

Prozessablauf .snap KI

1 Einleitung

Dieses Dokument beschreibt die Prozesse und Abläufe, sowie die Datenflüsse und die technischen und/oder organisatorischen Maßnahmen beim Bereitstellen und Betreiben der KI-Systeme, welche in den Produkten der euregon AG genutzt werden können.

Ziel und Zweck dieser Dokumentation ist es, Transparenz der Verarbeitung herzustellen, damit alle Beteiligten in der Kette die notwendigen Informationen erhalten, um Ihre Pflichten erfüllen zu können, insbesondere im Hinblick auf den Schutz der personenbezogenen Daten gem. DSGVO bzw. KDG.

Es geht in diesem Dokument um das Verständnis, wie das System aufgebaut ist. Eine Bewertung von Datenschutz und Rechtsgrundlage ist dem Dokument „Datenschutzerklärung KI“ zu entnehmen.

2 Anbieter- und Betreiber, Auftragsverarbeiter

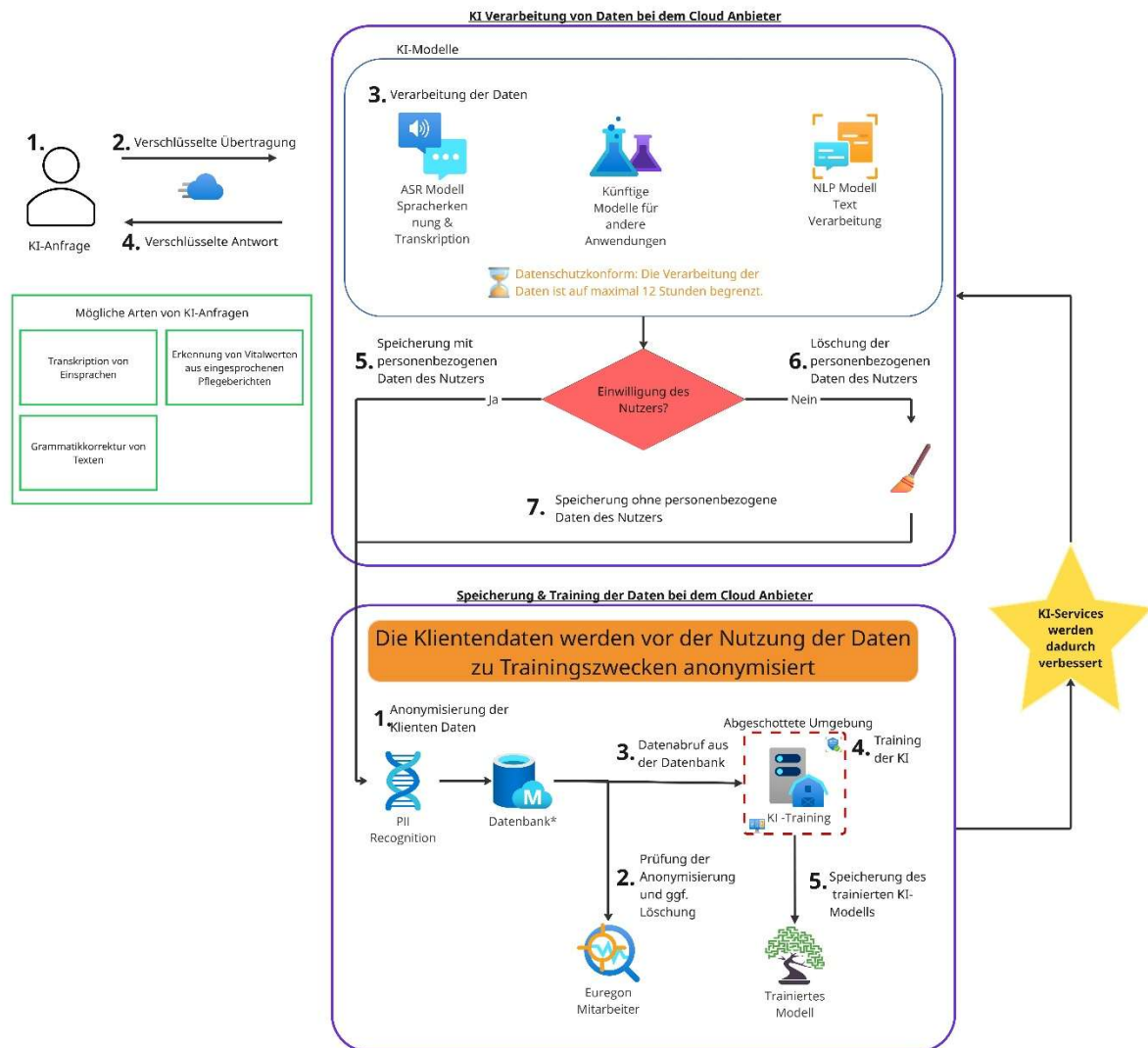
Wir, die euregon AG, entwickeln das KI-System, und bieten es Ihnen mit der .snap Software und den mobilen Apps zum Betrieb und zur Nutzung an. Entsprechend sind wir im Sinne der KI-Verordnung Anbieter des KI-Systems. Wenn Sie unsere Systeme einsetzen, dann sind Sie Betreiber. Die Verarbeitung im KI-System erfolgt auf Grundlage des zwischen Ihnen und der euregon geschlossenen Vertrags zur Auftragsverarbeitung.

Zur Bereitstellung der Services und der Rechenkapazitäten setzt die euregon Unterauftragsverarbeiter ein. Zum Zeitpunkt der Erstellung dieses Dokuments werden die Services von Microsoft Azure genutzt. Nachfolgend wird der Unterauftragsverarbeiter in diesem Dokument „Cloud-Anbieter“ genannt.

Sollte sich an den Unterauftragsverarbeitern etwas ändern, dann werden wir Sie, wie im Rahmen der Auftragsverarbeitung üblich, mit angemessener Vorlaufzeit informieren, und die Liste der Auftragsverarbeiter im AV-Vertrag entsprechend anpassen.

3 Verarbeitungsprozesse und betroffene Personen

Das folgende Schaubild macht die Verarbeitung und die Datenflüsse deutlich:



Prinzipiell gibt es zwei Verarbeitungsprozesse, die unterschiedliche technische Abläufe, sowie Maßnahmen zum Datenschutz benötigen. Entsprechend werden diese auch klar unterschieden.

- KI-System
- KI-Training

Das KI-Training ist streng genommen auch ein KI-System, die genannten Begriffe sollen aber die beiden Verarbeitungsprozesse differenzieren, wobei nachfolgend mit KI-System NICHT das KI-Training gemeint ist.

Betroffene Personen sind die Personen, die mit dem KI-System interagieren, also Ihre Mitarbeiter, nachfolgend „Nutzer“ genannt, und zum anderen die Personen, deren Daten die Nutzer z.B. im gesprochenen Text an das System zur Verarbeitung übergeben, also Ihre Patienten oder Bewohner, nachfolgend „Klienten“ genannt.

- Nutzer
- Klienten

4 KI-System

4.1 Beschreibung

Der Nutzer kann Informationen (z.B. Texte, eingesprochenes Audio) an das KI-System senden, um nach der Verarbeitung Ergebnisse zu erhalten. Dabei können verschiedene Verarbeitungsverfahren zum Einsatz kommen, je nach Use-Case, der angefordert wurde, z.B.:

- Spracherkennung und Umwandlung in Text (Transkription von Audio, ASR)
- Klassifizierung, Textkorrektur, Erkennung von Inhalt wie z.B. Vitalwerte, etc. (Natural Language Processing, NLP)

Ergebnisse der Verarbeitung werden zurückgesendet, und können dort vom Nutzer geprüft und weiterverarbeitet werden, z.B. um die Ergebnisse in der Dokumentation zu speichern.

4.2 Datenschutz und Datensicherheit

Die Daten werden von Ihrem Endgerät zum Cloud-Anbieter gesendet, auf dem das KI-System ausgeführt wird. Die Übermittlung der Daten zum Cloud-Anbieter und zurück zum Nutzer erfolgt verschlüsselt. Dabei wird https mit dem Verschlüsselungsprotokoll TLS 1.2 mit 256 Bit starkem Schlüssel verwendet.

Die übermittelten Daten werden nur zum Zweck der Erzeugung des Ergebnisses im KI-System verwendet, und danach sofort verworfen. Eine dauerhafte Speicherung findet nicht statt. Wenn das Ergebnis ohne Verzögerung ermittelt werden kann, dann werden die Daten sofort gelöscht. Bei komplexeren Verarbeitungen kann es sein, dass das Ergebnis nicht unmittelbar zur Verfügung gestellt werden kann. In diesem Fall wird das Ergebnis zur Abholung durch den Anfragenden im KI-System vorgehalten, und nach Abholung der Ergebnisse gelöscht. Sollten die Ergebnisse nie abgeholt werden, dann werden sowohl die Daten der Anfrage, als auch die berechneten Ergebnisse nach maximal 12 Stunden gelöscht.

Wenn die Ergebnisse dem Benutzer angezeigt werden, dann werden Sie als KI-generiert gekennzeichnet. Der Nutzer kann die Ergebnisse nun prüfen, und anschließend z.B. in die Dokumentation übernehmen.

5 KI-Training

5.1 Beschreibung

Die Qualität eines KI-Systems, z.B. die Erkennungsgenauigkeit, die Qualität der erzeugten Ergebnisse usw. kann nur durch kontinuierliche Verbesserung des Systems erreicht werden. Hierzu muss das System mit Daten trainiert werden, wodurch es immer besser lernt, wie Eingaben zu interpretieren sind.

Das Training eines KI-Systems setzt voraus, dass die Daten gespeichert werden, um das System kontinuierlich mit bestehenden und neuen Informationen zu trainieren.

Da es auch um personenbezogene Daten geht, werden hier besondere Maßnahmen umgesetzt, um den Datenschutz zu gewährleisten, und das System rechtskonform einsetzen zu können.

Dabei wird zwischen den beiden Gruppen betroffener Personen differenziert.

Klienten:

Daten von Klienten werden anonymisiert. Wenn eine Anonymisierung nicht möglich ist, dann werden die Daten gelöscht und nicht verwendet.

Nutzer:

Für Nutzer ist in der .snap Software eine Möglichkeit vorhanden, die Verwendung der personenbezogenen Daten des Nutzers zum Zweck des KI-Training zu erlauben.

Betroffen ist das Audio (die Stimme des Nutzers) und vom Nutzer freiwillig gegebene Daten, die in der „Datenschutzerklärung KI“ genauer benannt sind (z.B. Alter, Geschlecht, Muttersprache, etc.)

Wenn Sie eine Einwilligung des Nutzers, oder eine sonstige Rechtsgrundlage haben, dann können Sie die Verwendung der Daten durch Aktivieren eines Häkchens erlauben. Sie finden dieses Häkchen in „.snap Einstellungen“ unter „Einstellungen – Mobile Datenerfassung - .snap Mobil“. Für jeden einzelnen Mitarbeiter kann das Häkchen dort aktiviert werden.

5.2 Datenschutz und Datensicherheit

Der erste Schritt ist die Übermittlung der Daten an das KI-System, welches oben im Abschnitt KI-System beschrieben ist.

Im zweiten Schritt werden die Daten zum Zweck des KI-Training gespeichert und verarbeitet, sofern keine personenbezogenen Daten enthalten sind, oder eine Rechtsgrundlage vorliegt. Die Weitergabe aus dem KI-System an das KI-Training erfolgt innerhalb der Cloud-Infrastruktur, es findet kein Transit der Daten über offene Kanäle statt.

Text wird anonymisiert, bevor er gespeichert wird. Hierbei werden Daten, die eine Person identifizieren könnten, entfernt, oder so pseudonymisiert, dass eine Identifikation einer Person auszuschließen ist.

Da nicht nur Text, sondern auch das Audio (ein vom Nutzer eingesprochener Inhalt) gespeichert wird, wird dieses ebenfalls anonymisiert. Dabei werden die Stellen im Audio, die eine Person identifizieren

Prozessablauf KI

könnten, gelöscht oder übertönt, so dass das einzig datenschutzrelevante Datum die Stimme des Nutzers ist, welches auf Grundlage der von Ihnen verwalteten Erlaubnis (siehe oben) gespeichert wird.

Sollten im Audio mehrere Stimmen erkannt werden (da eine zweite Person während der Aufnahme gesprochen hat), dann ist nicht klar zu identifizieren, ob diese zweite Stimme rechtskonform verarbeitet werden darf. In diesem Fall wird auf die Verwendung der kompletten Audio-Datei verzichtet, und diese gelöscht.

Als zusätzliche Maßnahme werden die Daten stichprobenartig von autorisierten Mitarbeitern geprüft, und ggf. gelöscht, wenn eine unvollständige Anonymisierung festgestellt wird.