Security overview

This document addresses different aspects related to Frosmo security and customer data integrity.

Physical security

The Frosmo Ltd. headquarters is located at:

Panimokatu 2 A, third floor
00580 Helsinki
Finland

The premises can only be accessed with an electronic badge. The badges given to employees are listed and controlled.

The premises are equipped with an alarm system. The system detects door movement and motion in corridors. If an alarm goes off, the system alerts the security company, and security personnel will come and check the situation within minutes.

When a visitor arrives at the premises, a host lets the visitor in and accompanies the visitor throughout the visit. Visitor meetings are organized in a specific meeting room. Visitors are not allowed in areas reserved for software development or system operations.

Cleaning services are provided by a dedicated cleaning company and a known person is doing the cleaning at predefined times.

Server security

Frosmo cooperates with the following GDPR-compliant platform hosting partners for back-end server hosting:

- Hetzner Online AG for European customers
- Amazon Web Services (AWS) for customers outside Europe

Customer data is backed up from production servers to a specific backup server hosted by Hetzner. For more information about the backups and server logs, see Data privacy description.

On operating system level, servers and firewall settings are managed by Frosmo. Security updates are deployed constantly to keep all servers up to date with the latest security updates for data and access rights. The updates are deployed under the supervision of the Frosmo Chief Technology Officer (CTO).

The agreement with the hosting partners does not include access to operations related to Frosmo customer data. Frosmo personnel is solely responsible for managing all data collected by the Frosmo Platform.

By default, the Frosmo JavaScript library files are delivered through Amazon CloudFront. For more information, see Amazon's service-level agreement and product documentation. Frosmo can also use other services based on customer requirements.

Frosmo follows the best practices for managing AWS access keys. All JavaScript updates are deployed through automated processes, with each process using its own specific key with limited access.

Operational security

The Frosmo operational tools can only be accessed over an HTTP Secure (HTTPS) connection. Access to the tools is always protected with credentials. The core operations personnel may use superuser access to manage services. Superuser credentials can only be created during system installation and cannot be created using normal operations tools. Credentials generated using the normal operations tools are always for a lower access level and can be shared with customer representatives. Customers can only generate and manage credentials of the same level for other users in their own organization.

The Frosmo System Administrator is responsible for all system updates. All modifications to Frosmo products in the production environment are controlled by the CTO. All software modifications can be tracked in change logs and the version control system.

Team members working for a specific customer can be disclosed to the customer on request. A team rarely works with multiple customers in the same market sector. Customers can request a background check on Frosmo employees. In addition, comprehensive audits can be carried out either by the customer or by a third party on request.

The Frosmo production servers can only be accessed by using public key authentication (administrative access). Public keys are provisioned to trusted Frosmo employees when needed for the required access levels. All granted keys are recorded by the System Administrator and deployed to servers using an automatic deployment process that adds, removes, and updates keys on the production servers. All generated keys must follow the documented security guidelines and are always personal and protected by a passphrase known only to the key owner.

The workstations used by operation teams are always password-protected. Frosmo follows password encryption best practices. Antivirus and malware protection software is used. Files are not stored on local workstations but on secure network drives, and documents are mainly stored in protected cloud-based services, such as Google Drive and Atlassian Confluence. The network server provides snapshots of the data for the most common backup and recovery needs within the normal workflow. These snapshots are also replicated to secondary servers to provide recovery in case the primary server fails.

All operational networks are protected by firewalls and managed by designated employees.

Critical system passwords are renewed on a regular basis.

Disaster recovery and business continuity

In case of a natural or human-made disaster, or a critical software or hardware failure, Frosmo ensures recovery and continuation of service through, for example:

- **Cloud computing.** Frosmo uses Amazon Web Services (AWS), Atlassian Confluence, and G Suite, each a trusted cloud computing platform, for storing and/or serving data.
- **Data replication.** To ensure the availability of data, Frosmo replicates operational data to backup servers in multiple physical locations.

The Frosmo headquarters is located in one of the most politically, socioeconomically, and infrastructurally stable countries in the world, Finland. The region is also one of the safest from natural disasters. Disruptions of service due to natural or human-made disasters are thus highly unlikely.

Personnel security

The Frosmo work contract contains non-compete, confidentiality, and non-disclosure clauses. Additional non-disclosure agreements can be created for specific customers on request.

All new Frosmo employees are informed about physical and data security. This introduction is repeated at supervisors' discretion. The requirements and conditions for each customer are always discussed within the team when a new customer project starts.

Frosmo employees are encouraged to observe and report to their supervisors all issues (on any level of operations) that are likely to compromise customer data security.

After an employee leaves Frosmo, the employee's access rights are removed. This procedure covers physical access, data access, and any generated authentication keys.

Application security

Access to the Frosmo services administration can be limited based on the IP address so that accessing the Frosmo Control Panel (the user interface you use to access the Frosmo Platform features) is only allowed from the Frosmo premises and from specific IP addresses defined by the customer.

In addition, the Control Panel triggers a warning if an account is accessed from multiple computers, and allows the user to close redundant connections. Too many failed login attempts trigger a failure mode, which forces additional authentication checks for subsequent login attempts and notifies the System Administrator.

The Frosmo Platform can force all content that is provided through the Frosmo JavaScript library to the customer site to load resources only from specified domains. When this feature is enabled, the Frosmo Platform validates all modification content before it is saved to the Frosmo back end. If the content contains elements that could be used to load or inject resources from non-authorized domains, the content is rejected. This also restricts the domains to which you can create hyperlinks in modification content. You define the allowed domains in the Control Panel, and they apply to links, images, videos, and iframes.

You can also forbid the use of JavaScript code in modification content.

Data security

The Frosmo JavaScript library collects usage data in the visitor's browser and sends the data to the Frosmo back end over an HTTPS connection. The Frosmo JavaScript library also stores selected data locally in the visitor's browser.

Frosmo is committed to protecting the security of the visitors' personal data and has a variety of security technologies and procedures in place to prevent unauthorized access, use, or disclosure of data.

By default, the Frosmo Platform collects and processes only anonymous and pseudonymous information about visitors and their behavior on a website. The purpose and lawfulness of data processing is invariably determined by the customer and documented in the subscription agreement between Frosmo and the customer, and in the Frosmo General Terms of Service.

Customer data is always stored in such a way that the data of one customer cannot be mixed with the data of another customer. All software modifications can be tracked in change logs and a version control system (GitLab).

For more information about how Frosmo handles data privacy, see Data privacy description.