413/23 P, zur kontextbezogenen Beurteilung pseudonymisierter Daten aus Sicht des jeweiligen Empfängers.
- Europäischer Datenschutzausschuss, Guidelines 02/2026 on Anonymisation, Entwurf vom Juli 2026; öffentliche Konsultation bis 30.10.2026.

Anbieterbedingungen, technische Produktfunktionen, Speicherfristen und Verfügbarkeit bestimmter Datenkontrollen können sich ändern. Maßgeblich sind stets die zum Zeitpunkt der konkreten Verarbeitung geltenden Verträge, Datenverarbeitungsvereinbarungen, Produktdokumentationen und technischen Konfigurationen.