Data privacy description

This document describes:

- Roles and responsibilities of Frosmo and its customers in gathering and processing website visitors' personal data
- Procedures Frosmo uses to store and process personal data gathered from its customers' websites on their behalf to implement the various features of the Frosmo Platform, such as content targeting, conversion tracking, and content modifications
- Technical solutions and processes that ensure compliance with national and regional regulations regarding data privacy and protection

The purpose of this document is to ensure and demonstrate compliance with the transparency and accountability requirements of the European General Data Protection Regulation (GDPR).

Key terms and definitions

The following table lists some of the key terms used in this document.

Table: Terms and definitions used in the document

Term	Definition
Customer	Organization that has a valid subscription agreement with Frosmo.
Data controller	Natural or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data processor	Natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.
Frosmo Platform	The Frosmo Platform is a web UI development solution for improving website functionality and personalizing online user experience. The platform mainly works in the visitor's browser, through JavaScript tags placed directly in the web page HTML code. Optimization and personalization is based on visitor usage data collected from the browser. For more information, see Introduction to the Frosmo Platform.
Data subject	Natural person whose personal data is being processed; "one who can be identified, directly or indirectly, in particular by reference to an identifier". In the Frosmo context, the data subject is normally a visitor on a customer's website using the Frosmo Platform.

Personal data	Basically, any data related to an identified or identifiable natural person ("data subject"), for example: • Name • Postal address • Email address • Social security number • Date of birth • Gender • Profession • Image or video • IP address • Device ID • Fingerprint • Car registration number
Site	Customer's website that uses the Frosmo Platform.
Visitor	User of a website and, in case the site collects personal data about its visitors, a data subject. The Frosmo Platform identifies the visitor based on the Frosmo visitor ID stored in the browser's local storage. By default, the Frosmo Platform does not recognize the visitor across different browsers or devices

Data protection stakeholders

The main stakeholders in the protection of Frosmo customer data are:

- Data subject
- Customer
- Frosmo as a company
- Subcontractors (of Frosmo and, frequently, of the customer)

In a relationship between Frosmo and a customer, the customer always represents the data controller, and Frosmo acts as the data processor.

This means that the legitimate and specific purpose for collecting personal data through the Frosmo Platform is always determined by the customer. The customer is responsible for:

- Documenting the purpose of processing personal data
- Defining which data is needed for the purpose
- Defining whether the personal data is given to third parties
- Defining whether and how the personal data may be transferred outside the European Union (EU)
- Defining whether the data processing comprises profiling or automated decision-making
- Ensuring that the data subjects have given their consent to data collection
- Maintaining required documentation and monitoring the actions of third-party systems and subcontractors, if any

Frosmo, as a data processor, is committed to assisting its customers in these responsibilities regarding any personal data collected through the Frosmo Platform.

Data protection organization at Frosmo

Based on the nature of Frosmo's business, Frosmo is not required to appoint a data protection officer.

However, Frosmo has a data protection steering group with members representing different roles and departments. The group meets regularly to review system and process changes related to data protection. In addition, the group handles questions and requests about data protection from customers and other stakeholders.

Frosmo subcontractors and hosting practices

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

- Hetzner Online for European customers
- Amazon Web Services (AWS) for all customers

For European customers, Frosmo does not transfer personal data outside the European Union (EU) / European Economic Area (EEA).

The agreement with the hosting partners prohibits any operations related to Frosmo customer data. Frosmo personnel is solely responsible for managing and processing all data collected by the Frosmo Platform.

By default, the Frosmo JavaScript library files are delivered through Amazon CloudFront. Frosmo can also use other services based on customer requirements. The Frosmo JavaScript library handles the operations on the customer site but does not contain any data in itself.

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.

Data processing

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 library sends the data in the background so as not to interfere with the visitor's user experience.

The Frosmo JavaScript library also stores selected data locally in the visitor's browser.

Data collection

The data that may be collected depending on the technical implementation can be categorized into:

- **Modification performance data:** Basic modification events used for monitoring and reporting
- **Product data:** Information used in product recommendations
- **Server logs:** "Raw data" not collected through the Frosmo Platform and not used for profiling or targeting
- **Visitor data:**
    - **Background data:** Information about the visitor not related to a specific website
    - **Behavior data:** Visitor's actions on the website
    - **Conversion and transaction data:** Visitor's actions on the website in connection with purchases and other conversions
    - **Account data:** Personal data collected and stored temporarily for the purpose of transferring it to customer's back end or third-party systems controlled by the customer; only tracked when explicitly agreed with the customer

By default, the Frosmo Platform collects and processes only anonymous and pseudonymous information about visitors and their behavior on a website. The platform does not collect data that in itself enables the identification of an individual data subject.

The Frosmo Platform can collect additional information about visitors, including account data, such as email addresses and phone numbers. However, processing of such data must always be determined by the customer and documented. Frosmo only collects account data for the purpose of transferring the data to the customer's back end or third-party systems (such as CRM systems or marketing automation platforms) controlled by the customer.

For more information about how Frosmo collects and stores data, see Data collection and processing.

Purpose and lawfulness of data processing

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.

If so agreed, the Frosmo Platform will collect personal data for the purpose of passing it on to the customer's system or a third-party service, such as a marketing automation platform. The data will not be stored in the Frosmo back end, unless the customer has explicitly authorized this, and even then the information will only be stored on a temporary basis.

Frosmo never collects visitor data for its own purposes, or for the purpose of selling it to a third party.

Data security

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.

For example, The Frosmo operational tools can only be accessed over HTTPS. Access to the tools is always protected with credentials. The Frosmo production servers can only be accessed by using public key authentication. Public keys are provisioned to trusted Frosmo employees when needed for the required access levels. All operational networks are protected by firewalls and managed by designated employees.

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).

The employment and subcontracting contracts used by Frosmo contain confidentiality and non-disclosure clauses whereby the employees and subcontractors are obliged to keep the personal data confidential and not to use that data to any other purpose than for the proper performance of the Frosmo's services for the benefit of the customer.

For more information about data, application, and operational security at Frosmo, see Security overview.

Data storage and retention

The Frosmo Platform stores data in the Frosmo back end as well as in the browser's local storage and cookies. For more information data storage, see Dat a storage and retention.

Most of the data collected by the Frosmo Platform (for example, segmentation and modification IDs, site configurations, visitor context data, and analytics data) is stored for the duration of the subscription agreement between Frosmo and the customer.

When a subscription agreement is terminated, processing any data related to the sites of that specific customer account ceases immediately. After this, the data is stored in a format that prevents the platform using it or it being associated with a person. The data is then removed from the Frosmo systems according to the normal data retention cycle. Any data that must be manually removed, is removed within 6 months after the subscription agreement is terminated.

In the Frosmo back end, data is stored in:

- Server logs
- Databases
- Backup copies

Server logs

Server logs are files for recording events on a web server, namely information about incoming page requests. Website visitors do not have access to server logs; the logs are normally only accessible to the webmaster. The data in the server logs is only used for the technical monitoring of the platform, not for profiling, targeting visitors, or any commercial purposes.

Frosmo has full access to the server logs and complete knowledge on where each server log is stored. All the log data regarding the Frosmo Control Panel and resource files used on customer sites is controlled by Frosmo.

The log data is used to create usage statistics. Before refining the data for statistics, any personal data, such as IP addresses, are removed.

Databases

The Frosmo Platform stores data in several databases located in the Frosmo back end. In addition to the databases used across the platform, the Frosmo JavaScript library may use a dedicated Redis database (one per customer) for saving data related to custom implementations.

Backup copies

The Frosmo Platform data is regularly replicated for business continuity purposes. The backup copies cannot be accessed as such, and rolling back to one requires effort from the Frosmo System Administrator.

Transfer of data outside the EU/EEA

For European customers, Frosmo does not transfer personal data outside the European Union (EU) / European Economic Area (EEA).

When a content delivery network (CDN) is used to deliver the Frosmo JavaScript library to a website visitor's browser, in some cases there is a chance that the CDN server used is located outside the EU/EEA. However, the Frosmo JavaScript library as such does not contain personal data.

For more information about the Frosmo JavaScript library, see Technical overview.

Integrations with third-party systems

The Frosmo Platform can communicate with back-end systems and basically any analytics, marketing automation, or content management system, depending on the configuration of that system. The platform can act as a master API for utilizing data from several sources. Integrations can also be implemented as custom solutions.

Some common integrations include:

- Adding visitor email addresses to specific mailing lists based on segmentation.
- Retrieving information from and storing information to external databases. For example, Frosmo can retrieve user data from a customer's database and use the data to personalize website content, or send segmentation data to the customer's database.
- Retrieving information from data feeds, such as product data feeds, or back-end systems, such as customer relationship management (CRM) systems. For example, Frosmo can retrieve information about new products or products currently on sale from a data feed, and generate corresponding product recommendations to visitors.

The personal data retrieved from a customer's databases or other back-end systems is not stored in the Frosmo Platform, but transferred to the customer's system or third-party system used by the customer. However, Frosmo may combine it with segmentation data for personalization purposes. This type of data processing must always be determined by the customer and documented in the subscription agreement between Frosmo and the customer.

Access to data

Frosmo, as a data processor, always handles requests related to a specific data subject's access to their own personal data through the customer acting as the data controller regarding the specific site. Any personal data will be delivered only based on a written request or instructions given by the data controller to Frosmo.

The requests related to a specific data subject's access to their own personal data are handled by the data protection steering group and conveyed to Frosmo system administration for processing.

Contacting Frosmo for information

For queries and requests related to data access and data protection in general, customers can contact data.privacy@frosmo.com or their Frosmo Project Manager, who will convey the queries to the data protection steering group. All queries must be handled by the steering group to ensure the consistency and validity of the replies.

Refusing profiling

When a data subject refuses profiling on a site, the Frosmo Platform can discontinue all profiling for the corresponding Frosmo visitor ID. The platform does this by setting a cookie in the visitor's browser that prevents the use of the platform. After this, any collected data is stored in a format that prevents the platform from using it or associating it with a person. The data is then removed from the Frosmo back end according to the normal data retention cycle.

Frosmo can also implement selective profiling. This solution enables registering the visitor's profiling choice on the site and showing them content accordingly:

- Personalized, targeted content for visitors who consent to profiling
- Non-personalized, non-targeted content for visitors who refuse profiling

The Frosmo Platform identifies the visitor based on the Frosmo visitor ID stored in the browser's local storage. By default, the platform does not recognize the visitor across different browsers or devices.

Requesting deletion of data

When a data subject requests deletion of their personal data, processing any data related to the specific user ID ceases immediately. After this, the data is stored in a format that prevents the platform from using it or associating it with a person. The data is then removed from the Frosmo back end according to the normal data retention cycle.

Personal data will only be removed based on a written request from a customer, or based on explicit written instructions given by the customer to the website visitor.

Data breach notification

Data breach is an intentional or unintentional security incident that results in the loss of confidential information, such as personal data. In the case of a personal data breach, the data processor must inform the controller about it without delay. The controller, in turn, must inform the relevant supervisory authority.

At Frosmo, a data breach is addressed according to the same process as any other major technical or security incident. The key points of the process are the fast recognition of an anomaly, coordination of corrective actions, and creating and implementing a communication plan.