ROOMZ SA
Cardinal Passage 5
1700 Freiburg
SWITZERLAND

Technical and organizational measures (TOM)

ROOMZ takes the security of your data very seriously. This section details the security measures we have implemented to protect your data and demonstrate our compliance with the various laws in force.

CONFIDENTIALITY

DATA PROCESSING

ROOMZ mainly processes the following categories of data related to its services:

Category	Definition
Contact data	Personal data that our customers send us to create and manage their account.
Booking data	Information that the end users (meaning the employees, visitors or customers of our customers) enter in our systems by using the services.
Sensors data	Live presence from the ROOMZ Sensors to display free/busy resources and to unlock 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 assigned to a person.
Organization data	Non personal data that our customers send us to provide services (e.g. building details, floor plans, images, tags...)

The customer is the owner of its data, including any data created using the service.

Once their account has been created, customers have control over their data and they themselves determine the resources they wish to manage, as well as the users they want to create and the authorizations they assign to them. In this context, customers act as the **data controller** and ROOMZ as the **data processor**. The detailed terms and conditions of processing personal data are described in our Data Processing Agreement.

DATA GOVERNANCE

The fundamental principles of data protection are deeply rooted in ROOMZ's practices.

Data minimization - We collect no more data than is strictly necessary to provide our services.

Privacy by design & default - We apply data by design and by default principles in all our developments, including data protection impact analysis when needed.

Data retention

Category	Retention policy
Contact data	6 months after termination of the contract.
Booking data	Anonymized data may be retained indefinitely for analytics, services optimization and creation purposes. Per default, the booking data entered each day is anonymized every night. If they so wish, customers can activate a function that allows data to be stored non-anonymized for maximum 90 days and exported on request.
Sensor data	By default, using PIR (passive infrared) detection, sensor data is anonymous. This data may be retained indefinitely for analytics, services optimization and creation purposes.
Organization data	6 months after termination of the contract.

Security measures - We deploy security measures according to the risks involved; these measures are described in the following sections. Cyber risk management is integrated into management processes at all levels of the company and is regularly reviewed.

Certifications – ROOMZ Information Security Management System is ISO 27001:2022 certified and the company also maintains its Quality Management under ISO 9001:2015 certification.

Privacy Laws

GDPR - The General Data Protection Regulation is a law that governs the collection and use of personal data of residents of the European Union and grants them rights in relation to the control of this data. As the GDPR is generally considered to be the strictest privacy standard in the world, we have based our privacy program on its provisions and those of the Swiss law.

FADP - As a Swiss company, ROOMZ is subject to the Swiss Federal Act on Data Protection. The supervisory authority is the Federal Data Protection and Information Commissioner. Any complaint should be addressed to this authority.

DPO – ROOMZ has appointed a data protection officer, which contact details are:

DP&S Sàrl
Attn. Mr Stéphane Droxler
Ch de la Clé-des-Champs 8
CH-2022 Bevaix
email : privacy@roomz.io

Contracts & Policies - We make every effort to keep our contracts up to date with the latest regulations and standards. You can download our reference documents below:

- Terms & Conditions
- Data protection agreement (DPA)
- Privacy & cookies policy
- Technical Organizational Measures (TOM)

DATA SECURITY

ACCESS CONTROL

Access rights are granted according to necessity (principle of operational requirement). Administration rights are subject to stricter requirements, based on the least privileged and differentiated by subject areas, groups and roles concept. The process for granting and withdrawing access rights is formally documented.

TRACEABILITY

Logs include access to applications and technical error messages with a view to resolving problems. Given that we do not process sensitive personal data or perform risk profiling on our customers' data, audit logs have been activated for certain functions considered critical from an operational perspective.

DATA RESIDENCY

Data is hosted by Microsoft Azure in West Europe (Holland) and geo-replicated in North of Europe (Ireland). Exceptions may apply for certain data related to technical services, but no personal data is hosted outside the EU.

BACKUPS

ROOMZ leverages different types of storage for its operations. Each has its own independent backup policy that ensures data integrity and availability according to needs.

ENCRYPTION

Data in transit is encrypted using TLS 1.2 or higher version.
Data at rest is secured using AES 256 data encryption provided by Azure encryption services.

Infrastructure security

Data center

ROOMZ does not operate its own data centers but uses Microsoft Azure. These data centers meet various certification levels, including ISO 27001.

Access to IT infrastructure

Remote access to Microsoft data centers is personalized and restricted to a limited group of people, granted by the CTO and according to the least privilege principle. Access is secured with strong credentials and MFA authentication method.

Security measures

Disaster Recovery Plan - Our incident response plan contains several recovery scenarios, which are reviewed on a regular basis. For obvious security reasons, we do not communicate the details of these scenarios.

Segregation of environments

ROOMZ have separate development, test and production environments.
Customer accounts have logical tenant separation within the production environment.
Customer data is never stored nor copied or replicated in non-production environment.

Application security

Software Development Life Cycle & Code review

All software created by ROOMZ must comply with the Secure Coding Standard and all developers are trained in secure software development, based on the OWASP Top 10. During the design phase, threat modeling and security design reviews are performed for new releases and upgrades. After the code has been written, we carry out code reviews. After launch, we use suppliers to perform audits, at least once a year, in the form of penetration tests.

Identifiers management

The customer is responsible for controlling access to their user accounts and granting access to the user accounts to their personnel, who will receive individual login credentials for their user accounts.

ROOMZ administration access to the various services is limited to a small number of people, designated by the CTO, and is systematically carried out via nominative privileged accounts.

Change management

Any change affecting the security of information is controlled and approved by management. Changes are formally reviewed and documented before implementation.

Security features related to the product

Authentication methods – Users can log in using their existing Google or Microsoft accounts. The method leverages the robust security measures provided by these leading identity providers, ensuring a high level of protection and convenience. Alternatively, users have the option to create new credentials directly on our platform. All authentication methods will act as a Single Sign-On (SSO) on the solutions, granting access to all services managed by ROOMZ.

Authentication mechanism – ROOMZ supports OAuth2 protocol.

Multi Factor authentication - MFA authentication is supported by Microsoft and Google providers but is currently not supported with our own authentication.

Authorization management - The ROOMZ Portal platform enables administrators to manage their users' authorization levels.

Separation of Concerns (SoC) – The solution operates as a multi-tenant SaaS, where customers share the same application instance with logical separation of data ensuring data privacy and security.

HUMAN DEFENSE

EMPLOYEES

All employees are carefully selected, have their references assessed and must comply with the company's safety procedures. They are contractually bound by confidentiality clauses.

SECURITY AWARENESS AND TRAINING

Mandatory trainings are regularly organized.

INCIDENT MANAGEMENT

As part of the information security management system, a documented and tested incident management response plan as well as a business continuity plan are maintained.

SUB-CONTRACTORS

Outsourcing - Certain development tasks are outsourced to a European partner. External employees are integrated into the development team in the same way as internal staff and must commit to the same quality and safety procedure. Their work is supervised by an internal employee. External employees do not, however, have access to production environments or customer data.

List of Sub-contractors – You can find the list of our sub-contractors here.