

WDoku aus Sicht des Datenschutzes

Für: Datenschutzbeauftragte, Datenschutzkoordination

Verantwortlichkeit, Rechtsgrundlagen, Datenarten, Auftragsverarbeiter, Betroffenenrechte, Löschfristen und das Ergebnis unserer Schwellwertanalyse.

Das Wichtigste in Kürze

Ohne KIS-Anbindung werden keine Patientendaten und keine Gesundheitsdaten gespeichert oder verarbeitet. Verarbeitet werden Kontodaten der Ärztinnen und Ärzte sowie OPS-Codes, Zeitstempel und Saalbezeichnungen; mit der optionalen KIS-Anbindung zusätzlich die Leistungs-KIS-ID und die ICD-Codes des Eingriffs. Die Leistungs-KIS-ID erreicht die WDoku-Cloud nur als Hash, gebildet mit einem Schlüssel, der Ihr Haus nie verlässt. Wer Verantwortlicher ist, hängt davon ab, wer die Daten einbringt; den Auftragsverarbeitungsvertrag nach Artikel 28 schließen wir in jedem Fall, in dem er greift. Unsere Schwellwertanalyse nach den neun Kriterien des Europäischen Datenschutzausschusses ergibt keine Pflicht zu einer Datenschutz-Folgenabschätzung.

Wer ist Verantwortlicher

Maßgeblich ist nicht die Betriebsart allein, sondern die Frage, wer über Zweck und Mittel der Verarbeitung entscheidet. Daraus ergeben sich vier Konstellationen, und nur in zweien davon brauchen Sie einen Auftragsverarbeitungsvertrag.

Konstellation	Verantwortlicher	Auftragsverarbeitungsvertrag
Ärztin oder Arzt nutzt die App eigenständig in der Cloud	WDoku Marketing GmbH für dieses Nutzerkonto	Nicht erforderlich. Ihr Haus ist an dieser Verarbeitung nicht beteiligt
Teammodus in der Cloud, Einsicht der Weiterbildungsbefugten auf Freigabe	Zwei Verantwortliche nebeneinander: WDoku für die Plattform, Ihr Haus für die Verwendung der eingesehenen Daten	Nicht zwingend, weil wir insoweit nicht auf Weisung Ihres Hauses verarbeiten. Grundlage der Übermittlung ist die Freigabe der Ärztin oder des Arztes. Auf Wunsch schließen wir ihn trotzdem
Ihr Haus bringt Daten ein: Konten, Kataloge, Vorzahlen oder ein Export aus dem KIS	Ihr Haus	Erforderlich, nach Artikel 28
Betrieb auf einem eigenen Server	Ihr Haus	Erforderlich für die Fernwartung und für die optionalen Relay-Dienste (Mail-Versand, Push, Verzeichnis-Metadaten)

Für Ihr Verarbeitungsverzeichnis stellen wir eine Vorlage für den Klinik-Betrieb bereit. Sie gehört zu den Unterlagen, die Sie über wdoku.de/homepage/kontakt anfordern können. Wie die Daten in beiden Betriebsarten fließen, zeigt der Abschnitt Wie die Daten fließen auf der IT-Seite.

Wenn zwei Rollen zusammentreffen

Dieselbe Ärztin kann gleichzeitig in zwei Zeilen der Tabelle stehen. Wer sein Konto vor der Einführung privat angelegt hat und später den Teammodus Ihres Hauses nutzt, bleibt für dieses Konto in unserer Verantwortung und ist zugleich Beschäftigte Ihres Hauses. Das ist der Regelfall und kein Widerspruch: Die beiden Verantwortlichkeiten liegen nebeneinander, nicht übereinander.

Praktisch bedeutet das zweierlei. Ein Widerruf der Freigabe beendet die Einsicht Ihres Hauses, lässt das Konto aber unberührt, weil es nie Ihrem Haus gehört hat. Und wenn Ihr Haus WDoku wieder abbestellt, verschwinden die Konten nicht; die Ärztinnen und Ärzte behalten sie in der kostenlosen App.

Welche Datenarten entstehen

Der Zuschnitt ist bewusst schmal gehalten (Datenminimierung nach Artikel 25). Betroffene sind ausschließlich die Nutzerinnen und Nutzer im beruflichen Kontext.

- Konto und Profil: Name, Login-E-Mail, Passwort-Hash, Zeitstempel der Einwilligungen, Versionsstand der Rechtstexte.
- Erfasste Leistungen: OPS-Codes, Datum und Uhrzeit, Saalbezeichnung, optionale Notizen als Freitext.
- Logbuch: abonnierte Kataloge, Zählstände, Vorzahlen.
- Teammodus und Freigaben: Klinikzugehörigkeit, geteilte Leistungen, Klinik-E-Mail, Änderungshistorie.
- Kommunikation: Versandstatus von Betriebs- und Service-E-Mails, optionaler Newsletter mit getrenntem Opt-in.
- Betrieb: Server-Protokolle mit gefilterten Parametern, Audit-Ereignisse, Zähler für Rate-Limits.

Ohne KIS-Anbindung: keine Patientendaten, keine Gesundheitsdaten. OPS-Codes sind öffentliche Klassifikationscodes. Selbst wenn Zeitpunkt und Saal einer Leistung bekannt sind, lässt sich daraus kein Patient bestimmen: der OP-Plan mit Patientenbezug liegt ausschließlich bei der Klinik, in getrennter Infrastruktur und bei einem anderen Verantwortlichen. Mit der optionalen KIS-Anbindung liefert Ihr Haus zusätzlich die Leistungs-KIS-ID und die ICD-Codes des Eingriffs. Dann ist Ihr Haus der Verantwortliche und wir verarbeiten diese Daten in Ihrem Auftrag; Name, Geburtsdatum und Adresse überträgt WDoku Connect auch dann nicht. Die Leistungs-KIS-ID erreicht die WDoku-Cloud nur als Hash, gebildet mit einem Schlüssel, der Ihr Haus nie verlässt. Einen Klartextwert weist die Cloud ab. Ohne diesen Schlüssel können auch wir die Zuordnung zu einer Person nicht herstellen. Anonym sind die Daten damit nicht: Ihr Haus hält den Schlüssel, bleibt Verantwortliche, und die Kategorie im Auftragsverarbeitungsvertrag entfällt dadurch nicht.

Rechtsgrundlagen

Das Kopplungsverbot nach Artikel 7 Absatz 4 ist eingehalten: alle Kernfunktionen sind ohne die optionalen Einwilligungen nutzbar, die Newsletter-Checkbox ist nicht vorausgewählt, und eine Verweigerung hat keine Folgen für die übrige Nutzung.

- Artikel 6 Absatz 1 lit. b für die Bereitstellung des Kontos und die Betriebs- und Einrichtungskommunikation.
- Artikel 6 Absatz 1 lit. f für technische Hinweise, Missbrauchserkennung und die Protokollierung von Zugriffen.
- Artikel 6 Absatz 1 lit. a für alles Optionale: Teammodus, Freigabe an Weiterbildungsbefugte, Freigabe der Uhrzeiten, Spracheingabe, Newsletter.
- Beim Betrieb auf einem Server der Klinik folgt die Einsicht der Weiterbildungsbefugten aus dem Weiterbildungsverhältnis (lit. b bzw. lit. f). Der Arzt kann ihr nach Artikel 21 widersprechen.

Auftragsverarbeiter

Mit allen aufgeführten Dienstleistern bestehen Verträge nach Artikel 28. Übermittlungen in Drittländer sind der Ausnahmefall und jeweils vermerkt.

Dienstleister	Leistung	Standort
Hetzner Online GmbH	Hosting und Server-Infrastruktur	Deutschland
Google Ireland Ltd.	Absturzberichte der App (Crashlytics)	EU/USA mit Standardvertragsklauseln
Mistral AI	Spracheingabe, optional	Frankreich/EU

Dienstleister	Leistung	Standort
Plausible Insights OÜ	Reichweitenmessung der Website, anonymisiert und cookielos	EU
Brevo (Sendinblue GmbH)	E-Mail-Versand	EU
Capgo	Auslieferung von App-Updates	Zypern (EU)

Betroffenenrechte

- Artikel 15 (Auskunft): Der Export weist zusätzlich aus, wer Einblick hat: die aktuell befugten Weiterbildungsbefugten je Abteilung und, bei aktivem Teammodus, die Kolleginnen und Kollegen.
- Artikel 20 (Datenübertragbarkeit): Export als ZIP mit Excel, PDF und JSON, von der betroffenen Person selbst auslösbar.
- Artikel 17 (Löschung): umgesetzt als Anonymisierung nach einer dokumentierten Prozedur in zehn Schritten. Statistische Daten bleiben ohne Personenbezug erhalten. Der Vorgang verlangt eine erneute Passworteingabe.
- Artikel 21 (Widerspruch): Beim Betrieb auf einem Server der Klinik kann der Arzt der Einsicht der Befugten in der App widersprechen; der Widerspruch wirkt sofort.
- Transparenz über Zugriffe: Die Ärztin oder der Arzt sieht in der App, wann welcher Befugte die eigenen Daten aufgerufen hat. Grundlage ist das Audit-Log, das diese Zugriffe als eigene Ereigniskategorie führt.

Löschung und Aufbewahrung

Datenart	Frist
Server-Protokolle	90 Tage, danach automatische Löschung
Audit-Log (Zugriffe und Einwilligungen)	24 Monate
Änderungshistorie geteilter Leistungen	24 Monate
E-Mail-Verifikationscodes	Gültig 25 Stunden; offene Anfragen werden 30 Tage nach Ablauf gelöscht
Geräte-Fingerprint aus Einladungslinks	48 Stunden
Abgelaufene Kollegen-Einladungen	30 Tage
Offene Kollegen-Einladungen	90 Tage
Datenbanksicherungen	Spätestens nach 12 Monaten gelöscht
Konto und Leistungsdaten	Bis zur Anonymisierung auf Wunsch des Arztes

Eine Anonymisierung wirkt nicht rückwirkend in bereits erstellte Datensicherungen. Deshalb ist die Aufbewahrung der Sicherungen auf zwölf Monate begrenzt: nach spätestens einem Jahr ist eine Anonymisierung auch aus allen Sicherungen verschwunden.

Datenschutz-Folgenabschätzung

Wir haben eine Schwellwertanalyse nach den neun Kriterien der Artikel-29-Datenschutzgruppe durchgeführt, die der Europäische Datenschutzausschuss bestätigt hat.

Ergebnis: keines der neun Kriterien ist voll erfüllt, zwei sind teilweise berührt. Ein voraussichtlich hohes Risiko im Sinne von Artikel 35 liegt danach nicht vor, eine Folgenabschätzung ist nicht erforderlich.

- Kein Scoring und kein Profiling: Fortschrittsstatistiken sind Selbstbeobachtung des Arztes, keine

Bewertung durch WDoku.

- Keine automatisierten Entscheidungen mit Rechtswirkung.
- Keine systematische Überwachung öffentlicher Bereiche, kein dienstübergreifendes Tracking, cookielose Reichweitenmessung.
- Keine Verarbeitung in großem Umfang und kein Abgleich mit Fremdquellen.
- Teilweise berührt sind der KI-Sprachmodus und der Einsatz eines Sprachmodells. Beide sind optional, einwilligungsbasiert und eng auf einen Zweck begrenzt.

Die Vorprüfung stellen wir vollständig zur Verfügung, damit Sie die Argumentation nachvollziehen und für Ihr eigenes Haus bewerten können. Der Grenzfall ist der KI-Sprachmodus, und wir benennen ihn als solchen.

Sicherheit nach Artikel 32

Die technischen und organisatorischen Maßnahmen liegen als eigenes Dokument in neun Abschnitten vor: Zugangs- und Zugriffskontrolle, Verschlüsselung, Integrität und Protokollierung, Verfügbarkeit, Trennungskontrolle, Datenminimierung und Löschung, organisatorische Maßnahmen sowie eine Abgrenzung für Klinik-Installationen.

Die vollständige Fassung finden Sie im Merkblatt IT und Informationssicherheit und in der Datenschutzerklärung.

Kurz zusammengefasst: bcrypt und JWT mit Rotation, TLS 1.3 und AES-256, ein Audit-Log mit 24 Monaten Aufbewahrung, Rechenzentren in Deutschland nach ISO/IEC 27001:2022 und BSI C5 Typ 2. Beim Betrieb im eigenen Haus hat jede Installation ihre vollständig eigene Datenbank; in der Cloud erfolgt die Trennung der Zugriffe auf Anwendungsebene, serverseitig aus Rollen und Freigaben abgeleitet.

Häufige Fragen

Gibt es einen Auftragsverarbeitungsvertrag?

Ja, nach Artikel 28 DSGVO. Zwingend ist er, sobald Ihr Haus Daten einbringt oder WDoku auf einem eigenen Server betreibt; bei der reinen Einsicht auf Freigabe schließen wir ihn auf Wunsch. Das Muster fordern Sie über das Kontaktformular an, damit Ihre Prüfung sofort beginnen kann.

Warum nennt Ihr Vertragsmuster Gesundheits- und Patientendaten?

Weil dasselbe Muster jede Konstellation abdecken muss. Anlage 1 führt den größtmöglichen Umfang auf, und dazu gehört der Betrieb mit Anbindung an Ihr KIS. Ohne KIS-Anbindung fallen diese Kategorien nicht an. Wir streichen den nicht zutreffenden Teil auf Wunsch.

Wo stehen die Server?

Bei der Cloud-Variante in Deutschland, in Rechenzentren mit ISO/IEC 27001:2022 und BSI C5 Typ 2. Alternativ läuft WDoku auf einem Server in Ihrem Haus.

Verlassen Daten die EU?

Im Regelfall nicht. Die Ausnahme sind Absturzberichte der App über Google Ireland, abgesichert über Standardvertragsklauseln. Beim Endpunkt für die KI-Spracherkennung lassen wir die vertragliche Reichweite gerade prüfen und weisen das offen aus.

Brauchen wir eine Folgenabschätzung?

Nach unserer Schwellwertanalyse nicht. Die Bewertung für Ihr Haus liegt bei Ihnen; wir liefern die Vorprüfung als Arbeitsgrundlage zu. Dies ist keine Rechtsberatung.

Was ist mit der Spracheingabe?

Sie ist optional und muss aktiv gewählt werden. Im Standardmodus erfolgt die Erkennung auf dem Gerät, nur der Text wird übertragen. Im KI-Modus geht die Aufnahme an unseren Dienstleister; es findet keine dauerhafte

Speicherung und kein Training mit Nutzerdaten statt. In der App steht der ausdrückliche Hinweis, keine Patientendaten zu diktieren.

Wer ist Ihr Datenschutzbeauftragter?

Die ISIDAS GmbH, Ansprechpartner Frank Zimmer, erreichbar unter dsb-wdoku@isidas.de.

Diese Unterlage online, mit Verweisen auf die übrigen Rollen:
wdoku.de/homepage/einfuehrung/datenschutz

Diese Unterlage beschreibt den technischen und organisatorischen Stand von WDoku. Sie ist keine Rechtsberatung. Ob und wie Mitbestimmung, Datenschutz-Folgenabschätzung oder Vergaberecht im Einzelfall greifen, hängt vom konkreten Einsatz und von Ihrer Trägerschaft ab.

WDoku Marketing GmbH · Dr. Alfred-Neff-Str. 15 · 75015 Bretten · HRB 745718 Amtsgericht Mannheim · USt-IdNr. DE 357614122 · support@wdoku.de · wdoku.de