Technische Dokumentation

Version: 2.0 vom 10.02.2025

Slideroom GmbH
Gewerbepark Cité 4
76532 Baden-Baden

Tel.: 07221 40 37 633
info@slideroom.de
www.slideroom.de

Grenke Bank AG
IBAN: DE21 2013 0400 0060 3067 27
BIC: GREB DEH1 XXX

USt-IdNr. DE367213821
Amtsgericht Mannheim
HRB 750 207

Geschäftsführer:
Christian Vollmer
Maximilian Supper

Einleitung

Diese Dokumentation beschreibt die Architektur, Sicherheit und den Betrieb des PowerPoint Add-Ins slideroom.

Hinweis: Diese Dokumentation wird regelmäßig aktualisiert, um Änderungen an der Architektur, Sicherheitsmaßnahmen und anderen relevanten Informationen zu berücksichtigen. Eine Überprüfung und Aktualisierung erfolgt mindestens jährlich oder nach bedeutenden Änderungen an der Applikation.

Übersicht der Applikation

- **Name der Applikation:** slideroom
- **Technologie-Stack:** Vue.js mit TypeScript im Frontend, Kotlin mit Spring Boot im Backend, Deployment via Gradle. Nginx als Reverse Proxy.

Technische Dokumentation

1. Architektur

- **Datenbank:** PostgreSQL für strukturierte Daten und Microsoft Blob Storage für Dateispeicherung.
- **Protokolle:**
  - **HTTPS** zur sicheren Kommunikation
  - **REST API** zwischen Frontend und Backend sowie Nutzung der externen REST APIs von Pexels und Pixabay (optional wählbar für Benutzer).

2. Sicherheitsmaßnahmen (gem. Art. 32 DSGVO)

2.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Physische Sicherheit / Zutrittskontrolle

- Hosting in Azure-Rechenzentren in Deutschland. Höchster Sicherheitsstandard durch Azure.
- Keine unbefugten Personen vor Ort: Zutritt nur für autorisierte Personen.
- Alarm- und Videoüberwachungssysteme durch den Cloud-Anbieter.

Zugangskontrolle

- Keine unbefugte Systembenutzung: sichere Passwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung.
- Verschlüsselung von Datenträgern auf den Entwicklungs- und Administrationsgeräten.
- Für unsere Infrastruktur: SSH nur mit Schlüssel-Authentifizierung (nur CTO und Vertretung).

Zugriffskontrolle

- Rollenbasierte Zugriffskonzepte innerhalb der Anwendung (aktuell User/Admin) pro Organisation.
- Entwickler-/Mitarbeiterzugriff auf Infrastruktur nur für notwendige Wartung (Need-to-know-Prinzip).
- Protokollierung sämtlicher Zugriffe auf administrative Systeme.

Trennungskontrolle

- Getrennte Verarbeitung von Daten verschiedener Mandanten (Mandantenfähigkeit).
- Separate Entwicklungs-, Test- und Produktivumgebungen (Sandboxing).

2.2 Pseudonymisierung (Art. 32 Abs. 1 lit. a; Art. 25 Abs. 1 DSGVO)

- Hochgeladene Dateien werden pseudonymisiert gespeichert, sodass keine gezielte Suche nach Inhalten möglich ist.
- Personenbezogene Daten werden nur mit separaten Referenzen (IDs) verknüpft.
- Wenn möglich und sinnvoll, werden Daten in der Datenbank pseudonymisiert.
- Analytics Tools bekommen (sofern zugestimmt) nur pseudonymisierte Issue Reports.

2.3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Sichere Übertragung über HTTPS/TLS
- Für Dateien werden Checksummen erstellt die dann beim Abruf überprüft werden um eine Manipulation zu verhindern.

2.4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

- Schutz gegen Datenverlust und Ausfälle: regelmäßige Backups (alle 4 Stunden) mittels Azure Backup.
- Firewall, Virenschutz, USV in Azure-Infrastruktur.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

- Geplante Disaster-Recovery-Strategie (in Entwicklung).
- Rollback-Mechanismen durch regelmäßige Backups.
- Versionierung und Soft-Delete auf Dateiebene.

2.5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d; Art. 25 Abs. 1 DSGVO)

Datenschutz-Management

- Regelmäßige Kontrollen der Datenverarbeitungsprozesse, Dokumentation und Anpassung an aktuelle DSGVO-Anforderungen.

Incident-Response-Management

- Meldung von Sicherheitsvorfällen an Mandanten und schnelle Reaktion gemäß definierten Prozessen.

2.6 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Standardmäßig minimale Datenerhebung, Opt-in für erweiterte Analysen.

Auftragskontrolle

- Keine Weitergabe oder Verarbeitung ohne Weisung des Auftraggebers (Auftraggeber = Benutzer innerhalb der Organisation).
- Streng geregelte Auswahl etwaiger Subdienstleister (z. B. Cloud-Provider).

3. Datenfluss und Verarbeitung

Erhobene Daten

- **Personenbezogene Daten:** Name, E-Mail und Passwort (sicher gespeichert). Durch die notwendige Zugehörigkeit zu einer Organisation ist indirekt auch die Firmenzugehörigkeit bekannt.
- **Nutzungsdaten:** Login-Zeiten und Geräteinformationen über die Laufzeit der Session. Optional Opt-in für Seitenaufrufe und Klickverhalten (pseudonymisiert).
- **Dateien und Inhalte:** Hochgeladene Präsentationen und Medien und Metadaten.

Datenspeicherung

- **PostgreSQL:** Strukturierte Benutzerdaten und Metadaten. Passwörter und sensible Daten werden verschlüsselt gespeichert.
- **Microsoft Blob Storage:** Medieninhalte und Präsentationen, zugänglich nur für autorisierte Benutzer. Zusätzlich werden die Dateien vor der Ablage pseudonymisiert sodass nicht gezielt nach Inhalten gesucht werden kann. Gegen Manipulation der Dateien werden Checksummen berechnet und gespeichert.

Datenverarbeitung

- **Benutzerregistrierung und Authentifizierung:** Per Email/Passwort oder Microsoft SSO. Passwortverarbeitung durch Spring Security und verschlüsselte Speicherung des Hashes.
- **Dateiverwaltung:** Dateien können innerhalb der Applikation hochgeladen, gespeichert und abgerufen werden.
- **Analyse und Monitoring:** Seitenaufrufe und Klickverhalten (Opt-in), anonymisierte oder pseudonymisierte (wenn zugestimmt) Fehlerberichte und Logs zur Verbesserung der Anwendung.

4. Authentifizierung und Autorisierung

Authentifizierung

- **E-Mail und Passwort:** Passwortanforderungen (mind. 8 Zeichen, mit Sonderzeichen, Zahl und Großbuchstaben).
- **Microsoft SSO:** Über OAuth2. Nach Anmeldung erfolgt Token- und Sessionverarbeitung wie bei E-Mail-Authentifizierung. Die Sessioninfos von Microsoft werden nur zum Abruf von Benutzerdaten verwendet (bei der Registrierung) und zur Authentifizierung des Users und dann verworfen.
- **Mehrfaktor-Authentifizierung (MFA):** Kann optional aktiviert werden: entweder per E-Mail-Verifizierung oder TOTP (Authenticator-App). Organisationsrichtlinien, damit Administratoren MFA innerhalb einer Organisation erzwingen können, sind geplant.

Sicherheitsmechanismen

- **Token-Sicherheit:** Tokens zur Sessionzuordnung werden in HTTP-Only Cookies gespeichert (Secure, HttpOnly und SameSite=Strict).
- **Gerätebindung der Tokens:** Interne Mechanismen binden Tokens an das jeweilige Gerät.
- **Session-Management:** Session-Timeouts für „Angemeldet bleiben“ (1 Jahr) oder ohne (1 Tag). Auth-Cookies 5 Minuten, für den Refresh-Token („Angemeldet bleiben“) 1 Jahr, sonst "Session".

Autorisierung

- **Rollenbasierte Zugriffskontrolle:** Admin und User-Rollen; zukünftige Erweiterung geplant. Rollen und Berechtigungen sollen vom Administrator verwaltet werden können.
- **Berechtigungsprüfung:** Zugriffskontrolle bei jeder Anfrage; Prinzip des geringsten Privilegs.

5. Infrastruktur

Hosting-Umgebung

- **Cloud-Plattform:** Microsoft Azure in der Region Germany West Central für deutsche Datenschutzbestimmungen.

Netzwerkarchitektur

- **Virtuelles Netzwerk (VNet):** Eine VM, keine Segmentierung, NSG für Traffic-Kontrolle.
- **Load Balancer:** Aktuell nicht vorhanden, geplant für zukünftige Skalierung.

Sicherheitsmaßnahmen für VMs

- **Betriebssystem:** Ubuntu.
- **Zugriffskontrolle:** SSH-Zugriff mit Schlüssel-Authentifizierung, nur für Administratoren (CTO und Vertretung).

Verfügbarkeit und Skalierbarkeit

- **Skalierung:** Aktuell vertikal, horizontale Skalierung und Load Balancer bei wachsender Last geplant.

CI/CD-Prozesse

- **Build-Prozess:** Jenkins für Builds und Integration; nur Netzwerkzugriff intern.
- **Deployment:** Manuelles Deployment auf Produktivsystem, Testsystem wird automatisch deployed.

Backup und Disaster Recovery

- **Backups:** Alle 4 Stunden durch Azure-Backup-Mechanismen.
- **Wiederherstellung:** Rollback bei Problemen durch regelmäßige Backups möglich.
- **Disaster Recovery Plan:** Geplant für zukünftige Implementierung.

6. Betrieb und Wartung

Updates und Deployment

- **Update-Prozesse:** Nach Bedarf; ausführliche Tests auf einem Testsystem vor Deployment. Unit- und UI-Tests werden beim Build ausgeführt.

Überwachung und Monitoring

- **Monitoring-Tools:** Azure Alerts, Bugtracking (Azure Application Insights) (Opt-In für Benutzer möglich).
- **Alarmierung:** Administrator wird bei kritischen Zuständen umgehend informiert.

Zugriffskontrolle und Berechtigungsmanagement

- **Administrative Zugriffe:** Streng kontrolliert, nur CTO und Vertretung.
- **Protokollierung:** Alle Zugriffe werden zur Nachvollziehbarkeit protokolliert.

Wartung und Sicherheitsupdates

- **Patch-Management:** Automatische Updates für Betriebssystem und Anwendungsspezifisches.

- **Sicherheitsmeldungen:** Administrator verfolgt Sicherheitsupdates regelmäßig (mindestens monatlich). Zusätzlich wird auf Sicherheitshinweise seitens Azure umgehend reagiert.

7. Risiken und Maßnahmen

- **Unautorisierter Zugriff auf Benutzerdaten:** MFA, HTTPS-Verschlüsselung, Passwort-Hashes mit Salt, Begrenzung von Login-Versuchen.
- **Cross-Site Scripting (XSS):** XSS-Schutz durch serverseitige Validierung der Eingaben. Browserseitig werden Escapemechanismen von vue.js verwendet.
- **Schwache Passwortsicherheit:** Passwortanforderungen und -feedback, optional MFA.
- **Man-in-the-Middle (MitM) Angriffe:** HTTPS mit TLS, HSTS für HTTPS-Erzwingung, regelmäßige Erneuerung der Zertifikate.
- **SQL-Injection:** Verwendung von JPA/Hibernate mit parametrisierten Queries, Serverseitige Validierung.
- **Distributed Denial of Service (DDoS):** Rate Limiting, geplante Nutzung von Azure DDoS Protection Services (Firewall).
- **Sicherheitslücken in Drittanbieter-Bibliotheken:** Regelmäßige Aktualisierung und Sicherheitsaudits für externe Abhängigkeiten.
- **Datenverlust:** Regelmäßige Backups und geplante Implementierung eines Disaster Recovery Plans.
- **Fehlkonfiguration der Server:** Anwendung von Best Practices, geplante Verwendung von IaC-Tools.
- **Unautorisierter Zugriff auf Administrationsschnittstellen:** Beschränkter Zugriff auf Admin-Funktionen und Implementierung von MFA für Administratoren.