

# Die verschiedenen Sicherheitsmechanismen in Ihrer App

Wir nehmen den Schutz Ihrer Daten sehr ernst. Deshalb haben wir in unserer App verschiedene Sicherheitsmechanismen implementiert, die ineinandergreifen und ein Höchstmaß an Sicherheit gewährleisten. Im Folgenden erklären wir Ihnen die wichtigsten dieser Mechanismen.

## Sichere Anmeldung: Ihr persönlicher Zugang

Der erste Schritt zur Sicherheit ist eine sichere Anmeldung. Wir bieten Ihnen verschiedene Möglichkeiten, sich in unserer App anzumelden:

- **Password:** Sie können ein sicheres Passwort verwenden, um Ihr Konto zu schützen. Bitte beachten Sie folgende Tipps für ein sicheres Passwort:
  - Verwenden Sie eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
  - Verwenden Sie kein Passwort, das leicht zu erraten ist (z.B. Ihren Namen oder Ihr Geburtsdatum).
  - Verwenden Sie für jeden Dienst ein eigenes Passwort.
  - Ändern Sie Ihr Passwort regelmäßig.
- **Passkeys (Empfohlen):** Passkeys sind eine moderne und besonders sichere Methode zur Anmeldung. Sie nutzen die biometrischen Funktionen Ihres Geräts (z.B. Fingerabdruck oder Gesichtserkennung) oder einen Hardware-Sicherheitsschlüssel, um sich anzumelden. Passkeys sind deutlich sicherer als Passwörter, da sie nicht gestohlen oder erraten werden können. Erfahren Sie hier mehr zu Passkeys vom BSI: [Anmelden ohne Passwort mit Passkey](#)
- **Anmeldung mit Apple-ID/Google-ID (zukünftig):** In Zukunft werden wir auch die Anmeldung mit Ihrer Apple-ID oder Google-ID anbieten. Diese Dienste bieten bereits hohe Sicherheitsstandards und ermöglichen eine bequeme Anmeldung.

# Ende-zu-Ende-Verschlüsselung: Ihre Nachrichten bleiben privat

Wir verwenden in unserer App standardmäßig die Ende-zu-Ende-Verschlüsselung mit dezentraler Schlüsselverwaltung. Das bedeutet:

- Ihre Nachrichten werden auf Ihrem Gerät verschlüsselt, bevor sie das Internet erreichen.
- Nur der Empfänger kann die Nachrichten mit seinem persönlichen Schlüssel entschlüsseln.
- Wir als Anbieter haben keinen Zugriff auf Ihre Nachrichten.

**Optionale zentrale Schlüsselverwaltung (Komfortlösung):** Zusätzlich bieten wir optional eine zentrale Schlüsselverwaltung an, um den Komfort zu erhöhen. Beachten Sie jedoch, dass dies einen Kompromiss in Bezug auf die maximale Privatsphäre darstellt.

## Matrix-Protokoll: Eine sichere Basis für die Kommunikation

Die Ende-zu-Ende-Verschlüsselung unserer App basiert auf dem Matrix-Protokoll, einem offenen Standard für sichere und dezentrale Kommunikation. Das Matrix-Protokoll bietet folgende Vorteile:

- **Dezentralisierung:** Ihre Daten werden nicht zentral auf einem einzigen Server gespeichert, sondern können auf verschiedenen Servern verteilt sein. Dies erhöht die Ausfallsicherheit und schützt vor Zensur.
- **Ende-zu-Ende-Verschlüsselung:** Das Matrix-Protokoll unterstützt standardmäßig die Ende-zu-Ende-Verschlüsselung.
- **Offener Standard:** Der offene Standard ermöglicht es unabhängigen Experten, die Sicherheit des Protokolls zu überprüfen.

Erfahren Sie hier mehr zu Ende-zu-Ende-Verschlüsselung mit dem Matrix-Protokoll: [Matrix](#) und [Element.io](#).

## Zusätzliche Sicherheitsmaßnahmen

Neben den oben genannten Mechanismen setzen wir weitere Sicherheitsmaßnahmen ein, um Ihre Daten bestmöglich zu schützen:

- **Regelmäßige Sicherheitsupdates:** Wir aktualisieren unsere App regelmäßig, um bekannte Sicherheitslücken zu schließen.
- **Sichere Serverinfrastruktur:** Unsere Server sind durch modernste Sicherheitstechnologien geschützt.
- **Datenschutzkonforme Datenverarbeitung:** Wir verarbeiten Ihre Daten gemäß den geltenden Datenschutzbestimmungen (DSGVO).

# Was Sie selbst für Ihre Sicherheit tun können

Auch Sie können einen wichtigen Beitrag zu Ihrer Sicherheit leisten:

- **Verwenden Sie ein sicheres Passwort oder Passkeys:** Befolgen Sie unsere Tipps für sichere Passwörter oder nutzen Sie die noch sichereren Passkeys.
- **Halten Sie Ihre App auf dem neuesten Stand:** Installieren Sie regelmäßig die neuesten Updates unserer App.
- **Seien Sie vorsichtig bei verdächtigen Nachrichten:** Klicken Sie nicht auf Links oder Anhänge in Nachrichten von unbekannten Absendern.
- **Schützen Sie Ihr Gerät:** Verwenden Sie eine Bildschirmsperre und installieren Sie eine Antivirus-App.

# Fazit: Gemeinsam für Ihre Sicherheit

Wir setzen alles daran, Ihre Daten bestmöglich zu schützen. Durch die Kombination verschiedener Sicherheitsmechanismen und Ihre Mithilfe schaffen wir eine sichere Kommunikationsumgebung.

---

Version #4

Erstellt: 17 Januar 2025 18:05:24

Zuletzt aktualisiert: 21 Januar 2025 15:22:03