# Data Processing Agreement

Last Update: 24.06.2024

This Data Processing Agreement (hereinafter "**Agreement**") is entered into between you, our Customer as the controller (hereinafter referred to as "**Controller**") and us, ROOMZ SA, Passage du Cardinal 5, 1700 Fribourg, Switzerland as the processor (hereinafter referred to as "**Processor**").

Controller and Processor are hereinafter each referred to as a "**Party**" or together as the "**Parties**".

## 1. Subject and duration of the Agreement

1.1 This Agreement governs the processing of the personal data (as defined in Annex 1) of the Controller (hereinafter "**Data**") by the Processor or its employees and applies to all activities in which employees of the Processor or Sub-Processors commissioned by the Processor process Data on its behalf. This Agreement does not apply to data other than the Data defined in Annex 1, such as contact and usage data provided by and collected from employees and users through the use of the Processor's website. Processor is the controller of this type of data and provides information to the users through the publicly available privacy policy.

1.2 The Controller uses ROOMZ Displays and ROOMZ Sensors (hereinafter "**Devices**") for meeting rooms, huddle rooms and shared desk. The Devices and solutions are used exclusively for business purposes (B2B). The Devices connect to the ROOMZ Portal, which is operated in the cloud (hereinafter "**Portal**"). The Portal in turn has access to the booking system of the Controller (e.g. Office365) to read or enter bookings of the meeting rooms. The calendars of the Controller's employees cannot be accessed.

1.3 The duration of this Agreement (hereinafter "**Term**") corresponds to the duration of use of the Service.

## 2. Concretisation of the content of the Agreement

2.1 The Processor processes the Data exclusively on behalf of and according to the instructions of the Controller. The scope, purpose and type of the Order Processing as well as the categories of Data and the group of persons affected by the Order Processing are defined in Annex 1. The Controller represents and warrants that all instructions are in full compliance with applicable laws.

2.2 The contractually agreed processing of the Data is performed exclusively in Switzerland, a member state of the European Union or in another contracting state of the Agreement on the European Economic Area. The Parties agree that the processing of the Data may not take place in an unsafe third country without additional authorisation from the Controller. An unsafe third country is defined as one that does not have a confirmation issued by the European Commission or the Swiss Federal Council of an adequate level of data protection. Any transfer of the processing of the Data to an unsafe third country requires the prior consent of the Controller and may only take place if the special conditions of Chapter V of the GDPR or Section 3 of the FADP are fulfilled. In this case, appropriate guarantees must be in place to ensure an adequate level of data protection.

## 3. Technical and organisational measures

3.1 The Processor shall comply with the technical as well as the organisational measures described in the online document Technical and Organizational Measures for the protection of the Controller's Data. These technical and organisational measures shall form the basis of the Agreement. If the examination/audit of the Controller reveals a need for adjustments, the adjustments shall be implemented by mutual agreement.

3.2 The Processor shall provide the security in accordance with Art. 32 GDPR (EU) and Art. 8 FADP (CH). Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk regarding confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs and the type, scope and purposes of the processing as well as the varying probability of occurrence and severity of the risk to the rights and freedoms of natural persons are to be considered.

3.3 The technical and organisational measures are subject to technical progress and further development. In this respect, the Processor is permitted to implement alternative adequate measures. Thereby, the security level of the agreed and specified measures may not be undercut. Significant changes must be documented.

3.4 It is the responsibility of the Controller to restrict the access rights for the Processor to the minimum needed, as well as to limit the information stored in the meeting room events to the minimum needed. The Processor will provide the necessary documentation to limit access to the required data.

## 4. Correction, blocking and deletion of Data

4.1 The Controller may, both during the Term and after termination of this Agreement, request the rectification, erasure, blocking or release of the Data made available, unless an obligation to store the Data exists under the Swiss law or the law of the European Union or under the national law of the member states of the European Union.

## 5. Duties of the Processor

5.1 The Processor shall process the Data exclusively within the framework of the agreements made and in accordance with the Controller's instructions or insofar as the Processor is obliged to do so under the Swiss law or the law of the European Union or under the national law of the member states of the European Union. The Processor shall not use the Data provided to him by the Controller for any other purposes as the ones contractually defined, in particular not for his own. The Processor is not entitled to make the Data available to third parties without the prior written consent of the Controller. Copies or duplicates will only be made if it is necessary for the execution of the Order Processing or if it has been approved in advance in writing by the Controller.

5.2 The Processor shall be entitled to suspend the execution of any instruction if the Processor deems that an instruction issued by the Controller violates applicable legal regulations until such instruction is confirmed lawful or amended by the Controller. The Processor must inform the Controller immediately of such suspension.

5.3 If one of the Parties is subject to the legal obligation to appoint a company data protection officer in writing, it must comply with this obligation and subsequently provide the other Party with the contact details of this officer.

5.4 The Processor shall ensure that the employees involved in the processing of the Controller's Data are bound to the data secrecy and are trained regarding the protective provisions of the GDPR (EU) and the FADP (CH) as well as the binding instructions and purposes existing in the contractual relationship. The obligation to maintain the data secrecy shall continue to apply also after the end of the employee's respective work.

5.5 At the request of the Controller, the Processor shall provide the Controller with the information necessary for the procedural directory to be kept.

5.6 The Processor shall support the Controller in fulfilling the Controller's obligations under Art. 32 - 36 GDPR (EU) and Art.8 and 22 FADP (CH) to ensure the security of the Data. If the requests are too frequent or require considerable extra-effort, the Controller will adequately compensate the Processor for its work. The Processor shall notify the Controller about such additional cost in advance

5.7 The Processor shall support the Controller in fulfilling the Controller's obligations under Chapter III of the GDPR (EU) and Chapter IV of the FADP (CH) with regard to the rights of the persons concerned. The Processor shall inform the Controller in due time of any request (including, for example, the right of access, rectification, erasure and objection) it has received from the data subject. It will not itself comply with this request, unless expressly authorised to do so by the data controller.

5.8 The Processor shall inform the Controller in due time about control actions and any other measures taken by the supervisory authority.

5.9 The Processor shall inform the Controller in due time if the Data at the Processor's premises are endangered by seizure or confiscation, by insolvency or settlement proceedings or by other events or measures of third parties. The Processor shall in due time inform all persons responsible in this connection that the sovereignty and ownership of the Data is exclusively with the Controller as the responsible body.

5.10 The Processor shall regularly monitor the compliance with the aforementioned obligations and shall provide the Controller with appropriate evidence of this on request.

## 6. Subcontracting relationships

6.1 For the purposes of this provision, subcontracting relationships are understood to be those services which are directly related to the provision of the main service. This does not include ancillary services which the Processor uses, e.g. as telecommunication services, postal/transport services, maintenance and user service or the disposal of data carriers as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Processor is, however, obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Data even in the case of outsourced ancillary services.

6.2 The Processor shall have the general authorisation of the Controller to engage Sub-Processors to provide the service. The Processor is, however, obliged to take appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the Data even in the case of outsourced ancillary services.

The current list of Sub-Processors can be found on the Processor’s website under the compliance section. The Processor shall specifically inform the Controller in writing of any material changes to this list by the addition or replacement of Sub-Processors accessing customer data at least 30 days in advance, giving the controller sufficient time to object to such changes prior to the recruitment of the Sub-Processor(s) concerned. The Processor shall provide the Controller with the necessary information to enable it to exercise its right to object.

6.3 If the Sub-Processor provides the agreed service outside the European Union or the European Economic Area, the Processor shall ensure data protection by taking appropriate measures.

6.4 Any further outsourcing by the Sub-Processor requires the express consent of the Processor (at least in text form); all contractual regulations must also be imposed on the further Sub-Processor.

## 7. Control rights of the Controller

7.1 The Processor shall ensure that the Controller can satisfy himself of the Processor's compliance with its obligations under Art. 28 GDPR (EU) and Art. 8 and 9 FADP (CH). The Processor undertakes to provide the Controller with the necessary information on request and to provide evidence of the implementation of the technical and organisational measures. The evidence of such measures can be provided at the election of the Processor by:

- current certificates, reports or report extracts from independent bodies (e.g. auditors, data protection officers, IT security departments, data protection auditors, quality auditors); or
- an appropriate certification by means of an IT security audit or data protection audit.

## 8. Notification in the event of infringements by the Processor

8.1 The Processor shall inform the Controller without delay, but in any event within 72 hours, in the event of suspected violations of data protection or other irregularities in the processing of the Data.

## 9. Deletion and return of Data

9.1 Copies or duplicates of the Data may not be made without the knowledge of the Controller. Excluded from this are back-up copies, e.g. in the form of back-ups or snapshots, insofar as they are necessary to ensure proper data processing, as well as Data required to comply with statutory storage obligations.

9.2 Upon completion of the contractually agreed work or earlier upon request by the Controller - at the latest upon termination of the Agreement - the Processor shall delete or destroy all Data. The protocol of the deletion is to be presented upon request by the Controller. For the avoidance of doubt, the Processor may retain fully anonymized Data for its own purposes.

## 10. Liability

10.1 Without prejudice to the provisions of the GDPR (EU) and the FADP (CH), in the event of a breach by the processor of its obligations under these clauses, the Controller may instruct the Processor to suspend the processing of personal data until the Processor has complied with these clauses or the contract is terminated.

10.2 The Processor shall promptly inform the controller if it is unable to comply with these clauses for any reason.

10.3 The Controller shall be entitled to terminate the contract insofar as it relates to the processing of personal data in accordance with these clauses if:

- The processing of personal data by the Processor has been suspended by the Controller in accordance with point 10.1 and compliance with these clauses is not restored within a reasonable period and in any event within one month of the suspension.
- The Processor is in serious or persistent breach of these clauses or its obligations under the GDPR (EU) or the FADP (CH);
- The Processor fails to comply with a binding decision of a competent court or the FDPIC concerning its obligations under these clauses or other applicable laws.

10.4 The Processor shall be entitled to terminate the service insofar as it relates to the processing of personal data under these Clauses where, having informed the Controller that its instructions breach applicable legal requirements pursuant to Clause 5.2, and that the Controller insists that its instructions be followed.

## 11. Place of jurisdiction and applicable laws

11.1 These provisions are governed by Swiss law.

11.2 Any dispute arising from their conclusion, interpretation or performance shall be submitted to the exclusive jurisdiction of the Courts of the Canton of Fribourg, Switzerland.

Annex 1 – Type of Data

(1) Subject, type and purpose of the processing of Data

- For the login of the users (hereinafter "**User**"), as well as administrative processes around ROOMZ Accounts:
  *First name, surname, company name if applicable, address*
  *Contact details (e-mail, telephone number if applicable)*
  *Token (external OAuth provider) or password hash*
  *Personal preferences/settings*

- Information from the booking system (e.g. Office365) to update the display on the ROOMZ Display:
  *Booking System Credentials*
  *Start Meeting (date, time)*
  *End Meeting (date, time)*
  *Organizer (optional, adjustable) – Name and e-mail address*
  *Subject (optional, adjustable)*
  *Creation date of the calendar entry*
  *Private Flag*
  *Image attachment (if necessary), but only if the file is named «roomz.jpg» (otherwise any attachments will be ignored)*

  Only the calendars of the resources (rooms) are accessed, but not the personal calendars of the employees. This information is used to generate the image on the ROOMZ Display and update it. This data is usually stored for 24 hours when using a daily template or 1 week when using a weekly template.

- The following information is stored and processed for the evaluation of work area utilization:
  *Creation date of the calendar entry*
  *Meeting information (start and end date, creation date)*
  *Presence/non-presence*

- Live presence from the ROOMZ Sensors to display free/busy resources and to release meeting rooms during "no-shows". Due to the physical measuring principle of the sensors (PIR, passive infrared), this data is already anonymous at the time of collection and cannot be used for tracing or profiling a person in the system later, so it does not constitute personal data in the sense of the GDPR and FADP.

- The web and mobile applications *myROOMZ* are designed for the employees to help them searching and booking a workspace, limited to desks and parking spaces. In this context, ROOMZ stores the bookings information in an in-house developed booking system (ROOMZ Hosted). This allows the customer to avoid creating a resource for each workspace in the booking system. In this situation, the data is retained up to 2 years in case of analytics re-computing. After this period, the data is completely removed. It is also possible with the application to book a workspace in the future. To be efficient and to have a good user experience, ROOMZ contains the upcoming bookings of each workspace. The upcoming booking timeframe depends on the customer's configuration on the ROOMZ Portal. The following information is stored if *myROOMZ* is activated:
  *Start and End (date, time)*
  *Organizer (Name & e-mail for whom the workspace has been booked)*
  *Creator (different from Organizer in case someone book for someone else)*
  *Creation date of the calendar entry*
  *Workspace (name, id)*

*External visitor's e-mail address (only when provided)*

(2) Categories of data concerned

- Login data for the Users of the Software services
- Contact details for administration (notifications, billing, support)
- Calendar data from the booking system (resources, e.g. meeting room)

(3) Categories of persons concerned

- Employees or external visitors of the Controller