reflact AI Engine und ergänzende Bausteine und Services

Status compliance-relevanter Aspekte insbesondere im Hinblick auf Datenschutz und -sicherheit

Version 3.0 (Stand September 2025)

Inhalt

Änderungen gegenüber der letzten Version:

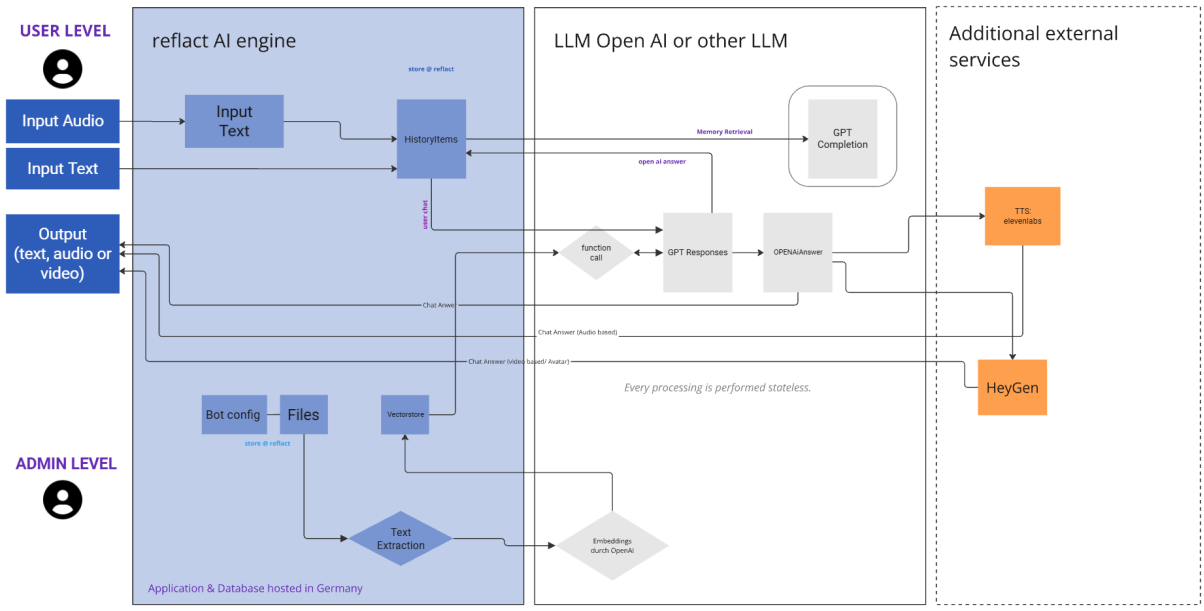
- Anpassung der LLM-API auf die Response API bei OpenAI
- Ergänzung der verfügbaren LLM-Modelle in der reflact AI engine
- Aufnahme von elevenlabs als zusätzlicher Service

Teil 1: Technischer Aufbau der reflact AI Engine und der ergänzenden Ebenen

Bei den von uns bereitgestellten KI-integrierenden Lösungen spielen drei nachstehend beschriebene Ebenen zusammen.

Ebene 1: reflact AI Engine

Die reflact AI Engine ist eine von der reflact AG entwickelte webbasierte Applikation, die es erlaubt, Bots bzw. Agenten zu entwickeln und in z.B. Digital Learning Angebote zu integrieren. Die Applikation wird von der reflact AG gehostet und betrieben und entspricht dem Konzept der **Retrieval Augmented Generation**:



Das Rechenzentrum, in dem die Applikation gehostet wird, ist ISO 27001 zertifiziert und befindet sich in Deutschland. Für eine optimale Performance des Systems ist das Datenbankmanagementsystem in eine Amazon Webservice basierte Umgebung der Firma Mongo (MongoDB Atlas) ebenfalls mit Datenstandort Deutschland ausgelagert.

Ebene 2: Der wichtige Basis-Baustein "Das Large Language Modell (LLM)"

Die reflact AI Engine setzt derzeit auf den aktuellen Large Language Modellen des Anbieters OpenAI auf. Derzeit können mittels der reflact AI Engine GPT 4 turbo, GPT 4o, GPT 4o mini, GPT 4.1, GPT 4.1 mini, GPT 4.1 nano, GPT 5, GPT 5 mini und GPT 5 nano sowie ausgewählte lokal bei reflact laufende LLMs über die entsprechenden APIs genutzt werden. Darüber hinaus kann über einen vorhandenen API-Key ein ChatGPT Account des Kunden direkt eingebunden werden. Es ist das erklärte Ziel der reflact, zukünftig auch andere LLMs mit der reflact AI Engine zu verbinden.

Die Art und Weise, wie der Rückgriff auf das LLM über APIs organisiert ist, stellt sicher, dass weder bereitgestellte Dokumente, noch die Prompts (Anweisungen) oder die Chat-Dialoge selbst zum Training des LLMs genutzt werden bzw. beim LLM-Anbieter gespeichert werden.

Die von uns verfolgte konkrete Realisation entspricht dem Konzept der sogenannten Retrieval Augmented Generation (RAG) und eröffnet damit grundsätzlich vielfältige Möglichkeiten zur Handhabung von datenschutzrelevanten Belangen. Das Datenflussmodell dazu ist bereits oben beschrieben.

Entscheidende, zusätzliche datenschutz-relevante Optionen stellt die reflact AI Engine ihrerseits bereit. So werden auch hohe Erwartungen - die sich aus den DSGVO-Regelungen oder solchen des EU-AI-Acts ergeben - ebenso handhabbar, wie wichtige Anforderungen aus Sicht vertraulicher Informationen und Inhalte.

Zu nennen sind hier explizit folgende reflact AI Engine Funktionen:

- Differenziertes **Rechte- und Rollen-Konzept** in der Administration der Bots, das sicherstellt, dass die Grundentscheidungen, z.B. kein Userdaten zum Training der KI, nicht absichtlich oder unabsichtlich verändert werden können.
- **Sofortige Löschung** der LLM-Anfragen bzw. Wahlmöglichkeit des Speicherzeitraums: Speicherung von Eingabe- und Ausgabe-Informationen in der reflact-Infrastruktur, sofortige Löschung der verarbeiteten Anfragen (z.B. zum sprachbasierten Generieren einer Antwort auf die Nutzerfrage) auf LLM Seite zum Session-Ende (auf Kundenwunsch Speicherung z.B. für verbesserte User Experience möglich). Die Art und Weise der Implementierung garantiert zudem, dass keine Inhalte zum Training des Modells verwendet werden.
- Ein differenziertes Konzept zur **Pseudonymisierung** der User ID gewährleistet, dass – sofern erforderlich – die Identifizierbarkeit einzelner Nutzerinteraktionen ausgeschlossen wird.
- **Word-Replacement**, Stop-Word-Listen, etc. erlauben besondere sicherheitsrelevante Einstellungen (z.B. keine Produktnennungen).
- Möglichkeiten der didaktisch-mitnehmenden und **compliance-sicheren** Hinführung und **Unterweisung** der End-Nutzer z.B. über editierbare Disclaimer, aber auch der Bot-Autoren und -Administratoren.
- **Transparenz-Funktionen** bezüglich des Weges, auf dem eine reflact AI Engine generierte Bot-Antwort entsteht, ebenso wie die Dokumentation z.B. von Zugriffen und die Etablierung entsprechender Löschregeln.
- **Speicherung** von unternehmensspezifischen Informationen über **Dokumente oder** sog. „**Wissensdatenbanken**“, ein reflact AI Engine Werkzeug - in der Anbieterlandschaft einzigartig.

Je nach angestrebtem Compliance-Ziel lassen sich zusätzliche Einstellungen in der Engine direkt und mittelbar via der ChatGPT-APIs vornehmen. Das Team der reflact AG erweitert die diesbezüglichen Möglichkeiten kontinuierlich.

Last but not least befähigt und begleitet die reflact AG ihre Kunden in der compliance-gerechten Nutzung der reflact AI Engine. So lassen sich die differenzierten Compliance-Ziele im konkreten Projekt gemeinsam erreichen.

Ebene 3: Ergänzende Bausteine („Karosserie-Elemente“)

Bots, die mithilfe der reflact AI Engine erstellt werden, können entweder direkt veröffentlicht und z.B. als SCORM-Objekt in ein Learning Management System eingebunden werden. Alternativ

können sie aber auch in andere Lernformate, d.h. ergänzende Bausteine zur Unterstützung spezifischer Nutzungsszenarien, integriert werden.

Diese Bausteine - wir sprechen oft von "Karosserie" - können durch die reflact AG selbst entwickelt oder als Fremdservices eingebunden sein. Ein Beispiel für eine reflact entwickelte Lösung ist z.B. das reflact Lerner-Cockpit als Rahmen oder ein Articulate 360 oder Adobe Captivate Training, für das die reflact AG eine eigene Integrationslösung entwickelt hat. In diesen Fällen besteht die Kommunikation zwischen den Bot-Inhalten und dem Nutzer über die reflact AI Engine. Interaktionen und Ergebnisse werden ausschließlich in der Engine gespeichert und verarbeitet. Teile der Interaktionen können über Javascript-Befehle wiederum an die SCORM-Schnittstelle übergeben werden, wie z.B. Content completed.

Im Falle von Fremdsystemen (z.B. Anbindung über APIs) sind die für diesen Service jeweils gültigen datenschutz- und datensicherheits-relevanten Regelungen maßgebend. Die reflact AG übernimmt keine Haftung, ist jedoch bemüht, durch Vor-Prüfung die grundsätzliche Eignung für den Enterprise-Kontext einzuschätzen.

Teil 2: Rechtliche Grundlagen für Datenschutz und Datensicherheit im Überblick

Verzeichnis von Verarbeitungstätigkeiten (VVT)

Die reflact führt ein Verzeichnis zu Verarbeitungstätigkeiten inklusive der jeweiligen Vereinbarungen zur Auftragsvereinbarung mit den genutzten Services. Zudem werden dort notwendige SCC (Standardvertragsklauseln) sowie der – sofern vorhanden - TIA (Transfer Impact Assessment) hinterlegt.

Die Datenschutz-Grundverordnung (DSGVO)

Als Anbieter der reflact AI Engine und ihrer ergänzenden Bausteine und zugehörigen Services, legen wir größten Wert auf die Einhaltung der Datenschutz-Grundverordnung (DSGVO). Unsere Lösung ist – so verdeutlichen es die in Teil 1 gegebenen Informationen zu den System-Ebenen einschließlich der gegebenen Konfigurations-Optionen – in jederlei Hinsicht geeignet, einen DSGVO-konformen Betrieb sicherzustellen.

Auch höchste Erwartungen in Bezug Aspekte von der Datenminimierung und Zweckbindung, über die Consent-Steuerung und Transparenz bis hin zu Anonymisierungsoptionen und weiteren Aspekten der Datensicherheit, werden in den KI-Projekten auf Basis der reflact AI Engine mit Blick auf den Schutz der personenbezogenen Daten unserer Kunden erfüllt.

Details im Abschnitt - "3.2. DSGVO konforme System und Prozesse unter Einsatz der reflact AI Engine".

Für die kundeninterne **Datenschutz-Folgenabschätzung (DSFA)** zur Identifikation und Handhabung potenziell hoher Risiken bei der Datenverarbeitung in Verbindung mit dem **neuen EU AI Act** empfehlen wir Folgendes:

- Eine DSFA nach DSGVO (insb. §35) und die Berücksichtigung des jüngst in Kraft getretenen EU AI Act sind von entscheidender Bedeutung zur Handhabung von Systemen, die ein hohes Risiko bei der Verarbeitung von personenbezogenen Daten vermuten lassen. So ist eine DSFA z.B. immer dann durchzuführen, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgt. Als besonders problematisch sind Konstellationen anzusehen, bei denen eine automatisierte Verarbeitung inklusive eines Profilings zur Grundlage für Entscheidungen mit Rechtswirkung für die natürliche Person werden.
- Die reflact AG wird Kunden, die potenziell riskante Nutzungsszenarien anstreben, auf die notwendige DSFA und die damit verbundenen Risiken hinweisen.
- Nach sorgfältiger Analyse der Verarbeitungsvorgänge sowie der Bewertung in Bezug auf Notwendigkeit, Verhältnismäßigkeit und etwaigen Risiken sind wir zur Einschätzung gekommen, dass bei den mit der AI Engine und ihren ergänzenden Bausteinen angestrebten Lösungen kein zusätzlicher Handlungsbedarf besteht. Gerade im Haupteinsatzfeld der reflact AI Engine - dem Lernen und Informieren - und den dabei durch die Engine geleisteten Unterstützungs- und Coachingbeiträge verbergen sich keine besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen.

Details im Abschnitt – „3.3. Datenschutz-Folgenabschätzung (DSFA) und Berücksichtigung des EU AI Act“

Vereinbarung zur Auftragsverarbeitung (AVV) mit unseren Kunden

Mit jedem unserer Kunden, der die reflact AI Engine über einen ersten Piloteinsatz hinaus einsetzen möchte, schließen wir eine Vereinbarung zur Auftragsverarbeitung ab.

Teil 3: Spezifische Aspekte und Dokumentationen im Fokus

3.1 Die Enterprise-Applikation reflact AI Engine

Die Entwicklung und Maintenance der reflact AI Engine erfolgt durch das erfahrene Entwickler- und Infrastruktur-Team der reflact AG entsprechend höchster Enterprise Standards.

Dazu gehören:

- **Sicherheitsmaßnahmen**: Unsere technischen und organisatorischen Maßnahmen (TOMs) gewährleisten dabei den umfassenden Schutz sensibler Daten. Dies umfasst verschlüsselte Datenübertragung, regelmäßige Sicherheitsüberprüfungen und den Einsatz von mehrstufigen Authentifizierungsprozessen.

- **Verfügbarkeitsmanagement**: Das Verfügbarkeits- und Disaster-Management (VDO) stellt sicher, dass die AI-Engine robust und zuverlässig bleibt. Regelmäßige Backups und Wiederherstellungspläne minimieren Ausfallzeiten und garantieren eine sehr gute

Systemverfügbarkeit.

- **Skalierbarkeit und Performance**: Die Architektur der AI-Engine ist darauf ausgelegt, flexibel auf wachsende Anforderungen zu reagieren. Durch kontinuierliche Performance-Optimierungen und skalierbare Infrastruktur können wir jederzeit hohe Verarbeitungsvolumina bewältigen, ohne die Systemleistung zu beeinträchtigen.

- **Kundenspezifische Anpassungen**: Wir bieten maßgeschneiderte Lösungen, die auf die spezifischen Anforderungen unserer Kunden zugeschnitten sind. Ob die Integration in bestehende Systeme oder Erweiterungen der Funktionalität – unser Team setzt individuelle Kundenwünsche mit höchster Präzision um.

- **Support und Monitoring**: Unser Support-Team überwacht die AI-Engine und steht für schnelle Problemlösungen bereit. Proaktive Überwachungssysteme identifizieren potenzielle Probleme frühzeitig und ermöglichen es uns, präventiv zu handeln, bevor es zu Beeinträchtigungen kommt.

- **Zukunftssicherheit**: Die kontinuierliche Anpassung an sich ändernde Marktanforderungen und technologische Entwicklungen gewährleistet, dass unsere AI-Engine stets auf dem neuesten Stand bleibt und auch langfristig konkurrenzfähig ist.

- Das Hosting der Applikation selbst erfolgt in der **ISO27001-zertifizierten Umgebung** der Hetzner Online GmbH.

3.2. DSGVO-konforme System und Prozesse unter Einsatz der reflact AI Engine

Als Anbieter eines KI-Systems, das auf der RAG-Logik (Retriever-Augmented Generation) unter Rückgriff auf die Services von OpenAI, legen wir größten Wert auf die Einhaltung der Datenschutz-Grundverordnung (DSGVO) und anderer rechtlicher Grundlagen, wie in diesem Dokument geschrieben. U.a. im Rückgriff auf die in Teil 1 beschriebenen Funktionen der reflact AI Engine und ihrer zusätzlichen Bausteine, sind wir in der Lage, für uns selbst und unseren Kunden eine DSGVO-konforme Arbeit zu ermöglichen und so zum wichtigen Schutz personenbezogenen Daten beizutragen.

Explizit möchten wir zusammenfassen:

1. Datenminimierung und Zweckbindung:

Wir verarbeiten nur die absolut notwendigen Daten, die für die Beantwortung Ihrer Anfragen erforderlich sind. Dabei achten wir darauf, dass alle Daten ausschließlich für den klar definierten Zweck genutzt werden, den wir Ihnen transparent kommunizieren.

2. Einwilligung und Rechtsgrundlage:

- Unsere Datenverarbeitung stützt sich auf klare rechtliche Grundlagen, wie die Erfüllung eines Vertrags oder / und die explizite Einwilligung durch den Kunden.

- Für jede Verarbeitung personenbezogener Daten, insb. wenn diese über das notwendige Maß hinausgeht, holen wir eine ausdrückliche Einwilligung bzw. einen Auftragsverarbeitungsvertrag bei unseren Kunden ein.
- Die Einwilligung vor der Nutzung eines reflact AI Engine basierten Bots kann unmittelbar im System oder in einem vorgelagerten Schritt (z.B. Einbindung eines LMS oder eines Learner Cockpits) erfolgen, sofern dies im Kundenprozess sinnvoll ist.

3. Transparenz und Information der Betroffenen:

- Unsere Kunden werden umfassend und in verständlicher Form darüber informiert, welche Daten wir erheben und wie diese verwendet werden.
- Wir bieten den Kunden jederzeit die Möglichkeit, ihre Daten einzusehen, zu korrigieren oder deren Löschung zu verlangen, um so die Rechte der Kunden als Betroffene vollumfänglich zu wahren.

4. Anonymisierung und Pseudonymisierung:

Wo immer möglich, anonymisieren wir personenbezogene Daten, sodass keine Rückschlüsse auf Einzelpersonen gezogen werden können. Sollte eine Anonymisierung nicht machbar sein, setzen wir auf weitere Maßnahmen wie z.B. eine Pseudonymisierung, um das Risiko der Re-Identifizierung zu minimieren.

5. Datensicherheit:

- Wir haben umfassende technische und organisatorische Maßnahmen ergriffen, um die Sicherheit Ihrer Daten zu gewährleisten. Dazu gehören Verschlüsselung, strenge Zugriffskontrollen und regelmäßige Überprüfungen unserer Sicherheitsprozesse.
- Der Zugang zu Ihren Daten ist streng limitiert und nur autorisierten Personen vorbehalten, um maximale Sicherheit zu gewährleisten.

Mit diesen Maßnahmen stellen wir sicher, dass die – über die reflact AI Engine realisierte Nutzung von ChatGPT folgend der RAG-Logik vollständig DSGVO-konform erfolgt und die Datenschutzrechte gewahrt sind.

3.3. Datenschutz-Folgenabschätzung (DSFA) und Berücksichtigung des EU AI Act

- Im Rahmen der Bereitstellung unserer reflact AI Engine einschließlich ihrer ergänzenden Bausteine und Services haben wir eine umfassende Datenschutz-Folgenabschätzung (DSFA) durchgeführt.
- Ziel dieser DSFA war es, mögliche Risiken für die Rechte und Freiheiten der betroffenen Personen, insbesondere im Hinblick auf die Verarbeitung personenbezogener Daten, zu identifizieren und zu bewerten. Darüber hinaus haben wir die Anforderungen des neuen

EU AI Act in unsere Überlegungen einbezogen, um sicherzustellen, dass unsere Anwendung den höchsten ethischen und rechtlichen Standards entspricht.

- Bei der Bewertung des Risikoprofils unserer Applikation sind wir zum Schluss gekommen, dass die über das System abgebildeten Unterstützungs- und Coaching-Funktionen als nicht hochrisikorelevant einzustufen sind. Diese Einschätzung beruht unter anderem darauf, dass diese Funktionen keine Entscheidungen von erheblicher rechtlicher oder ähnlicher Bedeutung für die betroffenen Personen treffen, wie es etwa bei automatisierten Entscheidungsprozessen in Bereichen wie Kreditvergabe, Strafverfolgung oder Gesundheitsversorgung der Fall wäre. Stattdessen dienen die Unterstützungs- und Coaching-Funktionen primär der Optimierung von Informations- und Lernprozessen und der Unterstützung der Anwender, ohne dabei tiefgreifende Eingriffe in persönliche oder sensible Bereiche vorzunehmen.

- Durch die Implementierung von angemessenen technischen und organisatorischen Maßnahmen, die auf die generelle Wahrung der Datenschutzinteressen der NutzerInnen abzielt, aber auch die entsprechende Sensibilisierung und Unterweisung der für die Art der Nutzung auschlaggebenden und verantwortlichen Auftraggeber (konkret der Administratoren und Trainer) stellen wir sicher, dass ein hohes Datenschutzniveau gewahrt bleibt und dass kein erhöhtes Risiko für die Rechte und Freiheiten der NutzerInnen entstehen kann.

- Nach sorgfältiger Prüfung und Analyse aller relevanten Datenverarbeitungsprozesse, unter Berücksichtigung der geltenden Datenschutzvorschriften, insbesondere der Datenschutz-Grundverordnung (DSGVO), sowie der Bestimmungen des EU AI Act, sind wir zu dem Schluss gekommen, dass keine weiteren Maßnahmen zur Risikominderung erforderlich sind. Die von uns getroffenen technischen und organisatorischen Maßnahmen gewährleisten ein angemessenes Schutzniveau für die Daten unserer Kunden und erfüllen gleichzeitig die Vorgaben des EU AI Act.

- Wir werden die datenschutzrechtlichen Rahmenbedingungen sowie die Anforderungen des EU AI Act sowie neue rechtliche Regelungen weiterhin regelmäßig überprüfen und sicherstellen, dass unsere Applikation stets den höchsten Standards des Datenschutzes und der ethischen Nutzung von KI entspricht.

reflact AG
September 2025