

Data Governance & Anonymisierung



Vertragspartner	SEEWARA GmbH und der jeweils betroffene Nutzerkreis gemäß Dokumenttitel
Anwendungsbereich	medicsign.de und app.medicsign.de
Hinweis	Regeln für Analytics, Benchmarking, Produktintelligenz und zukünftige Data-Layer-Modelle, arbeitsfähige Erstfassung für den operativen Plattformbetrieb

I. Grundsatz

Die in MedicalSign entstehende Prozess- und Strukturintelligenz kann einen erheblichen Produktwert darstellen. Dieser wirtschaftliche Wert ändert jedoch nicht die datenschutzrechtliche Zweckbindung. Daten werden deshalb in vier Klassen getrennt: Auftragsdaten, eigene Betriebsdaten, pseudonymisierte Analysedaten und vollständig anonymisierte Daten.

II. Datenklassen

Klasse	Beispiele	Zulässige Nutzung
A – Auftragsdaten	Mandatsdokumente, Arzt-/Antragstellerdaten, Vorgangsinhalte	nur Vertrag/Weisung bzw. konkrete Rechtsgrundlage
B – eigene Betriebsdaten	Account, Abrechnung, Security, Support	eigene legitime Zwecke gemäß Datenschutzerklärung
C – pseudonymisierte Analysedaten	ersetzte Identifikatoren, aber mögliche Rückführbarkeit	weiterhin personenbezogen; nur mit Rechtsgrundlage und Zweckbindung
D – anonymisierte Daten	nicht mehr identifizierbare aggregierte Prozessstatistiken	Produkt, Benchmarking, Forschung, Marktanalyse, Unternehmenssteuerung

III. Anonymisierung

Anonymisierung ist erst erreicht, wenn eine Person unter Berücksichtigung vernünftigerweise verfügbarer Mittel nicht mehr identifiziert werden kann. Das bloße Entfernen von Namen oder Ersetzen durch IDs ist regelmäßig nur Pseudonymisierung.

Für Benchmarking sollen Mindestgruppengrößen, Aggregation, Unterdrückung seltener Kombinationen und gegebenenfalls Zeit-/Regionscluster eingesetzt werden. Einzelne Ärzte oder kleine Einrichtungen dürfen aus veröffentlichten Auswertungen nicht vernünftigerweise rekonstruierbar sein.

IV. Produktanalyse

Zulässig ist die Verarbeitung erforderlicher Nutzungs- und Prozessmetadaten für Sicherheit, Fehleranalyse, Kapazitätsplanung und Produktverbesserung im Rahmen der jeweils einschlägigen Rechtsgrundlage. Für darüber hinausgehende wirtschaftliche Analysen ist vorrangig anonymisiertes Material zu verwenden.

V. Data Layer / angrenzende Märkte

Eine Nutzung identifizierbarer oder pseudonymisierter Ärzte-, Karriere-, Institutions- oder Vorgangsdaten für Recruiting, HR-Tech, Versicherer, Private Equity/M&A, Pharma/MedTech, Banken oder vergleichbare Dritte ist nicht durch den Plattformvertrag, den AVV oder das JCA pauschal freigegeben. Vor Aktivierung ist pro Use Case ein gesondertes Rechtsgrundlagen-, Transparenz-, Zweckbindungs-, Empfänger- und gegebenenfalls Einwilligungskonzept erforderlich.

Einwilligungen müssen insbesondere freiwillig, informiert, spezifisch, granular und widerruflich sein. Die Nutzung des Kernprodukts darf nicht unnötig von Einwilligungen in sachfremde Sekundärzwecke abhängig gemacht werden.

VI. Verbot stiller Zweckänderungen

Neue Monetarisierungs- oder Datenprodukte dürfen nicht allein dadurch aktiviert werden, dass bestehende AGB oder Datenschutzerklärungen allgemein weit formuliert sind. Wesentliche neue Zwecke erfordern eine gesonderte rechtliche Bewertung und gegebenenfalls neue Information, Vertragsgrundlage oder Einwilligung.

VII. Governance-Gate

- Use Case und wirtschaftlicher Zweck schriftlich beschreiben;
- Datenkategorien und Betroffenenengruppen bestimmen;

- Rolle (Controller/Processor/Joint Controller) festlegen;
- Art.-6- und gegebenenfalls Art.-9-Rechtsgrundlage dokumentieren;
- DSFA-Pflicht prüfen;
- Empfänger, Drittlandtransfers und Speicherdauer bestimmen;
- Anonymisierung/Pseudonymisierung technisch validieren;
- Freigabe vor Produktivstart dokumentieren.