Data Processing Agreement for ROOMS

Version 1.0 · As of 16 November 2026

This English version is provided for convenience; the German version is legally binding.

between

the customer (controller, the “Customer”), as stated in the customer account of the ROOMS console,

and

4Players GmbH, Paul-Stritter-Weg 2, 22297 Hamburg, Germany (processor, “4Players”).

§ 1 Subject matter and duration

1. 4Players provides the Customer with ROOMS, a browser-based video conferencing solution with chat, file sharing, whiteboards, notes and optional AI transcription (the “Service”), under the general terms and conditions for ROOMS (rooms.golem.de/terms, the “Terms”). In doing so, 4Players processes personal data on behalf of the Customer.
2. This agreement is Annex 1 to the Terms and is concluded together with them. It applies for the term of the contract for the Service, including a free trial, and beyond for as long as 4Players processes the Customer’s data.
3. This agreement does not apply to processing for which 4Players is itself the controller (contract and billing data, operation and security of the Service, abuse prevention); that processing is described in the privacy policy (rooms.golem.de/privacy).

§ 2 Nature, purpose and scope of processing

1. **Purpose:** holding online meetings in the Customer’s ROOMS instance.
2. **Nature of processing:** real-time transmission, storage, provision to participants, transcription and deletion.
3. **Types of data:**
   - display names, avatars, status and presence in rooms, roles and last visit;
   - audio and video streams (not stored);
   - chat messages (delivered only, not stored on 4Players’ servers);
   - shared files with file names, types and sizes;
   - whiteboards, notes and room documents;
   - transcripts with display names and times (when AI transcription is used);
   - bans and moderation events;
   - connection data and metadata.
4. **Categories of data subjects:** the Customer’s employees, guests and all other participants in the Customer’s meetings.
5. The Customer ensures that it has a legal basis for the processing, in particular for AI transcription. Before a participant is included in a transcription, the Service asks for their confirmation

(the microphone stays muted until they confirm).

6. Storage and transcription take place exclusively in the EU. Audio, video and chat are relayed through media servers in the region the Customer chooses through the gateway when setting up its instance. If the Customer chooses a region in the EU, no processing takes place outside the EU. If it chooses a region outside the EU, this is its instruction to relay media streams through servers in that region (without storage); § 6 applies.

§ 3 Instructions

1. 4Players processes the data only on documented instructions from the Customer, unless 4Players is required to do so by law; in that case, 4Players informs the Customer of that legal requirement before processing, unless the law prohibits this.
2. The instructions are set out in this agreement and the Terms and are given by the Customer mainly through the settings of the Service (for example permissions, encryption of rooms, retention of files, starting a transcription). The Customer gives further instructions in text form to datenschutz@4players.de.
3. If 4Players considers that an instruction infringes data protection law, it informs the Customer without delay.

§ 4 Obligations of 4Players

1. 4Players commits all persons with access to the data to confidentiality unless they are under a statutory obligation of confidentiality.
2. 4Players takes the technical and organisational measures set out in **Annex 1** and adapts them to the state of the art. Changes must not reduce the level of protection.
3. 4Players assists the Customer with appropriate measures in fulfilling the rights of data subjects (§ 7) and the obligations under Art. 32 to 36 GDPR, in particular data protection impact assessments.
4. 4Players notifies the Customer of personal data breaches without undue delay, at the latest within 48 hours of becoming aware of them, with the information under Art. 33(3) GDPR as far as available.
5. 4Players has appointed a data protection officer: 4Players GmbH, Data Protection Officer, Paul-Stritter-Weg 2, 22297 Hamburg, Germany, datenschutz@4players.de.

§ 5 Sub-processors

1. The Customer gives 4Players general authorisation to engage sub-processors. The sub-processors engaged at the conclusion of the contract are listed in **Annex 2** (published at rooms.golem.de/subprocessors) and are deemed approved.
2. 4Players informs the Customer by email to the address of the customer account at least 30 days before adding or replacing a sub-processor. The Customer may object to the change in text form within this period for good cause relating to data protection. If the parties cannot agree, the Customer may terminate the contract for the Service for good cause as of the time of the change; 4Players refunds prepaid fees pro rata.

3. 4Players contractually binds every sub-processor to data protection obligations equivalent to those of this agreement (Art. 28(4) GDPR).
4. Services that 4Players uses as ancillary services (for example telecommunications) are not sub-processing.

§ 6 Transfers to third countries

Processing outside the EU or the EEA, or by providers based in a third country, takes place only in the cases under § 2(6) and Annex 2, and only if the requirements of Art. 44 et seq. GDPR are met, in particular on the basis of an adequacy decision (for example the EU-US Data Privacy Framework) or the European Commission's standard contractual clauses.

§ 7 Rights of data subjects

1. If a data subject contacts 4Players about the Customer's data, 4Players forwards the request to the Customer without delay and does not answer it itself unless the Customer instructs it to.
2. Much of the data is held only on the participants' devices (chat histories, avatars, activity logs, copies of transcripts) and is not accessible to 4Players. The Customer can delete most data on the servers itself in the Service (rooms, files). Where this is not possible, 4Players assists on request, free of charge within a reasonable scope.

§ 8 Audits

1. On request, 4Players demonstrates compliance with this agreement with appropriate documentation, in particular a description of the measures in Annex 1 and information on their implementation.
2. In addition, after timely notice (usually 30 days), the Customer may carry out on-site audits during business hours, or have them carried out by an auditor bound to confidentiality, without disrupting operations unreasonably. The Customer bears the costs of an audit.

§ 9 Deletion and return

1. During the term, the Customer can download transcripts, files and other content in the Service.
2. 4Players deletes transcripts about 11 minutes after the end of each recording. During the term, the periods in Annex 1, no. 4 apply to the other content. After the contract for the Service ends, 4Players deletes the remaining content of the instance (whiteboards, notes, room documents, files, member records) within 30 days.
3. 4Players keeps the project record of the instance (address, plan, billing reference) as part of its billing records until the statutory retention period for the invoices expires.
4. Copies on participants' devices are outside 4Players' control.

§ 10 Liability, precedence, final provisions

1. Liability is governed by Art. 82 GDPR and the Terms.
2. In the event of conflicts between this agreement and the Terms, this agreement prevails in matters of data protection.

3. Changes to this agreement require text form. 4Players may change this agreement where necessary because of changes in law or in the Service, provided the level of protection does not decrease; the Customer is informed in advance by email.
4. German law applies. The place of jurisdiction is Hamburg, Germany, to the extent permitted by law.

Annex 1 – Technical and organisational measures (Art. 32 GDPR)

1. Confidentiality

Encryption and data minimisation in the Service

- New rooms are created with a password by default and are then end-to-end encrypted for audio, chat, profile data, whiteboards, notes and – by default – files (AES-256-GCM, encrypted in the browser). The password is transmitted only in the fragment of the invite link and is never sent to the server; the server stores only a hash of a key derived from it.
- Not end-to-end encrypted are video, metadata (file names, sizes, types, connection data, presence), addresses of links shown with a preview, and rooms without a password. All connections are encrypted in transit with TLS.
- Audio and video are not recorded. Chat histories are not stored on servers. For rate limiting, IP addresses are used only as a keyed hash.
- AI transcription: audio is buffered in memory only and not stored; for encrypted rooms the transcription service receives a key only for the duration of the recording, which is changed when the recording starts and ends. No voice identification, no summaries (additional functions of the transcription service are switched off and can be enabled only by the Customer itself), no use for training.

Physical access control – Servers, the transcription service and stored data are located exclusively in data centres in the EU: on servers rented from OVH and on own hardware in the WIIT data centre in Düsseldorf. Media servers outside the EU are used only under § 2(6) with the providers listed in Annex 2. Every data centre used has regulated access controls.

System access control – All systems are reachable only through a VPN. Administrators log in via SSH.

Data access control – Only administrators of 4Players have administrative access to the systems; their access is logged. ROOMS is an automated service: in normal operation, 4Players staff do not see any content. Administrators can view data only in a technical context, for example when fixing bugs or resolving technical problems. First-level support staff (Golem) have no access to the content of instances.

Separation control – Each instance is a separate project with its own projects in the transcription service. The data is logically separated in shared databases.

2. Integrity

- **Transfer control:** TLS for all connections; end-to-end encryption as above.
- **Input control:** moderation events (removing, banning, unbanning) are logged with the user and moderator IDs; so is administrative access.

3. Availability and resilience

All systems are set up redundantly and secured by backups. Emergency plans exist for outages.

4. Deletion and storage limitation

Data	Deletion
Participant records in a room	about 3 minutes after leaving
Member records (role, last visit)	90 days after the last visit, at the latest 30 days after the contract ends
Shared files	after the period chosen by the uploader (1 hour after the room empties, 1 day, 1 week) or with the room, at the latest 30 days after the contract ends
Whiteboards, notes, room documents	with the room, at the latest 30 days after the contract ends
Bans	when the ban expires
Transcripts in the transcription service	about 11 minutes after the recording ends (ROOMS deletes the session through the transcription service's API), retried for up to a day
Server logs	after 10 days
Project record of the instance (billing)	when the retention period for the invoices expires

5. Procedures for regular review

As required by law, 4Players has appointed a data protection officer who receives regular training. Because ROOMS is an automated service, there are no processes in which staff see content in normal operation; administrators' access in a technical context is logged.

Annex 2 – Sub-processors

The current list of sub-processors with purpose, data and location is published at rooms.golem.de/subprocessors. 4Players announces changes in accordance with § 5(2).