

Abbildung 1: Icon der App, Quelle: https://pixabay.com/vectors/clock-analog-time-watch-147257/

**Risikoanalyse**

**“Zeiterfassung“ - Mobile Anwendung auf Android Basis**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Kurs: DLBSEPPSD01\_D  
Bachelor of Science – Softwareentwicklung**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Erstellt von**

**Verfasser: Robin Amos**

**Matrikelnummer: 32209938**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Tutor: Prof. Dr. Thorsten Fröhlich Datum: 07.06.2025**  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Inhaltsverzeichnis**

[1. Datenübersicht 1](#_Toc200205236)

[2. Mögliche Risiken und Gefahrenquellen 1](#_Toc200205237)

[3. Bestehende Schutzmaßnahmen 2](#_Toc200205238)

[4. Zusätzliche empfohlene Maßnahmen 2](#_Toc200205239)

[5. Bewertung nach DSGVO-Risikoansatz 3](#_Toc200205240)

[Literaturverzeichnis 4](#_Toc200205241)

[Anhang 5](#_Toc200205242)

**Abbildungsverzeichnis**

[Abbildung 1 0](#_Toc200130075)

**Tabellenverzeichnis**

[Tabelle 1: Datenübersicht 1](#_Toc200204907)

[Tabelle 2: Mögliche Risiken und Gefahrenquellen 2](#_Toc200204908)

[Tabelle 3: Bewertung nach DSGVO-Risikoansatz 3](#_Toc200204909)

**Abkürzungsverzeichnis**

PIN = Personal Identification Number" – auf Deutsch: "Persönliche Identifikationsnummer

WLAN = Wireless Local Area Network

APP = Applikation

HTTPS = HyperText Transfer Protocol Secure

TLS = Transport Layer Security

MDM = Mobile Device Management

DSFA = Datenschutzfolgeabschätzung

# 1. Datenübersicht

|  |  |
| --- | --- |
| **Datenarten** | **Beschreibung** |
| Name, Adresse | Personenbezogene Daten |
| Auftragsdaten | Auftragstexte der weiteren Information zum Auftrag, Status und Priorität |
| Nutzerkennung | Mitarbeiter und Vorgesetzte |

Tabelle 1: Datenübersicht

# 2. Mögliche Risiken und Gefahrenquellen

|  |  |  |  |
| --- | --- | --- | --- |
| **Risiko** | **Eintritts-wahrscheinlichkeit** | **Schadenshöhe** | **Maßnahmen** |
| Verlust des Endgeräts | Mittel | Hoch | Geräte mir PIN sichern, App ohne lokale Datenspeicherung |
| Unbefugter Zugriff auf Firebase-Daten | Hoch | Hoch | Authentifizierung mit Firebase Authenticator, rollenbasierte Rechte, Zugriff auf Daten per Rolle, sichere Regeln in der Datenbank |
| Datenübertragung | Mittel | Hoch | Firebase überträgt Daten per HTTPS |
| Fehlende Verschlüsselung in Firebase Database | Mittel | Hoch | Firebase nutzt TLS & Verschlüsselung. Zusätzliche Verschlüsselung sensibler Felder möglich |
| App-Code kann ausgelesen werden (Reverse Engineering) | Niedrig | Hoch | Keine Zugangsdaten im Programmcode hardcoden |
| Daten werden unabsichtlich länger gespeichert als erlaubt | Mittel | Hoch | Fertige Aufträge sofort löschen, nachdem sie in die Rechnung eingebucht wurden |
| Gerät liegt entsperrt und unbeachtet frei | Mittel | Mittel | Automatische Sperre nach 1 Minute am Smartphone einrichten |
| WLAN-Debugging öffnet Gerät für unautorisierten Zugriff | Mittel | Hoch | Nur vertrauenswürdige Netze verwenden (Home WLAN), WLAN-Debugging verwenden |

Tabelle 2: Mögliche Risiken und Gefahrenquellen

# 3. Bestehende Schutzmaßnahmen

* **App nicht im Play Store** → kein öffentliches Angriffsrisiko
* **Interne Geräteverwaltung** → Geräte unter Kontrolle des Unternehmens
* **Firebase Authentication** → Zugriffsschutz durch Regeln und angelegte Benutzer
* **HTTPS-Verbindungen** → sichere Datenübertragung
* **Keine lokale Datenspeicherung in App** → bei Geräteverlust keine Kundendaten auf dem Gerät

# 4. Zusätzliche empfohlene Maßnahmen

* Mobile Device Management (MDM) einführen (Fernlöschung, Policy Enforcement)  
    
  Eine Fernlöschung der App ist aktuell nicht möglich, aber eine Löschung des Benutzers bzw. fehlende Login Informationen macht die App unbrauchbar.
* Datenschutz-Folgenabschätzung (DSFA) prüfen, falls viele Daten oder besondere Kategorien verarbeitet werden

Nicht erforderlich. Die Daten können jederzeit unwiderruflich gelöscht werden und es besteht keine Einschränkung oder Gefährdung natürlicher Personen. Es werden sensible Daten wie Name und Adresse erhoben, aber nicht verarbeitet oder verwendet. Es werden keine Daten an Dritte weitergegeben. Es wird keine automatische Überwachung stattfinden und keine automatisierten Entscheidungen des Systems getroffen, was die Daten oder die Verarbeitung der Daten angeht.

* Verschlüsselung auf Feldebene bei besonders sensiblen Daten

Keine zusätzliche Verschlüsselung vorgesehen, Temporäre Speicherung der Daten mit sofortiger Löschung möglich.

* Logging der Zugriffe für Nachvollziehbarkeit

Es ist kein explizietes Logging vorgesehen. Das Logging selbst wäre wieder eine Erhebung von Daten bezüglich des Mitarbeiters, wann dieser sein Handy benutzt hat. Die Realtime Database besitzt ein Zugriffmanagement, dieses zählt die Anzahl der autorisierten und die nicht autorisierten Zugriffe.

* Security Audit der Firebase-Regeln

Der Firebase Authenticator und die Regeln werden immer bei Löschung oder Neueintrag eines Benutzers überprüft.

# 5. Bewertung nach DSGVO-Risikoansatz

|  |  |
| --- | --- |
| **Kriterium** | **Bewertung** |
| Art der Daten | Personenbezogen (Name, Adresse) |
| Umfang der Datenverarbeitung | Moderat |
| Zugriffsberechtigte Personen | Eingeschränkt, Vorgesetzte und Mitarbeiter |
| Risiko für Betroffene bei Datenleck | Mittel |
| Risikobewertung insgesamt | Mittel |

Tabelle 3: Bewertung nach DSGVO-Risikoansatz

Schutzmaßnahmen sind notwendig.

# Literaturverzeichnis

Bildmaterial aus der Fotodatenbank:

Abbildung 1:

<https://pixabay.com/vectors/clock-analog-time-watch-147257/>

# Anhang