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.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
		operating system or browser.		▪ **Screen resolution detection disabled** is compliant as screen resolution reports are automatically disabled. 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	2.1 The provider makes available a standard Data Processing Agreement (DPA)	N/A	**Yes.** For Matomo Cloud, a standard Article 28 GDPR-compliant Data Processing Agreement is made available to customers and incorporated	None.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
processor regime.	that includes the mandatory clauses listed in Article 28 of the GDPR and qualifies the provider as a data processor.		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).	**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	N/A	**Yes.** For Matomo Cloud customers: Contact details are provided in DPA.	None.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
	and handle questions and complaints from prospects to clarify any doubts regarding compliance.		For On-Premise users, a dedicated privacy contact address and contact form are 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.

Objective	Criterion	Technical Measure	Criterion met	Action to be taken (for CNIL compliance mode)
				3. 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.	**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	**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)
		domains (“cross-site”), as well as a time-based 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.