GRILLE D'AUTO-ÉVALUATION CNIL RELATIVE À LA MISE EN ŒUVRE D'UNE SOLUTION DE MESURE D'AUDIENCE EXEMPTÉE DE CONSENTEMENT

Informations générales sur la solution évaluée :

- **Solution évaluée :** Suite Wysistat (Wysistat Analytics & Wysistat News & Wysistat Studio)
- **Éditeur et Sous-traitant :** Société IDfr (SAS à capitaux 100 % français – 17 F rue Savary, 25000 Besançon, France)
- **Référentiel juridique et technique applicable :** Outil d'auto-évaluation de la CNIL publié le 4 juillet 2025, Article 82 de la loi n° 78-17 du 6 janvier 1978 modifiée (Loi Informatique et Libertés transposant l'article 5, paragraphe 3, de la directive 2002/58/CE dite « ePrivacy »), Délibérations CNIL n° 2020-091 et n° 2020-092 du 17 septembre 2020, Règlement (UE) 2016/679 (RGPD), Avis 05/2014 du Groupe de travail « Article 29 » (WP216) sur les techniques d'anonymisation et Lignes directrices 01/2025 du CEPD sur la pseudonymisation.
- **Date de mise à jour de l'évaluation :** Novembre 2026
- **Point de contact DPO / Conformité :** rgpd@wysistat.com

Déclaration officielle de conformité

« D'après notre auto-évaluation, la solution Wysistat est conforme aux critères établis par la CNIL, et peut être mise en œuvre sans requérir le consentement des utilisateurs si elle est correctement configurée. »

Synthèse des 5 objectifs et 14 critères du référentiel CNIL

Objectif CNIL	Critères couverts	Mode d'application dans Wysistat	Statut de conformité
Objectif 1 : La seule finalité est la mesure d'audience	Critères 1.1 et 1.2	Natif par conception (Privacy by Design, Art. 25 RGPD), sans mode hybride ni option publicitaire	**Respecté**
Objectif 2 : Le fournisseur agit exclusivement en sous-traitant	Critères 2.1, 2.2, 2.3 et 2.4	Contrat DPA Art. 28 intégré, cloisonnement strict par client, hébergement 100 % en France	**Respecté**
Objectif 3 : Aucun suivi global ou inter-sites de la navigation	Critères 3.1, 3.2 et 3.3	Cookie first-party (13 mois) ou hachage serveur éphémère (24h), Referer réduit au domaine, écart argumenté et sécurisé (Regex + seuil 5 visites) sur les libellés génériques de campagne	**Respecté (avec écart argumenté et sécurisé sur 3.1)**
Objectif 4 : Production exclusive de statistiques anonymes	Critères 4.1, 4.2 et 4.3	Croisements guidés limités à 2 ou 3 dimensions simultanées, seuil de k-anonymat de 5 visites et regroupement consolidé dans « Autres »	**Respecté**
Objectif 5 : Information et effectivité du droit d'opposition	Critères 5.1 et 5.2	Modèle de mention légale et module d'opposition (Opt-out) multi-terminal fournis au Client	**Respecté (sous condition d'insertion par le Client)**

OBJECTIF 1 : Limiter strictement la finalité à la seule mesure d'audience

Critère 1.1 : Désactivation ou absence des fonctionnalités sortant du cadre de la mesure d'audience

- **Exigence du référentiel CNIL :** Le fournisseur de la solution donne les moyens de désactiver toute fonctionnalité excédant la stricte mesure d'audience (ciblage publicitaire, profilage marketing individuel, personnalisation commerciale, rejeu de session individuel non masqué, export de journaux d'événements individuels).
- **Mise en œuvre native chez Wysistat :** Afin d'éliminer tout risque d'erreur de paramétrage humain chez le Client, Wysistat a fait le choix architectural de ne proposer aucun « mode hybride » ni fonctionnalité publicitaire ou de profilage. La conformité est native dès la conception (article 25 du RGPD) : les fonctions incompatibles avec l'exemption CNIL n'existent pas dans le produit. Ni l'interface utilisateur, ni l'API REST JSON, ni le serveur MCP ne permettent d'accéder à des événements individuels (« hit par hit ») ou d'exporter des identifiants de visite.
- **Action requise par le Client :** Aucune. La garantie est appliquée nativement par l'architecture logicielle de Wysistat.
- **Statut : Respecté.**

Critère 1.2 : Minimisation des données collectées sur le terminal et encadrement des événements

- **Exigence du référentiel CNIL :** La précision des informations tirées des en-têtes HTTP (navigateur, système d'exploitation, appareil, écran, adresse IP) est réduite dès la collecte. La solution collecte au plus trois types d'événements génériques : le chargement d'une page, l'usage d'une fonctionnalité (clic, téléchargement, soumission d'objectif) et des mesures de temps, sans collecte de données personnelles.
- **Mise en œuvre native chez Wysistat :**
    - **Traitement de l'adresse IP en mémoire vive volatile :** Dès réception de la requête HTTP sur les serveurs français de Wysistat, l'adresse IP est lue uniquement en mémoire vive (RAM) pour être résolue en localisation géographique générale (Pays, Région, Département) et, en mode sans cookie, pour calculer un condensat cryptographique éphémère. L'adresse IP complète n'est jamais écrite sur disque dur ni dans les journaux de base de données.
    - **Généralisation du User-Agent :** L'en-tête User-Agent est traité à la volée pour écarter les robots (bots) puis réduit uniquement à la famille du navigateur (ex. Chrome, Firefox, Safari) et à la famille du système d'exploitation (ex. Windows, macOS, Android, iOS), sans conservation des numéros de version ou de sous-version.
    - **Catégorisation de la taille d'écran :** Les dimensions d'écran ne sont jamais conservées au pixel près ; elles sont immédiatement regroupées côté serveur en grandes catégories normalisées.
    - **Encadrement des événements et filtrage syntaxique (Regex Scrubbing) :** Wysistat ne collecte que trois types d'événements techniques : la page vue, le temps de lecture/présence et les interactions fonctionnelles définies via la méthode _setEvent (limitée à 3 niveaux de profondeur hiérarchique). Afin de prévenir toute injection accidentelle de donnée personnelle dans une URL ou un libellé d'événement, le moteur d'ingestion applique en mémoire vive un filtre par expression régulière (Regex) qui remplace automatiquement toute adresse électronique par :email, toute séquence de 5 chiffres ou plus par :id, tout identifiant UUID par :uuid et toute chaîne alphanumérique aléatoire de 16 caractères ou plus par :token.
- **Action requise par le Client :** Ne pas injecter volontairement de données nominatives (nom, prénom) dans les libellés du plan de marquage _setEvent.
- **Statut : Respecté.**

OBJECTIF 2 : Garantir que le fournisseur agit exclusivement en qualité de sous-traitant

Critère 2.1 : Contrat de sous-traitance conforme à l'article 28 du RGPD

- **Exigence du référentiel CNIL :** L'utilisation de la solution est encadrée par un contrat de sous-traitance conforme aux exigences de l'article 28 du RGPD, qualifiant l'éditeur du site de Responsable de traitement et le fournisseur de Sous-traitant.
- **Mise en œuvre chez Wysistat :** Un Accord de sous-traitance (DPA) en langue française, strictement conforme à l'article 28 du RGPD, fait partie intégrante des conditions contractuelles de Wysistat et figure en seconde partie du présent document.
- **Action requise par le Client :** à signer en annexe du contrat
- **Statut : Respecté.**

Critère 2.2 : Absence totale de mutualisation des données entre clients

- **Exigence du référentiel CNIL :** Les données sont collectées, traitées et stockées de manière strictement indépendante pour chaque client éditeur.
- **Mise en œuvre chez Wysistat :** Chaque compte client dispose d'un périmètre logique strictement isolé. Aucune mise en commun, aucune inter-corrélation et aucun rapprochement de visiteurs ne sont effectués entre les différents clients de Wysistat.
- **Action requise par le Client :** Aucune.
- **Statut : Respecté.**

Critère 2.3 : Absence de réutilisation des données pour le compte propre du fournisseur

- **Exigence du référentiel CNIL :** Le fournisseur s'interdit toute réutilisation des données collectées pour ses propres finalités (amélioration d'autres services commerciaux, ciblage publicitaire, revente ou constitution de panels tiers).
- **Mise en œuvre chez Wysistat :** La société IDfr s'engage contractuellement (article 3 du DPA) à ne jamais utiliser les données de ses clients pour son propre compte (sauf à des fins d'étude et d'amélioration du service). L'intégralité des infrastructures d'hébergement est située en France et détenue par des capitaux 100 % français, excluant tout transfert hors de l'Union européenne (Chapitre V du RGPD) et toute exposition aux lois extraterritoriales étrangères (US Cloud Act, FISA 702). La seule transmission externe possible concerne l'envoi des compteurs agrégés à l'ACPM (OJD) lorsque le Client a formellement mandaté Wysistat pour certifier sa fréquentation.
- **Action requise par le Client :** Aucune.
- **Statut : Respecté.**

Critère 2.4 : Point de contact dédié aux questions de conformité

- **Exigence du référentiel CNIL :** Le fournisseur met à la disposition de ses clients, de leurs DPO et de leurs prospects un point de contact dédié aux questions relatives à la protection des données.
- **Mise en œuvre chez Wysistat :** Une adresse électronique dédiée est active et mentionnée dans l'ensemble de la documentation contractuelle et publique : **rgpd@wysistat.com** (Société IDfr – 17 F rue Savary, 25000 Besançon).
- **Action requise par le Client :** Aucune.
- **Statut : Respecté.**

OBJECTIF 3 : Empêcher tout suivi global de la navigation en dehors du site

Critère 3.1 : Absence d'import externe, réduction du Referer et écart argumenté sur le traitement anonymisé des libellés de campagne (UTM)

- **Exigence du référentiel CNIL :** Désactivation de toute collecte ou import d'identifiant client (User-ID), réduction du site référent (Referer) à son seul nom de domaine, absence d'intégration avec des outils marketing tiers et neutralisation du traçage individuel via les paramètres de campagne dans les URLs.
- **Mise en œuvre chez Wysistat :**
    - **Zéro import externe :** Wysistat ne propose aucune fonctionnalité d'import de données CRM ni de collecte de User-ID.
    - **Réduction du Referer externe au domaine :** L'URL de provenance issue de l'en-tête HTTP Referer est systématiquement tronquée en mémoire vive pour ne conserver que le nom de domaine ou sous-domaine d'origine (ex. www.google.fr, com.google.android.googlequicksearchbox pour Google Discover), éliminant tout chemin ou paramètre d'URL externe.
    - **Purge immédiate des identifiants publicitaires individuels :** Les paramètres de suivi publicitaire individuel (gclid, fbclid, msclkid, dclid, twclid, mc_eid, li_fat_id, ttclid) ainsi que les paramètres granulaires utm_content et utm_term sont immédiatement supprimés de l'URL en mémoire vive dès réception de la requête.
    - **Écart argumenté et sécurisé sur les libellés génériques utm_source, utm_medium et utm_campaign :**
        i. *Fondement juridique :* Dans sa publication officielle du 4 juillet 2025 accompagnant la grille d'auto-évaluation, la CNIL précise qu'il « n'est pas exclu que certaines solutions ne remplissant pas l'ensemble des critères définis puissent tout de même être mises en œuvre de sorte à respecter l'exemption prévue par l'article 82 de la loi Informatique et Libertés. Il serait alors de la responsabilité du fournisseur de documenter son analyse pour démontrer que, bien que sortant du champ de l'outil d'auto-évaluation fourni par la CNIL, sa solution, telle que configurée, peut être mise en œuvre sans recueillir le consentement. »
        ii. *Nécessité technique liée à la disparition du Referer :* L'article 5 de la délibération CNIL n° 2020-091 reconnaît que l'analyse de la provenance du trafic agrégée de manière journalière est strictement nécessaire à l'éditeur pour dimensionner ses équipements serveurs et administrer son site. Or, les politiques de sécurité modernes des navigateurs (Referrer-Policy restrictives par défaut), les applications mobiles tierces et les clients de messagerie coupent l'en-tête HTTP Referer, faisant basculer des vagues majeures de trafic (lettres d'information, notifications, syndications) en « Accès direct » si les indicateurs génériques d'URL sont ignorés.
        iii. *Mesures techniques d'anonymisation à la source et en sortie :* Pour éliminer intégralement les deux risques motivant la restriction de la CNIL (risque d'injection d'un identifiant individuel dans l'URL et risque d'individualisation d'un visiteur), Wysistat applique trois verrous cumulatifs aux seuls libellés utm_source, utm_medium et utm_campaign : (a) un filtrage syntaxique immédiat par expression régulière (Regex) en mémoire vive qui remplace toute adresse e-mail par :email, toute suite de 5 chiffres ou plus par :id, tout UUID par :uuid et toute chaîne aléatoire de 16 caractères ou plus par :token ; (b) l'absence de toute exposition des données brutes ; et (c) l'application d'un seuil strict de *k-anonymat* fixé à **5 visites minimum** sur la période analysée, regroupant automatiquement tout libellé inférieur à 5 visites au sein d'une catégorie générique « Autres campagnes / Autres sources ». Il est ainsi mathématiquement impossible qu'un lien personnalisé ciblant un individu franchisse le seuil d'agrégation ou apparaisse dans l'interface ou l'API.
- **Statut : Respecté (avec écart argumenté et sécurisé par filtrage Regex et k-anonymat à 5 visites).**

Critère 3.2 : Absence d'identifiant inter-sites, durée de vie des traceurs et non-collecte des formulaires

- **Exigence du référentiel CNIL :** Tout cookie éventuel est strictement *first-party* et limité à 13 mois sans prorogation automatique ; toute empreinte serveur éventuelle inclut une composante propre au site et une composante temporelle courte ; l'adresse IP est supprimée après géolocalisation ; aucun marquage ne lit le contenu des champs de formulaires.
- **Mise en œuvre chez Wysistat :**
    - **Mode Cookie First-Party (Wysistat Analytics – Certification ACPM) :** Le cookie nommé Wysistat (ou l'entrée localStorage équivalente) est déposé exclusivement en *first-party* sur le domaine du site audité. Il contient uniquement un identifiant aléatoire de visite, un identifiant aléatoire d'internaute et les compteurs/horodatages techniques requis par le cahier des charges de l'ACPM. Sa durée de vie est limitée à **13 mois maximum et n'est jamais prorogée automatiquement** lors des nouvelles visites (recommandation CNIL n° 2020-092, § 51).
    - **Protection des formulaires :** Le script JavaScript de Wysistat ne lit jamais la valeur des champs de saisie (input, textarea, select) des formulaires.
- **Statut : Respecté.**

Critère 3.3 : Absence de mesure de couverture unifiée (Reach) ou de déduplication inter-sites

- **Exigence du référentiel CNIL :** La solution ne permet ni de dédoubler les visiteurs entre différents sites web ou applications, ni de calculer une couverture (*reach*) globale multi-domaines.
- **Mise en œuvre chez Wysistat :** Tant en mode Cookie First-Party (isolé par domaine navigateur) qu'en mode Sans Cookie (condensat intégrant le domaine du site client), un même internaute visitant deux sites distincts génère deux identifiants mathématiquement indépendants. Aucune déduplication inter-sites n'est réalisable.
- **Statut : Respecté.**

OBJECTIF 4 : Garantir que l'interface et les exports ne délivrent que des statistiques anonymes

Critères 4.1, 4.2 et 4.3 : Anonymat des statistiques affichées et exportées, encadrement des croisements (Option 2 : 2 à 3 dimensions guidées + consolidation sous 5 visites) et analyse d'anonymat selon l'Avis 05/2014 du G29

- **Exigence du référentiel CNIL :** L'interface comme les exports ne restituent que des statistiques anonymes (arrondies ou accompagnées d'une analyse d'anonymat démontrant le respect des trois critères de l'Avis 05/2014 du G29 : absence d'individualisation, de corrélation et d'inférence). Cet anonymat doit résister aux croisements de dimensions (Critère 4.2) et interdire toute reconstitution de parcours individuel (Critère 4.3).
- **Analyse d'anonymat (Avis 05/2014 du G29 / WP216 et Lignes directrices CEPD 01/2025) appliquée par Wysistat :**
    a. **Exclusion de toute individualisation (*Singling out* – Critère 4.3) :** Aucune fonctionnalité de l'interface web, des rapports planifiés, de l'API REST JSON ou du serveur MCP ne permet d'afficher ou d'exporter une liste d'événements individuels, une chronologie horodatée par visiteur ou un identifiant de visite. Les flux techniques bruts (pseudonymisés) ne sont conservés sur les serveurs d'IDfr que quelques heures pour consolider les visites et calculer les agrégats (et jusqu'à 3 mois maximum dans une base d'archive scellée et inaccessible aux clients, destinée uniquement aux audits officiels des contrôleurs de l'ACPM).
    b. **Prévention de la corrélation (*Linkability* – Critère 4.2) par croisements guidés (2 à 3 dimensions simultanées maximum) :** Pour éviter qu'une multiplication excessive de filtres simultanés ne fragmente les effectifs jusqu'à isoler un comportement singulier, Wysistat encadre structurellement les croisements dynamiques :
        - Toutes les dimensions disponibles sont préalablement généralisées à la collecte (famille de navigateur sans version, famille d'OS sans version, 3 catégories d'écran, localisation limitée au département, domaine référent tronqué, URLs et libellés nettoyés par Regex) ;
        - L'interface et l'API limitent les croisements guidés à **2 ou 3 dimensions simultanées au maximum** (par exemple : URL consultée × Canal/Domaine de provenance × Catégorie d'appareil).
    c. **Prévention de l'inférence (*Inference* et attaques par soustraction – Critères 4.1 et 4.2) par seuil de k-anonymat ($k = 5$) et regroupement consolidé :** Dans l'ensemble des tableaux simples ou croisés, des rapports de sources/campagnes et des exports (CSV, PDF, API REST, serveur MCP), **toute ligne ou combinaison de critères totalisant moins de cinq (5) visites sur la période analysée est masquée et additionnée au sein d'une ligne unique « Autres (lignes inférieures à 5 visites) »**. Afin de parer le risque statistique de déduction par soustraction (problème du « secret secondaire » où l'utilisateur soustrait les lignes visibles du total général lorsque la ligne « Autres » ne contient qu'une seule ligne masquée de 1 à 4 visites), si le groupe « Autres » totalise lui-même moins de 5 visites, il est automatiquement consolidé avec la dernière ligne valide du tableau (ou exclu du sous-total affiché). Ainsi, aucune différence entre un total et des sous-lignes ne peut jamais révéler un effectif inférieur à 5 visites.
- **Statut : Respecté.**

OBJECTIF 5 : Assurer l'information et le respect du droit d'opposition des personnes

Critères 5.1 et 5.2 : Information des utilisateurs et mécanisme d'opposition (Opt-out) effectif et persistant

- **Exigence du référentiel CNIL :** Les utilisateurs sont informés de la mesure d'audience dans la politique de confidentialité du site et disposent d'un mécanisme d'opposition simple, fonctionnel sur tous les navigateurs et terminaux, dont l'état de refus est mémorisé durablement.
- **Mise en œuvre chez Wysistat :** Wysistat met à la disposition de tous ses clients un paragraphe type d'information juridique ainsi qu'un module technique d'opposition (iframe / bouton d'opt-out hébergé sur https://www.wysistat.com/opt-out/verification.html ou script local). Conformément au critère 5.2 de la CNIL, lorsque l'internaute active son opposition, un témoin d'exclusion dédié (opt-out) est inscrit sur son navigateur afin de bloquer durablement toute collecte par le marqueur Wysistat. En outre, Wysistat respecte les signaux d'opposition standardisés envoyés par le navigateur.
- **Action requise par le Client :** Insérer le paragraphe d'information et le module d'opt-out Wysistat au sein de sa page « Politique de confidentialité » ou « Gestion des cookies ».
- **Statut : Respecté (sous condition d'intégration du module d'opt-out par le Client dans sa politique de confidentialité).**

Tous les renseignements technique pour la mise en œuvre sont fournis ici :
https://www.wysistat.net/wiki/analytics/exemption-cnil/