Configure Matomo Analytics to comply with CNIL consent exemption

CNIL consent-exemption for website analytics

Version 3.0 – October 2026

Contents

CNIL consent-exemption for website analytics 3

Start my CNIL compliance check 4

Restrictions and disabling the CNIL configuration 7

How to interpret the assessment results 7

Self-Assessment Table 8

Additional conditions 17

What the CNIL configuration affects 17

IP Anonymisation Enabled 17

PII Data Filtering Enabled 17

User ID Tracking Disabled 18

Device Model and Screen Resolution Detection Disabled 18

Major Browser and OS versions 18

Visits Log and Visitor Profiles Disabled 18

Segment Availability Restricted 18

Segmented Data Rounding Enabled 19

Referrer Anonymisation Enabled 19

Campaign Parameter Masking Enabled 19

Advertising Conversion Export Disabled 20

Ecommerce Data Collection Restricted 20

Ecommerce Order ID Anonymisation Enabled 20

A/B Testing Disabled 21

Heatmaps – Heatmap Recording Disabled 21

Heatmaps – Session Recording Disabled 21

Raw Data Retention Configured 21

Stack Trace Logging Disabled 21

Third-party cookies (Managed outside Matomo UI) 21

Opt-Out Configured (Managed outside Matomo UI) 22

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 setting, the table explains the CNIL requirement, its impact and current status. Use the toggle to apply individual settings or enforce all settings in one click for the selected website. If the publisher does not implement the CNIL requirement, 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.

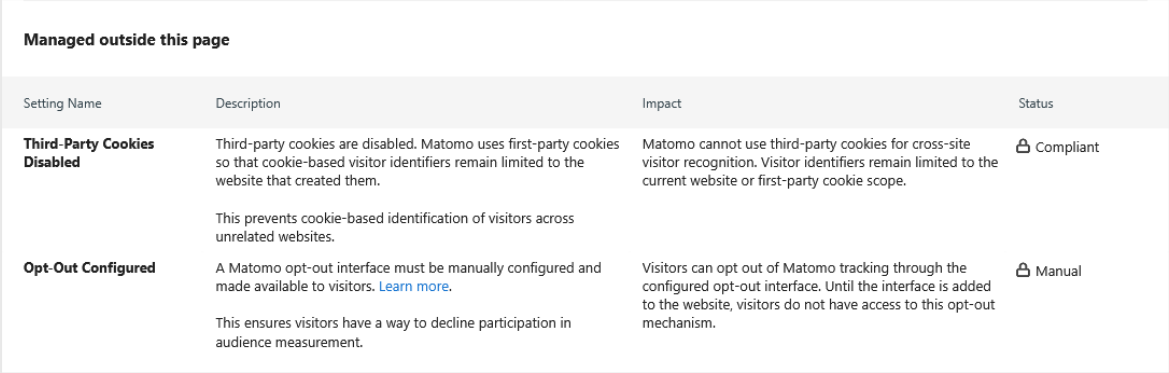
1. Log in to Matomo as a superuser.
2. Go to **Administration** > **Privacy** > **Compliance**.
3. Select to apply the CNIL configuration to a specific site or to all websites in your Matomo instance:
    a. **All Websites**: Enforcing CNIL settings overrides custom site settings for all websites. However, disabling a setting in the global CNIL configuration does not override the setting enabled at the individual website level. To fully disable a setting, review the individual website configurations and update them where necessary.
    b. **Single Website**: Applies the CNIL configuration only to the selected website, without affecting other websites in your Matomo instance.
4. After selecting the site, the table will refresh showing the assessment results for the selected website/app.
5. The **Status** column indicates which settings are currently compliant or non-compliant:
    a. **Compliant:** The requirement is already met because the relevant setting has been configured directly in Matomo, rather than being enforced through the CNIL configuration in this table.
    b. **Compliant (enforced):** The requirement is met by enforcing the CNIL configuration in this table.
    c. **Non-compliant**: The current configuration does not meet the CNIL consent exemption requirements. Review the **Description** and **Impact** columns to understand the requirement.
    d. **Manual**: Matomo cannot control or verify the status of this CNIL requirement. It must be completed and checked outside this page.

6. To apply all available CNIL settings at once, click **Enforce All Settings** and **Save**.



Matomo automatically applies the required configuration for all Matomo environment settings it can enforce.

7. Alternatively, review each setting and toggle on to enable the CNIL configuration described in the table. After using the toggle for all settings, click **Save** to apply the configuration.
8. When you toggle off, Matomo removes the applied CNIL configuration for the setting. Click **Save** apply the non-compliant configuration.
9. Settings listed under **Managed outside this page** cannot be configured directly on the CNIL configuration page.
    a. **Third-party cookies:** Matomo assesses whether third-party cookies are disabled based on its configuration. If enabled, update the relevant tracking settings to meet the CNIL exemption conditions.
    b. **Opt-out interface (Manual):** Manually verify that your opt-out interface meets the CNIL exemption conditions, as Matomo cannot automatically assess its implementation. You may need to update your website or other systems that integrate with Matomo to ensure CNIL compliance.



10. Use the **Self-Assessment Table** to understand and review each requirement against CNIL's published criteria for consent-exemption.

Setting Name	Description	Impact	Status	
IP Anonymisation Enabled	Visitor IP addresses are anonymised before they are processed and stored. This reduces the risk of identifying visitors through their IP address.	Full visitor IP addresses are unavailable. Geolocation reports may be less precise because part of the IP address is masked before location detection.	✓ Compliant	
IP Address Mask Length Configured	IP anonymisation is configured to mask **3 bytes** of each visitor's IP address. At least 2 bytes must be masked to provide the required level of anonymisation. This reduces the ability to identify visitors or determine their precise location.	3 bytes of each visitor IP address are removed before processing. Geolocation accuracy may be reduced, particularly at city level.	✓ Compliant	
PII Data Filtering Enabled	Personally identifiable information is filtered from URL query parameters using Matomo's recommended PII exclusion list. This prevents information such as names, email addresses, phone numbers, and account identifiers from being stored in URLs and reports.	Matching personal information is removed from tracked and stored URLs. Reports cannot display or analyse the filtered values.	Non-compliant	
User ID Tracking Disabled	User ID tracking is disabled. Tracking implementations must not send User IDs using setUserId or equivalent methods. This prevents visitors from being directly identified and associated across visits or devices.	User ID values are not collected. User ID reports, segments, and cross-visit analysis based on User ID are unavailable.	Non-compliant	
Device Model Detection Disabled	Device model detection is disabled. This reduces the risk of identifying visitors based on their specific device characteristics.	The **Visitors** > **Devices** > **Device Model** report is unavailable, and device model information is not collected.	Non-compliant	
Screen Resolution Detection Disabled	Screen resolution detection is disabled. This reduces the risk of identifying visitors based on their screen configuration.	Screen resolution information is not collected, and screen resolution reports under **Visitors** > **Devices** are unavailable.	Non-compliant	
Major Browser and OS Versions	Only major browser and operating system versions are stored. Minor and patch versions are removed. For example, Chrome 136 or iOS 18 may be stored, but not Chrome 136.0.7103 or iOS 18.5.1. This reduces the risk of identifying visitors using detailed browser and operating system information.	Browser and operating system version reports under **Visitors** > **Software** only show major versions. Detailed version analysis and segmentation are unavailable.	Non-compliant	
Visits Log and Visitor Profiles Disabled	Visits Log and Visitor Profile features are disabled. This prevents an individual visitor's browsing path and detailed visit-level behaviour from being reconstructed.	**Visitors** > **Visits Log** and Visitor Profile views are unavailable.	Non-compliant	
Segment Availability Restricted	Segments based on Visitor IP Address, Site Time - Hour representing the time of the last action, and Ad Click ID are disabled. This prevents these detailed attributes from being filtered or combined to identify a specific visitor.	Visitor IP Address, Site Time - Hour, and Ad Click ID cannot be used when creating or applying segments.	Non-compliant	
Segmented Data Rounding Enabled	Count-based metrics in segmented reports, exports, and API responses are rounded to the nearest 10. Any non-zero value below 10 is displayed as 10. Unsegmented reports continue to show exact totals. This protects visitor anonymity when reports are filtered into small subsets where low counts could reveal an individual.	Count-based metrics in segmented results are approximate. Segmented values may not add up to the corresponding unsegmented total.	Non-compliant	
Referrer Anonymisation Enabled	Only the referrer host or referrer type is collected. Full referrer URLs, including paths and query parameters, are not stored. This reduces the risk of collecting personal or sensitive information contained in referrer URLs.	Attribution reports remain available, but detailed referrer paths and query parameters cannot be viewed, reported, or segmented.	Non-compliant	
Campaign Parameter Masking Enabled	Campaign name and campaign keyword values are masked before storage. This prevents detailed campaign and advertising identifiers from being used beyond permitted audience measurement purposes.	Campaign attribution and aggregate acquisition metrics remain available, but original campaign names and keywords cannot be viewed or used to distinguish individual campaigns.	Non-compliant	
Advertising Conversion Export Disabled	Tracking and export functionality provided by the Advertising Conversion Export plugin is disabled. This prevents conversion information from being exported to advertising platforms, which is outside the permitted scope of the CNIL audience-measurement exemption.	Advertising conversion exports and related tracking features are unavailable. Conversion data cannot be sent to supported advertising platforms.	Non-compliant	
Ecommerce Data Collection Restricted	If Ecommerce analytics is enabled, the collection and use of detailed order-level and product-level information is restricted. This prevents order and product information from being used to identify individual visitors or purchases.	Overall ecommerce conversion and revenue metrics remain available. Segments based on Order ID, Order Revenue, Product Price, Product Name, and Product SKU are unavailable.	Non-compliant	
Ecommerce Order ID Anonymisation Enabled	Ecommerce order IDs are anonymised before they are stored. This reduces the risk of linking ecommerce transactions to identifiable visitors or individual purchases.	Original order IDs cannot be viewed. Ecommerce Order ID reports and related segments are unavailable.	✓ Compliant	
A/B Testing Disabled	A/B Testing features are disabled. This prevents visitors from being individually assigned or targeted based on tracked behaviour.	Experiments cannot run, and A/B Testing reports are unavailable. **Existing and historical experiment data is deleted when A/B Testing is disabled.**	Non-compliant	
Heatmaps - Heatmap Recording Disabled	Heatmap recording is disabled in the Heatmaps & Session Recording plugin. This prevents detailed collection of how individual visitors interact with page elements.	New heatmap interaction data is not collected, and heatmap reports are unavailable.	Non-compliant	
Heatmaps - Session Recording Disabled	Session recording is disabled in the Heatmaps & Session Recording plugin. This prevents an individual visitor's browsing session and page interactions from being recorded and replayed.	New session recordings are not collected. Session replay recordings and playback features are unavailable.	Non-compliant	
Raw Data Retention Configured	Raw data retention is configured to **744 days**. It must be set to a maximum of 759 days, approximately 25 months. This limits how long detailed visit information is retained and reduces the risk of it being used to identify someone.	Raw visit data older than 744 days is automatically deleted. Historical aggregated reports may remain available according to the configured report-retention settings.	✓ Compliant	
Stack Trace Logging Disabled	Stack traces are not stored when a crash is tracked. This keeps personal data that appears in error messages, file paths and URLs out of your crash reports.	Crash reports still show the error message, source file, line and column, but no stack trace. Tracing the exact sequence of calls that led to a crash becomes harder.	Non-compliant	

Restrictions and disabling the CNIL configuration

- For more information about how the CNIL configuration affects each setting 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, toggle off the setting 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.

Note: This assessment only applies to the Matomo configuration related to consent exemption. It does not evaluate or reflect the consent status collected through your Consent Management Platform (CMP) or other consent tools. If you use a CMP, consent choices collected through that platform are managed separately and are not represented in this compliance assessment.

1. Use the **Self-Assessment Table** below to understand how the CNIL compliance check applies to your Matomo configuration and why certain features should be disabled.
2. The **Objective**, **Criterion**, and **Technical Measure** columns are defined by CNIL and prescribe the conditions for compliance.
3. The **Criterion met** and **Action to undertake/Impact (for CNIL compliance mode)** columns explain how Matomo satisfies each CNIL requirement and what steps you need to take.
4. **Follow all instructions** listed in the table column **Action to undertake/Impact**.

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 undertake/Impact
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.	1. Enable CNIL compliance mode for the relevant site and go to **Privacy** > **Compliance**. 2. Click **Enforce All Settings**, or toggle on each required setting and click **Save**. 3. Refer to your CNIL assessment results and implement additional in-product configuration requirements for aspects outside Matomo's control (e.g., listed in the Matomo UI under "**Managed outside this page**").
	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.	1. Do not transmit custom dimensions or other parameters that carry detailed device strings or full User-Agent. 2. **Device Model Detection Disabled**: The **Visitors > Devices > Device Model** report is unavailable, and device model information is not collected. 3. **Major Browser and OS Versions**: Browser and operating system version reports under **Visitors > Software** only show major versions.

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
		operating system or browser.		Detailed version analysis and segmentation are unavailable. 4. Only derived, minimised fields are stored. 5. **Screen Resolution Disabled**: Screen resolution information is not collected, and screen resolution reports under **Visitors > Devices** are unavailable.
		(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.	1. **Ecommerce Data Collection** is restricted, and specific segments are disabled for Order ID, Order Revenue, Product Price, Product Name, Product SKU. Overall ecommerce conversion and revenue metrics remain available. 2. **Ecommerce - Order ID Anonymisation Enabled** - The Order ID is automatically anonymised. Original Order IDs cannot be viewed. Ecommerce Order ID reports and related segments are unavailable. 3. It is optional but recommended to completely disable Ecommerce tracking in your website's settings. 4. Ensure **no personal identifiers** are sent to Matomo (e.g. in Custom Dimensions). 5. 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	2.1 The provider makes available a	N/A	**Yes.** For Matomo Cloud, a standard Article 28 GDPR-	None.

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
under the processor regime.	standard Data Processing Agreement (DPA) that includes the mandatory clauses listed in Article 28 of the GDPR and qualifies the provider as a data processor.		compliant Data Processing Agreement is made available to customers and incorporated into contractual documentation. DPA is 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).	**Raw Data Retention Configured** - raw visit data older than 744 days is automatically deleted. Historical aggregated reports may remain available according to the configured report-retention settings. Longer retention periods, over 25 months exceed CNIL recommendations for exempt analytics data. You can configure a shorter retention period if preferred.
	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	None.

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
			enforced contractually and operationally.	
	2.4 The provider, acting as a data processor, makes available a point of contact to receive and handle questions and complaints from prospects to clarify any doubts regarding compliance.	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 available: privacy@matomo.org or contact form: matomo.org/contact.	None.
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.	1. **PII Data Filtering Enabled** - the Matomo-recommended URL parameter exclusion list is automatically applied to filter out personal information identifiers. 2. **Campaign Parameter Masking Enabled**- all campaign parameters (e.g., utm and mtm) and advertising identifiers are discarded at ingestion and not stored. Campaign attribution and aggregate acquisition metrics remain available, but original campaign names and keywords cannot be viewed or used to distinguish individual campaigns. 3. **Advertising Conversion Export Disabled** - tracking and export features of the Advertising Conversion Export plugin are disabled to prevent exporting conversion data to advertising platforms.

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
				4. **Referrer Anonymisation Enabled** - Only the referrer host or referrer type is collected. Full referrer URLs, including paths and query parameters, are not stored. Attribution reports remain available, but detailed referrer paths and query parameters cannot be viewed, reported, or segmented. . 5. Do not pass CRM IDs or enable third-party marketing connectors. 6. Ensure tagging does not inject prohibited parameters. Verify your tag recipes do not add such fields.
	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.	1. **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).	1. **IP Anonymisation Enabled** - anonymisation of visitors' IP addresses is automatically enabled to prevent the collection of full IP addresses. 2. **IP Address Mask Length** - IP anonymisation is configured to mask **3 bytes** of each visitor's IP address. At least 2 bytes must be masked to provide the required level of anonymisation.

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
		• 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 component (to ensure the fingerprint has a limited lifespan).	**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.	1. **Visits log and Visitor Profiles Disabled** - the Visits Log and Visitor Profiles are automatically disabled and cannot be viewed. 2. Aggregated real-time reports stay available while the Visits Log is turned off. Only the "Last 24 hours" and "Last 30 minutes" totals are shown, and counts are rounded. No individual visitor, visit, session or action level information is exposed.
		• Any tagging that allows the collection of personal information (e.g. via forms) is excluded.	**Yes.** Personal identifiers are stripped or rejected before storage.	1. **PII Data Filtering Enabled** - the Matomo-recommended exclusion list is automatically applied to filter out personal information identifiers. 2. **User ID Tracking Disabled** - User ID collection is disabled. Tracking implementations must not send User IDs using setUserId or equivalent methods. 3. You can apply additional filters by including the relevant parameters to the **Excluded Parameters** field in your website settings.

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
				4. 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 CNIL requirements are configured.
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 CNIL requirements are configured.
	4.2 Anonymisation is effective		**Yes.** Segments enabling singling-out (identifiers, precise	1. **Segmented Data Rounding Enabled** - Count-based metrics in segmented reports, exports, and

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
	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).		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.	API responses are rounded to the nearest 10. Any non-zero value below 10 is displayed as 10. Unsegmented reports continue to show exact totals. 2. **Segment Availability Restricted**- segments based on Visitor IP Address (visitIP), Site Time - Hour (**visitServerHour**) representing the time of the last action. Ad Click IDs are disabled (used in Advertising Conversion Export which is also disabled in CNIL 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.	1. **Heatmaps - Heatmap Recording Disabled** - Heatmaps are automatically disabled. New heatmap interaction data is not collected, and heatmap reports are unavailable. 2. **Heatmaps - Session Recording Disabled** - Session recordings are automatically disabled. New session recordings are not collected. Session replay recordings and playback features are unavailable. 3. **A/B Testing Disabled** - A/B testing features are disabled and all existing and historical experiment data is permanently deleted.
5.The right to object is respected.	5.1 An objection mechanism is implemented insofar as the processing of personal data within	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.	1. A Matomo opt-out interface must be manually configured and made available to visitors. Read more on how to configure opt-out of tracking. 2. 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).

Objective	Criterion	Technical Measure	Criterion met	Action to undertake/Impact
	the meaning of the GDPR exists.			3. Matomo does not determine compliance status for settings with a **Manual** status.
	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.	1. The opt-out is active and clearly accessible. 2. 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:

IP Anonymisation Enabled

IP addresses are anonymised to reduce the risk of identifying individuals while allowing coarse geographic analysis. IP anonymisation is configured to mask 3 bytes of each visitor's IP address. At least 2 bytes must be masked to provide the required level of anonymisation.

PII Data Filtering Enabled

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.

User ID Tracking Disabled

Matomo automatically disables the User ID feature in CNIL mode as explicit user identifiers are not permitted under the consent exemption. User ID reports, segments, and cross-visit analysis based on User ID are unavailable.

Device Model and Screen Resolution Detection Disabled

Device model detection, related device model reports and screen resolution reports are disabled under **Visitors > Devices**.

Collecting this detail increases the risk of fingerprinting and exceeds what the CNIL permits under the exemption.

Major Browser and OS versions

Browser and operating system version reports under **Visitors > Software** only show major versions. Minor and patch versions are removed and detailed version analysis and segmentation are unavailable. For example, Chrome 136 or iOS 18 may be stored, but not Chrome 136.0.7103 or iOS 18.5.1.

It is optional to disable the browser feature detection completely.

Visits Log and Visitor Profiles Disabled

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.

It prevents an individual visitor's browsing path and detailed visit-level behaviour from being reconstructed.

Aggregated real-time reports remain available when the Visits Log is turned off.

Visitors > Real-time continues to show aggregated counters for the **Last 24 hours** and **Last 30 minutes**. These counts are rounded so they cannot be used to expose information about individual visitors, visits, sessions or actions.

Segment Availability Restricted

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. Any non-zero value below 10 is displayed as 10. Rounding applies in reports, scheduled reports, exports, and Reporting API responses.

This behaviour helps protect visitor anonymity when reports are filtered into very small groups, where low counts could otherwise reveal whether a specific individual matched a segment.

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

In some cases, segmented totals may appear higher than unsegmented totals because small values are rounded up to protect visitor privacy. This is expected behaviour when CNIL enforcement is enabled.

Referrer Anonymisation Enabled

Only the referrer host or referrer type is collected. Full referrer URLs, including paths and query parameters, are not stored.

This reduces the risk of collecting personal or sensitive information that may be included in a referrer URL. Attribution reports remain available, but detailed referrer information cannot be viewed, reported on or used in segments.

Campaign Parameter Masking Enabled

Matomo does not store campaign parameters and advertising identifiers as they are stripped during data ingestion.

Campaign attribution and aggregate acquisition metrics remain available, but specific UTM parameter values are replaced with the placeholder label `(UTM parameter discarded)` in reports. This allows you to distinguish campaign traffic from organic traffic without storing the original campaign values.

Advertising Conversion Export Disabled

Tracking and export functionality provided by the Advertising Conversion Export plugin is disabled. This prevents conversion information from being sent to advertising platforms, which falls outside the permitted scope of the CNIL audience-measurement exemption.

Advertising conversion exports and related tracking features are therefore unavailable.

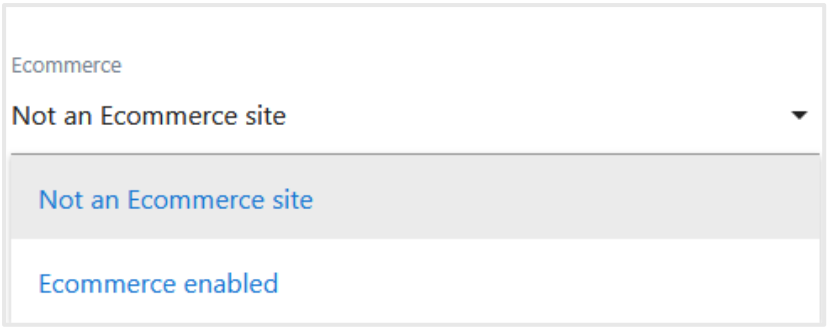
Ecommerce Data Collection Restricted

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`. This prevents order and product information from being used to identify individual visitors or purchases.

Overall ecommerce conversion and revenue metrics remain available.

If recommended by your privacy advisors, Ecommerce can be fully disabled

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 Enabled

When you enable this option, an Order ID will be automatically anonymised so no personal information will be tracked. It is important to note that if you enable this feature, in some cases duplicate orders may be counted if visitors refresh the order confirmation page, as there is no way to distinguish unique orders.

When CNIL mode is active, Ecommerce order IDs are anonymised to reduce the risk of linking ecommerce transactions to identifiable visitors or individual purchases.-Original Order IDs cannot be viewed and Order ID reports and related segments are unavailable.

Disabling Ecommerce tracking also disables Order ID collection.

A/B Testing Disabled

A/B testing features are disabled as it involves behavioural analysis that goes beyond basic audience measurement. **Enabling CNIL mode permanently deletes all existing and historical experiment data**. Experiments cannot run and A/B Testing reports are unavailable.

Heatmaps – Heatmap Recording Disabled

Heatmaps are disabled to prevent detailed data about how visitors interact with page elements from being collected. New heatmap interaction data is not recorded, and heatmap reports are unavailable.

Heatmaps – Session Recording Disabled

Session Recordings are disabled because no tracking of individual user's navigation is permitted and session replay feature deactivation is required. New session recordings are not collected, and session recording and playback features are unavailable.

Raw Data Retention Configured

Raw data retention is configured to 744 days and must not exceed 759 days (approximately 25 months). This limits how long detailed visitor information is retained, reducing the risk of it being used to identify an individual. Raw visit data is automatically deleted once it is older than the configured retention period.

Historical aggregated reports may remain available according to the configured report-retention settings.

Stack Trace Logging Disabled

When enabled, Matomo **Crash Analytics** does not store stack traces when tracking crashes. This helps protect personal data that may appear in error messages, file paths or URLs within stack traces.

Crash reports still include the error message, source file, line and column number. However, without a stack trace, identifying the sequence of function calls that led to a crash becomes more difficult.

Third-party cookies (Managed outside Matomo UI)

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.

Publishers must review if any third-party cookies are enabled on their website.

Opt-Out Configured (Managed outside Matomo UI)

An opt-out mechanism must be made available on your website so visitors can decline participation in audience measurement.

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?