# Data Processing Agreement

Meeting Room 365, LLC. Version 1, November 2, 2026.

## 1. Who this covers and when it applies

This agreement is between Meeting Room 365, LLC ("we", "us") and the customer that accepted our Terms of Service at meetingroom365.com/tos ("you"). It is part of the Terms. It takes effect when you accept the Terms, or on the date above if you already had. You do not need to sign it; if you want a countersigned copy, sign the last page and send it to support@meetingroom365.com.

It applies whenever we process personal data on your behalf to provide our services (room displays, room finder and analytics, desk booking, visitor management and maps). If it conflicts with the Terms, this agreement wins on personal data. If it conflicts with the Standard Contractual Clauses in section 9, the Clauses win.

Words like "personal data", "processing", "controller", "processor", "data subject" and "personal data breach" mean what they mean in the EU General Data Protection Regulation 2016/679 (GDPR).

## 2. Roles

You are the controller of the personal data, or a processor acting for your own client. We are your processor, or your subprocessor. Annex I lists the data, the people it is about and why we process it.

## 3. Your instructions

We process personal data only on your documented instructions. The Terms, this agreement, the way you configure the service and your requests to support are those instructions. We will tell you if we believe an instruction breaks the GDPR or other EU or member state data protection law. If EU or member state law requires us to process the data in another way, we will tell you first unless that law forbids it.

You are responsible for having a lawful basis for the processing and for giving your staff and visitors the notices the law requires.

## 4. Confidentiality

Everyone we allow to process the data is bound by a duty of confidentiality, by contract or by law.

## 5. Security

We maintain the technical and organizational measures in Annex II. We may change them, but never in a way that lowers the overall protection of the data.

## 6. Subprocessors

You give us general authorization to use the subprocessors listed in Annex III. We bind each one to data protection terms that protect the data at least as well as this agreement, and we remain liable to you for their work.

We will email you at least 30 days before we add or replace a subprocessor. You may object on reasonable data protection grounds within those 30 days. If we cannot address the objection, you may cancel the affected services before the change takes effect.

## 7. Help we give you

1. **Data subject requests.** If someone asks us directly to access, correct or delete their data, we pass the request to you and do not answer it ourselves unless you ask us to. We help you answer requests as far as the service allows.

2. **Breaches.** We notify you by email to your account administrators without undue delay, and within 48 hours, after we become aware of a personal data breach affecting your data. We tell you what we know, what we are doing about it, and keep you updated as we learn more.
3. **Assessments.** We give you the information we have that you need for a data protection impact assessment or a consultation with a supervisory authority.

## 8. Audits

We make available the information needed to show that we meet this agreement: this agreement, our security page at meetingroom365.com/security, and written answers to a reasonable security questionnaire, once a year. If that is not enough, or a supervisory authority requires it, you may audit us, or have an independent auditor bound by confidentiality do so, with 30 days' notice, during business hours, at your cost.

## 9. International transfers

We are in the United States. Where your use of the service transfers personal data from the European Economic Area to us, the Standard Contractual Clauses adopted by the European Commission in Decision 2021/914 apply, Module 2 (controller to processor). They are incorporated into this agreement by reference, and you and we are deemed to have signed them, with you as data exporter and us as data importer. These choices apply:

- Clause 7 (docking clause) applies.
- Clause 9(a): Option 2, general written authorization, with the 30 days' notice in section 6.
- Clause 11(a): the optional independent dispute resolution wording does not apply.
- Clause 13: the supervisory authority is the one set out in Clause 13(a) and Annex I.C.
- Clause 17: the Clauses are governed by the law of Ireland.
- Clause 18: disputes go to the courts of Ireland.
- Annexes I, II and III of the Clauses are Annexes I, II and III of this agreement.

**United Kingdom.** For transfers from the UK, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner (version B1.0, in force March 21, 2022) applies and is incorporated by reference. Table 1 is completed by Annex I. Table 2 is completed by the module and choices above. Table 3 is completed by Annexes I to III. For Table 4, either party may end the Addendum as its Section 19 allows.

**Switzerland.** For transfers from Switzerland, the Clauses apply as above, with the Swiss Federal Data Protection and Information Commissioner as supervisory authority and references to the GDPR read as references to the Swiss Federal Act on Data Protection.

## 10. When the service ends

When you stop using the service, ask support to erase your account and its data. We erase it from our live systems within 30 days, unless law requires us to keep it, and confirm when it's done. Copies in backups are overwritten as the backups rotate.

## 11. Liability and term

Each party's liability under this agreement is subject to the limitation of liability in the Terms, except where the Clauses in section 9 do not allow it. This agreement lasts as long as we process personal data for you.

## Annex I. Parties and processing

### A. Parties

| | |
|---|---|
| **Data exporter** | The customer that accepted the Terms, with the name, address and contact on its Meeting Room 365 account. Role: controller (or processor for its own client). Activity: uses our services for its rooms, desks, visitors and floor plans. |
| **Data importer** | Meeting Room 365, LLC, a Washington limited liability company. 440 N Barranca Ave #3659, Covina, CA 91723, United States. Contact: James Futhey, Security and Data Protection, support@meetingroom365.com. Role: processor. Activity: provides the services described in the Terms. |

### B. Description of the processing

| | |
|---|---|
| **Data subjects** | Your administrators and staff; people named in the calendars of rooms you connect (organizers and attendees); people who book desks; visitors and their hosts. |
| **Personal data** | Administrator names and email addresses; room and resource email addresses.<br>Calendar details shown on displays: meeting subject, organizer and times. We don't copy your calendars. We store the current and next meeting shown on each display, and room finder and analytics keep 15-minute snapshots of each room's status and occupancy, and, if you turn it on, the meeting subject and organizer.<br>Desk bookings: name, email and booking times.<br>Visitors: name, email, phone number, company, host, visit times, signed documents (such as NDAs) and photos, as your kiosk is configured to collect.<br>Support screenshots of our app on your displays.<br>Logs: IP addresses, email addresses and browser details of people using the admin and displays. |
| **Sensitive data** | None is intended. You should not configure the service to collect special category data. |
| **Frequency** | Continuous, while you use the service. |
| **Nature and purpose** | Hosting, storing, displaying and sending (by email and SMS) the data, solely to provide the services to you and to support you. |
| **Retention** | While your account is active. After the retention window set on your kiosk (730 days by default), visit records are anonymized and their files deleted. Everything else is deleted as section 10 describes. |
| **Transfers to subprocessors** | As listed in Annex III, for the purposes listed there, for as long as we provide the services. |

### C. Competent supervisory authority

The supervisory authority of the EU member state where you are established; if you are not established in the EU, the authority of the member state where your EU representative is; if you have no representative, the authority of the member state where the affected data subjects are.

## Annex II. Technical and organizational measures

### Encryption

- TLS 1.2 or later on every endpoint. Customer traffic is served through Cloudflare, in Full (Strict) mode.
- Calendar tokens and Exchange passwords are encrypted with AES-256. Servers use encrypted disks where the host supports it.
- Full-disk encryption on staff devices.

### Access control

- Sign-in through Microsoft and Google OAuth; we do not store your users' passwords.
- Production is reachable only by our engineering team, using SSH keys from disk-encrypted devices. Development happens on machines separate from production.
- Multi-factor authentication and a password manager for staff accounts.
- Domain verification, so only users in your organization can manage your displays.
- Optional IP filtering per display.

### Infrastructure and network

- Database access is restricted to our servers by firewall and requires authentication.
- Host firewalls that open only the ports each server needs; SSH by key only.
- Content Security Policy on our website, admin and API; DMARC, DKIM and SPF on our email.

### Development

- Every change is reviewed before release.
- Dependencies are reviewed and updated regularly.
- Access tokens and secrets are removed from application logs. Raw request logs are kept for 1 day.

### Availability and recovery

- Weekly database backups, stored off the production servers.
- Servers in several regions (EU, North America and Asia-Pacific).

### Incidents

- We notify affected customers of personal data breaches as section 7 describes.
- A public process for reporting security issues; we acknowledge reports within 48 hours.

### Data minimization

- We don't copy your calendars. We store only what Annex I lists.
- We never train AI models on your data. Some features and our support team use AI services listed in Annex III.
- Staff access customer data only to provide and support the service.

## Annex III. Subprocessors

Our current subprocessors, with what each does and where, are listed at **https://www.meetingroom365.com/security#subprocessors**. That list is part of this agreement. Changes follow section 6.

**AI.** Our only AI subprocessor is Anthropic (United States). It runs AI features such as floor-plan analysis, and the AI tools our support and engineering team use. No other AI provider receives your personal data. Anthropic does not train models on it.

## Signatures

This copy is unsigned. It already applies under section 1, so you don't need to sign it. For a countersigned copy, sign this page and email it to support@meetingroom365.com. We'll sign it and send it back.

| | **Meeting Room 365, LLC** | **Customer** |
|---|---|---|
| **Signature** | | |
| **Name** | James Futhey | |
| **Title** | | |
| **Company** | Meeting Room 365, LLC | |
| **Date** | | |