Février 2026

Consentement au tracking des ouvertures email

Ce que la CNIL impose — et ce que ça change pour vous

bad sender

Agitateur d'expertise emailing et CRM

Disclaimer !

Avant de commencer, un point important

Ce que vous allez entendre aujourd'hui -
Les éléments présentés dans cette session sont le fruit d'une veille active et approfondie sur le sujet : lectures de la documentation CNIL, participation aux discussions de l'écosystème email, échanges avec des experts ayant participé aux ateliers avec la CNIL.

Ce que cette session n'est pas - Badsender est un cabinet de conseil en emailing et délivrabilité, pas un cabinet juridique. Les recommandations partagées ici sont des conseils opérationnels, fondés sur notre lecture du dossier et sur les meilleures pratiques de l'industrie.
Ils ne se substituent pas à un avis juridique. Pour toute décision engageant la responsabilité de votre organisation, consultez votre DPO et/ou un cabinet spécialisé en droit des données personnelles.

La CNIL

réagit à des plaintes de personnes qui se sentent espionnées

Un email s'ouvre, une requête part vers un serveur, la marque sait qui, quand, sur quel appareil

La messagerie est un espace privé, la CNIL l'assimile à un terminal personnel

Résultat : les règles qui s'appliquent aux cookies s'appliquent aussi aux pixels d'email

Le pixel d'ouverture :

une image invisible, des données bien réelles

1/INTEGRATION

Une image 1×1 pixel est insérée dans l'email, hébergée sur un serveur distant

2/OUVERTURE

Le client mail charge l'image → envoie une requête au serveur

3/COLLECTE

Le serveur enregistre : qui a ouvert, quand, depuis quel appareil, depuis quelle IP

Ce n'est **pas un cookie**. Pas de bandeau de consentement web. Mais le **même cadre légal** s'applique.

La loi est déjà claire, la CNIL clarifie, elle ne crée pas

La règle de base

LA BASE LÉGALE

- ☑ Article 82 de la **loi Informatique & Libertés**
- ☑ Transposition de la **directive ePrivacy**
- ☑ Tout **traceur** qui lit/écrit sur le terminal d'un utilisateur → consentement obligatoire
- ☑ Sauf exception (technique, sécurité, mesure d'audience agrégée)

CONCRÈTEMENT

- ☑ Identifier nominativement qui ouvre vos emails = tracking individuel
- ☑ Tracking individuel = données personnelles
- ☑ Données personnelles sans consentement = non-conforme depuis mai 2018

Délai pour se mettre en conformité : 0 jour en théorie. En pratique, la CNIL commencera par des rappels à l'ordre avant de sanctionner.

Deux mondes distincts :

Ce qui est libre, ce qui est soumis à consentement

SANS CONSENTEMENT

- Mesurer les taux d'ouverture globaux (non nominatifs)
- Réaliser des A/B tests sur la performance d'ouverture d'une audience
- Tracker pour des raisons de sécurité (ex : lien de réinitialisation de mot de passe)
- Emails transactionnels à intérêt légitime (confirmation commande, facture, alerte sécurité)
- Monitoring délivrabilité par domaine (Orange, Gmail...) — position en cours d'évolution

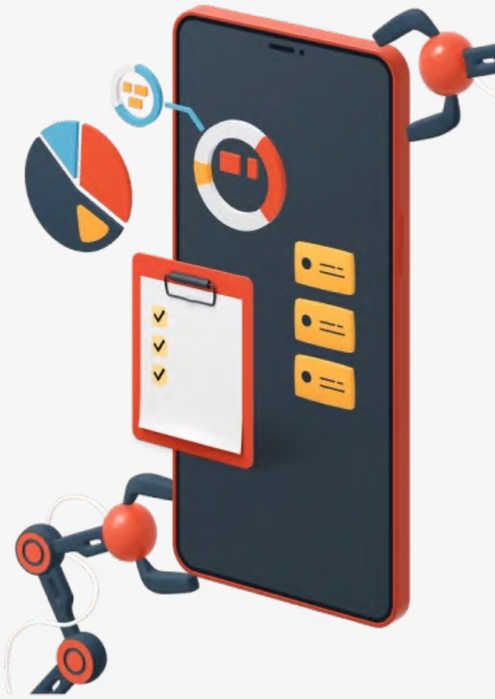
CONSENTEMENT REQUIS

- Identifier individuellement qui ouvre vos emails
- Cibler ou exclure des contacts en fonction de leurs comportements d'ouverture
- Adapter la fréquence d'envoi selon les ouvertures individuelles
- Personnaliser le contenu selon les interactions d'ouverture de chaque contact
- Rédiger "nous avons remarqué que vous ne lisez plus nos newsletters"

Nous attendons encore la version finale de la recommandation, mais les principes de base sont posés.

Les inactifs:

La vraie zone grise du dossier



LE PROBLÈME :

La définition courante d'un inactif = "*contact n'ayant pas ouvert (ou cliqué) depuis 6 mois*". **Sans consentement au tracking individuel, cette définition devient illégale.**

Ce que demandent les acteurs de la délivrabilité à la CNIL :

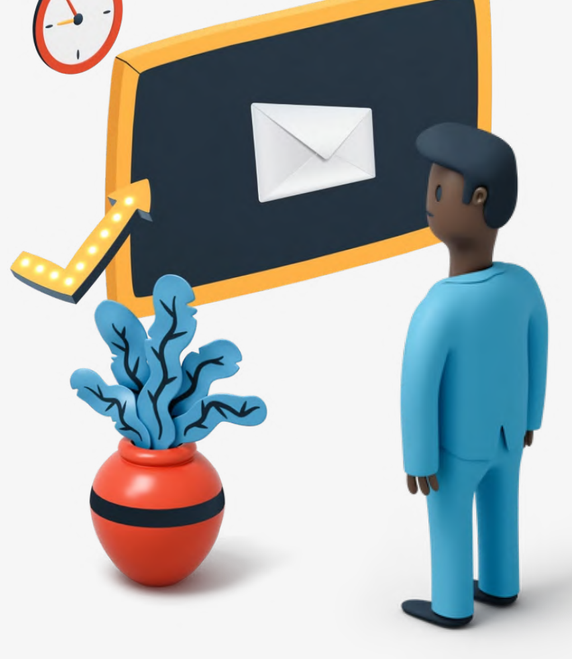
- ☑ Pouvoir conserver au minimum l'identifiant de campagne + le domaine du destinataire → mesure de performance non nominative
- ☑ Idéalement, conserver uniquement la date de dernière ouverture (ou clic) par individu, dans le seul but de cesser les envois si inactivité prolongée

Où en est-on ? La CNIL semble ouverte à une exemption pour la gestion des inactifs — mais ce point n'est pas encore tranché dans la recommandation finale. Limite identifiée : sur des bases petites, la date de dernière ouverture par individu peut suffire à réidentifier une personne.

Ce que vous devez faire dès maintenant : Commencer à réfléchir à des définitions d'inactivité alternatives : dernière visite web, dernier clic, dernier achat, dernier contact entrant.

Délivrabilité:

Ce qui change, ce qui reste possible



Ce qui reste possible sans consentement : Mesurer les taux d'ouverture par domaine (Orange, Gmail, Outlook…) pour le monitoring délivrabilité — à condition que les données soient anonymisées au niveau campagne + domaine, sans identification individuelle

CE QUI CHANGE

- Exclusion des inactifs basée sur l'ouverture individuelle (cf. slide précédente)
- Scénarios de réengagement sur non-ouvreurs
- Tout reporting individuel croisé avec comportement d'ouverture

CE QU'IL FAUT FAIRE ÉVOLUER

- Inactivité définie par le clic (plus fiable de toute façon, moins faussé par Apple MPP)
- Engagement multicanal : web, achat, contact entrant
- Scores d'engagement basés sur des signaux déclaratifs ou comportementaux non-tracking

Digital Omnibus:

Ce que l'Europe prépare, et pourquoi ça compte

Qu'est-ce que le Digital Omnibus ?

En novembre 2025, les États membres de l'UE ont publié leur premier retour du projet Digital Omnibus de la Commission Européenne, une réforme de la directive ePrivacy (DORP) qui pourrait modifier les règles du consentement.

CE QUI POURRAIT CHANGER

- ☐ Le consentement (opt-in) reste le standard pour le tracking individuel, pas de remise en question sur ce point
- ☑ Une exemption de consentement pourrait être accordée pour les mesures d'audience à faible risque, à usage interne unique et non croisées avec d'autres données

CE QUI NE CHANGE PAS

- ☐ Le tracking des ouvertures lié au profilage ou à la segmentation comportementale reste soumis à consentement
- ☐ Ce projet est européen, la CNIL française doit suivre, mais reste en avance sur le calendrier

Où en est-on ?

Le calendrier honnête

- ☑ Mai 2018 — **Entrée en vigueur du RGPD** → obligation légale déjà existante
- ☑ Juin 2025 — La CNIL publie son **projet de recommandation** + consultation publique
- ☑ Juillet 2025 — **Clôture de la consultation publique**
- ☑ Septembre 2025 — **Dernière concertation** avec les acteurs de l'écosystème email
- ☑ Novembre 2025 — Publication du retour des États membres sur le **Digital Omnibus**
- ☑ Décembre 2025 — La CNIL publie ses recommandations **cookies multi-terminaux** (traceurs web)
- ☐ Début 2026 — **Recommandation finale pixels email** attendue *(pas encore publiée à ce jour)*
- ☐ Aujourd'hui — Conformité exigée, recommandation finale en attente, sanctions pas encore déclenchées sur ce sujet spécifique

La CNIL commencera probablement par des rappels à l'ordre.
Mais "probablement" n'est pas une stratégie de conformité.

Plan d'action (1/2)

Collecter le consentement en amont

1. **Auditer vos formulaires de collecte actuels** → Avez-vous une case à cocher spécifique pour le tracking des ouvertures ? Non pré-cochée ?

2. **Rédiger une case à cocher intelligible** - Mauvais exemple : *"Acceptez-vous que nous trackions vos ouvertures ?"* Bon exemple : *"J'accepte que [Société] utilise des pixels de suivi pour me proposer des contenus adaptés à mes intérêts et réduire le nombre d'emails non pertinents que je reçois."*

3. **Mettre à jour votre politique de confidentialité** → Mentionner explicitement l'usage des pixels de suivi dans les emails, les finalités, la durée de conservation

4. **Lancer une campagne de recueil de consentement sur votre base existante** → Envoyer un email dédié sans tracking pour recueillir l'accord des abonnés existants → Un bloc de recueil pourrait aussi être intégré de manière permanente dans vos communications

Plan d'action (2/2)

Adapter vos outils et vos process

5. **Intégrer un lien de retrait du consentement tracking dans vos emails** → À côté du lien de désabonnement dans le footer → Mettre à jour le centre de préférences si vous en avez un

6. **Interroger votre routeur sur ses capacités de conformité** Questions à poser :

- Peut-il désactiver le tracking pour les contacts sans consentement ?
- Propose-t-il un pixel d'audience anonymisé en remplacement ?
- Peut-il intégrer automatiquement un pixel identifiant vs. pixel d'audience selon le consentement au moment de l'envoi ? → Les routeurs sont co-responsables de traitement. S'ils ne sont pas conformes, vous pouvez vous retourner contre eux.

7. **Alerter votre DPO et documenter** → Cartographier les traitements impactés (ouvertures, clics, scénarios d'automation) → Mettre en place la conservation de la preuve de consentement → Revoir les mentions dans vos registres de traitement

8. **Repenser vos définitions d'inactifs et vos scénarios d'automation** → Basculer sur des signaux clic, visite web, achat pour définir l'engagement

Et dans votre outil ?

Ce qui est déjà en place

Le principe global - Généralement, les outils d’envoi d’emails disposent d'un attribut natif trackingConsent sur la fiche profil. Quand un profil a un consentement négatif, aucune interaction de tracking n'est enregistrée ni stockée (ni l'ouverture, ni le clic email, ni le clic SMS, ni les goals de visite ou de transaction).

Ce qui est couvert techniquement :

- ☑ Ouverture email non enregistrée pour les profils sans consentement
- ☑ Clics email et SMS non enregistrés
- ☑ Appareil et user-agent non stockés
- ☑ Goals transactionnels non rattachés à la campagne
- ☑ Le consentement est visible dans la fiche profil, onglet "Interactions"

Impact sur le reporting et les scénarios : Un profil sans consentement est traité comme un "non-ouvreur permanent" dans tous les ciblages et scénarios. Un bloc d'attente "ouverture" le renverra toujours vers la branche de sortie.

Les limites identifiées

Ce qu’il faut creuser…

⚠️ **Le pixel reste en place même sans consentement**

⚠️ **Pas de pixel d'audience anonymisé en remplacement** - *Est-ce que l’outil propose un pixel d'audience non-nominatif pour les profils sans consentement ? Ce qui permettrait de conserver des stats globales de campagne même sur les contacts non-consentants.*

⚠️ **Les données historiques ne sont pas supprimées au retrait du consentement** - *Est-ce que le retrait du consentement a pour effet de supprimer les informations d'ouverture et clics récoltées auparavant ?*

⚠️ **Le “TrackingConsent” est global et ne concerne pas uniquement les ouvertures** - Ce qui veut dire qu’en utilisant cet attribut dans la fiche de profil d’un contact, on perdra aussi les statistiques de clic, de goals de visite… qui sont potentiellement des consentements distincts.

Prochaines actions

Dès la semaine prochaine ?

🔍 **Semaine prochaine** - Auditer vos formulaires et votre politique de confidentialité, avez-vous déjà une case tracking ? Une mention dans votre Privacy Policy ?

📞 **Dans les 30 jours** - Contacter votre routeur pour connaître ses fonctionnalités de gestion du consentement au tracking

📋 **Dans les 60 jours** - Briefer votre DPO, documenter les traitements impactés, et définir une rédaction pour la case à cocher tracking

Ressource : article complet sur badsender.com — "CNIL et consentement au tracking des ouvertures email : ce qui change pour vos campagnes"
→ https://www.badsender.com/2025/07/02/legislation-taux-ouverture-emailing/

Nous Contacter

Par **email** : yesreply@badsender.com
Par **téléphone** : +33 1 76 38 00 26

Toute l'information sur nos offres de **conseil**, de **déploiement** et de **production** sont disponibles sur badsender.com/agence

bad sender

Agitateur d'expertise emailing et eCRM