

ACADEX

Technische und organisatorische Maßnahmen

gemäß Art. 32 DSGVO

Version 1.0

Stand: 28. September 2026

Arbeitsfassung

Acadex Solutions UG (haftungsbeschränkt)

Reuterweg 5 · 49637 Menslage · Deutschland

Hinweis zur Arbeitsfassung

Diese Fassung bildet den für die Veröffentlichung vorgesehenen technischen Ist-Zustand ab. Geplante oder noch nicht vollständig umgesetzte Maßnahmen werden nicht als bestehende Maßnahmen formuliert. Die beschriebenen serverseitigen Website-Statistiken und Product Metrics werden in dieser Fassung als implementierter Release-Zustand zugrunde gelegt. Vor vertraglicher Verwendung sollte das Dokument rechtlich geprüft werden.

1. Zweck und Geltungsbereich

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen, die Acadex zum Schutz personenbezogener Daten im Rahmen der Verarbeitung über die Acadex-Plattform einsetzt.

Die Maßnahmen dienen insbesondere dazu, ein dem jeweiligen Risiko angemessenes Schutzniveau hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der eingesetzten Systeme und Dienste sicherzustellen.

Die beschriebenen Maßnahmen beziehen sich auf den aktuellen technischen und organisatorischen Stand des Dienstes. Maßnahmen, die lediglich geplant oder noch nicht vollständig umgesetzt sind, werden nicht als bestehende Schutzmaßnahmen aufgeführt.

Die konkrete Verarbeitung kann abhängig von der Konfiguration des jeweiligen Accounts oder der jeweiligen Institution variieren. Dies betrifft insbesondere die Auswahl externer Modellanbieter und die damit verbundenen Verarbeitungsorte.

2. Vertraulichkeit

2.1 Administrative Zugriffe

Der administrative Zugriff auf die Produktivsysteme ist auf die technische Leitung sowie gegebenenfalls weitere Personen beschränkt, die diesen Zugriff für ihre jeweilige Aufgabe benötigen.

Der administrative Zugriff auf Server erfolgt ausschließlich über SSH unter Verwendung personenbezogener kryptografischer Schlüssel. Eine passwortbasierte SSH-Anmeldung ist deaktiviert.

Administrative Benutzerkonten werden personenbezogen vergeben und nicht zwischen mehreren Personen geteilt. Berechtigungen werden nur entsprechend des betrieblichen Bedarfs vergeben.

Die für Hosting, Serveradministration und Quellcodeverwaltung verwendeten administrativen Konten bei STRATO, Plesk und GitHub sind durch Multi-Faktor-Authentifizierung geschützt.

Administrative Tätigkeiten und produktive Deployments werden derzeit durch die technische Leitung durchgeführt.

2.2 Authentifizierung von Nutzenden

Nutzerkonten werden derzeit über E-Mail-Adresse und Passwort authentifiziert.

Passwörter werden nicht im Klartext gespeichert, sondern ausschließlich mithilfe von Argon2id gehasht.

Für authentifizierte Zugriffe auf die Anwendung werden kurzlebige, kryptografisch signierte Zugriffstoken verwendet.

Persönliche Zugänge werden jeweils einer einzelnen Person zugeordnet. Gespräche, Erinnerungen, Watchlists, Dokumente und weitere personenbezogene Inhalte werden dem jeweiligen Account zugeordnet.

2.3 Verschlüsselung bei der Übertragung

Verbindungen zwischen Clients und Acadex sowie zwischen Acadex und angebundenen Auftragsverarbeitern werden über verschlüsselte Transportverbindungen auf Basis von TLS hergestellt.

Unverschlüsselte Übertragungen personenbezogener Anwendungsdaten sind für den regulären Betrieb nicht vorgesehen.

2.4 Verschlüsselung gespeicherter Inhalte

Folgende Inhaltsdaten werden innerhalb der Anwendungsdatenbank mittels AES-256-GCM verschlüsselt:

- Gesprächsinhalte
- gespeicherte Erinnerungen
- Inhalte hochgeladener Dokumente
- Chat-Titel
- die zu einzelnen Verarbeitungsvorgängen gespeicherten Anfrageinhalte

Für jeden Verschlüsselungsvorgang wird ein eigener Nonce verwendet.

Der zur Entschlüsselung erforderliche Schlüssel wird getrennt von der Anwendungsdatenbank aufbewahrt.

Eine isolierte Kopie der Anwendungsdatenbank enthält damit nicht alle zur Entschlüsselung dieser Inhalte erforderlichen Informationen.

2.5 Verwaltung von Geheimnissen und Zugangsdaten

Dauerhaft benötigte Zugangsdaten, API-Schlüssel und kryptografische Geheimnisse werden nicht im Quellcode hinterlegt.

Sie werden in einem ausschließlich hierfür verwendeten, verschlüsselten Passwortmanager verwahrt. Das für dessen Zugriff erforderliche Schlüsselmaterial wird auf einem getrennten physischen Medium aufbewahrt; eine gesicherte Kopie dieses Schlüsselmaterials ist vorhanden.

Für den laufenden Betrieb werden benötigte Geheimnisse durch die technische Leitung zur Laufzeit als Umgebungsvariablen bereitgestellt.

Der Zugriff auf diese Geheimnisse ist derzeit auf die technische Leitung beschränkt.

Secrets und Zugangsdaten werden ungefähr alle drei Monate sowie anlassbezogen rotiert, insbesondere wenn ein Verlust ihrer Vertraulichkeit vermutet oder festgestellt wird.

2.6 Nicht in gleicher Weise verschlüsselte Daten

Nicht alle gespeicherten Informationen können auf Anwendungsebene mit derselben Verschlüsselung versehen werden.

Insbesondere muss der Text, der für die semantische Suche innerhalb gespeicherter Erinnerungen verwendet wird, maschinell durchsuchbar bleiben und wird daher derzeit nicht mit derselben feldweisen AES-256-GCM-Verschlüsselung gespeichert.

Ebenfalls nicht mit dieser feldweisen Inhaltsverschlüsselung geschützt werden insbesondere öffentliche bibliografische Datensätze, technische Identifikatoren, Zeitstempel sowie für den Betrieb erforderliche Metadaten.

3. Trennung und Zugriffskontrolle

3.1 Trennung personenbezogener Inhalte nach Accounts

Personenbezogene Inhalte werden einem konkreten Nutzeraccount zugeordnet.

Datenbankabfragen, die auf nutzerspezifische Inhalte zugreifen, werden auf den jeweiligen Account beschränkt.

Persönliche Zugänge innerhalb institutioneller Accounts teilen nicht automatisch Gespräche, Erinnerungen oder Watchlists miteinander.

3.2 Trennung der Systemumgebungen

Produktions-, Entwicklungs- und Testumgebungen verwenden voneinander getrennte Datenbanken.

Produktionsdaten werden nicht regulär zur Befüllung von Entwicklungs- oder Testumgebungen verwendet.

3.3 Netzwerkseitige Trennung

Anwendung, Datenbank, Cache, Suchindex und interne Inferenzdienste werden in voneinander isolierten Containern innerhalb eines privaten Netzwerks betrieben.

Von außen erreichbar ist ausschließlich die hierfür vorgesehene Zugriffsschicht beziehungsweise der Reverse Proxy.

Interne Dienste werden nicht unmittelbar dem öffentlichen Netzwerk ausgesetzt.

4. Begrenzung externer Verarbeitung

4.1 Datenminimierung bei externen Modellanbietern

Wenn für eine Anfrage ein externer Modellanbieter eingesetzt wird, werden nur die Informationen übertragen, die für die jeweilige Verarbeitung erforderlich sind.

Dazu können insbesondere gehören:

- die aktuelle Nutzereingabe
- relevanter Gesprächskontext
- für die Anfrage abgerufene Erinnerungen
- relevante bibliografische Informationen
- für die Bearbeitung erforderliche Dokumentinhalte

Die gesamte Datenhaltung eines Nutzeraccounts wird einem Modellanbieter nicht pauschal zur Verfügung gestellt.

4.2 Zulässige Modellanbieter

Acadex unterstützt direkte oder über kontrollierte Cloud-Pfade angebundene Modelle beziehungsweise APIs von Mistral, OpenAI, Anthropic und Google.

Welche Modellanbieter und Verarbeitungsprofile für einen Account verwendet werden dürfen, wird durch die jeweilige Konfiguration bestimmt.

Für institutionelle Accounts können dadurch insbesondere Vorgaben zum Verarbeitungsort oder zu zugelassenen Auftragsverarbeitern technisch umgesetzt werden.

Die technische Unterstützung eines Modellanbieters durch Acadex bedeutet nicht automatisch, dass dieser Anbieter personenbezogene Daten jedes Kunden verarbeitet.

4.3 Lokal ausgeführte Verarbeitung

Die Erzeugung von Embeddings erfolgt auf von Acadex kontrollierter Infrastruktur.

Die betreffenden Inhalte müssen hierfür nicht an einen externen Embedding-Anbieter übermittelt werden.

Weitere lokal ausgeführte Dienste werden entsprechend ihrer tatsächlichen Verarbeitung dokumentiert.

5. Integrität, Protokollierung und Nutzungsmetriken

5.1 Schutz vor unbeabsichtigten Änderungen

Zugriff auf personenbezogene Inhalte erfolgt über authentifizierte Anwendungs- und Administrationsschnittstellen.

Datenbankzugriffe aus der Anwendung werden innerhalb der jeweiligen Account- und Berechtigungskontexte ausgeführt.

5.2 Protokollierung und Fehleranalyse

Gesprächsinhalte werden nicht in operative Logs geschrieben.

Zur technischen Fehleranalyse können interne Nutzerkennungen protokolliert werden, damit Fehler einem konkreten Account oder Verarbeitungsvorgang zugeordnet werden können.

IP-Adressen werden im laufenden Betrieb zur Durchsetzung technischer Schutzmaßnahmen, insbesondere von Rate Limits, verarbeitet. Sie werden nicht zu Werbezwecken oder für Nutzerprofile verwendet.

Operative Logs verbleiben für sieben Tage auf dem jeweiligen Produktivsystem.

Anschließend werden erforderliche Logs komprimiert und verschlüsselt auf einen separaten Archivserver übertragen. Die archivierten Logs werden für höchstens drei Monate aufbewahrt und anschließend gelöscht.

Der Zugriff auf operative und archivierte Logs ist auf administrative Zugänge beschränkt.

5.3 Website-Statistiken

Acadex erstellt auf eigener Infrastruktur aggregierte Statistiken über Aufrufe ausgewählter Websitebereiche. Diese Auswertung dient der grundlegenden Reichweiten- und Produktsteuerung und wird ohne externen Analytics-Anbieter durchgeführt.

Für den Analytics-Datensatz werden insbesondere keine dauerhaften Besucherkennungen, Browser-Fingerprints, URL-Queryparameter, Suchbegriffe oder vollständigen Referrer-URLs gespeichert. Vollständige IP-Adressen werden nicht als dauerhafte Analytics-Merkmale übernommen.

Gezählt werden primär definierte Seiten beziehungsweise Seitenkategorien und Zeiträume. Die Nutzungsstatistik ist technisch und organisatorisch von den operativen Serverlogs getrennt.

5.4 Produktmetriken

Zur Beurteilung der grundlegenden Nutzung und wirtschaftlichen Entwicklung verarbeitet Acadex eine begrenzte Menge klar definierter Produkt- und Vertragszustände.

Dazu gehören insbesondere Registrierung, erstmalige erfolgreiche Nutzung einer zentralen Produktfunktion (Aktivierung), Beginn oder Wechsel eines Tarifs sowie Kündigung. Daraus können aggregierte Kennzahlen wie Aktivierungsrate, Conversion, Retention, Churn, MRR oder ARR gebildet werden.

Soweit möglich, werden diese Zustände aus bereits vorhandenen Account-, Vertrags-, Billing- oder Betriebsdaten abgeleitet. Eine zusätzliche umfassende Event-Tracking-Infrastruktur oder ein vollständiger Klickstream wird hierfür nicht betrieben.

5.5 Ausschluss von Inhaltsdaten

Für Product Analytics werden insbesondere nicht ausgewertet:

- Gesprächsinhalte und Nutzereingaben
- generierte Antworten
- Inhalte hochgeladener Dokumente
- gespeicherte Erinnerungen
- Forschungsthemen und bibliografische Suchbegriffe
- individuelle Klick- oder Navigationspfade

Die Trennung wird durch die Auswahl der erfassten Zustände und die Struktur der Metrikdaten umgesetzt.

5.6 Löschung und Aggregation von Product Metrics

Accountbezogene Product-Metric-Daten werden mit dem jeweiligen Account gelöscht, soweit keine abweichende gesetzliche Aufbewahrungspflicht oder ein anderer eigenständiger Verarbeitungszweck besteht.

Bereits erzeugte Statistiken können erhalten bleiben, sofern sie so aggregiert wurden, dass eine Zuordnung zu einzelnen Personen nicht mehr möglich ist.

Die langfristige statistische Auswertung erfolgt grundsätzlich auf Grundlage solcher aggregierten Kennzahlen.

5.7 Datenminimierung bei neuen Metriken

Bei der Einführung neuer Kennzahlen wird geprüft, ob die gewünschte Aussage ohne zusätzliche personenbezogene Ereignisdaten gewonnen werden kann. Soweit eine Kennzahl aus bestehenden Account-, Vertrags-, Billing- oder Betriebsdaten abgeleitet werden kann, wird diese Ableitung gegenüber der Einführung zusätzlicher Tracking-Ereignisse bevorzugt.

6. Löschung und Datenlebenszyklus

6.1 Primär- und Sekundärdaten

PostgreSQL dient als primärer Datenspeicher für nicht aus anderen Systemen rekonstruierbare Anwendungs- und Nutzerdaten.

Qdrant und Elasticsearch enthalten abgeleitete beziehungsweise indizierte Daten. Die dort gespeicherten Informationen können aus den jeweiligen Primärdaten erneut erzeugt werden.

Bibliografische Forschungsdaten können ebenfalls aus den verwendeten externen Datenquellen rekonstruiert werden.

Diese Unterscheidung wird bei Datensicherung, Wiederherstellung und Löschung berücksichtigt.

6.2 Löschung durch Nutzende

Nutzende können innerhalb der Anwendung einzelne Gespräche, Erinnerungen und hochgeladene Dokumente löschen, ohne hierzu den Support kontaktieren zu müssen.

6.3 Löschung eines Accounts

Bei Löschung eines Accounts werden die diesem Account zugeordneten Nutzerdaten einschließlich accountbezogener Product-Metric-Zustände aus den aktiven Anwendungssystemen entfernt, soweit keine gesetzliche Aufbewahrungspflicht oder ein anderer eigenständiger Verarbeitungszweck entgegensteht.

Die referenzielle Löschung innerhalb der relationalen Datenhaltung wird über Datenbankbeziehungen und kaskadierende Löschregeln umgesetzt und hängt nicht ausschließlich davon ab, dass der Anwendungscode jede betroffene Tabelle einzeln berücksichtigt.

Abgeleitete Nutzerdaten in Qdrant und Elasticsearch werden im Rahmen des Löschprozesses ebenfalls entfernt beziehungsweise aus dem verbleibenden Primärdatenbestand neu erzeugt.

6.4 Prüfung der Löschlogik

Das Datenbankschema wird automatisiert darauf geprüft, ob Tabellen mit nutzerbezogenen Daten von der vorgesehenen Löschlogik erfasst werden.

Wird eine entsprechende Tabelle ohne die erforderliche Einbindung erkannt, schlägt die Prüfung fehl.

6.5 Löschung aus Sicherungskopien

Bereits gelöschte Daten können bis zum Ablauf der jeweiligen Aufbewahrungsdauer noch in bestehenden Sicherungskopien enthalten sein.

Sicherungskopien werden nicht für den regulären Produktivbetrieb verwendet. Nach Ablauf ihrer vorgesehenen Aufbewahrungsfrist werden sie gelöscht beziehungsweise im Rahmen der Backup-Rotation ersetzt.

Eine Wiederherstellung aus einem älteren Backup führt nicht dazu, dass zwischenzeitlich wirksam gelöschte Daten dauerhaft erneut in den Produktivbetrieb übernommen werden.

7. Verfügbarkeit, Datensicherung und Wiederherstellung

7.1 Hosting

Die Produktivsysteme von Acadex werden auf Infrastruktur der STRATO GmbH in Deutschland betrieben.

Anwendung, Datenbank und die von Acadex gehaltenen Sicherungskopien werden auf Infrastruktur innerhalb Deutschlands betrieben.

7.2 Aktuelle Systemarchitektur

Die produktive Anwendung wird derzeit auf einer einzelnen Anwendungsinstanz betrieben.

Die Architektur ist technisch für den Betrieb mehrerer Instanzen vorbereitet. Eine produktive Hochverfügbarkeitskonfiguration ist derzeit jedoch nicht umgesetzt.

Der Ausfall dieser Instanz oder zentraler Infrastrukturkomponenten kann daher gegenwärtig zu einer Unterbrechung des Dienstes führen.

Eine garantierte Verfügbarkeit oder ein allgemeines Service Level Agreement wird derzeit nicht zugesagt.

7.3 Datensicherung nach Datenklassen

Acadex unterscheidet bei der Datensicherung zwischen primären Nutzerdaten und rekonstruierbaren Sekundär- beziehungsweise Forschungsdaten.

Nicht ohne Weiteres rekonstruierbare Nutzerdaten werden primär in PostgreSQL gespeichert und unabhängig vom vollständigen Forschungsdatenbestand gesichert.

Für PostgreSQL werden automatisierte Sicherungskopien in einem deutlich kürzeren Intervall als für den vollständigen Datenbestand erstellt.

Intervall der PostgreSQL-Sicherung: [EINTRAGEN]

Aufbewahrungsdauer der PostgreSQL-Sicherungen: [EINTRAGEN]

Vollständige Sicherungen des gesamten Datenbestands werden ungefähr quartalsweise erstellt.

Der vollständige Datenbestand umfasst mehr als 3 TB und besteht zu großen Teilen aus bibliografischen Daten, Suchindizes, Embeddings und weiteren Informationen, die aus Primärquellen oder den primären Anwendungsdaten rekonstruiert werden können.

Qdrant- und Elasticsearch-Daten sowie bibliografische Daten können daher bei Bedarf erneut aufgebaut beziehungsweise aus den zugrunde liegenden Quellen wiederhergestellt werden.

7.4 Wiederherstellung

Die Wiederherstellbarkeit der PostgreSQL-Sicherungen wird unabhängig von der Wiederherstellung des vollständigen Forschungsdatenbestands betrachtet.

Verfahren und Intervall für PostgreSQL-Restore-Tests: [EINTRAGEN]

Für die Wiederherstellung des vollständigen Datenbestands werden derzeit keine verbindlichen Recovery Time Objectives (RTO) oder Recovery Point Objectives (RPO) zugesagt.

7.5 Überwachung

Die Produktsysteme werden administrativ überwacht.

Ein automatisiertes externes Uptime-Monitoring mit Alarmierung ist derzeit nicht im Betrieb und wird daher in diesem Dokument nicht als implementierte Maßnahme beschrieben.

Zusätzliches strukturiertes Monitoring und Alerting ist geplant. Konkrete Umsetzung und betrieblicher Umfang: [EINTRAGEN]

8. Entwicklung und Deployment

Der Quellcode von Acadex wird über GitHub versioniert und in einem strukturierten Monorepository verwaltet.

Änderungen werden in separaten Entwicklungszweigen vorgenommen und über Pull Requests in die vorgesehenen Hauptzweige übernommen. Code Reviews sind Bestandteil des Entwicklungsprozesses.

Für die Anwendung bestehen automatisierte Unit Tests sowie für ausgewählte Funktionen User-Acceptance-Tests.

Eine CI/CD-Pipeline unterstützt Build, Test und Deployment.

Die produktiven Deployments werden derzeit durch die technische Leitung durchgeführt.

Die Anwendung wird containerisiert auf Basis von Docker betrieben.

Betriebssystemaktualisierungen werden über die Serververwaltungsumgebung Plesk verwaltet.

Updates von Docker-Images und darin enthaltenen Softwarekomponenten werden derzeit anlassbezogen vorgenommen.

9. Unterauftragsverarbeiter

Externe Dienstleister, die im Rahmen ihrer Tätigkeit personenbezogene Daten im Auftrag verarbeiten, werden entsprechend den datenschutzrechtlichen Anforderungen eingebunden.

Die jeweils eingesetzten Unterauftragsverarbeiter, deren Funktion und die relevanten Verarbeitungsorte werden separat dokumentiert.

Welche Modellanbieter tatsächlich personenbezogene Inhalte eines konkreten Accounts erhalten können, hängt von dessen Konfiguration ab.

Die Unterstützung eines Anbieters durch die Acadex-Plattform bedeutet nicht automatisch, dass dieser Anbieter Daten jedes Kunden verarbeitet.

Änderungen bei Unterauftragsverarbeitern erfolgen nach Maßgabe des Auftragsverarbeitungsvertrags.

10. Umgang mit Sicherheitsvorfällen

Für technische Sicherheitsvorfälle liegt die operative Verantwortung bei der technischen Leitung.

Die externe Kommunikation mit betroffenen Kunden oder Institutionen erfolgt in Abstimmung mit der für Kundenbetreuung zuständigen Person.

Wird Acadex im Rahmen einer Verarbeitung als Auftragsverarbeiter tätig und wird eine Verletzung des Schutzes personenbezogener Daten festgestellt, informiert Acadex den jeweiligen Verantwortlichen ohne unangemessene Verzögerung.

Acadex unterstützt den Verantwortlichen im Rahmen der verfügbaren Informationen bei der Bewertung und Dokumentation des Vorfalls sowie bei den daraus folgenden gesetzlichen Pflichten.

Für Sicherheitsvorfälle wird ein dokumentiertes Verfahren mit Zuständigkeiten für technische Eindämmung, Untersuchung, Dokumentation, Bewertung und Kommunikation geführt.

11. Überprüfung der Wirksamkeit

Die Wirksamkeit der Schutzmaßnahmen wird durch automatisierte technische Prüfungen und betriebliche Kontrollen überprüft.

Dazu gehören insbesondere:

- automatisierte Unit Tests
- ausgewählte User-Acceptance-Tests
- Code Reviews im Pull-Request-Prozess
- automatisierte Prüfung der Löschlogik im Datenbankschema
- Prüfung neuer Product Metrics auf Datenminimierung und Ausschluss von Inhaltsdaten
- technische Fehleranalyse anhand begrenzter Protokolldaten
- regelmäßige Rotation von Secrets und Zugangsdaten

- Multi-Faktor-Authentifizierung für administrative Plattformzugänge
- Prüfung der Wiederherstellbarkeit von Sicherungskopien; ein regelmäßiges PostgreSQL-Restore-Testverfahren wird gemäß Abschnitt 7.4 noch formalisiert

Die technischen und organisatorischen Maßnahmen werden darüber hinaus anlassbezogen nach wesentlichen Änderungen der Systemarchitektur oder relevanten Sicherheitsvorfällen überprüft. Ein fester regelmäßiger formaler Review-Prozess wird derzeit noch etabliert.

Regelmäßiger Review-Zyklus: [EINTRAGEN]

12. Dokumentpflege

Diese technischen und organisatorischen Maßnahmen werden getrennt vom Hauptvertrag versioniert, da sich technische Schutzmaßnahmen im Laufe des Betriebs weiterentwickeln können.

Änderungen werden dokumentiert.

Die jeweils für ein Vertragsverhältnis maßgebliche Fassung ergibt sich aus dem Auftragsverarbeitungsvertrag und der dort vereinbarten Einbeziehung dieser Anlage.

Hinweis: Diese Arbeitsfassung ersetzt keine individuelle rechtliche Beratung. Vor Einbeziehung in Kundenverträge sollten die finalen Maßnahmen und Formulierungen juristisch geprüft werden.