Review

Sicherheits-Whitepaper: Enterprise-Grade Datenschutz und Informationssicherheit

Datum: Januar 2025

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

> **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.

Unsere Sicherheitsmaßnahmen orientieren sich an internationalen Standards:

- **ISO/IEC 27001**: Informationssicherheits-Managementsysteme
- **OWASP Top 10**: Web Application Security Best Practices
- **DSGVO**: Datenschutz-Grundverordnung (EU)
- **NIST Cybersecurity Framework**: Cybersecurity Best Practices

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. Für Hosting und Auslieferung der Web-Anwendung wird Vercel genutzt, für die Verarbeitung und Skalierung der Backend-Services Google Cloud, und für Authentifizierung, Mandantenverwaltung sowie Datenpersistenz Supabase. Die Kombination dieser Komponenten ermöglicht eine klar segmentierte Sicherheitsdomäne pro Schicht (Frontend, Identität/Daten, Verarbeitung) und reduziert dadurch die Angriffsfläche.

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.

4. Systemüberblick und Datenfluss

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

Komponentenübersicht

- **Web-Anwendung (Vercel):** Vercel übernimmt die sichere Auslieferung statischer und dynamischer Frontend-Artefakte, TLS-Terminierung sowie Edge-nahe Performance-Optimierungen. Sicherheitsrelevante Konfigurationen (z. B. Strict-Transport-Security, Content-Security-Policy) werden in der Delivery-Schicht verankert.
- **Identität & Daten:** Stellt Authentifizierung, Organisations- und Rollenmodell sowie relationale Datenpersistenz bereit. Zugriffskontrollen werden konsequent serverseitig durchgesetzt.
- **Verarbeitung:** Hier werden dokumentenverarbeitende Workloads in isolierten Containern ausgeführt. Stateless Server ermöglicht elastische Skalierung bei gleichzeitiger Begrenzung von Ressourcen.
- **Storage:** Für Dateiobjekte und temporäre Artefakte wird ein cloudbasierter Objektspeicher eingesetzt. Dateien werden in logisch getrennten Namensräumen pro Organisation abgelegt.

Datenfluss im Detail

1. **Upload:** Nach dem Upload eines Dokuments wird die Datei zunächst serverseitig validiert (Format, Integrität, Header).
2. **Verarbeitung:** Erst nach erfolgreicher Validierung wird ein Verarbeitungsvorgang erstellt. In der ersten Phase werden Dokumente zerlegt (z. B. Seiten/Folien), in der zweiten Phase erfolgt die inhaltliche Analyse. Der Zugriff auf Zwischenergebnisse erfolgt ausschließlich innerhalb der Processing-Domäne.
3. **Bereitstellung:** Ergebnisse werden im Anwendungskontext des jeweiligen Mandanten angezeigt. Exportfunktionen werden über kontrollierte, zeitlich begrenzte Downloadmechanismen realisiert.

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:

- Mandantenisolierung (Vertraulichkeit)
- Integrität der Findings und Metadaten (Verlässlichkeit der Ergebnisse)
- Verfügbarkeit der Verarbeitungspipeline

6. Identität, Authentifizierung und Autorisierung

Die Plattform implementiert ein mandantenfähiges Identitätsmodell, in dem Benutzer immer einer Organisation zugeordnet sind.

- **Authentifizierung:** Schutz gegen Credential-Stuffing, Enumeration und Session-Fixation. Token werden kurzlebig gehalten und sind rotationsfähig.
- **RBAC & Ownership:** Die Autorisierung folgt einem rollenbasierten Modell (RBAC). Zusätzlich wird bei jeder Anfrage die Ressourcenzugehörigkeit (Ownership) geprüft.
- **Mandantenisolierung (Datenbank):** Umsetzung durch Row-Level-Security (RLS) und Policies in Supabase. Diese fungieren als „Last Line of Defense“ gegen horizontalen Zugriff. Sicherheitskritische Operationen laufen ausschließlich über serverseitige Services mit minimierten Credentials.

7. Kryptographie und Datenverschlüsselung

- **In Transit:** Jegliche Kommunikation (Browser-Plattform, Inter-Service) erfolgt über TLS-gesicherte Kanäle. HSTS wird erzwungen.
- **At Rest:** Persistierte Daten (Dateiobjekte, Metadaten, Findings) werden durch providerseitige Verschlüsselungsmechanismen (AES-256) geschützt.
- **Secrets Management:** Keine Hardcoded Secrets. Bereitstellung zur Laufzeit über dedizierte Mechanismen; Zugriff nur für berechtigte Runtime-Identitäten.

8. Sichere Dokumentverarbeitung

- **Upload-Validierung:** Prüfung gegen Allow-Lists (MIME-Type, Signaturen) und Größenlimits.
- **Dateinamen:** Interne Speicherung nutzt zufällige Objekt-IDs, um Path-Traversal-Angriffe zu verhindern.
- **Temporäre Artefakte:** Zugriff über kurzlebige, signierte URLs, die logisch pro Organisation separiert sind.
- **Löschung:** Umfassende Löschung von Primärdateien, Artefakten und Metadaten ohne verbleibende „dangling references“.

9. Applikationssicherheit

- **Input-Validierung:** Strikte Schema-Validierung aller API-Eingaben; semantische Konsistenzprüfungen.
- **Datenbank:** Nutzung parametrisierter Abfragen/ORM zur Vermeidung von Injection-Angriffen.
- **Browser-Security:** Einsatz von Security Headern (CSP, HSTS, X-Content-Type-Options, X-Frame-Options) und CSRF-Schutz (SameSite-Cookies).
- **Rate Limiting:** Begrenzung von Anfragen auf kritischen Endpunkten (Login, Upload) zur Missbrauchsprävention.

10. Infrastruktur- und Betriebssicherheit

- **Isolation:** Backend-Services laufen als isolierte Container (Google Cloud Run) mit dedizierten IAM-Identitäten.
- **Ressourcensteuerung:** Elastische Skalierung mit Begrenzung von CPU/Memory pro Instanz und Quotas zur Vermeidung von „Noisy Neighbor“-Effekten.
- **Konfiguration:** „Immutable Infrastructure“-Ansatz mit versionierten Deployments.

11. Logging, Monitoring und Auditierbarkeit

- **Telemetrie:** Strukturierte Logs und Metriken zur Überwachung von Verfügbarkeit und Sicherheit. Sensitive Daten werden in Logs redigiert.
- **Audit-Events:** Erfassung sicherheitsrelevanter Aktionen (Login, Freigaben, Exporte) mit Zeitstempel, Actor und Kontext für End-to-End Traceability.

12. Incident Response und Business Continuity

- **Incident Response:** Definiertes Verfahren zur Behandlung von Sicherheitsereignissen (Eindämmung, Wiederherstellung, Analyse).
- **Backup & Recovery:** Reproduzierbare Deployments und Strategien zur Wiederherstellung der Verfügbarkeit unter Wahrung der Datenminimierung.

13. Secure Software Development Lifecycle (SSDLC)

- **Code Quality:** Review-Prozesse mit Sicherheitsfokus für kritische Komponenten.
- **Abhängigkeiten:** Kontinuierliche Überwachung auf Schwachstellen (Scanning in CI/CD).
- **Deployment:** Automatisierte Pipelines; Secrets-Injektion erst zur Laufzeit.

14. Datenschutz und DSGVO

Die Verarbeitung erfolgt im Auftrag des Kunden (Auftragsverarbeitung) unter Berücksichtigung von Art. 32 DSGVO.

- **Datenminimierung:** Keine unnötige Extraktion oder dauerhafte Speicherung personenbezogener Daten.
- **Sub-Prozessoren:** Transparenz über eingesetzte Dienstleister (Vercel, Google Cloud, Supabase, OpenAI) und vertragliche Regelung der Datenresidenz.

15. Datenverwendung: ausschließlich für Ihre Analyse

Dokumente und abgeleitete Inhalte werden ausschließlich zur Durchführung der beauftragten Analyse verarbeitet. **Eine Nutzung für Training, Fine-Tuning oder Forschung ist ausgeschlossen.**

16. Sicherheitsnachweise und kontinuierliche Verbesserung

Regelmäßige Sicherheitsprüfungen (Code-Reviews, Scans, manuelle Verifikation). Findings fließen in die Roadmap ein.

17. Anhang: Begriffe und Abkürzungen

- **AES:** Advanced Encryption Standard (typischerweise 256-Bit)
- **TLS:** Transport Layer Security
- **RBAC:** Role-Based Access Control
- **RLS:** Row-Level Security
- **OWASP:** Open Worldwide Application Security Project
- **NIST CSF:** National Institute of Standards and Technology Cybersecurity Framework