ROOM ATLAS BUSINESS

Data processing agreement

This translation is for your information. Only the German version (room-atlas.com/avv) is binding.

Agreement under Art. 28(3) GDPR between the company that books Room Atlas Business (“controller”) and Green T GmbH & Co. KG, Klingenberg 20, 25451 Quickborn, Germany (Pinneberg Local Court, HRA 8141 PI), represented by its general partner Green T Corporate GmbH (Pinneberg Local Court, HRB 13322 PI), which is represented by its managing directors Stefan Heyn and Jonas Heyn (“processor”). The agreement is an integral part of every Room Atlas Business subscription and supplements the terms (room-atlas.com/agb). Version: 20 November 2026.

1. Subject and duration

- The processor provides the controller with Room Atlas Business (the “main contract”): projects and rooms with customer details and measurements, syncing between the devices and accounts of the team, projects in the team, the team chat with files, Business Support, reports and the AI features.
- In doing so, it processes personal data that the controller and its team members record about their customers in Room Atlas on behalf of the controller.
- The agreement applies as long as Business exists and beyond that as long as the processor still processes such data.

2. Nature, purpose and scope of the processing

The processor provides the following services:

- storing and syncing projects and rooms with customer details, photos, scans, surveys, measurements, impulse responses, settings and images from product suggestions between the devices of the controller and its team members (each team member through their own account);
- hearing profiles: hearing test values of the person for whom a room is calibrated, with the filter bands calculated from them. Once it has been confirmed in the app that the person has consented, they are stored with the room, synced and shared in the team; only the hearing profile goes into room files, never the filter bands;
- projects in the team: providing projects and rooms that a team member shares with others, with the rights “View only” or “Can edit”. When the sharing of a project ends, every team member who did not create it loses it, with its rooms, customer details and hearing profiles. Anyone who no longer belongs to the company (left the team, removed, no seat any more) loses all of the company's projects, including those they created themselves, on all their devices and in their sync. The owner of the company keeps their projects;
- team chat: messages and attached files (room files, projects as ZIP files, preview images);
- product suggestions in the picture: when a team member triggers them, the room photo, a mask of the marked area, product images and product details go to OpenAI via room-atlas.com, and the image with the product comes back. The processor does not store the photo;
- managing the team (invitations, roles, rights);
- sending system emails and notifications (such as invitations, replies in support);
- Business Support in chat and by email;
- backing up and deleting the data.

Not processed on behalf: reports as PDF (they are created on the device and are only passed on by the controller); 3D models of the controller’s own products (they contain no personal data). Hearing profiles are health data (Art. 9 GDPR): before entering them, the controller obtains the explicit consent of the data subject and informs them that they can withdraw it at any time. The processor processes data about the own account,

the subscription and billing as an independent controller; the privacy policy (room-atlas.com/datenschutz) applies to this. The processor pursues no other purposes with the data. Types of data and data subjects: Annex 1.

3. Instructions

- The processor processes the data only on documented instructions from the controller, including with regard to transfers to third countries, unless it is required to do so by Union or Member State law. In that case it informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (Art. 28(3)(a) GDPR).
- The main contract and this agreement are the first instruction. Further instructions are the use of the features of Room Atlas by the controller and its team members, such as deleting a project or removing a team member, as well as instructions in text form (email is sufficient) to info@room-atlas.com.
- The owner of the company in Room Atlas and the legal representatives of the controller are entitled to give instructions.
- If the processor considers an instruction unlawful, it points this out without delay. It may suspend its execution until it is confirmed.

4. Confidentiality

- The processor only uses persons who are bound to confidentiality or subject to a statutory obligation of secrecy. The obligation continues after the end of their work.
- It accesses content only where this is necessary for operation, security or a request from the controller.

5. Security of processing

- The processor takes the technical and organisational measures under Art. 32 GDPR set out in Annex 2 and keeps them up to date with the state of the art.
- It may replace them with equivalent or better ones; the level of protection must not decrease. It informs the controller of material changes in text form.

6. Sub-processors

- The controller approves the sub-processors in Annex 3 (general authorisation under Art. 28(2) GDPR).
- If the processor wants to add or replace a sub-processor, it gives notice in text form at least 30 days in advance. The controller can object within this period for an important reason under data protection law. If the parties find no solution, the controller can terminate Business as of the date of the change.
- The processor contractually binds every sub-processor to the same data protection obligations. It is liable for them as for its own actions.
- Data only goes to third countries with appropriate safeguards (Annex 3): adequacy decision, EU-US Data Privacy Framework or EU standard contractual clauses.

7. Rights of data subjects

- The processor supports the controller with appropriate measures in responding to requests from data subjects (Art. 12 to 22 GDPR).
- The controller can exercise most rights itself in Room Atlas: view, change, export as a file (room file, project as ZIP file) and delete customer details and projects.
- The processor forwards requests from data subjects that reach it directly to the controller without delay.

8. Assistance, notification of breaches

- The processor assists the controller with the obligations under Art. 32 to 36 GDPR: security, notification of personal data breaches, data protection impact assessments and prior consultation of the supervisory authority.
- It notifies the controller of a breach of the security of its personal data without undue delay, at the latest 48 hours after becoming aware of it, in text form, with the information under Art. 33(3) GDPR as far as available.

9. Evidence and audits

- The processor makes available to the controller all information necessary to demonstrate compliance with the obligations of this agreement, such as the description of the measures (Annex 2) and the contracts and certifications of its sub-processors.
- The controller can carry out audits once a year, including inspections, or have them carried out by an auditor bound to confidentiality (Art. 28(3)(h) GDPR): with at least 14 days' notice and during normal business hours, and more often if there is a specific reason. The controller can accept evidence such as certificates of the sub-processors instead of an inspection.

10. End of the agreement, return and deletion

- Until Business ends, the controller can export its projects and rooms as files at any time and delete them in the app.
- When Business ends, Room Atlas removes the hearing profiles of the rooms. The owner keeps their projects and rooms as long as their account exists. Team members lose all of the company's projects with their rooms, customer details and hearing profiles, also on their devices and in their sync. The processor deletes the company 90 days after Business ends, with its memberships, projects in the team, team chat and report templates, including their files; if no Business subscription ever ran, 90 days after the company was created. The owner's account remains.
- On instruction, the processor hands over the data (export as a file) or deletes it within 30 days (Art. 28(3)(g) GDPR), unless there is a statutory obligation to retain it. On request, it confirms the deletion in text form.
- Backups are overwritten on a rolling basis: at the database provider after 7 days, the own encrypted backup after 14 days.

11. Liability, final provisions

- Liability is governed by Art. 82 GDPR and the main contract.
- In matters of data protection, this agreement takes precedence over the main contract. Changes must be in text form. German law applies.
- The agreement is concluded with the booking of Business. It applies without a signature because both parties accept it electronically (Art. 28(9) GDPR). A copy is always available at room-atlas.com/avv and as a PDF.

Annex 1: Subject matter of the processing

- **Types of data:** details of the controller's customers per project and room (name, street, postcode, town, email, phone); room data (name, description, photos, scans, surveys, floor plans, furnishings, speaker and listening positions); measurements, impulse responses and settings; images from product suggestions; own paragraphs in reports; messages and files in the team chat and in Business Support; hearing profiles (hearing test values and the filter bands calculated from them, health data under Art. 9 GDPR); team data (email address, role, rights, status of the invitation).
- **Data subjects:** customers and prospects of the controller and their contacts; persons who appear in photos

or messages; persons whose hearing test values are entered; team members of the controller.

- **Locations:** database, sign-in and file storage in Frankfurt am Main; server functions of the website in Frankfurt am Main; own encrypted backup in Falkenstein (Germany); email sending from Ireland, receipt of replies in the USA; product suggestions in the picture at OpenAI, also in the USA; notifications on iPhone and iPad via Apple.
- **Deletion:** by the controller in the app, otherwise under section 10.

Annex 2: Technical and organisational measures (Art. 32 GDPR)

- **Access:** sign-in with email and password (at least 8 characters, passwords known from data leaks blocked) or with Apple or Google; passkeys and two-factor sign-in; brake against guessing; sessions that expire; sign out on all devices in the app.
- **Access control:** row and path protection in database and file storage: every account only sees its own content, projects in the team only those shared, the team chat only members of the company with a seat. Keys with full rights only on the server side, no keys in the source code.
- **Separation:** Room Atlas data in its own database, separate from other products of the processor.
- **Encryption:** transfer only via TLS; disks and backups of the database provider encrypted (AES-256); own backup encrypted before it leaves the server.
- **Data minimisation:** sound recordings and the microphone calibration remain on the device. Hearing profiles only leave the device once it is confirmed in the app that the person has consented (section 2); they are then synchronised with the room, shared in the team with those the project is released to, and included in room files, but never the filter bands calculated from them. They never go to OpenAI or to support. Originals of edited pictures remain on the device. Photos in the team chat without their metadata (such as the location). The team chat only accepts files from Room Atlas. The server does not store photos for product suggestions; according to OpenAI, data from the interface is not used for training and is kept for at most 30 days for abuse detection.
- **Availability:** daily backup by the database provider (7 days) and an own, encrypted daily backup of database and file storage in Germany (14 days); daily backup on the user’s device (14 days); the projects are also on the controller’s devices.
- **Integrity:** syncing with a version number and checksum per entry; conflicts are not silently overwritten; security headers on the website.
- **Processor control:** data processing agreements with all sub-processors (Annex 3); annual review.
- **Organisation:** two-factor on all provider accounts; emergency access in the password manager; regular review of code and configuration for security and data protection.

Annex 3: Approved sub-processors

- **Supabase Pte. Ltd.** , 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513: database, sign-in, file storage, syncing, projects in the team, team chat. Location: Frankfurt am Main (AWS eu-central-1); access from outside the EU cannot be ruled out. Safeguard: data processing agreement with EU standard contractual clauses.
- **Vercel Inc.** , 440 N Barranca Ave #4133, Covina, CA 91723, USA: room-atlas.com with account, company and team, Business Support and forwarding of product suggestions. Location: server functions Frankfurt am Main, static delivery worldwide. Safeguard: data processing agreement, EU-US Data Privacy Framework, EU standard contractual clauses.
- **OpenAI Ireland Ltd.** , Dublin, Ireland, with OpenAI, L.L.C., USA: product suggestions in the picture, only when a team member triggers them. Location: also USA. Safeguard: data processing agreement with EU standard contractual clauses.
- **Plus Five Five, Inc. (Resend)** , 2261 Market Street #5039, San Francisco, CA 94114, USA: sending system emails (such as team invitations) and receiving replies to support. Location: sending Ireland

(eu-west-1), receipt and account data USA. Safeguard: data processing agreement, EU-US Data Privacy Framework, EU standard contractual clauses.

- **Hetzner Online GmbH** , Industriestraße 25, 91710 Gunzenhausen, Germany: own encrypted backup of database and file storage. Location: Falkenstein (Germany). Safeguard: data processing agreement.
- **Apple Inc.** , One Apple Park Way, Cupertino, CA 95014, USA: delivery of notifications to iPhone and iPad (Apple Push Notification Service). Location: USA. Safeguard: EU-US Data Privacy Framework, EU standard contractual clauses.
- **Fly.io, Inc.** , USA: operation of the test version in the browser, as far as team members use it. Location: Frankfurt am Main. Safeguard: data processing agreement with EU standard contractual clauses.

The processor gives notice of changes to this list at least 30 days in advance in text form (section 6).