

Datenschutzerklärung KI

1 Erläuterung und Zweckbestimmung

Mittels KI soll eine noch bessere Unterstützung für die Arbeit mit der Software im Alltag erzielt werden. KI kann z.B. die Dokumentation erleichtern bzw. beschleunigen. Die Qualität der Dokumentation kann erheblich verbessert werden, da z.B. aus eingesprochenen Texten grammatikalisch korrekte Sätze gebildet werden können. Weiterhin kann Text inhaltlich interpretiert werden, und so z.B. Vitalwerte extrahiert werden, automatisiert eine Anamnese erstellt werden, und viele Dinge mehr. Nicht zuletzt wird die Dokumentation beschleunigt, da die Texte nicht mehr getippt werden müssen, was auch die Fehlerrate deutlich verringern dürfte.

Bei KI-Systemen kommen sogenannte KI-Modelle zum Einsatz. Diese können genutzt werden, nachdem Sie vorher mit Daten trainiert wurden. Insofern muss man deutlich zwischen dem Trainieren eines Modells und dem Betrieb des KI-Systems differenzieren. Während das fertig nutzbare KI-System so gestaltet wird, dass es aus Sicht des Datenschutzes anonym ist (da weder durch einen Prompt, noch durch eine API oder ähnliches personenbezogene Daten extrahiert werden können), wird man für das Trainieren von KI-Modellen, welche die Basis für das fertige KI-System bilden, die Verarbeitung von Daten mit Personenbezug in Betracht ziehen. Sofern personenbezogene Daten verarbeitet werden, wird dies nachfolgend erläutert, die betroffenen Personen und Daten- oder Datenkategorien genannt, und unsere Empfehlung für die rechtliche Grundlage erläutert.

Bei den personenbezogenen Daten, die hier verarbeitet werden, muss man wiederum 2 betroffene Personengruppen unterscheiden. Zum einen sind die Personen betroffen, welche einen Text einsprechen. Hier handelt es sich um Mitarbeiter des Pflegedienstes. Zum anderen sind Personen betroffen, die in den eingesprochenen Texten oder Prompts erwähnt werden. Dies könnten z.B. Klienten oder deren Angehörige sein, und dabei z.B. Namen, Adressen, oder sonstige Informationen, die direkt oder indirekt (z.B. durch Verknüpfung mit anderen Informationen) einen Personenbezug zulassen.

Eine detaillierte Beschreibung der Verarbeitungsvorgänge, der Datenflüsse und der Datenspeicherungen, verbunden mit Schaubildern und technischen Maßnahmen (z.B. Verschlüsselung) kann dem zugehörigen Dokument „Prozessablauf KI“ entnommen werden.

2 Geltungsbereich

Diese Datenschutzerklärung gilt für die Auftragsverarbeitung personenbezogener Daten im Rahmen unserer Dienstleistungen für die Nutzung von KI Funktionen in .snap Software. Details zur Auftragsverarbeitung ergeben sich aus dem gültigen Auftragsverarbeitungsvertrag. Rechtsgrundlage ist die Datenschutz-Grundverordnung (DSGVO). Für Einrichtungen in Trägerschaft der katholischen Kirche gelten die entsprechenden Regelungen des kirchlichen Datenschutzgesetzes (KDG).

3 Fertiges KI-System

3.1 Betroffene Personen

Das fertige KI-System ist aus der Betrachtung hinsichtlich personenbezogener Daten, wie vorstehend beschrieben, als anonym zu bewerten. Zum System gesendete Informationen sind Ende-zu-Ende verschlüsselt, und werden nur für die Erzeugung der Ergebnisse verwendet.

Sowohl die bei der Anfrage zum KI-System gesendeten Daten, als auch die erzeugten Ergebnisse werden nicht dauerhaft gespeichert, sondern sofort nach Auslieferung der Ergebnisse gelöscht. Wenn die Ergebnisse unmittelbar erzeugt werden können, dann werden sie als direkte Antwort an den Anfragenden ausgeliefert und danach sofort gelöscht. Wenn aufgrund der Komplexität der Anfrage eine längere Verarbeitungsdauer erforderlich ist, dann werden die Ergebnisse im KI-System vorgehalten und zum Abrufen bereitgestellt. Unmittelbar nach dem Abruf werden die Daten und die Ergebnisse gelöscht. Sollte kein Abruf erfolgen, dann werden die Daten und Ergebnisse nach spätestens 12 Stunden gelöscht.

Da keine dauerhafte Speicherung der Daten stattfindet, ist auch keine weitergehende Dokumentation von Speicherdauer oder Löschfristen definiert oder erforderlich. Auch die Erfüllung von Betroffenenrechten ist hier nicht relevant.

Betroffene Personengruppen	Daten oder Datenkategorien
Mitarbeiter des Pflegedienstes	• Spracheingaben (Die Audio-Datei, auf der die Stimme des Sprechers zu hören ist)
Klienten des Pflegedienstes	• Sprachaufzeichnungen, in denen auch Informationen zum Gesundheitszustand enthalten sein können. • Gesundheitsdaten, wie z.B. Vitalwerte, Diagnosen, Medikationen) • Transkriptionen und Analyseergebnisse der Spracheingaben

3.2 Rechtsgrundlage

Als Verantwortlicher der Datenverarbeitung benötigen Sie eine entsprechende Rechtsgrundlage. Hierzu geben wir folgende Empfehlung:

Für Mitarbeiter:

Besondere Kategorien von Daten im Sinne des Art. 9 DSGVO werden hier nicht erhoben.

Als Rechtsgrundlage kommt Art. 6 Abs. 1 lit. b DSGVO in Betracht. Gegenstand der Beschäftigung ist die Pflege derjenigen Patienten, mit denen der Arbeitgeber (d.h. Sie als Verantwortlicher) einen entsprechenden Pflegevertrag hat. Der Einsatz von KI-Funktionen in der .snap Software kann im Rahmen des Beschäftigungsverhältnisses nur durchgeführt werden, wenn die vom Arbeitgeber im Rahmen seines Direktionsrecht beschaffte Software genutzt wird. Andernfalls kann der Arbeitgeber

seinen gesetzlichen und vertraglichen Dokumentationspflichten nicht oder nicht hinreichend nachkommen.

Alternativ oder ergänzend kommt auch Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) in Betracht. Der Arbeitgeber hat ein berechtigtes Interesse an der Nutzung der Software zur Dokumentation, aber auch sonstiger Daten der von ihm betreuten Patienten.

Schließlich kommt auch Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) in Betracht. Unter Berücksichtigung der oben genannten Rechtsgrundlagen besteht aber aus unserer Sicht hierfür kein Erfordernis.

Für Klienten:

Als Rechtsgrundlage kommt hier Art. 6 Abs. 1 lit. b DSGVO sowie Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse) in Betracht. Die Erhebung von Patientendaten ist zur Durchführung des Pflegevertrages zwischen dem Verantwortlichen und dem Klienten regelmäßig erforderlich. Ohne diese Daten können die ggf. notwendigen oder jedenfalls nützlichen Maßnahmen nicht getroffen werden. Sofern die Erforderlichkeit zur Durchführung des Vertrages nicht gegeben ist, kann die Verarbeitung dennoch aufgrund eines berechtigten Interesses gerechtfertigt sein.

Aufgrund der Verarbeitung von Gesundheitsdaten müssen zusätzlich die Bedingungen des Art. 9 DSGVO erfüllt werden. Zulässig ist die Verarbeitung gem. Art. 9 Abs. 2 lit. h DSGVO. Hiervon werden sämtliche Formen gesundheitsbezogener Handlungen präventiver, diagnostischer, kurativer und nachsorgender Art sowie die in diesem Zusammenhang erforderliche Verwaltungstätigkeit und die Arbeit von Abrechnungsstellen erfasst.

4 Training des KI-Systems

4.1 Betroffene Personen

Anders als beim fertigen KI-System sollen beim KI-Training personenbezogene Daten ihrer Mitarbeiter verarbeitet und gespeichert werden. Konkret geht es darum, dass die eingesprochenen Daten aufbewahrt werden, um das fertige KI-System damit zu trainieren, und die Erkennungs- und Verarbeitungsqualität des fertigen Systems auch konkret für Ihre Mitarbeiter (Aussprache, etc.) zu verbessern.

Das KI-System kann wiederholt und mehrfach mit diesen Daten neu- oder nachtrainiert werden. Aus diesem Grund werden die Daten auf Grundlage einer Einwilligung (siehe weiter unten „Rechtsgrundlage“) dauerhaft gespeichert. Eine Löschung wird durchgeführt, wenn der betroffene Mitarbeiter von seinem „Recht auf Vergessenwerden“ gem. Art. 17 DSGVO Gebrauch macht. Dieses Recht muss der Mitarbeiter bei Ihnen als Verantwortlichem geltend machen. Wir als Auftragsverarbeiter werden diese Löschung nach Ihrer Weisung durchführen, wenn die Weisung von einer weisungsbefugten Person (siehe AV-Vertrag bzw. Anhang weisungsbefugte Personen) an uns gestellt wird.

Verarbeitet und gespeichert werden nur personenbezogene Daten von Mitarbeitern, NICHT jedoch die personenbezogenen Daten von Klienten. Aufgrund der besonders schützenswerten Natur der

personenbezogenen Daten von Klienten werden diese für das KI-Training nicht verwendet. Eventuell vorhandene personenbezogene Patientendaten werden vor der Speicherung anonymisiert. Dabei erkennt das System diese Informationsteile in den Daten und entfernt diese (z.B. durch Löschen oder Übertönen der Stellen im Audio).

Betroffene Personengruppen	Daten oder Datenkategorien
Mitarbeiter des Pflegedienstes	- Spracheingaben (Die Audio-Datei, auf der die Stimme des Sprechers zu hören ist) - Ggf. freiwillig bereitgestellte Informationen zur Person, wie z.B. Geschlecht, Alter, Muttersprache, Sprachniveau, etc.

4.2 Rechtsgrundlage

Aufgrund der Tatsache, dass durch Anonymisierung keine Patientendaten mit Personenbezug für das KI-Training verwendet werden, benötigen Sie hier auch keine Rechtsgrundlage und es müssen auch keine Betroffenenrechte erfüllt werden.

Für die Daten der Mitarbeiter empfehlen wir als infrage kommende Rechtsgrundlage eine Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO.

Diese Einwilligung können Sie in der .snap Software verwalten. Für jeden Mitarbeiter, für den aus Ihrer Sicht eine ausreichende Rechtsgrundlage vorliegt (z.B. Einwilligung), können Sie in den Einstellungen von .snap Mobil das Häkchen „KI-Training“ setzen. Damit erteilen Sie uns als Auftragsverarbeiter die Weisung, die Daten dieses Mitarbeiters für die Verbesserung des Systems zu speichern und zu verwenden.

In diesem Fall speichern wir zu den Daten des Mitarbeiters (z.B. die Spracheingabe) auch Informationen, um den Mitarbeiter im System zu identifizieren. Diese Identifizierbarkeit benötigen wir, um die Betroffenenrechte gem. Art. 15 bis 18 DSGVO erfüllen zu können (z.B. Löschung).

5 Risikoklassifizierung nach EU-KI-Verordnung (AI-Act)

Das KI-System unterstützt Personal in Pflegeeinrichtungen bei der Erbringung und Dokumentation von pflegerischen Maßnahmen. Die vom System erzeugten Ergebnisse werden von der Pflegekraft geprüft und genauso weiterverarbeitet, als wären diese manuell erfasst/eingegeben worden. Es erfolgt keine medizinische Diagnose oder gar Therapieentscheidungen.

Nach Prüfung der Anwendungsfälle gem. Anhang III der EU-KI-Verordnung fällt das System nicht unter die Kategorie der Hochrisiko-KI-Systeme, da es keine medizinischen Entscheidungen autonom trifft und keine Anwendungen der in Anhang III gelisteten Hochrisiko-Kategorien umfasst.

Das System verarbeitet Daten zu Unterstützungszwecken, hat jedoch keinen direkten Einfluss auf kritische Entscheidungen.

Diese Einschätzung wird auch dadurch gesichert, dass die Ergebnisse durch das Fachpersonal geprüft werden, bevor sie in die Dokumentation einfließen. Die Weiterentwicklung (Stichwort „KI-Training“) trägt zur Qualitätsverbesserung bei der Erkennung bei, und damit zur Minimierung von Fehl-Erkennungen.

Datenschutzerklärung KI

Version 1.2 Revision am 24.09.2025

Seite 4 von 6

Das System fällt in die Kategorie „Begrenztes Risiko“ („Limited Risk“) gem. Art. 6 i.V.m. Anhang III und Art. 52 EU-KI-Verordnung.

6 Einordnung nach Medizinprodukteverordnung (MDR)

Das eingesetzte KI-System fällt nicht unter die Definition eines Medizinprodukts im Sinne der MDR (Medical Device Regulation, Verordnung (EU) 2017/745).

Nach Art. 2 Abs. 1 MDR gelten Softwareprodukte nur dann als Medizinprodukte, wenn sie einen spezifischen medizinischen Zweck erfüllen, insbesondere zur Diagnose, Vorbeugung, Überwachung, Vorhersage, Prognose, Behandlung oder Linderung von Krankheiten.

Das hier eingesetzte System dient ausschließlich der technischen Unterstützung bei der Dokumentation und Durchführung der Pflege. Es trifft keine eigenständigen medizinischen Entscheidungen und ersetzt weder Diagnose noch Therapie.

7 Technische und/oder organisatorische Maßnahmen zum Datenschutz

In der Gestaltung der Prozesse und der Durchführung von Datentransfers oder Datenspeicherungen wurde streng darauf geachtet, dass unbefugte Dritte keinen Zugang zu den Daten erlangen können. Die Details sind dem Dokument „Prozessablauf KI“ zu entnehmen, in welchem die Verarbeitung transparent dokumentiert ist. Hier ist auch erkennbar, welche Datenflüsse es gibt, und welche Sicherheitsmaßnahmen zum Einsatz kommen (z.B. Verschlüsselung).

Als Cloud-Provider für die Prozesse im Rahmen der KI-Datenverarbeitung kommt Microsoft Azure zum Einsatz. Als Serverstandort wurde explizit „EU“ gewählt.

Microsoft hat umfassende Maßnahmen implementiert, um den Datenschutz und die Datensicherheit in Azure zu gewährleisten. Microsoft verpflichtet sich, Kundendaten zu schützen und stellt klare Richtlinien und Prozesse bereit, um auf behördliche Anfragen zu reagieren. Es wird betont, dass keine staatlichen Stellen direkten oder uneingeschränkten Zugriff auf Kundendaten erhält (siehe hierzu: <https://azure.microsoft.com/de-de/explore/trusted-cloud/privacy>)

Microsoft bietet die Möglichkeit, Kundendaten innerhalb der Europäischen Union (EU) und der europäischen Freihandelszone (EFTA) zu speichern und zu verarbeiten, um den regionalen Datenschutzanforderungen gerecht zu werden (siehe hierzu: <https://www.microsoft.com/de-de/trust-center/privacy/european-data-boundary-eudb>). euregon hat diese Möglichkeit genutzt, so dass eine Verarbeitung innerhalb der EU und der EFTA gewährleistet ist.

Microsoft Azure erfüllt eine Vielzahl von gängigen Datenschutzstandards, einschließlich der DSGVO, ISO-Zertifizierungen und anderer Standards (siehe hierzu: <https://azure.microsoft.com/de-de/explore/trusted-cloud/privacy>).

Zur vertraglichen Absicherung bietet Microsoft das „Data Processing Addendum (DPA)“, welches auch die Standardvertragsklauseln (SCCs) der europäischen Kommission enthält (siehe hierzu: <https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>). Dieses dient somit als geeignete Garantie im Sinne des Art. 46 DSGVO.

Weiterhin ist Microsoft unter dem EU-US-Data Privacy Framework in den USA zertifiziert. (siehe hierzu: <https://www.dataprivacyframework.gov/participant/6474>). Damit ist auch eine

Datenschutzerklärung KI

Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses gegeben, was gem. Art. 45 DSGVO möglich ist.

Darüber hinaus bietet Microsoft auch sogenannte „Binding Corporate Rules“, die auch für die Nutzung von Azure relevant sind. Dabei handelt es sich um interne Datenschutzrichtlinien des Unternehmens, die von den Datenschutzbehörden genehmigt wurden.