Configure Matomo Analytics to comply with CNIL consent exemption

CNIL consent-exemption for website analytics

Version 1.0 - March 2026

Contents

CNIL consent-exemption for website analytics 3
Start my CNIL compliance check 4
Restrictions and disabling the CNIL configuration 6
How to interpret the assessment results 6
Self-Assessment Table 7
Additional conditions 15
What the CNIL configuration affects 15
Device model and screen resolution detection disabled 15
Major browser and operating system versions 15
Ecommerce - Restricted 16
Ecommerce - Order ID anonymisation 16
PII data filtered 16
Turn off Visits Log and Visitor profiles 16
Marketing and advertising features 17
Referrer Anonymisation 17
User ID disabled 17
IP address anonymisation 17
Data retention period 17
Limit available segments 17
Segmented data rounding enabled 17
A/B Testing 18
Heatmaps – Disable Heatmap/Session Recording 18
Third-party cookies 18
Opt out 18

CNIL consent-exemption for website analytics

In response to the "Cookies : solutions pour les outils de mesure d'audience " (*Cookies: solutions for audience measurement tools*) published by CNIL on 4 July 2025, we confirm that based on our self-assessment, the Matomo Cloud and Matomo On-Premise solutions comply with the criteria established by the CNIL (Cookies : solutions pour les outils de mesure d'audience and outil_d_auto-evaluation_mesure_d_audience.pdf), and may be implemented without requiring user consent if properly configured.

To comply with CNIL requirements, Matomo **must be configured as described** in this document:

- enabling the CNIL compliance configuration mode in the UI; and
- ensuring that additional modifications of Matomo, which are under Matomo Customers' control, are also applied according to the configuration described in this document.

This solution is **strictly limited** to the following purposes:

- Performance measurement;
- Detection of navigation issues;
- Optimisation of technical performance or ergonomics;
- Estimation of required server capacity;
- Analysis of viewed content.

It explicitly excludes any marketing-related measurement, including but not limited to:

- Measurement of conversion channel performance, advertising campaign performance, acquisition channel performance, ad fraud prevention, etc.
- Creation of user cohorts for presenting differentiated content, whether cohort membership is defined randomly or based on previously collected information.

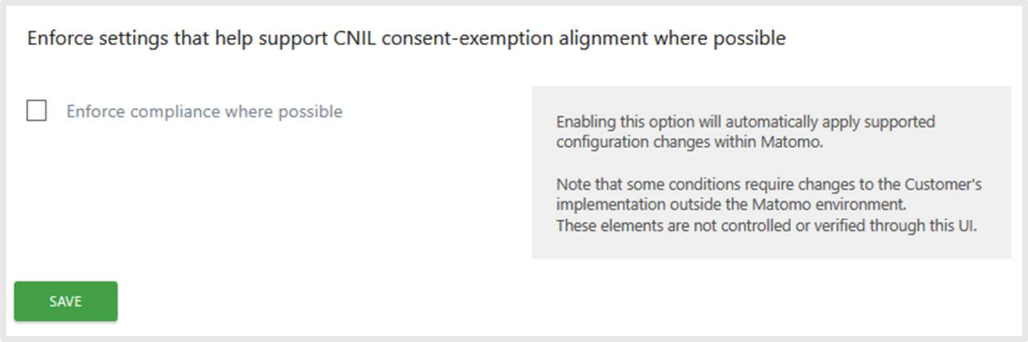
A Matomo configuration is correctly implemented when it meets all criteria listed in the Self-Assessment Table below. For each criterion, if an action is required by the website publisher, it is indicated in the **"Action to be taken"** column. If the publisher does not implement the specified measure, the solution may no longer qualify for the exemption from consent collection.

This evaluation is solely intended to assess whether an audience measurement solution can be implemented without prior consent and is not designed to evaluate the overall legal compliance of the solution with applicable regulations.

Start my CNIL compliance check

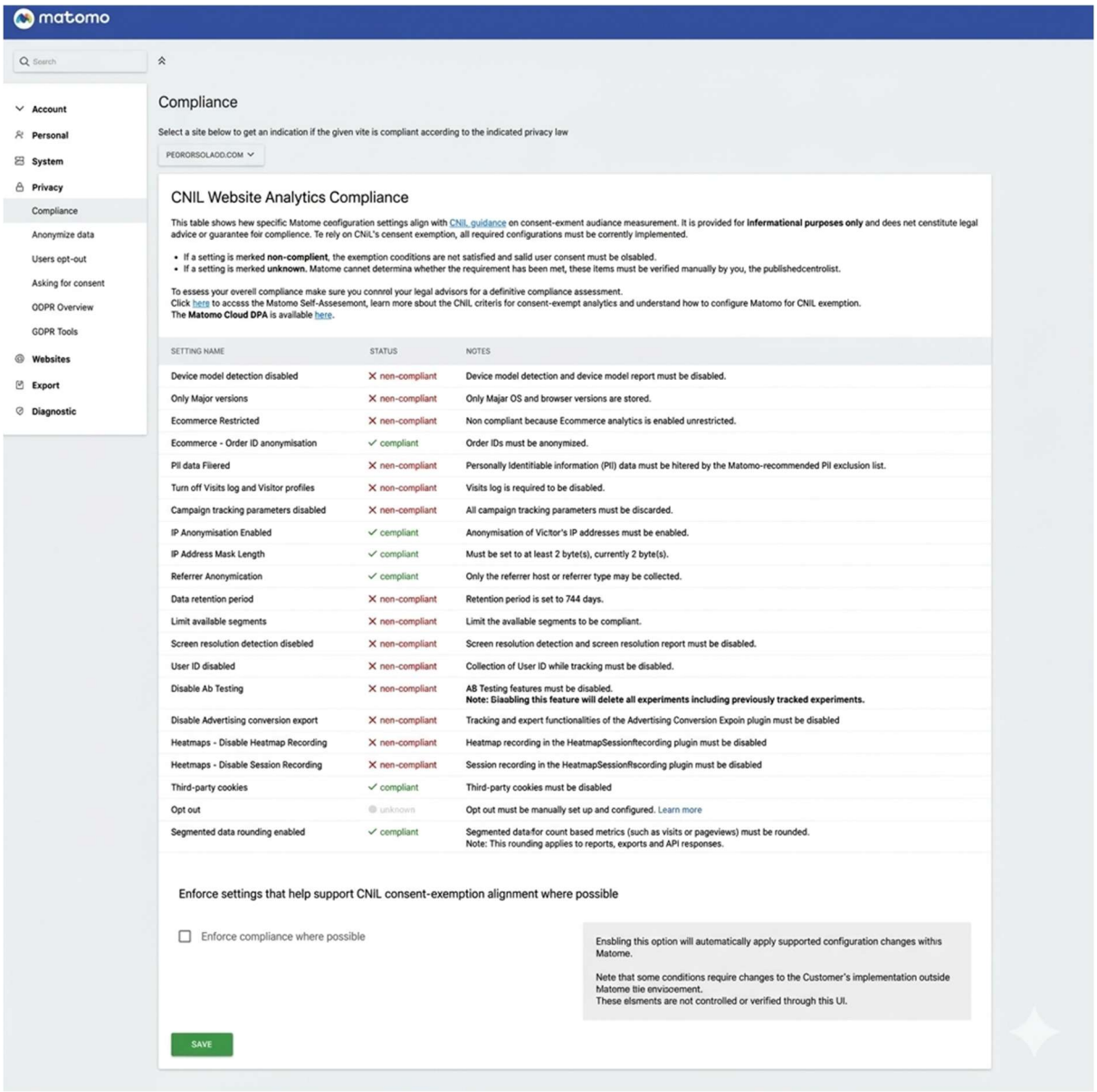
Running the compliance check analyses your current Matomo Cloud or On-Premise configuration against the CNIL requirements.

1. Log in to Matomo as a superuser.
2. Go to **Administration** > **Privacy** > **Compliance**.
3. Use the dropdown to **choose the site** for CNIL compliance. The required CNIL settings will be applied to the selected website (at the site level) and shown in the **Custom site settings**.
4. After selecting the site, the page will refresh showing the assessment results for the selected website/app.
5. The **Status** column indicates which settings are compliant or non-compliant:
    a. A **compliant** status means your current configuration meets the CNIL consent exemption requirements.
    b. A **non-compliant** status indicates that one or more settings must be configured to align with the CNIL requirements.
    c. An **unknown** status requires that you **manually configure and verify** if it meets the CNIL exemption conditions as Matomo cannot make that determination.
6. After reviewing the results, you can enable the CNIL compliance mode by scrolling down to the section **Enforce settings that help support alignment**.
7. Enable the option, **Enforce compliance where possible**.



8. Click **Save** and Matomo will automatically apply a CNIL-compliant configuration for the selected site.
9. Use the Self-Assessment Table below to understand and review each requirement against CNIL's published criteria for consent-exemption.

10. Although Matomo disables features that are not permitted under the exemption, you will need to manually review and configure any requirements marked with an **Unknown** status.



Restrictions and disabling the CNIL configuration

- To understand which features are disabled or restricted by this configuration, refer to the section **What the CNIL configuration affects** (included at the end of this guide).
- While CNIL enforcement is active, **do not enable** any functionality that falls outside the CNIL consent exemption conditions.
- Make sure that any Custom Goals or Events you create, fall within the permitted categories of events.
- To remove the CNIL configuration and re-enable restricted features, you can disable the setting, **Enforce compliance where possible** and click **Save**.

How to interpret the assessment results

The following table reflects our self-assessment of Matomo configuration designed for CNIL consent-exemption for audience measurement. It confirms that, when enabled, the feature adheres to the requirements.

Use the **Self-Assessment Table** below to understand how the CNIL compliance check applies to your Matomo configuration and what actions are required. It explains why certain features are disabled when CNIL enforcement is enabled, which requirements are handled automatically, and which settings you must manually review.

1. The **Objective**, **Criterion**, and **Technical Measure** columns are defined by CNIL and prescribe the conditions for compliance.
2. The **Criterion met** and **Action to be taken (for CNIL compliance mode)** columns explain how Matomo satisfies each CNIL requirement and what steps you need to take.
3. **Follow all instructions** listed in the table column **Action to be taken (for CNIL compliance mode)**.

Self-Assessment Table

This Self-Assessment Table is based on the self-assessment tool concerning the implementation of an audience measurement solution exempt from consent, published by CNIL in July 2025.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
1. The sole purpose for which the tool is used is the measurement of the audience of the website or application.	1.1 The provider makes available instructions for disabling any functionality that falls outside the defined scope.	N/A	**Yes.** The Matomo CNIL compliance mode automatically disables all functionalities incompatible with the consent exemption. Activation of such functionalities is technically prevented while the mode is enabled. Clear documentation and in-product information are provided to explain the scope and limitations of this mode.	**Check the following:** 1. Enable CNIL compliance mode for the relevant site or application: ▪ Go to **Privacy** > **Compliance**. ▪ Select the option **Enforce compliance where possible** and click **Save**. 2. After running the compliance check, refer to your CNIL assessment results and implement additional in-product configuration requirements for aspects outside Matomo's control (e.g., marked in the Matomo UI as "**unknown**").
	1.2 The data collected is minimised in relation to the intended purpose of audience measurement.	(A) If data from HTTP header fields ("headers") is collected (such as browser version, operating system, device type, screen size), this data must be minimised. Example: Only collect the major version of the	**Yes.** The full User-Agent string is never stored or exported.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Device model detection disabled** is compliant as related device model reports are automatically disabled. ▪ **Only Major versions** is compliant as only derived, minimised fields are stored. ▪ **Screen resolution detection disabled** is compliant as screen resolution reports are automatically disabled.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
		operating system or browser.		2. Do not transmit custom dimensions or other parameters that carry detailed device strings or full User-Agent.
		(B) The solution collects no more than three types of events: • The simple presence of a person on a page, along with information related to that page (e.g. name, type, etc.) • The use of a feature by that person (e.g. button click, link click), along with related information (e.g. destination, label, etc.) • Statistics on page load time, scrolling behaviour, or time spent on a page.	**Yes.** Data collection is limited to permitted events. Ecommerce analytics may be enabled only without collecting order identifiers or exposing e-commerce segments allowing identification or singling-out.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Ecommerce Restricted Ecommerce** analytics is enabled, but specific segments are disabled for Order ID, Order Revenue, Product Price, Product Name, Product SKU). ▪ **Ecommerce - Order ID anonymisation** with **restricted** Ecommerce analytics, the **Order ID** is automatically anonymised. 2. It is optional but recommended to completely disable Ecommerce tracking in your **website's settings**. 3. Ensure **no personal identifiers** are sent to Matomo (e.g. in Custom Dimensions). 4. When creating Custom Events, ensure that they fall into the three categories of events permitted by CNIL (listed in the **Technical Measure** column).
2. The provider offers the service under the processor regime.	2.1 The provider makes available a standard Data Processing Agreement (DPA) that includes the mandatory clauses listed in Article 28 of	N/A	**Yes.** For Matomo Cloud, a standard Article 28 GDPR-compliant Data Processing Agreement is made available to customers and incorporated into contractual documentation. DPA is	None.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
	the GDPR and qualifies the provider as a data processor.		incorporated by reference into our TOS. In On-Premise deployments, the publisher remains solely responsible for hosting and processing.	
	2.2 No pooling of raw audience measurement data from multiple clients is implemented by the provider.	N/A	**Yes.** Matomo does not pool or mix data from multiple clients. Each Customer's data is fully isolated and stored in a separate database (in Matomo Cloud) or within the infrastructure they themselves control (if self-hosted).	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Data retention period** is automatically set to 180 days. Longer retention periods, over 25 months exceed CNIL recommendations for exempt analytics data.
	2.3 No reuse of data for the provider's own purposes, regardless of the intended use (e.g. service improvement, fraud prevention, etc.), is implemented.	N/A	**Yes.** Data is processed solely on behalf of the publisher. Matomo complies with the requirement that data is not reused by the provider for its own purposes. In self-hosted mode, this is guaranteed technically; in Cloud mode it is enforced contractually and operationally.	None.
	2.4 The provider, acting as a data processor, makes available a point of contact to receive and handle	N/A	**Yes.** For Matomo Cloud customers: Contact details are provided in DPA. For On-Premise users, a dedicated privacy contact address and contact form are	None.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
	questions and complaints from prospects to clarify any doubts regarding compliance.		available: privacy@matomo.org or contact form: matomo.org/contact.	
3. The tool does not allow tracking of the individual outside the targeted website or application.	3.1 No import of external data is possible.	• Deactivation of any collection or import of customer identifiers (or "CRM"), UTM parameters, or campaign identifiers in URLs. • The referrer, if collected, is limited to the domain ("host"). • Any integration with third-party tools is excluded.	**Yes.** External data import is not possible. CRM identifiers and user identifiers are rejected. Only the referrer host is retained.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **PII data filtered** - the Matomo-recommended URL parameter exclusion list is automatically applied to filter out personal information identifiers. ▪ **Campaign tracking parameters disabled** - all campaign parameters (e.g., utm and mtm) and advertising identifiers are stripped at ingestion and not stored. ▪ **Disable Advertising conversion export** - tracking and export features of the Advertising Conversion Export plugin are disabled to prevent exporting conversion data to advertising platforms. ▪ **Referrer Anonymisation** - only the domain of a referrer URL is collected in CNIL compliance mode. 2. Do not pass CRM IDs or enable third-party marketing connectors. 3. Ensure tagging does not inject prohibited parameters. Verify your tag recipes do not add such fields.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
	3.2 No identifier that enables tracking across multiple domains is used.	• If the identifier used is a cookie, it is set internally ("first-party") to prevent global navigation tracking.	**Yes. Matomo uses first-party cookies by default.** This means that the cookies Matomo sets are tied to publisher's own website's domain (e.g. `example.com`), not to a third-party domain.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Third-party cookies** and cross-domain tracking features are disabled. 2. Do not enable the Matomo cross-domain tracking.
		• If the IP address is used, it is only for city-level geolocation and is then pseudonymised by removing at least the last octet.	**Yes.** IP addresses are truncated by removing the last two octets (IPv4) or the last two bytes (IPv6).	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **IP anonymisation** - anonymisation of visitors' IP addresses is automatically enabled to prevent the collection of full IP addresses. ▪ **IP address mask length** - the IP address mask length is set to 2 bytes.
		• Any method aimed at generating an identifier using device characteristics (digital fingerprinting) includes a site-specific component in the hash calculation (e.g. the current domain) to prevent tracking across multiple domains ("cross-site"), as well as a time-based	**Yes.** Matomo uses config_ID – a site-specific hash of device/ browser characteristics rotated every 24h to prevent cross-site tracking. Read more about the config_id.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Turn off Visits log and Visitor profiles** - the Visits Log and Visitor Profiles are automatically disabled.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
		component (to ensure the fingerprint has a limited lifespan).		
		• Any tagging that allows the collection of personal information (e.g. via forms) is excluded.	**Yes.** Personal identifiers are stripped or rejected before storage.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **PII data filtered** - the Matomo-recommended exclusion list is automatically applied to filter out personal information identifiers. ▪ **User ID disabled** - User ID collection is disabled. 2. You can apply additional filters by including the relevant parameters to the **Excluded Parameters** field in your website settings. 3. Do not send names, emails, post codes or other personal data and user identifiers in events, URLs, Page Titles, or Custom Dimensions.
	3.3 Any functionality aimed at cross-referencing, deduplicating, or measuring a unified reach of content ("reach") is excluded.	• Deactivation of tools related to measuring reach.	**Yes.** In CNIL compliance no features aimed at cross-referencing, deduplicating or measuring reach are enabled.	None if other features disabled as required.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
4.The data is used solely to produce anonymous statistical data.	4.1 Whether for visualisation within the tool's interface or during export, all reports generated by the solution contain only anonymous statistics.	Aggregation and rounding to the nearest ten. If this is not possible, an analysis is conducted to justify the anonymity of the data (see the G29 opinion on the subject).Le G29 publie un avis sur les techniques d'anonymisation | CNIL	**Yes.** All visit-level views and APIs (Visits Log, Visitor Profile, real-time, raw exports) are disabled. All visualisations within the tool's interface or during export and all reports generated by the solution contain only anonymous statistics. Only aggregated statistics remain accessible. Warehouse or data-sync that could bypass aggregation is disabled. Viewing or exporting Visit-level RAW data is not possible. Rounding to the nearest ten is described below.	None if other features disabled as required.
	4.2 Anonymisation is effective regardless of the selection criteria chosen by the client of the solution (a combination of criteria must not allow a user to be singled out).		**Yes.** Segments enabling singling-out (identifiers, precise timestamps, fingerprint components, Ecommerce identifiers) are disabled. When segmentation is used, count-based metrics are rounded to the nearest multiple of 10 in reports, exports, and API responses.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Limit available segments** - specific segments are automatically restricted: ▪ **visitServerHour**: Site time - hour (time of last action); ▪ **visitIP**: visitor's IP address; ▪ **Ad Click ID**: Used in Advertising Conversion Export which is also disabled in CNIL mode.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
	4.3 No tracking of the navigation of an individual user is possible.	Deactivation of any session replay-type functionality.	**Yes.** Heatmaps and session recordings are disabled and cannot be collected, viewed or exported. Individual navigation paths cannot be reconstructed.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Heatmaps - Disable Heatmap Recording** - Heatmaps are automatically disabled. ▪ **Heatmaps - Disable Session Recording** - Session recordings are automatically disabled. ▪ **Disable AbTesting** - A/B testing features are disabled and all existing experiments will be permanently deleted.
5.The right to object is respected.	5.1 An objection mechanism is implemented insofar as the processing of personal data within the meaning of the GDPR exists.	Objection available in the form of a button or clickable link within the privacy policy of the visited website or application.	**Yes.** Matomo provides an opt-out iframe or link that may be embedded by the publisher in the privacy policy, allowing users to object to audience measurement.	**Check the following:** 1. When CNIL compliance mode is enabled: ▪ **Manually embed and configure** the opt-out mechanism. ▪ Keep the opt-out active and clearly visible on the website (e.g. in the publisher's privacy policy which should be clearly linked and visible and inform visitor of use of Matomo trackers). 2. CNIL compliance **cannot be confirmed** until the opt-out is set up. Read more on how to configure opt-out of tracking.
	5.2 Sufficient measures are implemented to ensure that the refusal is respected over time.	Place an opt-out cookie or measure and add a digital fingerprint to a blocklist	**Yes.** The opt-out mechanism relies on a dedicated opt-out cookie ensuring that the user's objection is persistently respected over time.	**Check the following:** 1. When CNIL compliance mode is confirmed: ▪ The opt-out is active and clearly accessible. ▪ The manually configured opt-out mechanism stops tracking when visitors request to opt out.

Additional conditions

Matomo also complies with the additional conditions as stated at Cookies : solutions pour les outils de mesure d'audience | CNIL:

- Lifespans of the Matomo trackers are limited to **maximum 13 months** by default and can be shortened and monitored by the publishers. The lifespan duration is not automatically extended upon new visits.
- Retention periods can be set to **maximum 25 months** and monitored by the publishers.
- Matomo Cloud collects, processes and stores data independently for each publisher.
- The trackers are completely independent from one another and from any other tracker.
- Creation of user cohorts for presenting differentiated content whether cohort membership is defined randomly or based on previous collected data is disabled.
- No A/B testing is configured by the publisher.

What the CNIL configuration affects

When the CNIL configuration is enabled, Matomo applies a restricted configuration for the selected website or app. This configuration limits data collection and feature availability to what the CNIL permits for audience measurement. The following features are disabled or offer limited use:

Device model and screen resolution detection disabled

Device model detection, related device model reports and screen resolution detection are disabled. Collecting this detail increases the risk of fingerprinting and exceeds what the CNIL permits under the exemption.

Major browser and operating system versions

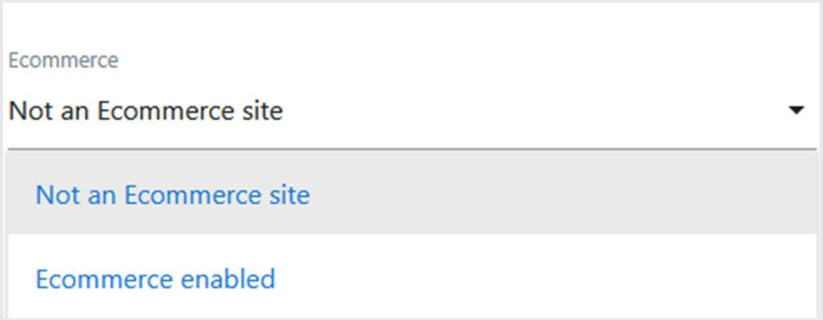
Matomo stores only major versions of operating systems and browsers. It is optional to disable the browser feature detection completely.

Ecommerce - Restricted

When CNIL mode is active, Matomo automatically sets Ecommerce to **Restricted**. This disables the Ecommerce **Order ID** feature and related segments, `Order ID`, `Order Revenue`, `Product Price`, `Product Name`, and `Product SKU`.

It is optional (and recommended) to disable Ecommerce tracking:

1. Go to **Administration** > **Websites** (Measurables) > **Manage** and open the relevant site settings.
2. Scroll down to the **Ecommerce** section.
3. Set the **Ecommerce** dropdown to **Not an Ecommerce site**.



Ecommerce - Order ID anonymisation

When CNIL mode is active, Matomo restricts Ecommerce tracking and anonymises Order IDs. Disabling Ecommerce tracking also disables Order ID collection.

PII data filtered

Matomo prevents the storage of personal data. Names, email addresses, postcodes, and similar identifiers are stripped or rejected before storage. URLs, page titles, and custom dimensions are monitored to prevent the ingestion of personal data.

External data imports are blocked. CRM identifiers, user IDs, and similar identifiers are rejected. Learn more about the **Matomo-recommended PII list of exclusions** to understand which URL parameters Matomo will automatically exclude from tracking and reports.

Turn off Visits Log and Visitor profiles

All visit-level views and APIs are disabled. This includes the Visits Log, Visitor Profile, real-time reports, and raw data exports. Only aggregated and anonymous statistics remain available in the interface and in exports.

Marketing and advertising features

Third-party marketing integrations and conversion exports are disabled. Matomo does not store campaign parameters and advertising identifiers as they are stripped during data ingestion.

Referrer Anonymisation

Only the referrer host or referrer type is retained. Full referrer URLs and parameters are not stored.

User ID disabled

Matomo automatically disables the User ID feature in CNIL mode as explicit user identifiers are not permitted under the consent exemption.

IP address anonymisation

IP addresses are anonymised to reduce the risk of identifying individuals while allowing coarse geographic analysis. The IP mask length is set to at least two bytes.

Data retention period

The data retention period is automatically set to 180 days. Refer to the **Additional conditions** where retention periods can be set to maximum 25 months and monitored by the publishers.

Limit available segments

All visit-level views and APIs (Visits Log, Visitor Profile, real-time, raw exports) are disabled. It includes visualisations within the tool's interface or during export and all reports generated by the solution contain only anonymous statistics.

Specific segments are automatically restricted:

- **visitServerHour**: Site time - hour (time of last action).
- **visitIP**: visitor's IP address.
- **Ad Click ID**: Used in Advertising Conversion Export which is also disabled in CNIL mode.

Warehouse or data-sync that could bypass aggregation is disabled. Viewing or exporting Visit-level RAW data is not possible.

Segmented data rounding enabled

When CNIL enforcement is enabled and a segment is applied, Matomo rounds count-based metrics to the nearest multiple of 10. This rounding applies in reports, scheduled reports, exports, and Reporting API responses.

Percentages, rates, averages, and monetary values are not affected. Totals are calculated from the original values and then rounded before display.

A/B Testing

A/B testing features are disabled. A/B testing involves behavioural analysis that goes beyond basic audience measurement. **Enabling CNIL mode permanently deletes all existing experiments**.

Heatmaps – Disable Heatmap/Session Recording

Heatmaps and Session Recordings are disabled. These features analyse detailed user interactions and replay individual sessions, which creates a high risk of identifying users without consent.

Third-party cookies

Matomo uses first-party cookies by default. This means that the cookies Matomo sets are tied to publisher's own website's domain (e.g. example.com), not to a third-party domain. Cross-domain tracking features are disabled.

Third-party cookies must be disabled so that Matomo only sets cookies on the first-party domain of the website or application being measured. Using third-party cookies would allow cross-site tracking and user correlation across multiple websites, which is not permitted under the CNIL consent exemption.

Opt out

Matomo provides an opt-out mechanism in the form of an iframe or link. Publishers can embed this in their privacy policy to allow visitors to decline being included in audience measurement. Learn more about **how to let visitors opt-out of tracking?**