Vertrag zur Auftragsverarbeitung für ROOMS

Fassung 1.0 · Stand: 16. November 2026

zwischen

dem Kunden (Verantwortlicher, im Folgenden „Kunde“), wie im Kundenkonto der ROOMS-Konsole angegeben,

und

4Players GmbH, Paul-Stritter-Weg 2, 22297 Hamburg (Auftragsverarbeiter, im Folgenden „4Players“).

§ 1 Gegenstand und Dauer

1. 4Players stellt dem Kunden ROOMS bereit, eine browserbasierte Videokonferenzlösung mit Chat, Dateiablage, Whiteboards, Notizen und optionaler KI-Transkription (im Folgenden „Dienst“), nach den Allgemeinen Geschäftsbedingungen für ROOMS (rooms.golem.de/de/terms, im Folgenden „AGB“). Dabei verarbeitet 4Players personenbezogene Daten im Auftrag des Kunden.
2. Dieser Vertrag ist Anlage 1 der AGB und wird mit ihnen abgeschlossen. Er gilt für die Laufzeit des Vertrags über den Dienst einschließlich einer kostenlosen Testphase und darüber hinaus, solange 4Players Daten des Kunden verarbeitet.
3. Für die Verarbeitung von Daten, für die 4Players selbst Verantwortlicher ist (Vertrags- und Abrechnungsdaten, Betrieb und Sicherheit des Dienstes, Missbrauchsschutz), gilt dieser Vertrag nicht; sie ist in der Datenschutzerklärung (rooms.golem.de/de/privacy) beschrieben.

§ 2 Art, Zweck und Umfang der Verarbeitung

1. **Zweck:** Durchführung von Online-Meetings in der ROOMS-Instanz des Kunden.
2. **Art der Verarbeitung:** Übertragung in Echtzeit, Speicherung, Bereitstellung an Teilnehmer, Transkription und Löschung.
3. **Datenarten:**
   - Anzeigenamen, Avatare, Status und Anwesenheit in Räumen, Rollen und letzter Besuch;
   - Audio- und Videoströme (nicht gespeichert);
   - Chat-Nachrichten (nur zugestellt, nicht auf Servern von 4Players gespeichert);
   - geteilte Dateien mit Dateinamen, -typen und -größen;
   - Whiteboards, Notizen und Raumdokumente;
   - Transkripte mit Anzeigenamen und Zeitangaben (bei Nutzung der KI-Transkription);
   - Sperren und Moderationsereignisse;
   - Verbindungs- und Metadaten.
4. **Kategorien betroffener Personen:** Beschäftigte des Kunden, Gäste und alle anderen Teilnehmer der Meetings des Kunden.
5. Der Kunde stellt sicher, dass er für die Verarbeitung eine Rechtsgrundlage hat, insbesondere für die KI-Transkription. Der Dienst holt vor der Einbeziehung eines Teilnehmers in eine Transkription

dessen Bestätigung ein (Mikrofon bleibt bis zur Bestätigung stumm).

6. Speicherung und Transkription finden ausschließlich in der EU statt. Audio, Video und Chat werden über Medienserver in der Region übertragen, die der Kunde beim Einrichten seiner Instanz über das Gateway wählt. Wählt der Kunde eine Region in der EU, findet keine Verarbeitung außerhalb der EU statt. Wählt er eine Region außerhalb der EU, ist das seine Weisung, Medienströme über Server in dieser Region zu übertragen (ohne Speicherung); es gilt § 6.

§ 3 Weisungen

1. 4Players verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, es sei denn, 4Players ist gesetzlich zur Verarbeitung verpflichtet; in diesem Fall teilt 4Players dem Kunden diese Pflicht vor der Verarbeitung mit, soweit das Gesetz dies nicht verbietet.
2. Die Weisungen sind in diesem Vertrag und den AGB festgelegt und werden vom Kunden vor allem durch die Einstellungen des Dienstes erteilt (zum Beispiel Berechtigungen, Verschlüsselung von Räumen, Aufbewahrungsdauer von Dateien, Start einer Transkription). Weitere Weisungen erteilt der Kunde in Textform an datenschutz@4players.de.
3. Ist 4Players der Ansicht, dass eine Weisung gegen Datenschutzrecht verstößt, weist 4Players den Kunden unverzüglich darauf hin.

§ 4 Pflichten von 4Players

1. 4Players verpflichtet alle Personen, die Zugang zu den Daten haben, zur Vertraulichkeit, soweit sie nicht einer gesetzlichen Verschwiegenheitspflicht unterliegen.
2. 4Players trifft die technischen und organisatorischen Maßnahmen nach **Anlage 1** und passt sie dem Stand der Technik an. Änderungen dürfen das Schutzniveau nicht unterschreiten.
3. 4Players unterstützt den Kunden mit geeigneten Maßnahmen bei der Erfüllung der Rechte betroffener Personen (§ 7), bei den Pflichten nach Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen.
4. 4Players meldet dem Kunden Verletzungen des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, mit den Angaben nach Art. 33 Abs. 3 DSGVO, soweit verfügbar.
5. 4Players hat einen Datenschutzbeauftragten bestellt: 4Players GmbH, Der Datenschutzbeauftragte, Paul-Stritter-Weg 2, 22297 Hamburg, datenschutz@4players.de.

§ 5 Unterauftragsverarbeiter

1. Der Kunde erteilt 4Players die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter stehen in **Anlage 2** (veröffentlicht unter rooms.golem.de/de/subprocessors) und gelten als genehmigt.
2. 4Players informiert den Kunden mindestens 30 Tage vor dem Hinzufügen oder Ersetzen eines Unterauftragsverarbeiters per E-Mail an die Adresse des Kundenkontos. Der Kunde kann der Änderung innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund in Textform widersprechen. Können sich die Parteien nicht einigen, kann der Kunde den Vertrag über den Dienst zum Zeitpunkt der Änderung aus wichtigem Grund kündigen; im Voraus gezahlte Entgelte erstattet 4Players anteilig.

3. 4Players verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieses Vertrags entsprechen (Art. 28 Abs. 4 DSGVO).
4. Leistungen, die 4Players als Nebenleistung in Anspruch nimmt (zum Beispiel Telekommunikation), sind keine Unterauftragsverarbeitung.

§ 6 Übermittlung in Drittländer

Eine Verarbeitung außerhalb der EU oder des EWR oder durch Anbieter mit Sitz in einem Drittland erfolgt nur in den Fällen nach § 2 Abs. 6 und Anlage 2 und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere auf Grundlage eines Angemessenheitsbeschlusses (zum Beispiel EU-US Data Privacy Framework) oder von Standardvertragsklauseln der EU-Kommission.

§ 7 Rechte betroffener Personen

1. Wendet sich eine betroffene Person mit einem Anliegen zu Daten des Kunden an 4Players, leitet 4Players die Anfrage unverzüglich an den Kunden weiter und beantwortet sie nicht selbst, es sei denn, der Kunde weist dies an.
2. Viele Daten liegen nur auf den Geräten der Teilnehmer (Chat-Verläufe, Avatare, Aktivitätsprotokolle, Kopien von Transkripten) und sind 4Players nicht zugänglich. Daten auf den Servern kann der Kunde überwiegend selbst im Dienst löschen (Räume, Dateien). Wo das nicht möglich ist, unterstützt 4Players auf Anfrage, in vertretbarem Umfang kostenlos.

§ 8 Kontrollrechte

1. 4Players weist dem Kunden die Einhaltung dieses Vertrags auf Anfrage mit geeigneten Unterlagen nach, insbesondere mit einer Beschreibung der Maßnahmen nach Anlage 1 und Auskünften zu ihrer Umsetzung.
2. Darüber hinaus kann der Kunde nach rechtzeitiger Anmeldung (in der Regel 30 Tage) während der Geschäftszeiten Kontrollen vor Ort durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, ohne den Betrieb unverhältnismäßig zu stören. Die Kosten einer Kontrolle trägt der Kunde.

§ 9 Löschung und Rückgabe

1. Während der Laufzeit kann der Kunde Transkripte, Dateien und andere Inhalte im Dienst herunterladen.
2. Transkripte löscht 4Players etwa 11 Minuten nach Ende der jeweiligen Aufnahme. Während der Laufzeit gelten für die übrigen Inhalte die Fristen nach Anlage 1, Nr. 4. Nach Ende des Vertrags über den Dienst löscht 4Players die übrigen Inhalte der Instanz (Whiteboards, Notizen, Raumdokumente, Dateien, Mitgliedsdaten) innerhalb von 30 Tagen.
3. Den Projekt-Datensatz der Instanz (Adresse, Tarif, Abrechnungsbezug) bewahrt 4Players als Teil der Abrechnungsunterlagen bis zum Ablauf der gesetzlichen Aufbewahrungsfrist der Rechnungen auf.
4. Kopien auf den Geräten der Teilnehmer liegen außerhalb des Einflussbereichs von 4Players.

§ 10 Haftung, Vorrang, Schlussbestimmungen

1. Für die Haftung gelten Art. 82 DSGVO und die AGB.
2. Bei Widersprüchen zwischen diesem Vertrag und den AGB geht dieser Vertrag in Fragen des Datenschutzes vor.
3. Änderungen dieses Vertrags bedürfen der Textform. 4Players kann diesen Vertrag ändern, soweit dies wegen gesetzlicher Änderungen oder Änderungen des Dienstes nötig ist und das Schutzniveau nicht sinkt; der Kunde wird vorab per E-Mail informiert.
4. Es gilt deutsches Recht. Gerichtsstand ist Hamburg, soweit gesetzlich zulässig.

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

1. Vertraulichkeit

Verschlüsselung und Datenminimierung im Dienst

- Neue Räume werden standardmäßig mit Passwort angelegt und sind dann Ende-zu-Ende verschlüsselt für Audio, Chat, Profildaten, Whiteboards, Notizen und – standardmäßig – Dateien (AES-256-GCM, Verschlüsselung im Browser). Das Passwort wird nur im Fragment des Einladungslinks übertragen und nie an den Server gesendet; der Server speichert nur einen Hash eines daraus abgeleiteten Schlüssels.
- Nicht Ende-zu-Ende verschlüsselt sind Video, Metadaten (Dateinamen, -größen, -typen, Verbindungsdaten, Anwesenheit), Adressen von Links mit Vorschau und Räume ohne Passwort. Alle Verbindungen sind auf dem Transportweg mit TLS verschlüsselt.
- Audio und Video werden nicht aufgezeichnet. Chat-Verläufe werden nicht auf Servern gespeichert. Für Ratenbegrenzung werden IP-Adressen nur als verschlüsselter Hash verwendet.
- KI-Transkription: Audio wird nur im Arbeitsspeicher gepuffert und nicht gespeichert; der Transkriptionsdienst erhält für verschlüsselte Räume einen Schlüssel nur für die Dauer der Aufnahme, der beim Start und Ende gewechselt wird. Keine Stimmerkennung, keine Zusammenfassungen (Zusatzfunktionen des Transkriptionsdienstes sind ausgeschaltet und können nur vom Kunden selbst aktiviert werden), keine Nutzung zum Training.

Zutrittskontrolle – Server, Transkriptionsdienst und gespeicherte Daten liegen ausschließlich in Rechenzentren in der EU: auf bei OVH gemieteten Servern und auf eigener Hardware im Rechenzentrum von WIIT in Düsseldorf. Medienserver außerhalb der EU werden nur nach § 2 Abs. 6 bei den Anbietern nach Anlage 2 genutzt. Jedes eingesetzte Rechenzentrum hat geregelte Zutrittskontrollen.

Zugangskontrolle – Alle Systeme sind nur über ein VPN erreichbar. Administratoren melden sich per SSH an.

Zugriffskontrolle – Administrativen Zugriff auf die Systeme haben nur Administratoren von 4Players; ihre Zugriffe werden protokolliert. ROOMS ist ein automatisierter Dienst: Im Regelbetrieb sehen Beschäftigte von 4Players keine Inhalte. Administratoren können Daten nur in technischem Zusammenhang einsehen, etwa bei Fehlerbehebungen oder technischen Störungen. Mitarbeiter des First-Level-Supports (Golem) erhalten keinen Zugriff auf Inhalte der Instanzen.

Trennungskontrolle – Jede Instanz ist ein eigenes Projekt mit eigenen Projekten im Transkriptionsdienst. Die Daten liegen logisch getrennt in gemeinsamen Datenbanken.

2. Integrität

- **Weitergabekontrolle:** TLS für alle Verbindungen; Ende-zu-Ende-Verschlüsselung wie oben.
- **Eingabekontrolle:** Moderationsereignisse (Entfernen, Sperren, Entsperren) werden mit Nutzer- und Moderatorkennung protokolliert; administrative Zugriffe ebenfalls.

3. Verfügbarkeit und Belastbarkeit

Alle Systeme sind redundant aufgebaut und durch Backups gesichert. Für Ausfälle gibt es Notfallpläne.

4. Löschung und Speicherbegrenzung

Daten	Löschung
Teilnehmerdaten im Raum	etwa 3 Minuten nach dem Verlassen
Mitgliedsdaten (Rolle, letzter Besuch)	90 Tage nach dem letzten Besuch, spätestens 30 Tage nach Vertragsende
Geteilte Dateien	nach der vom Hochladenden gewählten Frist (1 Stunde nach Leeren des Raums, 1 Tag, 1 Woche) oder mit dem Raum, spätestens 30 Tage nach Vertragsende
Whiteboards, Notizen, Raumdokumente	mit dem Raum, spätestens 30 Tage nach Vertragsende
Sperren	mit Ablauf der Sperre
Transkripte im Transkriptionsdienst	etwa 11 Minuten nach Ende der Aufnahme (ROOMS löscht die Sitzung über die API des Transkriptionsdienstes), Wiederholung bis zu einem Tag
Server-Logs	nach 10 Tagen
Projekt-Datensatz der Instanz (Abrechnung)	nach Ablauf der Aufbewahrungsfrist der Rechnungen

5. Verfahren zur regelmäßigen Überprüfung

4Players hat nach den gesetzlichen Vorgaben einen Datenschutzbeauftragten bestellt, der regelmäßig geschult wird. Weil ROOMS ein automatisierter Dienst ist, gibt es keine Abläufe, in denen Beschäftigte im Regelbetrieb Inhalte sehen; Zugriffe von Administratoren im technischen Zusammenhang werden protokolliert.

Anlage 2 – Unterauftragsverarbeiter

Die jeweils aktuelle Liste der Unterauftragsverarbeiter mit Zweck, Daten und Standort ist veröffentlicht unter rooms.golem.de/de/subprocessors. Änderungen kündigt 4Players nach § 5 Abs. 2 an.