

# Leistungsbeschreibung

## d.velop pilot

### 1 Überblick

d.velop pilot (i.F. „die Software“) versetzt Sie in die Lage, mittels Eingaben in natürlicher Sprache mit Ihren Dokumenten zu interagieren. Die Software greift dazu auf aktuelle Techniken der Künstlichen Intelligenz, sogenannte Large Language Models (LLMs) zurück. Ihre Eingaben in Form natürlich-sprachlicher Anfragen werden mit Hilfe von LLMs interpretiert und in entsprechende Aktionen der Software übersetzt. Auf diese Weise erhalten Sie z.B. die Möglichkeit, lange Dokumente kompakt zusammenfassen zu lassen. d.velop pilot ist eine optionale Produkt-Erweiterung zu Ihrem bestehenden d.velop documents und wird ausschließlich für die Cloud-Versionen von d.velop documents angeboten.

### 2 Funktionsumfang

d.velop pilot erweitert Ihr bestehendes d.velop documents Archiv um die folgenden beiden Komponenten:

- ♦ **Intelligenter Import** – Im Rahmen des Imports von Dokumenten werden Dokumentarten und -eigenschaften mittels LLMs ermittelt. Die so gefundenen Inhalte werden Nutzer:innen im Indexierungsdialog der inbound-App angezeigt und entsprechend kenntlich gemacht. Darüber hinaus verfügen Nutzer:innen über die Möglichkeit, mittels einer Chat-Funktion gezielt Fragen über das verarbeitete Dokument zu formulieren (sog. Prompts) und so weitere Eigenschaften zu ermitteln oder vordefinierte Prompts auf Dokumenten auszuführen.
- ♦ **LLM-Kontextaktion** – d.velop pilot stellt in der Detailansicht für Dokumente eine Kontextaktion bereit, die Ihnen Zugriff auf weitere Produktmerkmale auf Basis von LLMs bietet. Zum jeweiligen Dokument werden Absenderinformationen und eine Kurzzusammenfassung ermittelt. Je nach Dokumentart werden weitere Informationen automatisch ermittelt. Darüber hinaus haben Sie auch hier die Möglichkeit, mit Hilfe einer Chat-Funktion in natürlicher Sprache Fragen zum Dokumentinhalt zu formulieren.

Die oben genannten Leistungsmerkmale werden zusätzlich zur Funktionalität von d.velop documents angeboten. Sie benötigen für die Nutzung ein existierendes d.velop documents (cloud).

### 3 Nutzung externer KI-Anbieter

LLMs sind Gegenstand der aktuellen Entwicklung und werden von spezialisierten Anbietern bereitgestellt. d.velop pilot bietet Ihnen aktuell die Wahl zwischen LLMs folgender Anbieter bzw Plattformen:

- Aleph Alpha GmbH,
- OpenAI OpCo, LLC,
- Microsoft Azure OpenAI Services.


Über einen Konfigurations-Dialog in der von d.velop documents bereitgestellten ConfigApp haben Sie die Möglichkeit, den verwendeten Anbieter auszuwählen. Bitte beachten Sie, dass die Leistungsfähigkeit der Software maßgeblich durch diese Auswahl beeinflusst wird.

Zur Bereitstellung der o.g. Leistungsmerkmale übertragen wir Ihre Eingaben, d.h. den Klartext aller verarbeiteten Dokumente sowie Ihre natürlich-sprachlichen Eingaben an den ausgewählten KI-Anbieter. Die Übertragung erfolgt per verschlüsselter Kommunikation über eine vom Anbieter bereitgestellte API. Es gelten die Datenverarbeitungs-Richtlinien des jeweiligen Anbieters. Nähere Informationen entnehmen Sie bitte den beiliegenden Datenschutzhinweisen bzw. AVVs.

Im Falle der Nutzung des Angebots von OpenAI OpCo, LLC weisen wir explizit darauf hin, dass eine Übertragung Ihrer Daten in ein Drittland außerhalb der Europäischen Union stattfindet. Wir raten dringend dazu, vor einer Verarbeitung sensibler Inhalte, insbesondere besonderer Kategorien personenbezogener Daten i.S. der DSGVO, eine gesonderte Risikoabwägung vorzunehmen.

#### 4 Abgrenzung von bestehenden Leistungsmerkmalen

d.velop pilot integriert sich in Ihr bestehendes d.velop documents Archiv. Allerdings erfolgt eine Verarbeitung von Inhalten im Rahmen der o.g. Leistungsmerkmale ausschließlich auf Basis einer expliziten Nutzerinteraktion. Diese ist gegeben, wenn:

- ♦ Sie im Rahmen der Nutzung der inbound-App für den Import neuer Dokumente explizit das Import-Profil „KI gestützte Erkennung“ auswählen. Alle Inhalte, die in einem Stapel verarbeitet werden, der mit diesem Import-Profil konfiguriert wurde, werden mit Hilfe von LLMs analysiert. Die enthaltenen Daten (Klartext der Dokumente) werden an den ausgewählten LLM-Anbieter übertragen.
- ♦ Sie in der Detailansicht eines Dokuments mit der Schaltfläche (  ) die d.velop pilot Kontextaktion auswählen.

Nutzen Sie keine dieser beiden Interaktionen, werden keine Inhalte an den ausgewählten KI-Anbieter übertragen.

#### 5 Nutzung Ihrer Eingaben

d.velop behält sich vor, die Daten, die Sie in den oben genannten Leistungsmerkmalen verarbeiten, in anonymisierter Form zur Verbesserung unserer Produkte zu verwenden. Dabei erfassen wir sowohl die Inhalte im Klartext als auch die natürlich-sprachlichen Eingaben, die Sie im Rahmen der Interaktion mit der Software tätigen. Wir speichern diese Daten für maximal 90 Tage. Die Speicherinfrastruktur wird durch Amazon Web Services bereitgestellt. Die Speicherung und Verarbeitung erfolgen verschlüsselt. Die Daten sind im Rahmen der beiliegenden TOM vor dem Zugriff Dritter geschützt.

#### 6 Gewährleistungsausschluss / Verantwortlichkeiten

LLMs stellen eine neuartige Technik dar, die sich noch in Entwicklung befindet. Im Unterschied zu d.velop documents machen wir für d.velop pilot keine Zusicherungen hinsichtlich der Verarbeitung von Sozialdaten i.S.d. § 67 Abs. 2 SGB X, der Wahrung des Bankgeheimnisses und des Schutzes von Berufsgeheimnisträgern i.S.d. §§ 203, 204 StGB. Wir raten daher dringend von der Nutzung des Produktes in den genannten Kontexten ab.

Wir übernehmen keine Gewähr dafür, dass die mittels d.velop pilot erzielten Ergebnisse (z.B. die ermittelten Dokumentarten und -eigenschaften) oder sonstige LLM-basierte Inhalte (i) vollständig, angemessen oder zutreffend sind, und (ii) dass es nicht zu Datenverlust oder Beeinträchtigung der Datenintegrität hinsichtlich importierter Dokumente kommt.

Ferner ist es in Ihrer alleinigen Verantwortung, zu prüfen und dafür zu sorgen, dass

- ♦ LLM-basierte Software für den von Ihnen verfolgten Nutzungszweck eingesetzt werden darf, und
- ♦ von Ihnen importierte Dokumente und Prompts nicht gegen Rechte Dritter verstoßen. Insoweit haben Sie ggf. vorab die erforderlichen Einwilligungen oder Lizenzen von diesen Dritten einzuholen.

## 7 Bekannte Einschränkungen

d.velop pilot unterliegt den folgenden Einschränkungen:

- Temporäre Ausfälle / Rate Limits – Die Nutzung der angebundenen LLM-Dienste (OpenAI / Aleph Alpha) unterliegt Einschränkungen hinsichtlich der maximalen Anzahl pro Minute verarbeiteter Daten. Diese Einschränkungen können vorübergehend dazu führen, dass einzelne Anfragen nicht korrekt verarbeitet werden bzw. kein Ergebnis liefern.
- Lange Antwortzeiten – LLMs basieren auf sehr aufwändigen Berechnungen. Daher kann es zu Wartezeiten von 20-30s für einzelne Anfragen kommen.
- Timeouts – Jenseits dieser Wartezeiten kann die Verarbeitung langer Dokumente zu Timeouts führen. In diesen Fällen erhalten Sie im Chat keine Antwort. Einzelne Ergebnisse in der LLM-Kontextaktion stehen vorübergehend nicht zur Verfügung.
- Halluzination – In bestimmten Fällen kann es nicht-deterministisch dazu kommen, dass die zu Grunde liegenden LLMs Informationen erfinden. Dieses „Halluzination“ genannte Problem stellt eine prinzipielle Einschränkung aktueller LLMs dar.
- Training Cutoff – Die zu Grunde liegenden LLMs integrieren Trainingsdaten bis zu einem gewissen Zeitpunkt. Sie sind daher nicht in der Lage, Ihre Daten mit aktuellen Informationen zu vernetzen. Dies stellt eine prinzipielle Einschränkung der verwendeten LLMs dar.