Online privacy technologies and the Frosmo Platform

The requirements for internet privacy are getting ever stricter as online service providers rely increasingly on visitor data for personalization and optimization. While visitor data has many valid uses, such as providing a visitor with relevant and interesting content, collecting data through cookies and other tracking technologies is sometimes seen as intrusive, especially when the intention is to sell the data to third parties.

While Frosmo never collects visitor data for its own purposes, or for the purpose of selling the data to a third party, the Frosmo scripts are technically third-party content on websites, and some privacy technologies therefore affect the Frosmo Platform.

This document gives an overview of the most common privacy technologies and their effect on the Frosmo Platform.

For more information about how the Frosmo Platform collects and processes data, see Data privacy description and Default configuration and data tracking for a visitor.

Private browsing

All the major browsers, such as Google Chrome, Microsoft Edge, Mozilla Firefox, and Safari, contain different levels or privacy settings. The easiest way to enable the features without manually adjusting the browser settings is to use a private browsing mode (known in Chrome as incognito mode). In a private browsing mode, the browser creates a temporary browsing session separated from the browser's main session and user data. Browsing history is not saved, and local data associated with the session, such as cookies, are cleared when the session ends, that is, when the visitor closes the browser tab or window.

Visitors can also use privacy browsers (for example, Brave, Epic, and DuckDuckGo), which contain more built-in privacy features than the standard browsers, and often use a private browsing mode by default. Privacy browsers also typically block ads while preventing websites from collecting any data about the visitor.

Blockers

Third-party blocking technologies can roughly be classified into:

- **Ad blockers.** Typically free-of-charge browser extensions or standalone apps that prevent displaying third-party ads on web pages. Blocking is based on filter lists containing the names of tracking files or systems that are filtered out. The most common ad blockers include AdBlock and AdBlock Plus. Basic ad blocking features are also built in to the most common browsers, such as Chrome, Firefox, and Safari.
- **Tracking blockers.** Software or browser settings that prevent programmatic trackers from collecting data about the visitor's online activity. Tracking blocker features include hiding user search queries, private browsing, prevention or deletion of third-party cookies, and hiding the visitor's IP address.
- **Privacy blockers.** Browsers, browser extensions, or standalone apps that combine ad blocking and tracking blocking features and often aim to protect the visitor's overall online privacy. These blockers often affect even the most basic analytics tools, such as Google Analytics. Blocking can also involve setting up a private VPN network for browsing. The most common wide-spectrum privacy blockers include Ghostery, Privacy Badger, and uBlock Origin.

How private browsing and blockers affect the Frosmo Platform

We have compiled some of the most common questions about how online privacy technologies affect the Frosmo Platform.

The Frosmo Platform interprets a private browsing session as a new visitor. This means that no segmentation data or other data previously stored in the browser is available for the session. Each new private browsing session is counted as a new visitor.

You can still personalize content in real-time based on visitor actions, such as clicks and product views.
The Frosmo Platform is not an ad serving solution and therefore is not on any basic ad blocking lists. However, privacy blockers that block any third-party data and scripts effectively prevent the Frosmo Platform from working.

For example, the following privacy technologies block the Frosmo Platform:

- F-Secure FREEDOME VPN (only when tracking protection is enabled, and only for pages that use HTTP)
- Ghostery (when the "Beacon" category is selected)
- Opera's built-in ad blocker
- uBlock Origin

While it's estimated that in 2020, up to 50% of internet users use some kind of ad blocking tool, the use of wide-spectrum privacy blockers is less common. If a visitor uses privacy blockers that prevent third-party scripts and requests from working on your site, the Frosmo Platform will not work. This is because the Frosmo scripts are considered third-party for your site.

For more information about how to address the issue, contact Frosmo support.
If your site uses shared context, and if a visitor uses private browsing modes that block third-party data, the Frosmo Platform will not work. This is because the shared context data, which the platform relies on, is third-party for your site.

For more information about how to address the issue, contact Frosmo support.
The Frosmo Platform collects and stores selected data in the browser's local storage and cookies. For more information about the data stored in the visitor's browser, see Data storage and retention.

The legislation in most countries requires online service providers to acquire visitor's consent for setting cookies. Therefore, many service providers implement a cookie consent element on their websites that allows the visitor to select the types of cookies they accept or refuse. The cookies are roughly categorized as:

- **Strictly necessary.** The website does not function properly without the cookies.
- **Analytics.** Cookies that enable counting visits and traffic sources for website monitoring and optimizing.
- **Targeting.** Cookies that enable providing the visitor with personalized content.
- **Advertising.** Usually third-party cookies that enable ad services to show relevant ads on the website.

How you should classify Frosmo cookies on your site depends on the Frosmo Platform setup and purpose on your site. If you effectively cannot provide the core service of your site without the Frosmo Platform, you can classify Frosmo cookies as strictly necessary. This is the case, for example, if the front page of your site is built on recommendations displayed through the Frosmo Platform.

However, Frosmo cookies are also used for analytics and targeting. If a visitor does not give their consent to such cookies, you must make sure that you will not collect personal data of that visitor and that you will not show personalized content to them.

Selective profiling allows you to display modifications to visitors based on whether or not they consent to personalized, targeted modifications. For more information about how to use selective profiling on your site, contact Frosmo support.