dormakaba information on data protection in the resivo cloud solution.

resivo data protection

dormakaba

Declaration of obligation on data protection

Our data processing principles (GDPR compliance)

The General Data Protection Regulation (GDPR) was passed by the European Union to ensure the protection of natural persons during the processing of personal data within Europe. By complying with the GDPR, dormakaba also complies with the German Federal Data Protection Act (BDSG) 6 and the Swiss Federal Act on Data Protection (DSG). dormakaba complies with the requirements of the legal bases according to the latest case law without exception.

Data Processing Agreement (DPA)

Commissioning of dormakaba by customers for data processing is set out in writing in the Data Processing Agreement (the DPA is part of the dormakaba SaaS contract). The processing is carried out to enable the performance of services within the scope of the contract. The data processor (dormakaba) is not permitted to process customers' personal data, or pass it on to third parties, for its own purposes.

dormakaba organisation
Protecting your data

Technical and organisational measures

dormakaba (the data processor) employs technical and organisational measures to guarantee a level of security proportionate to the risk.

a) Confidentiality
- Physical access control: protection against unauthorised access to data processing systems. Use of physical access control systems, e.g. chip cards, keys, electric strikes, guard service, alarm systems, video surveillance, documentation of visitors and issuing visitor passes.
- System access control: protection against unauthorised use of a system. Implementation of user guidelines for the allocation of passwords and instruction on security guidelines.
- Data access control: protection against unauthorised access, reading, copying, modification or removal of data within a system. Use of authorisation concepts and on-demand access rights, access logging, observance of the need-to-know principle (data economy).
- Separation control: separate processing of personal data which was provided or collected for different reasons.
- Pseudonymisation: as long as the reason for processing allows it, personal data is processed in such a way that the data cannot be attributed to a specific affected person without additional information being acquired.

b) Integrity
- Transfer control: no unauthorised reading, copying, modification or removal during electronic transfer. Use of transfer control systems, e.g. e-mail encryption. Virtual private networks (VPN), SSL-encrypted transfers to service providers; electronic signature.
- Input control: this allows you to determine whether and by whom personal data has been entered, modified and removed in data processing systems (e.g. through use of a document management system).

c) Availability and resistance
- Availability control: protection against accidental or intentional destruction or loss, e.g. through emergency plans, back-up strategy, uninterruptible power supply (UPS), antivirus, firewall, regular penetration tests of infrastructure security, information security management.
- Rapid restoration of availability and access to personal data, e.g. through highly redundant storage of personal data, use of centralised security patch management.

d) Process for regular testing, assessment and evaluation of TOMs
- Group-wide data protection management, defined roles and responsibilities for data protection officers, coordinators and managers.
- Order management: data is only processed on behalf of the customer if the customer requests this, e.g. through unambiguous contract design, formalised order management, careful selection of service providers, inspection obligation and follow-up checks.

FAQ: person data collected in resivo

Who stores and processes data?

Building management employees who use resivo. Tenants of rental properties which are located within buildings equipped with resivo.

Which data will be stored and processed?

Building management employees: building management employees use the resivo admin portal and the resivo utility app. Both applications are accessible to the user after proper registration.

The following information (master data) is required for registration:

- First name and surname
- Email address (business email address).

To be able to see the names of the employees, permission to log in to the resivo system must be granted. The employees' activities are then stored in a modification log for 180 days to ensure that modifications can be tracked. The tasks that can be performed in the resivo admin portal and the utility app (e.g. move-in process, key creation, etc.) are logged. In keeping with the Privacy by Design concept (whereby data protection is already technically integrated in data processing operations), the data cannot be extracted and is deleted automatically after 180 days.

Tenant information:

As a rule, the required information is provided in a data-protection-compliant manner. This means that only system-relevant tenant information can be entered in the resivo system.

Specific tenant information (master data):

- First name and surname
- Link to the affected rental property
- Tenant's email address and/or mobile phone number
- Lease start date
- Lease end date
- Tenant's access media

Additional tenant information
(optional; at the discretion of the building company):
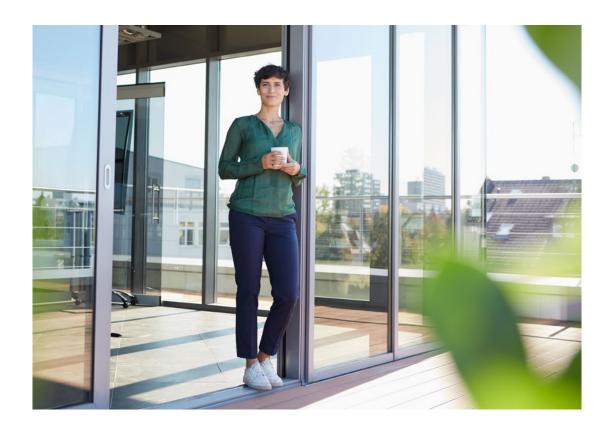
- Tenant access information at common doors (access log)

By design, the tenant information is visible to selected resivo admin portal users who possess
a) Access rights for the building and
b) Role authorisation for viewing tenant information (role: tenant management)

The tenant information is no longer visible to building management after completion of the move-out process. Only the access log of the common doors can contain tenant information from the past 90 days. By design, the access log can be viewed by resivo admin portal users who possess a) access rights for the building and b) role authorisation for viewing the access log (role: access log).

How long is the data stored for?

- Master data of building management employees:
  until the user is actively deleted
- Modification log: 180 days
- Tenant information master data: deleted immediately after move-out.
- Access information: after 90 days

Measures that dormakaba uses to protect your tenant information and data

- Role-based user system
- Extraction prevented by design
- By default, data is deleted once it ceases to be relevant (move-out, 90-day interval, 180-day interval)
- Password-protected login
- Exclusive customer zone
  - Access from the system can only be granted to customers
    (as well as to dormakaba support staff, dormakaba sales staff, dormakaba product management and installation and support partners)

- Restricted database access – access is only granted to a very limited number of dormakaba employees (development), who are subject to a special data protection and confidentiality agreement.
- Information security. dormakaba and the computer centre that serves dormakaba are certified according to ISO 27001. This ensures that the personal data of customers and their employees is protected. The certification remains valid for the full term of the contract.

Security features within the product:

Authentication and passwords:
- Login (two-factor authentication. Users who log in to the SaaS software will be offered the chance to set up two-factor authentication for their account for added security).
  - Encryption: all communication on public networks in the dormakaba resivo apps is encrypted and protected by HTTPS with Transport Layer Security (AES 128 GCM SHA 256, 128 bit keys, TLS 1.3 with PFS). This means that all data transfer is encrypted.

- Password strength – resivo users (tenants as well as administration employees) can only use passwords with at least 8 characters and at least one upper-case letter, one lower-case letter, one special character and one number.

User roles and rights concept
- There are various user roles as well as a rights concept for use of the resivo utility app and the resivo admin portal. One, several or all of the following permissions can be assigned to a user:
  - User administration: create, add and delete users; assign or revoke permissions. Recommended for users who are supposed to take on the role of app administrator or superior in the building management.
  - Building management: this permission allows buildings, rental properties and rental property doors to be added, processed or deleted.
  - Access management: add master key or guest access, open common doors using remote opening.
  - Tenant management: add tenant, move in/out, issue invitations for the resivo home app. Suitable for those responsible for tenant management.
  - Component management: create, maintain (battery replacement, firmware update) and delete common doors. Suitable for users who perform commissioning and maintenance and offer support.

Information and communication management:
- Push notifications, SMS and/or email notifications when new residents are added and granted access to a rental property
- SMS and/or email notifications when access to a rental property is requested

Logs:
- Access log, see SaaS contract for description
- History log (modification log)

dormakaba resivo

resivo by dormakaba is a future-oriented, cloud-based access management system. It offers significant advantages for property administrators, building owners and tenants compared to conventional mechanical locking systems. No more worrying about lost or stolen keys. Flat hand-offs are easier and more convenient for the tenant. resivo saves time by simplifying the procedures for granting access to suppliers, service providers and tradesmen. Tenants decide for themselves who should have access to their flat and when – even from afar. resivo unlocks a whole new dimension of building utilization packed with advantages.

Door
Hardware

Electronic
Access & Data

Mechanical
Key Systems

Lodging
Systems

Entrance
Systems

Service

Any questions?
We will be happy
to assist you.

Visit us:

resivo.dormakaba.com

dormakaba.com