

Cookies, RGPD et consentement Ce qu'un site doit vraiment afficher

Un bandeau cookies ne suffit pas à rendre un site conforme. Le vrai sujet est de savoir quels traceurs sont déposés, lesquels nécessitent un consentement, comment respecter le refus, et comment conserver la preuve des choix. Pour une PME, l'objectif n'est pas de tout mesurer à tout prix, mais de collecter moins, collecter mieux, et disposer de données exploitables légalement.

Publié le 9 juillet 2026

Ce document reproduit le contenu publié à l'adresse indiquée en pied de page, dans sa version disponible à la date de sa génération. Il est fourni à titre exclusivement informatif et ne constitue ni un conseil juridique, réglementaire, fiscal ou professionnel, ni une garantie d'exhaustivité, d'exactitude ou d'actualité. Les textes officiels et la situation propre du lecteur doivent être vérifiés avant toute décision. Dans les limites permises par la loi applicable, Nasteo n'assume aucune responsabilité au titre des décisions prises ou des conséquences résultant de l'utilisation de ce document.

La conformité ne se limite pas à une bannière cookies

Sur un site web, les cookies et traceurs peuvent servir à faire fonctionner le site, mesurer l'audience, suivre les conversions publicitaires, personnaliser des contenus, intégrer des vidéos, afficher une carte, déclencher un chat ou alimenter des outils marketing.

Le point essentiel est simple : tous les cookies ne suivent pas les mêmes règles. Certains traceurs sont nécessaires au fonctionnement du service et peuvent être déposés sans consentement. D'autres, notamment les cookies publicitaires, les traceurs de réseaux sociaux ou certains outils de mesure, nécessitent une information claire et un consentement préalable.

La CNIL rappelle qu'en application de la directive ePrivacy, les internautes doivent être informés et donner leur consentement avant le dépôt ou la lecture de certains traceurs, tandis que d'autres sont dispensés du recueil de ce consentement. En droit français, ces règles sont notamment transposées à l'article 82 de la loi Informatique et Libertés.[1]

Pour une PME, la bonne question n'est donc pas seulement : avons-nous une bannière cookies ? La vraie question est : savons-nous quels traceurs sont réellement présents, à quoi ils servent, lesquels nécessitent un consentement, et comment nous pouvons prouver que le choix utilisateur est respecté ?

Le bon objectif n'est pas de tout mesurer à tout prix. Il est de collecter moins, collecter mieux, avec des choix respectés et des données exploitables légalement.

Une bannière cookies ne prouve pas la conformité

Beaucoup de sites affichent aujourd'hui une bannière cookies. Pourtant, cela ne signifie pas forcément que le site est conforme.

Une bannière peut être présente mais mal configurée. Elle peut proposer un bouton "Tout accepter" plus visible que le refus, déposer des traceurs avant le choix de l'utilisateur, oublier les scripts chargés via Google Tag Manager, ne pas permettre de revenir facilement sur son choix, ou présenter des catégories trop vagues.

Pour un dirigeant de PME, le sujet n'est pas de devenir spécialiste du RGPD. Le sujet est de comprendre ce qui doit être vérifié : quels traceurs sont présents, pourquoi ils sont là, qui les dépose, à quel moment, avec quelle information, avec quel consentement, et avec quelle preuve.

Cookie, traceur, pixel, script : de quoi parle-t-on ?

Le mot "cookie" est souvent utilisé pour désigner des réalités différentes. La CNIL précise que les termes "cookie" ou "traceur" recouvrent notamment les cookies HTTP, les pixels invisibles, les identifiants générés par un logiciel ou un système d'exploitation, ainsi que certaines techniques comme le fingerprinting.[1]

Terme | Exemple | Usage fréquent

Cookie technique Session, panier, authentification Faire fonctionner le site
Cookie de préférence Langue, affichage, choix utilisateur Personnaliser l'interface
Cookie de mesure d'audience Statistiques de consultation Analyser la fréquentation
Cookie publicitaire Retargeting, ciblage, conversion Mesurer ou personnaliser la publicité
Pixel Meta Pixel, LinkedIn Insight Tag Suivre une conversion ou une audience
Script tiers Chat, carte, vidéo, A/B testing Ajouter un service externe
Fingerprinting Empreinte du terminal Identifier ou suivre sans cookie classique
CMP Consent Management Platform Gérer les choix de consentement

Le risque est de croire que seuls les cookies visibles dans le navigateur comptent. En réalité, un site peut intégrer des traceurs via le thème, un plugin WordPress, Google Tag Manager, un formulaire, un outil de chat, une vidéo intégrée, un module de réservation, une carte interactive ou un outil publicitaire.

Tous les cookies ne nécessitent pas un consentement

La règle n'est pas : "tout cookie est interdit sans consentement". Certains traceurs sont nécessaires au fonctionnement du service.

La CNIL indique que le consentement préalable est requis pour les cookies qui ne sont pas strictement nécessaires à la fourniture d'un service demandé par l'utilisateur ou qui n'ont pas pour finalité exclusive de permettre ou faciliter une communication électronique. Elle cite notamment les cookies publicitaires et certains cookies de réseaux sociaux comme nécessitant une information et un consentement préalables.[1]

Type de traceur Consentement généralement requis ? Exemple
Authentification Non, si nécessaire au service Connexion compte client
Panier e-commerce Non, si nécessaire à l'achat Contenu du panier
Sécurité Non, si nécessaire Limitation des tentatives de connexion
Préférence d'interface Parfois non, si attendu par l'utilisateur Langue ou présentation
Mesure d'audience strictement limitée Parfois non, sous conditions Statistiques exemptées
Publicité personnalisée Oui Retargeting, profilage
Réseaux sociaux Oui dans la plupart des cas Boutons de partage traçants
Vidéo ou carte tierce avec traceurs Souvent oui YouTube, Google Maps selon configuration

Point de départ

Le premier livrable utile n'est pas une bannière. C'est un inventaire des traceurs réellement présents sur le site.

Ce qu'un site doit vraiment afficher

Un site ne doit pas seulement afficher une bannière. Il doit fournir une information claire et permettre un choix réel.

La CNIL précise que l'information doit être visible, mise en évidence, complète, rédigée en termes simples et compréhensibles, et permettre aux internautes d'être informés des finalités des cookies ainsi que de l'identité des responsables des traitements.[1]

Élément Rôle
Bandeau de premier niveau Informer rapidement et proposer un choix.
Bouton accepter Permettre l'acceptation explicite.
Bouton refuser Permettre le refus aussi simplement que l'acceptation.
Bouton personnaliser Permettre le choix par finalité.
Détail des finalités Expliquer statistiques, publicité, personnalisation, réseaux sociaux.
Liste des partenaires Identifier les tiers concernés lorsque nécessaire.
Lien de gestion des cookies Permettre de modifier ou retirer le consentement.
Politique cookies Documenter les traceurs, finalités, durées et tiers.
Politique de confidentialité Expliquer les traitements de données personnelles au-delà des cookies.
Preuve du consentement Conserver la configuration et les choix de manière démontrable.

La bannière n'est donc qu'un point d'entrée. La conformité dépend aussi de ce qui se passe derrière : blocage préalable, gestion des choix, preuve, documentation et maintenance.

Accepter et refuser : le même niveau de simplicité

La CNIL indique que l'utilisateur doit pouvoir accepter ou refuser le dépôt et la lecture des cookies avec le même degré de simplicité. Elle précise aussi que le consentement doit pouvoir être retiré simplement et à tout moment.[1]

Mauvaise pratique Pourquoi c'est problématique
Bouton "Tout accepter" visible, refus caché Choix déséquilibré.
Refus accessible seulement après plusieurs clics Refus plus complexe que l'acceptation.
Cases précochées Consentement non réellement actif.

Poursuite de navigation assimilée à un accord Consentement insuffisant.

Couleurs trompeuses Incitation artificielle à accepter.

Absence de bouton "Tout refuser" Choix incomplet.

Retrait du consentement introuvable Choix non réversible.

Point de vigilance

Quels traceurs bloquer avant consentement ?

Tant que l'utilisateur n'a pas donné son consentement, les cookies soumis au consentement ne peuvent pas être déposés ou lus sur son terminal. La CNIL le rappelle explicitement dans ses règles sur les cookies et traceurs.[1]

Traceur ou service Point de vigilance

Google Ads / remarketing Ne doit pas se déclencher sans consentement si finalité publicitaire.
--

Meta Pixel Traçage publicitaire à bloquer avant consentement.

LinkedIn Insight Tag Mesure publicitaire et audience B2B.

Google Analytics À analyser selon configuration et finalité.
--

Hotjar / Microsoft Clarity Analyse comportementale potentiellement intrusive.

Chat marketing Peut déposer des traceurs tiers.

YouTube / Google Maps Peuvent entraîner des appels tiers selon l'intégration.

Boutons sociaux Souvent liés à des traceurs tiers.
--

A/B testing marketing Peut nécessiter consentement selon finalité.
--

Le piège fréquent vient de Google Tag Manager : la bannière peut sembler fonctionner, mais des balises se déclenchent quand même avant le consentement. Il faut tester le site en conditions réelles, avec un navigateur propre, sans avoir déjà accepté les cookies.

Consentement obligatoire ou exemption possible ?

La mesure d'audience est l'un des sujets les plus mal compris. Certains outils de statistiques peuvent être exemptés de consentement s'ils respectent des conditions strictes. Cela ne signifie pas que tous les outils d'analytics sont exemptés.

Situation Lecture pratique

Statistiques internes limitées Exemption possible sous conditions.
--

Analytics avec finalité marketing Consentement souvent nécessaire.
Reciblage publicitaire Consentement requis.
Partage large avec des tiers Attention forte.
Données croisées avec publicité Consentement requis.
Outil configuré pour exemption À vérifier précisément, finalités et paramètres compris.
Google Analytics classique Prudence : consentement généralement nécessaire selon configuration.

Pour une PME, le bon réflexe est de ne pas supposer qu'un outil est exempté parce qu'il "fait seulement des statistiques". Il faut vérifier la finalité réelle, les données collectées, les tiers impliqués et la configuration.

Google Analytics, Consent Mode v2 et outils publicitaires

Beaucoup d'entreprises utilisent Google Analytics, Google Ads, Meta Pixel ou LinkedIn Ads. Ces outils peuvent être utiles, mais ils nécessitent une configuration rigoureuse.

Le Consent Mode de Google ne remplace pas le consentement. Il permet d'adapter le comportement des balises Google selon les choix exprimés par l'utilisateur. Depuis 2024, le Consent Mode v2 est devenu un point de configuration important pour les annonceurs qui utilisent les services publicitaires Google dans l'Espace économique européen.

Outil Point de vigilance
Google Consent Mode v2 Important depuis mars 2024 pour les annonceurs EEE utilisant Google Ads ; nécessite une CMP et des balises correctement configurées.
Google Analytics Finalité statistique ou marketing, configuration, consentement.
Google Ads Conversion, remarketing, Consent Mode, signaux transmis.
Meta Pixel Ciblage, conversion, audiences.
LinkedIn Insight Tag Suivi B2B, conversion, retargeting.
Tag Manager Déclenchement conditionné aux choix utilisateur.
CMP Bonne configuration des catégories, finalités et scripts.
Complianz / CookieYes / Axeptio / Didomi À configurer, pas seulement installer.

À retenir

Le risque est de confondre outil et conformité. Installer une CMP ne suffit pas. Il faut que les scripts soient réellement pilotés par le choix utilisateur.

Politique cookies, politique de confidentialité : ne pas confondre

Document Rôle
Politique cookies Expliquer les traceurs, finalités, durée, tiers et gestion du consentement.
Politique de confidentialité Expliquer plus largement les traitements de données personnelles.
Mentions légales Identifier l'éditeur, l'hébergeur et les responsables.
CGV / CGU Encadrer la relation contractuelle ou l'usage du service.

Un site peut avoir une politique de confidentialité correcte mais une gestion cookies insuffisante. La politique cookies doit être adaptée au site réel : traceurs utilisés, finalités, durées, tiers, moyens de retrait et coordonnées de contact.

Plugins et CMP : les erreurs fréquentes

Sur WordPress, les erreurs viennent souvent de l'empilement d'outils. La conformité dépend rarement d'un seul plugin. Elle dépend de la façon dont le thème, les extensions, les scripts tiers et la CMP sont configurés ensemble.

Erreur fréquente Conséquence
Installer une CMP sans scanner le site Traceurs oubliés.
Laisser les scripts dans le thème Scripts chargés malgré le refus.
Ajouter Tag Manager sans règles de consentement Balises déclenchées trop tôt.
Activer plusieurs plugins cookies Conflits et choix incohérents.
Oublier les iframes YouTube ou Maps Traceurs tiers non maîtrisés.
Oublier les pixels publicitaires Collecte avant consentement.
Ne pas tester en navigation privée Résultat faussé.
Copier un texte générique Information non adaptée au site.
Ne pas prévoir de lien "Gérer mes cookies" Retrait difficile.

Ce qu'il faut prouver

La CNIL indique que chaque acteur se prévalant du consentement doit être en mesure d'en apporter la preuve. Elle cite notamment la conservation d'éléments horodatés, des captures d'écran du rendu affiché, des audits réguliers ou les informations relatives aux outils de recueil du consentement et à leurs configurations successives.[1]

Preuve Exemple
Version de la bannière Capture écran desktop et mobile.
Configuration CMP Catégories, finalités, scripts associés.
Historique des changements Date de modification des réglages.
Politique cookies Version publiée et date de mise à jour.
Liste des traceurs Scan ou inventaire périodique.
Tests avant consentement Preuve que les scripts soumis au consentement sont bloqués.
Tests après refus Preuve que le refus est respecté.
Tests après acceptation Preuve que seuls les scripts autorisés partent.
Registre ou fiche interne Responsable, outil, finalité, base légale.
Contrats sous-traitants CMP, analytics, emailing, hébergement.

Durées à maîtriser

La durée de conservation du choix utilisateur doit être documentée. En pratique, une durée de l'ordre de 6 mois pour conserver le choix de consentement ou de refus est couramment retenue comme bonne pratique. Pour certains traceurs de mesure d'audience exemptés, la durée de vie du traceur doit rester limitée, avec une référence pratique de 13 mois maximum lorsque les conditions d'exemption sont respectées.

Consentement et conversion : éviter les faux arbitrages

Certaines entreprises craignent qu'une bannière conforme réduise les données analytics ou publicitaires. C'est possible. Mais une bannière agressive ou trompeuse crée un autre risque : perte de confiance, non-conformité, mauvaise expérience utilisateur.

Mauvaise approche Meilleure approche
Forcer l'acceptation Expliquer clairement les finalités.
Cacher le refus Proposer un vrai choix.
Charger tous les scripts Déclencher selon consentement.
Mesurer sans contrôle Distinguer analytics exemptés et marketing.

Accumuler les pixels | Auditer les outils réellement utiles.

Copier une bannière générique | Configurer selon le site réel.

Pour un dirigeant, c'est aussi un sujet de qualité de pilotage. Des données collectées dans de mauvaises conditions peuvent être difficiles à exploiter sereinement.

Les sanctions et contrôles : un risque réel, à proportionner

Les cookies restent un sujet de contrôle important pour la CNIL. En 2025, des sanctions élevées ont été prononcées contre de grands acteurs pour des manquements liés aux cookies, à l'information et au consentement, notamment Google et Shein selon la presse économique et généraliste.[6]

Pour une PME, l'enjeu n'est pas de comparer son risque à celui d'un géant du numérique. L'enjeu est de comprendre que les traceurs sont un sujet contrôlé, documenté et sanctionnable. Les manquements peuvent entraîner des demandes de mise en conformité, des contrôles, des mises en demeure ou des sanctions selon le contexte.

À retenir

Méthode simple pour auditer son site

1. Lister les outils installésWordPress, thème, plugins, CMP, Tag Manager, Analytics, pixels, chat, formulaires, cartes, vidéos, newsletter, CRM.
2. Scanner les traceursUtiliser la CMP, les outils navigateur, un scanner cookies ou un audit manuel pour repérer les cookies et scripts réellement présents.
3. Classer par finalitéTechnique, préférences, audience, publicité, réseaux sociaux, personnalisation, sécurité, formulaire, paiement.
4. Identifier les traceurs soumis au consentementPublicité, retargeting, réseaux sociaux, analytics non exemptés, mesure comportementale, A/B testing marketing.
5. Vérifier le blocage avant consentementTester en navigation privée, vider les cookies, refuser, accepter, personnaliser, puis observer les scripts déclenchés.
6. Corriger la bannièreBoutons équilibrés, langage clair, refus aussi simple que l'acceptation, personnalisation, retrait accessible.
7. Mettre à jour les documentsPolitique cookies, politique de confidentialité, mentions de tiers, durées, finalités, lien de gestion.
8. Documenter la preuveCaptures, configuration CMP, liste des traceurs, date de test, responsable, résultats.
9. Refaire le contrôle après chaque évolutionNouveau plugin, campagne Ads, pixel, formulaire, vidéo, module de réservation ou changement Tag Manager.

Les pièges à éviter

- ?Penser qu'une bannière suffitLa conformité reste seulement apparente si les scripts partent avant le choix.
- ?Copier le texte d'un autre siteL'information devient inexacte et non adaptée aux traceurs réels.
- ?Oublier Google Tag ManagerLes balises peuvent se déclencher hors contrôle.
- ?Ne pas proposer "Tout refuser"Le choix peut devenir déséquilibré.
- ?Déposer des pixels avant choixLa collecte peut intervenir sans consentement valable.
- ?Oublier le retrait du consentementLe choix n'est pas réellement réversible.
- ?Ne pas documenter les preuvesLa conformité devient difficile à démontrer.
- ?Ne jamais refaire d'auditUn site conforme hier peut ne plus l'être demain.

Checklist dirigeant : que vérifier maintenant ?

Visuel de contenu à créer : [image-cookies-rgpd-consentement-site-web-checklist.webp](#)

Question Si la réponse est floue
Savons-nous quels cookies et traceurs sont présents ? Impossible de vérifier la conformité.
Les traceurs sont-ils classés par finalité ? Information utilisateur imprécise.
Les scripts publicitaires sont-ils bloqués avant consentement ? Risque de dépôt non autorisé.
Le refus est-il aussi simple que l'acceptation ? Consentement contestable.
L'utilisateur peut-il modifier son choix à tout moment ? Retrait du consentement insuffisant.
Google Tag Manager respecte-t-il les choix ? Balises déclenchées trop tôt.
Les outils analytics sont-ils exemptés ou soumis au consentement ? Configuration incertaine.
Consent Mode v2 est-il correctement configuré si Google Ads est utilisé ? Mesure et ciblage publicitaire dégradés ou mal pilotés.
La politique cookies est-elle à jour ? Information incorrecte.
Une preuve des choix et réglages est-elle conservée ? Conformité difficile à démontrer.
La durée de conservation du choix est-elle documentée ? Gestion du consentement insuffisamment maîtrisée.
Un contrôle est-il prévu après ajout d'un plugin ou pixel ? Dérive dans le temps.

Ce que les lecteurs demandent souvent

Un bandeau cookies suffit-il à rendre un site conforme ?

Faut-il toujours un bouton “Tout refuser” ?

Tous les cookies nécessitent-ils un consentement ?

Google Analytics peut-il être utilisé sans consentement ?

Consent Mode v2 rend-il automatiquement le site conforme ?

Combien de temps conserver le choix de consentement ?

Faut-il une politique cookies séparée ?

Les cookies WooCommerce nécessitent-ils un consentement ?

Conclusion, Le vrai sujet n'est pas la bannière, c'est la maîtrise des traceurs

Un site conforme n'est pas un site qui affiche simplement une fenêtre cookies. C'est un site qui sait quels traceurs il utilise, pourquoi il les utilise, lesquels nécessitent un consentement, comment le choix est recueilli, comment il est respecté, comment il peut être retiré et comment la preuve est conservée.

Pour une PME, la démarche peut rester pragmatique : inventorier, classer, bloquer, informer, tester, documenter et maintenir.

La bonne question finale n'est donc pas : “avons-nous une bannière cookies ?” Mais plutôt : “savons-nous vraiment ce que notre site dépose sur le terminal de nos visiteurs, et pouvons-nous prouver que leurs choix sont respectés ?”

Sources

- CNIL, Cookies et traceurs : que dit la loi ? : article 82, consentement préalable, traceurs exemptés, preuve du consentement.
- CNIL, Cookies et traceurs : comment mettre mon site web en conformité ? : recommandations pratiques pour les sites web.
- CNIL, Cookies : solutions pour les outils de mesure d'audience : conditions d'exemption et outils de mesure.
- Directive ePrivacy 2002/58/CE, modifiée notamment par la directive 2009/136/CE, à l'origine du principe de consentement préalable pour les traceurs non nécessaires.
- RGPD, articles 4(11) et 7 : définition et conditions du consentement.

- Reuters, France fines Shein over cookies, 2025 et presse généraliste sur les sanctions cookies Google / Shein.