Tableau d’auto-évaluation

Ce tableau d’auto-évaluation est basé sur l’**Outil d’auto-évaluation – Mise en œuvre d’une solution de mesure d’audience exemptée de consentement**, publié par la CNIL en juillet 2025.

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
1. L’unique finalité pour laquelle l’outil est utilisé est celle de la mesure de l’audience du site ou de l’application	1.1 Le prestataire met à disposition des instructions pour désactiver toute fonctionnalité qui sort du cadre déterminé	N/A	**Oui**. Le mode de conformité CNIL de Matomo désactive automatiquement toutes les fonctionnalités incompatibles avec l’exemption de consentement. L’activation de ces fonctionnalités est techniquement empêchée tant que ce mode est activé. Une documentation claire et des informations intégrées au produit sont fournies pour expliquer la portée et les limitations de ce mode.	**Vérifiez les éléments suivants :** 1. Activez le mode de conformité CNIL pour le site ou l’application concerné : Accédez à **Vie privée > Conformité**, sélectionnez l’option « **Enforce All Settings** », puis cliquez sur « **Enregistrer** ». 2. Consultez les résultats de votre évaluation CNIL et effectuez les configurations supplémentaires nécessaires dans les produits concernés pour les éléments qui échappent au contrôle de Matomo (par exemple, ceux répertoriés dans l’interface de Matomo sous « **Managed outside this page** »).

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
	1.2 Les données collectées sont minimisées au regard de la finalité de mesure d'audience poursuivie	(A) Si des données provenant des champs d'en-tête (« *headers* ») HTTP sont collectées (version de navigateur, système d'exploitation, matériel, taille d'écran), ces données sont minimisées (version majeure système d'exploitation/navigateur par exemple)	**Oui**. La chaîne complète du User-Agent n'est jamais stockée ni exportée.	**Vérifiez les éléments suivants :** 1. Ne transmettez pas de dimensions personnalisées, ni d'autres paramètres contenant des chaînes détaillées d'appareil ou une chaîne User-Agent complète. 2. **Détection du modèle d'appareil désactivée :** Le rapport Visiteurs > Périphériques > Modèle du périphérique n'est pas disponible et aucune information sur le modèle de l'appareil n'est collectée. 3. **Uniquement les versions majeures :** Les rapports sur les versions des navigateurs et des systèmes d'exploitation, accessibles sous Visiteurs > Logiciel, affichent uniquement les versions majeures. L'analyse détaillée des versions et la segmentation par version détaillée ne sont pas disponibles. 4. Seules des données dérivées et minimisées sont stockées.

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				5. **Détection de la résolution d'écran désactivée :** Aucune information sur la résolution d'écran n'est collectée et les rapports correspondants, accessibles sous Visiteurs > Périphériques, ne sont pas disponibles.
		(B) La solution collecte au plus trois types d'évènements : • La simple présence d'une personne sur une page et les informations associées à cette page (nom, type, etc.). • L'utilisation par cette personne d'une fonctionnalité (clic bouton, clic lien) et les informations .associées (destination, label, etc.) • Les statistiques de temps de chargement, de défilement ou de temps passé sur une page.	**Oui.** La collecte de données est limitée aux événements autorisés. Le rapport Ecommerce peut être activée uniquement si aucun identifiant de commande n'est collecté et si aucun segment ecommerce permettant l'identification ou la singularisation n'est exposé.	**Vérifiez les éléments suivants :** 1. **Ecommerce restreint** : La collecte des données Ecommerce est limitée et certains segments sont désactivés (Order ID, Order Revenue, Product Price, Product Name, Product SKU). Les indicateurs globaux de conversion et de chiffre d'affaires Ecommerce restent disponibles. – **Ecommerce - Anonymisation de l'identifiant de commande** L'identifiant de commande (Order ID) est automatiquement anonymisé. Les identifiants de commande d'origine ne peuvent plus être consultés. Les rapports sur les identifiants de commande

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				Ecommerce et les segments associés ne sont pas disponibles. 2. Il est facultatif, mais recommandé, de désactiver complètement le suivi Ecommerce dans les paramètres de votre site. 3. Assurez-vous qu'aucun identifiant personnel n'est transmis à Matomo (par exemple, dans les dimensions personnalisées). 4. Lors de la création d'événements personnalisés (Custom Events), assurez-vous qu'ils appartiennent à l'une des trois catégories d'événements autorisées par la CNIL (indiquées dans la colonne « Mesure technique »).
2. Le prestataire propose le service sous le régime de la sous-traitance	2.1 Le prestataire met à disposition un accord de traitement des données (ou « *data processing agreement* », DPA) standard qui inclut les	N/A	**Oui.** Pour Matomo Cloud, un contrat de sous-traitance des données conforme à l'article 28 du RGPD (Data Processing Agreement – DPA) est mis à la disposition de la	N/A

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
	mentions obligatoires listées à l'article 28 du RGPD et le qualifie en tant que sous-traitant		clientèle et intégré à la documentation contractuelle. Le DPA est incorporé par référence dans nos Conditions Générales d'Utilisation (Nos CGU : TOS). Dans les déploiements OnPremise, l'éditeur·ice du site demeure le ou la seule responsable de l'hébergement et du traitement des données.	
	2.2 Aucune mise en commun par le prestataire de données brutes de mesure d'audience provenant de sa clientèle n'est mise en œuvre.	N/A	**Oui.** Matomo ne mutualise, ni ne mélange les données de ses différents clients et clientes. Les données de chaque client et cliente sont entièrement isolées et stockées dans une base de données distincte (dans Matomo Cloud), ou au sein de l'infrastructure qu'ils et elles contrôlent	**Période de conservation des données** : Les données brutes des visites datant de plus de 744 jours sont automatiquement supprimées. Les rapports agrégés historiques peuvent rester disponibles selon les paramètres de conservation des rapports configurés. Les durées de conservation supérieures à 25 mois dépassent les recommandations de la CNIL pour

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
			eux-mêmes (en cas d'auto-hébergement).	les données de mesure d'audience exemptées de consentement. Vous pouvez configurer une durée de conservation plus courte si vous le souhaitez.
	2.3 Aucune réutilisation des données pour le propre compte du prestataire et quelle que soit la finalité (amélioration de son service, lutte contre la fraude, etc.) n'est mise en œuvre.	N/A	**Oui.** Les données sont traitées exclusivement pour le compte de l'éditeur ou éditrice. Matomo respecte l'exigence selon laquelle les données ne sont pas réutilisées par le fournisseur à ses propres fins. En mode auto-hébergé, cela est garanti techniquement ; en mode Cloud, cela est appliqué contractuellement et opérationnellement.	N/A
	2.4 Le prestataire met à disposition en tant que sous-traitant un point de contact afin de recevoir et traiter	N/A	**Oui.** Pour la clientèle Matomo Cloud : les coordonnées de contact sont fournies dans le DPA. Pour les utilisateur·ices	N/A

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
	les questions et réclamations de leurs prospect pour clarifier les doutes sur la conformité.		OnPremise, une adresse de contact dédiée à la protection de la vie privée ainsi qu'un formulaire de contact sont disponibles : privacy@matomo.org ou formulaire de contact : matomo.org/contact.	
3. L'outil ne permet pas un suivi de la personne en dehors du site ou de l'application visée.	3.1 Aucun import de données externes n'est possible.	• Désactivation de toute collecte ou import d'identifiant clientèle (ou « *CRM* »), d'UTM ou d'identifiant de campagne dans les URLs. • Le référent (« *referrer* »), s'il est collecté, se limite au domaine (« *host* »). • Toute intégration avec des outils tiers est exclue.	**Oui.** L'importation de données externes n'est pas possible. Les identifiants CRM et les identifiants utilisateurs sont rejetés. Seul l'hôte du référent est conservé.	**Vérifiez les éléments suivants :** 1. **PII Filtrage des données activé** : La liste d'exclusion des paramètres d'URL recommandée par Matomo est automatiquement appliquée afin de filtrer les identifiants contenant des données personnelles. 2. **Valeurs des paramètres de la campagne masquées** : Tous les paramètres de campagne (par exemple, utm et mtm) ainsi que les identifiants publicitaires sont supprimés lors de la collecte des données et ne sont pas stockés. L'attribution des campagnes et les indicateurs agrégés d'acquisition restent

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				disponibles, mais les noms et mots-clés des campagnes d'origine ne peuvent plus être consultés ni utilisés pour distinguer les campagnes individuelles. 3. **Advertising Conversion Export Disabled** : Les fonctionnalités de suivi et d'exportation du plugin Advertising Conversion Export sont désactivées afin d'empêcher l'exportation des données de conversion vers les plateformes publicitaires. 4. **Anonymisation du référent** : Seuls le domaine du référent ou le type de référent sont collectés. Les URL de provenance complètes, y compris les chemins et les paramètres de requête, ne sont pas stockées. Les rapports d'attribution restent disponibles, mais les chemins et les paramètres de requête détaillés des URL de provenance ne peuvent plus être consultés, affichés dans les rapports ni utilisés pour la segmentation.

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				5. Ne transmettez pas d'identifiants CRM et n'activez pas de connecteurs marketing tiers. 6. Assurez-vous qu'aucun paramètre interdit n'est transmis via vos règles de tagging.
	3.2 Aucun identifiant permettant un suivi à travers plusieurs domaines n'est utilisé.	• Si l'identifiant utilisé est un cookie, celui-ci est déposé en interne (ou « *first-party* ») afin d'empêcher un suivi global de la navigation.	**Oui**. Matomo utilise par défaut des cookies first-party. Cela signifie que les cookies définis par Matomo sont liés au domaine du site de l'éditeur rice (par exemple *example.com*), et non à un domaine tiers.	**Vérifiez les éléments suivants :** 1. Les fonctionnalités Cookies tiers et **cross domain tracking** sont désactivées. 2. N'activez pas le suivi inter-domaine (cross domain tracking) de Matomo.
		• L'IP si elle est utilisée, permet la localisation à l'échelle de la ville puis est pseudonymisée en enlevant au moins le dernier octet.	**Oui**. Les adresses IP sont tronquées en supprimant les deux derniers octets (IPv4) ou les deux derniers bytes (IPv6).	**Vérifiez les éléments suivants :** 1. **Anonymisation des IP activée** : l'anonymisation des adresses IP des visiteurs est automatiquement activée afin d'empêcher la collecte d'adresses IP complètes. 2. **Longueur du masque d'adresse IP** : L'anonymisation

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				des adresses IP est configurée pour masquer 3 octets de chaque adresse IP des visiteurs. Au moins 2 octets doivent être masqués pour garantir le niveau d'anonymisation requis.
		• Toute mesure visant à générer un identifiant en utilisant les caractéristiques du terminal (empreinte numérique ou « *fingerprinting* ») intègre une composante spécifique au site lors du calcul du hash (par exemple le domaine en cours de visite) pour empêcher un suivi à travers plusieurs domaines (ou « *cross-site* »), ainsi qu'une composante temporelle (permettant de s'assurer que l'empreinte numérique (ou « *fingerprint* ») ait une durée de vie limitée).	**Oui**. Matomo utilise le *config_ID*, un hachage spécifique au site basé sur les caractéristiques de l'appareil et du navigateur, qui est renouvelé toutes les 24 heures afin d'empêcher le suivi inter-site. Pour en savoir plus sur le *config_id*.	**Vérifiez les éléments suivants** : 1. **Visits Log and Visitor Profile Disabled** : les fonctionnalités **Journal des Visites** et **Afficher le profil du visiteur** sont automatiquement désactivées et ne peuvent plus être consultées. 2. Les rapports agrégés en temps réel restent disponibles lorsque le journal des visites est désactivé. Seuls les totaux « Last 24 hours » et « Last 30 minutes » sont affichés, et les valeurs sont arrondies. Aucune information individuelle sur les visiteurs, les visites, les sessions ou les actions n'est accessible.

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
		• Tout marquage permettant de récupérer des informations personnelles (par exemple par le biais de formulaires) est exclu.	**Oui.** Les identifiants personnels sont supprimés ou rejetés avant stockage.	Vérifiez les éléments suivants : 1. **PII Filtrage des données activé** : La liste d'exclusion recommandée par Matomo est automatiquement appliquée afin de filtrer les identifiants contenant des données personnelles. 2. **Identifiant utilisateur désactivé** : La collecte des identifiants utilisateur (User ID) est désactivée. Les implémentations de suivi ne doivent pas transmettre d'identifiants utilisateur à l'aide de la méthode setUserId ou de méthodes équivalentes. 3. Vous pouvez appliquer des filtres supplémentaires en ajoutant les paramètres concernés dans le champ ***Excluded Parameters*** dans les paramètres de votre site. 4. Ne transmettez pas de noms, d'adresses e-mail, de codes postaux ni d'autres données personnelles ou identifiants utilisateur dans les événements, les URL, les titres de page ou les dimensions

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				personnalisées (Custom Dimensions).
	3.3 Toute fonctionnalité visant à croiser, dédoubler ou mesurer un taux de couverture (« *reach* ») unifié d'un contenu est exclue.	Désactivation des outils relatifs à la mesure du taux de couverture (« *reach* »).	**Oui**. Pour la conformité CNIL, aucune fonctionnalité visant à effectuer du recoupement, de la déduplication ou de la mesure de portée n'est activée.	Néant, si les autres fonctionnalités sont désactivées comme requis.
4. Les données servent uniquement à produire des données statistiques anonymes.	4.1 Autant pour la visualisation mise à disposition dans l'interface de l'outil que lors d'export, l'ensemble des rapports générés par la solution comportent uniquement des statistiques anonymes.	Agrégation et la présentation à la dizaine la plus proche. A défaut, une analyse est menée pour justifier du caractère anonyme des données (voir l'avis du G29 sur le sujet)	**Oui.** Toutes les vues et API au niveau des visites (Visits Log, Visitor Profile, temps réel, exports bruts) sont désactivées. Toutes les visualisations dans l'interface de l'outil ou lors d'un export, ainsi que tous les rapports générés par la solution, ne contiennent que des statistiques anonymes. Seules des statistiques agrégées restent accessibles. Le *Warehouse* ou le *data-sync*, qui pourraient	Néant, si les autres fonctionnalités sont désactivées comme requis.

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
			contourner l'agrégation, sont désactivés. Il n'est pas possible de consulter ou d'exporter des données brutes au niveau de la visite. L'arrondi à la dizaine la plus proche est décrit ci-dessous.	
	4.2 L'anonymisation est effective quels que soit les critères de sélection choisi par la clientèle de la solution (une combinaison de critère ne doit pas permettre d'isoler un·e utilisateurice).		**Oui**. Les segments permettant la singularisation (identifiants, horodatages précis, composants d'empreinte numérique, identifiants ecommerce) sont désactivés. Lorsque la segmentation est utilisée, les métriques basées sur des dénombrements sont arrondies au multiple de 10 le plus proche dans les rapports, les exports et les réponses d'API.	**Vérifiez les éléments suivants :** 1. **Disponibilité du segment restreinte** : Les segments suivants sont désactivés : • **visitServerHour :** Heure du site – Heure (heure de la dernière action) ; • **visitIP :** adresse IP du visiteur ; • **Ad Click ID** : Identifiants de clic publicitaire utilisés par le plugin Advertising Conversion Export, également désactivé en mode de conformité CNIL. 2. **Arrondi des données segmentées active** : Les métriques de comptage dans

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				les rapports segmentés, les exportations et les réponses de l'API sont arrondies à la dizaine la plus proche. Toute valeur non nulle inférieure à 10 est affichée comme 10. Les rapports non segmentés continuent d'afficher les totaux exacts.
	4.3 Aucun suivi de la navigation d'un utilisateur ou d'une utilisatrice unique n'est possible.	Désactivation de toute fonctionnalités du type rejeu de session (« *session replay* »)	**Oui.** Les Heatmaps et les Session Recordings sont désactivés et ne peuvent pas être collectés, consultés ou exportés. Les parcours individuels de navigation ne peuvent pas être reconstitués.	**Vérifiez les éléments suivants :** 1. **Heatmaps - Heatmap Recording Disabled** : Les cartes de chaleur (Heatmaps) sont automatiquement désactivées. Aucune nouvelle donnée d'interaction avec les cartes de chaleur n'est collectée et les rapports correspondants ne sont pas disponibles. 2. **Heatmaps - Session Recording Disabled** : Les enregistrements de session sont automatiquement désactivés. Aucun nouvel enregistrement de session n'est collecté. Les enregistrements de sessions précédentes et les

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				fonctionnalités de lecture ne sont plus disponibles. 3. **A/B Testing Disabled** : Les fonctionnalités d'A/B testing sont désactivées et toutes les données des expérimentations existantes et passées sont définitivement supprimées.
5. Le droit à l'opposition des personnes est respecté.	5.1 Une modalité d'opposition est mise en œuvre dans la mesure ou un traitement de données à caractère personnel au sens du RGPD existe.	• Opposition disponible sous la forme d'un bouton ou lien cliquable au sein de la politique de confidentialité du site ou application visité.	**Oui.** Matomo fournit un iframe ou un lien d'opt-out que l'éditeur·ice peut intégrer dans sa politique de confidentialité, permettant aux utilisateur·ices de s'opposer à la mesure d'audience.	**Vérifiez les éléments suivants :** 1. **Désinscription** : Une interface d'opposition au suivi Matomo doit être configurée manuellement et mise à la disposition des visiteurs. Pour en savoir plus, consultez la documentation sur la configuration de l'opposition au suivi. 2. Maintenez le mécanisme d'opposition au suivi actif et clairement visible sur votre site web, par exemple dans votre politique de confidentialité. Celle-ci doit être facilement accessible et informer les visiteurs de l'utilisation des traceurs Matomo. 3. Matomo ne détermine pas le statut de conformité des

Objectif	Critère	Mesure technique	Critère respecté	Action à entreprendre / Impact
				paramètres portant la mention « **Manual** »
	5.2 Des moyens suffisants sont mis en œuvre pour prendre en compte le refus dans la durée.	• Procéder au dépôt d'un cookie d'opposition ou à la mesure et l'ajout à une liste de blocage d'une empreinte numérique (ou « fingerprinting »).	**Oui.** Le mécanisme d'opt-out repose sur un cookie d'opt-out dédié, garantissant que l'opposition de l'utilisateur·ice est respectée de manière persistante dans le temps.	**Vérifiez les éléments suivants :** 1. Le mécanisme d'opposition au suivi a été configuré manuellement et reste actif et facilement accessible aux visiteurs. 2. Le mécanisme d'opposition au suivi interrompt effectivement le suivi lorsqu'un visiteur choisit de s'y opposer.