Sicherheits-Whitepaper

Enterprise-Grade Datenschutz und Informationssicherheit

Plattform: Review
Version: 1.0
Datum: Januar 2025

Zielgruppe
IT-Entscheidungsträger, Sicherheitsverantwortliche, Datenschutz- und Compliance-Teams

Dieses Dokument unterliegt der Versionskontrolle und beschreibt den aktuellen Stand der Sicherheitsarchitektur.

Wichtiger Hinweis

Dieses Dokument beschreibt die Sicherheits- und Datenschutzarchitektur der Plattform in aggregierter Form. Es hat keinen Anspruch auf Vollständigkeit und eingesetzte Sicherheitsmechanismen können sich kontinuierlich ändern.

Standards und Compliance

Unsere Sicherheitsmaßnahmen orientieren sich an internationalen Standards:

- **ISO/IEC 27001:** Informationssicherheits-Managementsysteme
- **SOC 2 Type II:** Service Organization Control 2
- **OWASP Top 10:** Web Application Security Best Practices
- **DSGVO:** Datenschutz-Grundverordnung (EU)
- **NIST Cybersecurity Framework:** Cybersecurity Best Practices
- **CIS Controls:** Center for Internet Security Controls

Inhaltsverzeichnis

1 Dokumentkontrolle

Dieses Whitepaper ist Bestandteil der technischen Dokumentation der Plattform. Änderungen werden versioniert und nachvollziehbar dokumentiert.

Version	Datum	Änderungen
1.0	Januar 2025	Erstveröffentlichung

Geltungsbereich

Der Geltungsbereich umfasst die Web-Anwendung, die dazugehörigen API-Endpunkte sowie die dokumentenverarbeitenden Services, die in einer cloudbasierten, mandantenfähigen Architektur betrieben werden. Das Dokument adressiert technische und organisatorische Maßnahmen zur Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Informationen.

2 Executive Summary

Dieses Sicherheits-Whitepaper beschreibt die technische Sicherheitsarchitektur und die datenschutzrelevanten Kontrollen der Plattform „Review" für die Verarbeitung geschäftskritischer Dokumente. Der Fokus liegt auf der Absicherung des gesamten Datenlebenszyklus – von der Aufnahme und Validierung hochgeladener Dateien über die isolierte Verarbeitung bis zur kontrollierten Bereitstellung von Ergebnissen.

Die Plattform ist nach dem Prinzip „Security by Design" aufgebaut. Sicherheitskontrollen werden nicht als nachgelagerte Maßnahme betrachtet, sondern sind integraler Bestandteil der Architektur, der Entwicklungsprozesse sowie des Betriebs. Die Umsetzung folgt etablierten Sicherheitsprinzipien wie „Least Privilege", „Defense in Depth" und „Secure Defaults" und orientiert sich an anerkannten Rahmenwerken (u. a. ISO/IEC 27001, NIST CSF, OWASP ASVS).

Die Plattform wird in einer modernen Cloud-Umgebung betrieben. Die Architektur trennt Frontend, Identitäts-/Datenebene und Verarbeitungsschicht, was eine klar segmentierte Sicherheitsdomäne pro Schicht ermöglicht und dadurch die Angriffsfläche reduziert.

Wir arbeiten ausschließlich mit führenden Cloud-Providern zusammen, die höchste Sicherheitsstandards einhalten und umfassend zertifiziert sind. Alle unsere Infrastruktur-Partner verfügen über umfassende Zertifizierungen, einschließlich SOC 2 Type II sowie DSGVO-Konformität, und unterliegen regelmäßigen externen Sicherheitsaudits. Cloud-Provider verfügen zusätzlich über ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018.

3 Architekturprinzipien

Die Sicherheitsarchitektur folgt einem mehrschichtigen Schutzkonzept. Maßnahmen auf Netzwerk-, Identitäts-, Daten- und Anwendungsebene greifen ineinander und sind so ausgelegt, dass der Ausfall oder die Umgehung einer einzelnen Kontrolle nicht zu einem vollständigen Sicherheitsverlust führt.

- **Zero Trust:** Standardannahmen entsprechen einem „Zero Trust"-Modell: Jede Anfrage wird als potenziell untrusted betrachtet, unabhängig davon, ob sie aus dem internen oder externen Netz kommt. Identität, Kontext und Berechtigungen werden pro Request verifiziert, und sensitive Operationen sind zusätzlich durch explizite Autorisierungsprüfungen abgesichert.

- **Sichere Voreinstellungen:** Die Plattform setzt auf sichere Voreinstellungen. Funktionen, die Daten exponieren (z. B. Dateiabrufe, Link-Sharing, Exportfunktionen), sind per Default restriktiv konfiguriert und erfordern explizite Freigaben. Konfigurationsabweichungen werden als Ausnahme behandelt und sind nachvollziehbar dokumentiert.
- **Defense in Depth:** Wir implementieren eine mehrschichtige Verteidigungsstrategie, die mehrere unabhängige Sicherheitsebenen umfasst. Perimeter-Schutz auf Netzwerk- und API-Ebene, Authentifizierung und Autorisierung für Identitäts- und Zugriffskontrolle, Datenverschlüsselung zum Schutz ruhender und übertragener Daten, Input-Validierung zum Schutz vor Angriffen, Fehlerbehandlung zur Verhinderung von Informationsleckage sowie Monitoring zur Früherkennung von Sicherheitsvorfällen.

4 Systemüberblick und Datenfluss

Die Plattform verarbeitet Dokumente in einem strukturierten, kontrollierten Prozess. Ziel ist eine nachvollziehbare und auditierbare Verarbeitung, bei der jede Datenbewegung einer kontrollierten Sicherheitsdomäne zugeordnet werden kann.

4.1 Komponentenübersicht

Die Web-Anwendung wird über ein modernes Edge-Netzwerk ausgeliefert, das die sichere Auslieferung statischer und dynamischer Frontend-Artefakte, TLS-Terminierung sowie Edge-nahe Performance-Optimierungen übernimmt. Sicherheitsrelevante Konfigurationen (z. B. Strict-Transport-Security, Content-Security-Policy) werden in der Delivery-Schicht verankert.

Die Identitäts- und Datenebene stellt Authentifizierung, Organisations- und Rollenmodell sowie relationale Datenpersistenz bereit. Zugriffskontrollen werden konsequent serverseitig durchgesetzt. Die Verarbeitung erfolgt in isolierten Containern, die elastische Skalierung bei gleichzeitiger Begrenzung von Ressourcen ermöglichen.

Für Dateiobjekte und temporäre Artefakte wird ein cloudbasierter Objektspeicher eingesetzt. Dateien werden in logisch getrennten Namensräumen pro Organisation abgelegt, wobei eine strikte Isolation sicherstellt, dass keine Cross-Organization-Zugriffe möglich sind.

4.2 Datenfluss im Detail

Nach dem Upload eines Dokuments wird die Datei zunächst serverseitig validiert (Format, Integrität, Dateisignatur-Prüfung). Erst nach erfolgreicher Validierung wird ein Verarbeitungsvorgang erstellt. Die Verarbeitung erfolgt in isolierten, kontrollierten Schritten. Der Zugriff auf Zwischenergebnisse erfolgt ausschließlich innerhalb der isolierten Verarbeitungsumgebung.

Ergebnisse werden im Anwendungskontext des jeweiligen Mandanten angezeigt. Exportfunktionen werden über kontrollierte, zeitlich begrenzte Downloadmechanismen realisiert. Signed URLs haben eine kurze Gültigkeitsdauer, um das Zeitfenster für potenzielle Missbräuche zu minimieren.

5 Bedrohungsmodell und Sicherheitsziele

Die Sicherheitskontrollen sind auf typische Bedrohungen für webbasierte B2B-Dokumentenplattformen ausgerichtet. Dazu zählen unautorisierte Datenzugriffe (horizontal/vertikal), Datenexfiltration, Injection-Angriffe, Identitätsmissbrauch sowie Denial-of-Service-Szenarien.

Primäre Sicherheitsziele sind die Mandantenisolierung zur Gewährleistung der Vertraulichkeit, die Integrität der Analyseergebnisse und Metadaten für die Verlässlichkeit der Ergebnisse sowie die Verfügbarkeit der Verarbeitungsprozesse.

6 Identität, Authentifizierung und Autorisierung

Die Plattform implementiert ein mandantenfähiges Identitätsmodell, in dem Benutzer immer einer Organisation zugeordnet sind. Die Authentifizierung bietet Schutz gegen Credential-Stuffing, Enumeration und Session-Fixation. Token werden kurzlebig gehalten und sind rotationsfähig. Nach mehreren fehlgeschlagenen Login-Versuchen wird das Konto automatisch für einen definierten Zeitraum gesperrt.

Die Autorisierung folgt einem rollenbasierten Modell (RBAC) mit hierarchischer Rollenstruktur. Zusätzlich wird bei jeder Anfrage die Ressourcenzugehörigkeit (Ownership) geprüft. Dies verhindert sowohl vertikale Privilege Escalation als auch horizontale Zugriffe auf Ressourcen anderer Organisationen.

Die Mandantenisolierung auf Datenbankebene wird durch Row-Level-Security (RLS) und Policies umgesetzt. Diese fungieren als „Last Line of Defense" gegen horizontalen Zugriff. Sicherheitskritische Operationen laufen ausschließlich über serverseitige Services mit minimierten Credentials.

Für Enterprise-Kunden bieten wir eine domain-basierte Whitelist, die automatische Zuweisung basierend auf E-Mail-Domains ermöglicht. Die Benutzerregistrierung wird durch Administratoren kontrolliert, und ein Invite-System mit sicheren, zeitlich begrenzten Einladungstokens stellt sicher, dass nur autorisierte Benutzer Zugriff erhalten. Generische Fehlermeldungen verhindern Account-Enumeration-Angriffe.

7 Kryptographie und Datenverschlüsselung

Jegliche Kommunikation (Browser-Plattform, Inter-Service) erfolgt über TLS-gesicherte Kanäle. Wir verwenden moderne Verschlüsselungsprotokolle (TLS 1.2+, bevorzugt TLS 1.3) für alle externen und internen Verbindungen. HSTS wird in Produktion erzwungen, um Downgrade- und SSL-Stripping-Angriffe zu verhindern. Perfect Forward Secrecy wird durch moderne Cipher Suites und TLS 1.3 gewährleistet, wie von unseren Cloud-Providern standardmäßig unterstützt.

Persistierte Daten (Dateiobjekte, Metadaten, Analyseergebnisse) werden durch providerseitige Verschlüsselungsmechanismen (AES-256) geschützt. Die Verschlüsselung ruhender Daten erfolgt automatisch in allen Storage-Systemen. Datenbankverbindungen werden über SSL/TLS abgesichert, wobei in Produktionsumgebungen explizit unsichere Konfigurationen abgelehnt werden.

Secrets Management erfolgt ohne Hardcoded Secrets. Die Bereitstellung erfolgt zur Laufzeit über dedizierte Mechanismen, und der Zugriff ist nur für berechtigte Runtime-Identitäten möglich. Wir verwenden ausschließlich moderne, kryptographisch sichere Standards: AES-256 für symmetrische Verschlüsselung, RSA-2048+ für asymmetrische Verschlüsselung und SHA-256+ für sichere Hash-Funktionen.

8 Sichere Dokumentverarbeitung

Upload-Validierung erfolgt durch Prüfung gegen Allow-Lists (MIME-Type, Signaturen) und Größenlimits. Dateien werden auf Dateisignaturen geprüft, Dateierweiterungen werden validiert, und Content-Types werden serverseitig überprüft. Größenlimits für Uploads und Request-Bodies sind definiert, um Denial-of-Service-Angriffe durch übergroße Requests zu verhindern.

Die interne Speicherung nutzt zufällige Objekt-IDs und organisationsbasierte Strukturen, um Path-Traversal-Angriffe zu verhindern. Eine zentrale Pfadvalidierung stellt sicher, dass alle Pfade innerhalb der erwarteten Struktur bleiben und Cross-Organization-Zugriffe technisch verhindert werden.

Temporäre Daten sind über kurzlebige, signierte URLs zugänglich, die logisch pro Organisation separiert sind. Die Löschung erfolgt umfassend: Primärdateien, temporäre Daten und Metadaten werden ohne verbleibende Referenzen entfernt. Auf Anfrage ist eine sofortige Löschung jederzeit möglich, und alle Löschvorgänge werden vollständig protokolliert.

9 Applikationssicherheit

- **Input-Validierung:** Erfolgt durch strikte Schema-Validierung aller API-Eingaben. Semantische Konsistenzprüfungen stellen sicher, dass Eingaben nicht nur syntaktisch korrekt, sondern auch semantisch sinnvoll sind. Alle Eingaben werden zur Laufzeit validiert, bevor sie verarbeitet werden.
- **Datenbanksicherheit:** Datenbankzugriffe erfolgen über parametrisierte Abfragen, wodurch SQL-Injection-Angriffe technisch verhindert werden. Direkte String-Konkatenation in Queries ist ausgeschlossen. Path Traversal wird durch zentrale Pfadvalidierung verhindert, die strikte Validierung erwarteter Pfadstrukturen, Blockierung von Traversal-Sequenzen und Verhinderung von Cross-Organization-Zugriffen umfasst.
- **Browser-Security:** Durch den Einsatz von Security Headers (CSP, HSTS, X-Content-Type-Options, X-Frame-Options) und CSRF-Schutz (SameSite-Cookies, Token-basierte CSRF-Protection) gewährleistet. Cryptographically Secure Tokens werden mit timing-attack-resistenten Vergleichsmechanismen verglichen, um Timing-Angriffe zu verhindern.
- **Rate Limiting:** Begrenzt Anfragen auf kritischen Endpunkten (Login, Upload) zur Missbrauchsprävention. Login-Versuche und File-Uploads unterliegen strikten Rate-Limits, die auf Endpoint-Kritikalität basieren. Adaptive Limits können nutzer-, organisations- und IP-basiert umgesetzt werden.
- **CORS-Konfigurationen:** Sind restriktiv und originbasiert. Nur explizit erlaubte Origins werden akzeptiert, wobei Entwicklungs- und Produktionsumgebungen strikt getrennt konfiguriert sind. Preflight-Requests werden korrekt behandelt, und der Einsatz von `Vary: Origin` verhindert Cache-Poisoning-Angriffe.

10 Infrastruktur- und Betriebssicherheit

Backend-Services laufen als isolierte Container mit dedizierten Identitäten. Jeder Container erhält nur die minimal erforderlichen Berechtigungen für seine spezifische Funktion. Elastische Skalierung erfolgt mit Begrenzung von CPU/Memory pro Instanz und Quotas zur Vermeidung von „Noisy Neighbor"-Effekten.

Die Konfiguration folgt einem versionierten Deployment-Ansatz. Alle Infrastruktur-Änderungen werden versioniert und nachvollziehbar dokumentiert. Rollback-Fähigkeit ist Bestandteil der Betriebsanforderungen, um fehlerhafte Releases schnell zu neutralisieren.

Network Segmentation erfolgt durch virtuelle Private Clouds für Isolation. Firewall-Regeln sind restriktiv auf allen Ebenen konfiguriert. Enterprise-Grade DDoS-Schutz wird durch die Cloud-Provider bereitgestellt. Secrets Management erfolgt über Provider-native Services, die sichere Verwaltung von Secrets und Credentials gewährleisten.

Die Infrastruktur ist hochverfügbar mit automatischer Skalierung. Regelmäßige, automatisierte Backups erfolgen mit Verschlüsselung. Umfassende Disaster-Recovery-Pläne werden regelmäßig getestet, um die Wiederherstellung der Verfügbarkeit unter Wahrung der Datenminimierung sicherzustellen.

10.1 Partner-Zertifizierungen

Wir arbeiten ausschließlich mit führenden Cloud-Providern zusammen, die höchste Sicherheitsstandards einhalten und umfassend zertifiziert sind. Alle unsere Infrastruktur-Partner verfügen über umfassende Zertifizierungen, einschließlich SOC 2 Type II sowie DSGVO-Konformität, und unterliegen regelmäßigen externen Sicherheitsaudits. Cloud-Provider verfügen zusätzlich über ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018.

- **Vercel** (Web-Anwendung, CDN, Edge-Netzwerk) ist SOC 2 Type II und ISO/IEC 27001 zertifiziert und bietet Enterprise-Grade TLS-Terminierung und DDoS-Schutz. Die Cloud-spezifischen ISOs 27017/27018 werden über Sub-Provider abgedeckt.
- **Google Cloud Platform** (Verarbeitungsservices, Storage) verfügt über SOC 2 Type II, ISO/IEC 27001, 27017, 27018 Zertifizierungen und bietet Enterprise-Grade Infrastruktur mit automatischer Skalierung.
- **Supabase** (Datenbank, Authentifizierung) ist SOC 2 Type II zertifiziert, HIPAA-ready und bietet DSGVO-konforme Datenverarbeitung in der EU.
- **OpenAI** wird für ergänzende Verarbeitungsfunktionen genutzt, das SOC 2 Type II, ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018 zertifiziert und DSGVO-konform ist.

Die Vorteile dieser Partner-Auswahl liegen in bewährten Sicherheitsstandards durch regelmäßige externe Sicherheitsaudits, kontinuierlicher Verbesserung durch kontinuierliche Investitionen in Sicherheitsmaßnahmen, transparenten und nachprüfbaren Sicherheitszertifizierungen sowie redundanter und hochverfügbarer Infrastruktur mit automatischem Failover.

10.2 EU-Hosting und Datenresidenz

Die primäre Datenverarbeitung erfolgt in der Europäischen Union (Frankfurt, Deutschland) in ISO/IEC 27001-zertifizierten Rechenzentren. Datenbank-Hosting, Storage-Hosting und Verarbeitungsservices laufen in der EU (Frankfurt). Dies gewährleistet vollständige Einhaltung der DSGVO-Anforderungen durch EU-Datenresidenz.

11 Logging, Monitoring und Auditierbarkeit

Telemetrie erfolgt durch strukturierte Logs und Metriken zur Überwachung von Verfügbarkeit und Sicherheit. Sensitive Daten werden in Logs automatisch redigiert. Die Redaction umfasst API-Keys, JWT-Tokens, Session-Tokens, Datenbank-URLs mit Credentials sowie pattern-basierte Erkennung verschiedener Secret-Formate.

Audit-Events erfassen sicherheitsrelevante Aktionen (Login, Freigaben, Exporte, Admin-Operationen) mit Zeitstempel, Actor und Kontext für End-to-End Traceability. Audit-Logs sind unveränderlich und werden separat von Anwendungslogs gespeichert. Stack Traces werden in Produktion entfernt, Dateipfade werden aus Fehlermeldungen entfernt, und generische Fehlermeldungen ohne interne Details werden verwendet, um Informationsleckage zu verhindern.

Security Monitoring umfasst zentrale Log-Sammlung, strukturierte Logs, Erkennung von Sicherheitsereignissen sowie Überwachung fehlgeschlagener Login-Versuche. Die Erkennung von Anomalien in Login-Mustern, Rate-Limit-Events, ungewöhnlichen Upload-/Analysevolumina sowie Fehlerprofilen in Verarbeitungsprozessen ermöglicht frühzeitige Detektion von Missbrauch, Credential-Angriffen und stabilitätskritischen Lastsituationen.

12 Incident Response und Business Continuity

Incident Response ist als Prozess definiert mit Triage, Containment, Eradication, Recovery und Postmortem. Technische Maßnahmen umfassen Token-/Secret-Rotation, temporäre Einschränkung von Endpoints, Isolation betroffener Komponenten und Forensik über Audit Logs. Kommunikation und Eskalation werden gemäß Schweregrad und vertraglichen Regelungen durchgeführt.

Wir haben definierte Prozesse für die Meldung von Datenpannen gemäß Art. 33/34 DSGVO. Kontinuierliches Monitoring ermöglicht frühzeitige Erkennung von Sicherheitsvorfällen. Die Meldung an die zuständige Aufsichtsbehörde erfolgt innerhalb von 72 Stunden nach Bekanntwerden. Betroffene Personen werden ohne unzumutbare Verzögerung informiert, wenn ein hohes Risiko besteht. Alle Datenpannen und ergriffenen Maßnahmen werden vollständig dokumentiert.

Backup & Recovery erfolgt durch reproduzierbare Deployments und Strategien zur Wiederherstellung der Verfügbarkeit unter Wahrung der Datenminimierung. Regelmäßige, automatisierte Backups mit Verschlüsselung gewährleisten, dass Daten im Falle eines Ausfalls wiederhergestellt werden können.

13 Secure Software Development Lifecycle (SSDLC)

Code Quality wird durch Review-Prozesse mit Sicherheitsfokus für kritische Komponenten gewährleistet. Alle Code-Änderungen werden durch mindestens einen weiteren Entwickler geprüft, wobei besonderes Augenmerk auf sicherheitskritische Bereiche gelegt wird.

Abhängigkeiten werden kontinuierlich auf Schwachstellen überwacht. Automatisierte Scans in CI/CD-Prozessen identifizieren bekannte Vulnerabilities in Dependencies. Regelmäßige Updates stellen sicher, dass bekannte Schwachstellen schnell gepatcht werden.

Deployment erfolgt über automatisierte Prozesse. Secrets-Injektion erfolgt erst zur Laufzeit, niemals im Code oder in Konfigurationsdateien. Alle Deployments sind versioniert und nachvollziehbar. Rollback-Fähigkeit ist Bestandteil des Deployment-Prozesses, um fehlerhafte Releases schnell zu neutralisieren.

14 Datenschutz und DSGVO

Die Verarbeitung erfolgt im Auftrag des Kunden (Auftragsverarbeitung) unter Berücksichtigung von Art. 32 DSGVO. Unsere Plattform erfüllt vollständig die Anforderungen der Datenschutz-

Grundverordnung (DSGVO) und verarbeitet personenbezogene Daten ausschließlich im Rahmen der gesetzlichen Bestimmungen.

14.1 Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)

Die Verarbeitung erfolgt zur Erbringung der vertraglich vereinbarten Dienstleistung (Dokumentenanalyse) gemäß Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung). Für Sicherheitsmaßnahmen, Betrugsprävention und Systemstabilität erfolgt die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO (Berechtigtes Interesse). Optionale Funktionen können auf Grundlage von Art. 6 Abs. 1 lit. a DSGVO (Einwilligung) verarbeitet werden.

14.2 Grundsätze der Datenverarbeitung

Daten werden ausschließlich für die beauftragte Analyse verwendet (Zweckbindung gemäß Art. 5 Abs. 1 lit. b DSGVO). Nur notwendige Daten werden erhoben und verarbeitet (Datenminimierung gemäß Art. 5 Abs. 1 lit. c DSGVO). Automatische Löschung erfolgt nach definierter Zeit oder auf Anfrage (Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e DSGVO). Umfassende technische und organisatorische Maßnahmen gewährleisten Integrität und Vertraulichkeit (Art. 5 Abs. 1 lit. f DSGVO).

14.3 Betroffenenrechte (Art. 15-22 DSGVO)

Wir unterstützen vollständig alle DSGVO-Betroffenenrechte und stellen entsprechende Prozesse bereit. Das Recht auf Auskunft (Art. 15 DSGVO) ermöglicht umfassende Information über verarbeitete personenbezogene Daten. Das Recht auf Berichtigung (Art. 16 DSGVO) ermöglicht Korrektur unrichtiger oder Vervollständigung unvollständiger Daten. Das Recht auf Löschung (Art. 17 DSGVO) ermöglicht Löschung personenbezogener Daten auf Anfrage, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Das Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO), das Recht auf Datenübertragbarkeit (Art. 20 DSGVO), das Widerspruchsrecht (Art. 21 DSGVO) und das Beschwerderecht (Art. 77 DSGVO) werden vollständig unterstützt. Kontaktmöglichkeiten für alle DSGVO-Rechte sind in der Datenschutzerklärung dokumentiert, und definierte Prozesse gewährleisten fristgerechte Bearbeitung gemäß gesetzlicher Vorgaben (in der Regel innerhalb von 30 Tagen).

14.4 Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Wir implementieren umfassende technische und organisatorische Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus. Verschlüsselung ruhender Daten (AES-256) erfolgt in allen Storage-Systemen, Verschlüsselung übertragener Daten (TLS 1.2+) für alle Kommunikationswege. Authentifizierungsmechanismen für alle Zugriffe, rollenbasierte Zugriffskontrolle (RBAC), private Storage-Bereiche ohne öffentliche Zugriffsmöglichkeiten, regelmäßige Überprüfung und Rotation von Zugangsberechtigungen sowie sichere Session-Verwaltung gewährleisten Zugriffskontrolle.

Datenintegrität wird durch Schutz vor unbefugter Veränderung durch Verschlüsselung und Zugriffskontrollen, Validierung von Datenintegrität bei Übertragung und Speicherung sowie Audit-Logging für alle kritischen Operationen gewährleistet. Verfügbarkeit wird durch hochverfügbare Infrastruktur mit automatischem Failover, regelmäßige automatisierte Backups, Disaster-Recovery-Pläne sowie Schutz vor Verlust und Zerstörung durch redundante Speicherung sichergestellt. Kontinuierliche Überwachung der Wirksamkeit der TOM, regelmäßige Sicherheitsüberprüfungen und Penetrationstests sowie Anpassung der Maßnahmen an sich entwickelnde Bedrohungen gewährleisten regelmäßige Überprüfung.

14.5 Datenverarbeitungsverträge (AVV/DVV) gemäß Art. 28 DSGVO

Wir haben mit allen Auftragsverarbeitern, die personenbezogene Daten im Rahmen unserer Dienstleistung verarbeiten, Datenverarbeitungsverträge (AVV) gemäß Art. 28 DSGVO abgeschlossen. Diese Verträge stellen sicher, dass die Verarbeitung ausschließlich nach unseren Weisungen erfolgt, angemessene technische und organisatorische Maßnahmen umgesetzt werden, die Vertraulichkeit und Sicherheit der Daten gewährleistet ist, keine Weitergabe an Dritte ohne unsere Zustimmung erfolgt und Unterstützung bei der Erfüllung von Betroffenenrechten gewährleistet ist.

Unsere Auftragsverarbeiter:

- **Supabase** (Datenbank, Authentifizierung): SOC 2 Type II zertifiziert, HIPAA-ready und DSGVO-konform. Funktion: Datenbank-Hosting, Authentifizierung und Mandantenverwaltung. Datenresidenz: EU (Frankfurt, Deutschland). DPA: Im Service-Agreement enthalten und aktiv akzeptiert.
- **Google Cloud Platform**: SOC 2 Type II, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 zertifiziert und DSGVO-konform. Funktion: Container-Hosting für Verarbeitungsservices und Objektspeicher. Datenresidenz: EU (Frankfurt). DPA: Aktiviert.
- **Vercel** (Hosting, CDN): SOC 2 Type II und ISO/IEC 27001 zertifiziert und DSGVO-konform. Funktion: Web-Anwendung Hosting, Edge-Netzwerk und TLS-Terminierung. Cloud-spezifische ISOs 27017/27018 über Sub-Provider. Datenresidenz: Global mit EU-Optimierung. DPA: Im Service-Agreement enthalten und aktiv akzeptiert.
- **OpenAI**: SOC 2 Type II, ISO/IEC 27001, ISO/IEC 27017 und ISO/IEC 27018 zertifiziert und DSGVO-konform. Datenresidenz: USA mit EU-US Data Privacy Framework. Business Terms mit DPA-Klauseln sind aktiv akzeptiert. Verarbeitung erfolgt ausschließlich für spezifische, begrenzte Funktionen.

Transparenz und Nachvollziehbarkeit werden durch vollständige Liste der Auftragsverarbeiter in der Datenschutzerklärung, regelmäßige Überprüfung der AVV-Konformität, Dokumentation aller Datenflüsse und Verarbeitungszwecke sowie Transparenz über Sub-Processor-Änderungen gewährleistet.

14.6 Datenresidenz und internationale Datenübertragungen

Die primäre Datenverarbeitung erfolgt in der Europäischen Union (Frankfurt, Deutschland). Datenbank-Hosting, Storage-Hosting und Verarbeitungsservices laufen in der EU (Frankfurt).

Soweit Daten in Drittländer (insbesondere USA) übertragen werden, erfolgt dies auf Grundlage geeigneter Garantien gemäß Art. 44 ff. DSGVO. Wir verwenden die von der Europäischen Kommission genehmigten Standardvertragsklauseln (SCC), nutzen das EU-US Data Privacy Framework, soweit der Dienstleister zertifiziert ist, implementieren zusätzliche technische Maßnahmen zur Gewährleistung eines angemessenen Datenschutzniveaus und übertragen nur die für die Verarbeitung erforderlichen Daten.

15 Datenverwendung: ausschließlich für Ihre Analyse

Unsere Plattform verarbeitet Dokumente und abgeleitete Inhalte ausschließlich zur Durchführung der vom Kunden beauftragten Analyse. Diese Zweckbindung ist sowohl technisch als auch

vertraglich abgesichert. Eine Nutzung für Training, Fine-Tuning oder Forschung ist ausgeschlossen. Dokumentinhalte werden nicht an Dritte zu anderen Zwecken weitergegeben, und Ihre Daten bleiben vollständig isoliert und werden nicht mit anderen Kundendaten kombiniert.

16 Sicherheitsnachweise und kontinuierliche Verbesserung

Regelmäßige Sicherheitsprüfungen (Code-Reviews, Scans, manuelle Verifikation) werden durchgeführt. Findings fließen in die Roadmap ein. Regelmäßige Sicherheitsupdates, schnelle Bereitstellung kritischer Patches, Testverfahren vor Deployment und Rollback-Pläne für Notfälle gewährleisten Security Updates.

Security Assessments umfassen regelmäßige Sicherheitsüberprüfungen, Schwachstellenbewertungen, automatisierte Schwachstellenscans sowie sicherheitsfokussierte Code-Reviews. Threat Intelligence umfasst Verfolgung aktueller Bedrohungen, Monitoring von Schwachstellen-Datenbanken, Verfolgung von Security-Advisories sowie Verfolgung von Branchenbest-Practices.

17 Anhang: Begriffe und Abkürzungen

AES	Advanced Encryption Standard (typischerweise 256-Bit)
API	Application Programming Interface
AVV/DPA	Auftragsverarbeitungsvertrag / Data Processing Agreement
CORS	Cross-Origin Resource Sharing
CSP	Content Security Policy
CSRF	Cross-Site Request Forgery
DSGVO	Datenschutz-Grundverordnung
HSTS	HTTP Strict Transport Security
OWASP	Open Worldwide Application Security Project
RBAC	Role-Based Access Control
RLS	Row-Level Security
SOC 2	Service Organization Control 2
TOM	Technische und organisatorische Maßnahmen
TLS	Transport Layer Security
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework
XSS	Cross-Site Scripting

18 Kontakt

Für Fragen zu Sicherheitsmaßnahmen oder Compliance-Anforderungen kontaktieren Sie bitte unser Sicherheitsteam.

Dokumentversion: 1.0
Letzte Aktualisierung: Januar 2025
Nächste Überprüfung: Quartal 2, 2025