

DATENSCHUTZ-HANDBUCH

# DSGVO & Sicherheit

matchminutes.ai

---

*Datenverarbeitung, Rechtsgrundlagen, technische Maßnahmen und Sub-Prozessoren – vollständig dokumentiert.*

AI Sports Boutique GmbH i. G. · Stand: Juli 2026

# Inhalt

---

# 1. Unser Grundsatz

---

matchminutes.ai wurde von Anfang an für den deutschen und europäischen Markt entwickelt. Datenschutz ist kein nachträglicher Aufkleber, sondern die Grundlage der Architektur.

Dieses Handbuch dokumentiert vollständig, welche Daten wo verarbeitet werden, auf welcher Rechtsgrundlage das geschieht und welche technischen Maßnahmen sie schützen. Es richtet sich an Datenschutzbeauftragte, IT-Verantwortliche und Geschäftsführungen, die matchminutes vor dem Einsatz prüfen.

## Die wichtigsten Punkte in Kürze

- Speicherung und Protokollerstellung erfolgen auf Servern in Deutschland (Frankfurt).
- Audiodaten werden nach der Transkription gelöscht; es verbleibt nur das Textprotokoll.
- Meeting-Inhalte werden nicht für das Training von KI-Modellen verwendet.
- Für den Meeting-Bot wird ein US-Dienstleister eingesetzt; die Übermittlung ist über Standardvertragsklauseln abgesichert.
- Ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO wird bereitgestellt.

## 2. Warum Meeting-Werkzeuge besonders sensibel sind

---

In wenigen Arbeitskontexten werden so viele schutzwürdige Daten gleichzeitig verarbeitet wie in Besprechungen.

### **Stimmen sind biometrische Daten**

Nach Art. 9 DSGVO zählen Stimmufnahmen zu den besonders schutzwürdigen personenbezogenen Daten – vergleichbar mit Fingerabdrücken. Für ihre Verarbeitung gelten erhöhte Anforderungen.

### **Betriebsgeheimnisse und Strategien**

Was in Geschäftsleitungsrunden, Budgetgesprächen oder Kundenterminen besprochen wird, ist regelmäßig hochsensibel und wettbewerbsrelevant.

### **Namen, Meinungen, Beschlüsse**

Wer was gesagt hat, welche Position jemand vertritt und wie abgestimmt wurde – all das ist personenbezogen. Eine Weitergabe an Dienstleister ohne Auftragsverarbeitungsvertrag wäre ein Verstoß gegen die DSGVO.

### **Viele Anbieter verarbeiten in den USA**

Zahlreiche verbreitete Werkzeuge stammen von US-Anbietern. Daten auf US-Servern unterliegen dem CLOUD Act: US-Behörden können Zugriff verlangen, ohne dass europäischer Rechtsschutz greift.

### 3. Wer verarbeitet welche Daten

Vollständige Transparenz über jeden Dienst, der an der Verarbeitung beteiligt ist.

#### Meeting-Bot und Audioaufzeichnung

| Merkmal                | Angabe                                           |
|------------------------|--------------------------------------------------|
| Dienstleister          | Recall.ai                                        |
| Verarbeitungsort       | USA                                              |
| Übermittlungsgrundlage | Standardvertragsklauseln nach Art. 46 DSGVO      |
| Zweck                  | Beitritt zum Meeting, Audioaufzeichnung          |
| Verarbeitete Daten     | Audiostrom, Teilnehmer-Metadaten                 |
| Rechtsgrundlage        | Art. 6 Abs. 1 lit. b DSGVO in Verbindung mit AVV |
| Besonderheit           | Audio wird nach der Transkription gelöscht       |

#### Transkription und Protokollerstellung

| Merkmal            | Angabe                                                                 |
|--------------------|------------------------------------------------------------------------|
| Dienstleister      | KI-Infrastruktur mit EU-Verarbeitung                                   |
| Verarbeitungsort   | Europäische Union                                                      |
| Zweck              | Erstellung des Protokolls aus dem Transkript                           |
| Verarbeitete Daten | Transkripttext (kein Audio)                                            |
| Rechtsgrundlage    | Art. 6 Abs. 1 lit. b DSGVO in Verbindung mit Datenverarbeitungsvertrag |
| Besonderheit       | Keine Nutzung der Inhalte für Modelltraining                           |

#### Datenbank und Protokollarchiv

| Merkmal            | Angabe                                             |
|--------------------|----------------------------------------------------|
| Dienstleister      | Supabase auf Hetzner-Infrastruktur                 |
| Verarbeitungsort   | Deutschland (Frankfurt, eu-central-1)              |
| Zweck              | Speicherung der fertigen Protokolle und Kontodaten |
| Verarbeitete Daten | Protokolle, Konto-Metadaten                        |
| Rechtsgrundlage    | Art. 6 Abs. 1 lit. b DSGVO in Verbindung mit AVV   |

#### E-Mail-Zustellung

| Merkmal          | Angabe                            |
|------------------|-----------------------------------|
| Dienstleister    | Resend                            |
| Verarbeitungsort | Europäische Union                 |
| Zweck            | Versand der Protokolle per E-Mail |

| Merkmal            | Angabe                            |
|--------------------|-----------------------------------|
| Verarbeitete Daten | Empfängeradresse, Protokollinhalt |
| Rechtsgrundlage    | Art. 6 Abs. 1 lit. b DSGVO        |
| Besonderheit       | Übertragung TLS-verschlüsselt     |

#### Einordnung zur Drittlandübermittlung

Speicherung und Protokollerstellung finden ausschließlich in Deutschland beziehungsweise der EU statt. Beim Einsatz des Meeting-Bots für Online-Meetings wird der Audiostrom über einen US-Dienstleister verarbeitet. Diese Übermittlung ist durch Standardvertragsklauseln nach Art. 46 DSGVO abgesichert; das Audio wird nach der Transkription gelöscht.

Wer eine Verarbeitung ohne jede Drittlandberührung benötigt, kann Präsenzmeetings oder die Browser Extension nutzen – dort entfällt der Bot.

## 4. Sub-Prozessoren

Vollständige Liste aller Dienstleister, die im Auftrag von matchminutes personenbezogene Daten verarbeiten.

| Dienstleister       | Ort               | Zweck                                               |
|---------------------|-------------------|-----------------------------------------------------|
| Hetzner Online GmbH | Deutschland       | Server-Hosting und Rechenleistung                   |
| KI-Infrastruktur    | EU                | Transkription und Protokollerstellung               |
| Cloudflare Inc.     | EU (vertraglich)  | DDoS-Schutz und Content Delivery, kein Datenzugriff |
| Stripe Inc.         | EU                | Zahlungsabwicklung für kostenpflichtige Tarife      |
| Recall.ai           | USA (SCC Art. 46) | Meeting-Bot für Zoom, Teams und Google Meet         |
| Resend              | EU                | E-Mail-Zustellung                                   |

Die jeweils aktuelle Fassung dieser Liste ist auf Anfrage erhältlich. Über Änderungen informieren wir Vertragskunden vorab.

## 5. Was wir konkret tun

---

### Speicherung in Deutschland

Protokolle, Kontodaten und Archiv liegen auf Servern in Frankfurt. Ein dauerhafter Datenexport findet nicht statt.

### Löschung der Audiodaten

Die Audiodatei wird unmittelbar nach der Transkription gelöscht. Es verbleibt ausschließlich das Textprotokoll – kein Rohton, keine Kopien, kein Archiv.

### Auftragsverarbeitungsvertrag

Für den geschäftlichen Einsatz stellen wir einen Auftragsverarbeitungsvertrag nach Art. 28 DSGVO bereit. Er regelt Weisungsbindung, Vertraulichkeit, technische Maßnahmen, Unterauftragsverhältnisse und Löschung.

#### Hinweis für Unternehmen

Wenn du matchminutes geschäftlich einsetzt, ist der Abschluss eines Auftragsverarbeitungsvertrags erforderlich. Bitte fordere ihn vor dem produktiven Einsatz unter [info@matchminutes.ai](mailto:info@matchminutes.ai) an.

### KI-Verarbeitung mit vertraglicher Bindung

Die eingesetzten KI-Dienste sind vertraglich zur datenschutzkonformen Verarbeitung verpflichtet. Eine Nutzung Ihrer Inhalte für Trainingszwecke findet nicht statt.

### Datensparsamkeit nach Art. 5 DSGVO

Gespeichert wird nur, was nötig ist: das fertige Protokoll. Keine Audioarchive, keine Trainingsdaten, keine Profilbildung.

### Zugriffsschutz und Verschlüsselung

Alle Übertragungen sind TLS-verschlüsselt. Protokolle sind ausschließlich dem jeweiligen Konto zugänglich; ein Zugriff durch Mitarbeitende erfolgt nur, wenn er zur Fehlerbehebung zwingend erforderlich ist.

### Unterstützung bei der Informationspflicht

Der Meeting-Bot kündigt sich beim Beitritt automatisch im Chat an. Wir empfehlen zusätzlich, Teilnehmende bereits in der Kalendereinladung zu informieren.

### Aufsichtsbehörde und Datenschutzbeauftragter

Die Verarbeitungstätigkeiten sind beim Bayerischen Landesamt für Datenschutzaufsicht angezeigt. Ein Datenschutzbeauftragter ist bestellt.

## 6. Technische und organisatorische Maßnahmen

Art. 32 DSGVO verpflichtet zu geeigneten technischen und organisatorischen Maßnahmen. Die folgende Übersicht dokumentiert die getroffenen Vorkehrungen.

| Maßnahme                               | Umsetzung                                                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>Verschlüsselung im Ruhezustand</b>  | Gespeicherte Daten sind mit AES-256 verschlüsselt                                                         |
| <b>Verschlüsselung bei Übertragung</b> | Alle Verbindungen über TLS 1.3                                                                            |
| <b>Mandantentrennung</b>               | Vollständige Trennung der Kundendaten, kein gemeinsamer Datenbankzugriff                                  |
| <b>Backups</b>                         | Redundante Sicherung an mehreren Standorten in Deutschland                                                |
| <b>Verfügbarkeit</b>                   | Professionelle DDoS-Abwehr                                                                                |
| <b>Berechtigungskonzept</b>            | Least-Privilege-Prinzip; Protokollinhalte sind für das Team nicht routinemäßig einsehbar                  |
| <b>Meldung von Vorfällen</b>           | Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden                                                  |
| <b>Authentifizierung</b>               | Mehrfaktor-Authentifizierung für Administrationszugänge; für Nutzerkonten in Pro und Enterprise verfügbar |
| <b>Folgenabschätzung</b>               | Datenschutz-Folgenabschätzung nach Art. 35 DSGVO für kritische Verarbeitungsvorgänge durchgeführt         |

## 7. EU AI Act

---

Die Verordnung (EU) 2024/1689 reguliert den Einsatz von KI-Systemen in der Europäischen Union.

matchminutes ordnet sich der Kategorie geringes Risiko zu: Das System unterstützt Menschen bei einer Aufgabe und trifft keine autonomen Entscheidungen über Personen.

### Erfüllte Anforderungen

- Transparenzpflicht nach Art. 50: Der Meeting-Bot kündigt die KI-gestützte Aufzeichnung beim Beitritt automatisch an
- Keine autonomen Entscheidungen über Personen
- Kein Einsatz zur biometrischen Kategorisierung
- Keine Social-Scoring-Funktionen
- Konformitätserklärung auf Anfrage verfügbar

### Britische Kunden: UK-GDPR

Das Vereinigte Königreich verfügt seit 2021 über eine eigene Datenschutzgesetzgebung, die inhaltlich weitgehend der EU-DSGVO entspricht.

- Die beschriebenen Maßnahmen erfüllen die Anforderungen beider Regelwerke
- Zuständige Aufsichtsbehörde im Vereinigten Königreich ist das Information Commissioner's Office
- Der Datentransfer zwischen EU und UK ist durch den Angemessenheitsbeschluss von Juni 2021 abgedeckt
- Ein Auftragsverarbeitungsvertrag nach UK-GDPR Art. 28 ist auf Anfrage erhältlich

## 8. Deine Pflichten als Verantwortlicher

Datenschutzkonformität entsteht im Zusammenspiel. matchminutes ist Auftragsverarbeiter – verantwortlich im Sinne der DSGVO bleibst du.

### Aufnahme ohne Einwilligung ist strafbar

Nach § 201 StGB ist die Aufnahme des nicht öffentlich gesprochenen Wortes ohne Einwilligung strafbar. Das gilt unabhängig von der DSGVO und unabhängig vom eingesetzten Werkzeug.

Hol vor jeder Aufnahme die Zustimmung aller Beteiligten ein. Der automatische Hinweis des Meeting-Bots informiert die Teilnehmenden, ersetzt aber nicht deine Verantwortung als Gastgeber.

Besondere Vorsicht gilt bei Gesprächen mit externen Personen, Bewerbenden oder Betriebsratsmitgliedern.

### Checkliste vor dem Einsatz

- Teilnehmende werden vor der Aufnahme informiert – idealerweise in der Kalendereinladung und zu Beginn des Termins
- Es liegt eine Rechtsgrundlage vor (Einwilligung oder berechtigtes Interesse nach Abwägung)
- Ein Auftragsverarbeitungsvertrag mit dem Anbieter ist abgeschlossen
- Die Verarbeitung ist im Verzeichnis der Verarbeitungstätigkeiten dokumentiert
- Bei Beschäftigtendaten wurde geprüft, ob der Betriebsrat einzubinden ist
- Das Protokoll enthält keine über den Zweck hinausgehenden personenbezogenen Details
- Aufbewahrungs- und Löschfristen für Protokolle sind intern festgelegt

### Mitbestimmung nicht übersehen

Werkzeuge, die zur Überwachung von Verhalten oder Leistung geeignet sind, unterliegen in Deutschland regelmäßig der Mitbestimmung des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG.

Kläre das vor der Einführung. Eine nachträgliche Auseinandersetzung kostet mehr Zeit als eine frühzeitige Abstimmung.

## 9. Häufige Fragen

---

### **Darf ich ein Meeting ohne Zustimmung aller Teilnehmenden aufnehmen?**

Nein. Nach § 201 StGB ist die Aufnahme nicht öffentlich gesprochener Worte ohne Einwilligung strafbar und mit Freiheitsstrafe bis zu drei Jahren bedroht. Zusätzlich benötigst du nach der DSGVO eine Rechtsgrundlage für die Verarbeitung. In der Praxis: Teilnehmende in der Einladung und zu Beginn des Termins informieren.

### **Was ist ein Auftragsverarbeitungsvertrag und brauche ich einen?**

Ein Auftragsverarbeitungsvertrag nach Art. 28 DSGVO regelt das Verhältnis zwischen dir als Verantwortlichem und matchminutes als Auftragsverarbeiter. Für den geschäftlichen Einsatz ist er erforderlich. Du erhältst ihn unter [info@matchminutes.ai](mailto:info@matchminutes.ai).

### **Wo liegen die Server?**

Speicherung und Protokollerstellung erfolgen in Deutschland beziehungsweise der EU. Beim Einsatz des Meeting-Bots für Online-Meetings wird der Audiostrom über einen US-Dienstleister verarbeitet, abgesichert durch Standardvertragsklauseln. Bei Präsenzaufnahmen und der Browser Extension entfällt dieser Schritt.

### **Was geschieht mit dem Audio nach der Transkription?**

Es wird gelöscht. Wir führen keine Audioarchive. Im Konto verbleibt ausschließlich das Textprotokoll.

### **Werden meine Meeting-Inhalte für KI-Training verwendet?**

Nein. Die eingesetzten Dienste sind vertraglich verpflichtet, Inhalte nicht für Trainingszwecke zu verwenden.

### **Was ist der CLOUD Act und warum ist er relevant?**

Der US CLOUD Act von 2018 erlaubt US-Behörden den Zugriff auf Daten bei US-Unternehmen – auch wenn diese auf europäischen Servern liegen. Betroffen sind unter anderem Microsoft, Google und Amazon Web Services. Durch die Speicherung bei einem deutschen Anbieter ohne US-Konzernbindung besteht dieses Risiko für deine Protokolldaten nicht.

### **Kann ich matchminutes ohne jede Drittlandberührung nutzen?**

Ja. Nutze dafür die Präsenzaufnahme oder die Browser Extension anstelle des Meeting-Bots. Speicherung und Verarbeitung finden dann ausschließlich in Deutschland und der EU statt.

## 10. Dokumente und Ansprechpartner

---

Die folgenden Unterlagen stellen wir auf Anfrage zur Verfügung:

- Auftragsverarbeitungsvertrag nach Art. 28 DSGVO
- Technische und organisatorische Maßnahmen in vollständiger Fassung
- Aktuelle Sub-Prozessor-Liste
- Konformitätserklärung zum EU AI Act

### Kontakt

**AI Sports Boutique GmbH i. G.**

Datenschutzbeauftragter bestellt

[info@matchminutes.ai](mailto:info@matchminutes.ai) · +49 (0) 911 59 821 255

#### Rechtlicher Hinweis

Dieses Handbuch dokumentiert die Datenverarbeitung bei matchminutes.ai und dient der Information. Es ersetzt keine Rechtsberatung.

Für die datenschutzrechtliche Bewertung des Einsatzes in deinem Unternehmen wende dich an deinen Datenschutzbeauftragten oder eine fachkundige Rechtsberatung.

Maßgeblich sind die jeweils gültige Datenschutzerklärung sowie der abgeschlossene Auftragsverarbeitungsvertrag.