DATA RING

LIVRE BLANC

Pixels de suivi dans les courriels

Comprendre la délibération CNIL n° 2026-042 et anticiper la mise en conformité avant le 14 juillet 2026

À l'attention des directions juridiques, marketing et informatiques

Mai 2026

Sommaire

1. Synthèse exécutive

Texte	Délibération CNIL n° 2026-042 du 12 mars 2026[1]
Publication	Journal officiel — 14 avril 2026
Fondement	Article 82 de la loi Informatique et Libertés ; directive ePrivacy ; lignes directrices CEPD 2/2023
Champ	Pixels invisibles insérés dans les courriers électroniques
Échéance	14 juillet 2026 – début des contrôles annoncés
Sanction maximale	Jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial (article 20 loi informatique et libertés)

La Commission nationale de l'informatique et des libertés (CNIL) a clarifié, par une délibération du 12 mars 2026 publiée le 14 avril 2026, le régime juridique applicable aux pixels de suivi insérés dans les courriers électroniques. Cette intervention met fin à une incertitude qui durait depuis plusieurs années, à un moment où les plaintes adressées à l'autorité se multipliaient.

Le principe est désormais établi : l'insertion d'un pixel de suivi dans un courriel constitue une opération de lecture d'informations dans le terminal de l'utilisateur au sens de l'article 82 de la loi Informatique et Libertés. Elle est, par principe, soumise au consentement préalable du destinataire, sauf à relever de l'une des deux exemptions strictement encadrées par la recommandation. La portée pratique de cette recommandation est considérable. La grande majorité des dispositifs d'emailing actuellement déployés ne prévoient aucune demande de consentement spécifique pour ces technologies. La quasi-totalité des acteurs du marché doivent donc procéder à une mise en conformité — et ce, dans un calendrier resserré : la CNIL a prévu une période de transition courte de trois mois, expirant le 14 juillet 2026, à l'issue de laquelle les contrôles seront engagés.

> **Point d'attention immédiat**
>
> *La CNIL a précisé que le régime du consentement applicable aux pixels est indépendant de celui applicable à l'envoi du courriel lui-même. Concrètement, un pixel inséré dans un courriel B2B de prospection ou dans un courriel transactionnel, et pour lequel l'opt-out reste la règle, peut requérir un consentement spécifique dès lors que l'adresse est nominative. C'est un changement structurant pour les pratiques de marketing B2B.*

2. Contexte : pourquoi la CNIL est-elle intervenue ?

[1] Recommandation de la CNIL sur les pixels de suivi.

Un pixel de suivi (également appelé « pixel espion » ou « pixel de tracking ») est une image de très petite taille, généralement réduite à un seul pixel et le plus souvent transparente, hébergée sur un serveur distant et insérée dans le corps d'un courrier électronique. Au moment où le destinataire ouvre le message, son pixel de messagerie effectue une requête vers le serveur hébergeant l'image afin de la télécharger et de l'afficher. Ce processus, invisible pour l'utilisateur, permet à l'expéditeur de collecter une série d'informations : identifiant unique du destinataire, date et heure d'ouverture, adresse IP, type de terminal et, fréquemment, données de localisation.

L'usage de ces pixels est très largement répandu dans les communications classiques pour des finalités variées : mesure de la délivrabilité (ouverture, horaire et parfois support utilisé), mesure d'audience, personnalisation des contenus, détection de fraude. Leur utilisation dans les communications électroniques est très répandue. La CNIL indique dans sa recommandation qu'elle constate une hausse du nombre de signalement et de plaintes de la part des personnes concernées vis-à-vis du traçage opéré au sein d'une messagerie électronique.

La position retenue par la CNIL s'inscrit dans la continuité directe des lignes directrices 2/2023 du Comité européen de la protection des données (CEPD), adoptées le 7 octobre 2024, qui ont précisé le champ d'application technique de l'article 5, paragraphe 3, de la directive « vie privée et communications électroniques ». Elle prolonge également la recommandation cookies de septembre 2020, dont elle reprend la logique tout en l'adaptant aux spécificités de l'environnement courriel.

3. Ce que dit la délibération de la CNIL

3.1. Une qualification juridique structurante

La CNIL considère que l'utilisation de pixels de suivi dans un courriel engendre des opérations de lecture d'informations stockées dans le terminal de l'utilisateur, au sens de l'article 82 de la loi Informatique et Libertés. Ces dispositifs relèvent dès lors pleinement du régime applicable aux « cookies et autres traceurs ».

3.2. Le périmètre couvert

La recommandation s'applique à l'ensemble des pixels insérés dans des courriers électroniques, indépendamment du contexte d'envoi (B2C, B2B, communications associatives ou institutionnelles).

4. Qualification des acteurs : qui est responsable ?

La répartition des responsabilités constitue l'un des apports importants de la recommandation. La CNIL identifie trois figures.

4.1. L'expéditeur : Responsable de traitement

L'expéditeur du courriel — entendu comme l'acteur ayant décidé de l'envoi, qu'il en soit ou non l'émetteur technique — est qualifié de responsable du traitement dès lors qu'il détermine les finalités et les moyens liés à l'utilisation des pixels. Cette qualification s'impose y compris en cas de recours à un prestataire technique d'emailing. C'est donc l'entreprise cliente qui assume, en première ligne, l'obligation de recueillir et de documenter le consentement.

4.2. Le prestataire d'emailing : Sous-traitant en principe

Le prestataire technique (plateforme d'envoi, fournisseur de pixels) agit en principe en qualité de sous-traitant au sens de l'article 28 du RGPD, dès lors qu'il met en œuvre les pixels selon les instructions de l'expéditeur et pour son compte. Il appartient à l'expéditeur de s'assurer que les contrats de sous-traitance encadrent strictement les opérations confiées.

4.3. La situation de coresponsabilité

La CNIL identifie expressément des situations dans lesquelles un prestataire peut basculer en coresponsabilité avec l'expéditeur : tel est notamment le cas lorsqu'il exploite les données collectées pour ses propres finalités (par exemple à des fins d'amélioration de ses services, d'entraînement de modèles ou de constitution de bases statistiques). Cette situation impose alors une répartition formelle des obligations sous la forme d'un accord de coresponsabilité conformément à l'article 26 du RGPD.

> **Vigilance contractuelle**
>
> *Les contrats actuellement en vigueur avec les prestataires d'emailing ont, dans leur grande majorité, été rédigés sous le seul prisme de la sous-traitance. Une revue contractuelle est nécessaire pour identifier les éventuelles situations de coresponsabilité et, le cas échéant, conclure un accord conforme à l'article 26 du RGPD.*

5. Consentement vs exemption : la ligne de partage

La recommandation distingue clairement les finalités soumises au consentement préalable de celles qui bénéficient d'une exemption.

Consentement requis :

01 L'analyse du taux d'ouverture des courriels pour mesurer et optimiser les performances des campagnes en personnalisant le contenu des messages ou en adaptant la fréquence d'envoi ou le canal de communication (courriel, SMS, notification push, etc). Cette finalité inclut les procédés de fiabilisation de cette mesure (exemple : lutte contre la fraude publicitaire)

02 La création de profils des destinataires au regard des préférences et centres d'intérêt manifestés afin de les cibler dans d'autres contextes que les courriels (sur des sites web, des applications mobiles ou via d'autres canaux de communication).

03 La détection et l'analyse de suspicions de fraude, telles que l'identification d'ouvertures inhabituelles ou massives de courriels, susceptibles d'indiquer un comportement automatisé (par exemple, inscriptions massives à un jeu concours, tentatives d'exfiltration d'informations, etc.).

04 La mesure individuelle du taux d'ouverture des courriels à des fins de délivrabilité lorsqu'elle n'est pas réalisée pour des finalités exemptées du recueil du consentement.

Exemptions (encadrees) :

01 **L'exemption « Sécurité »**

La mise en œuvre de mesures de sécurité participant à l'authentification de l'utilisateur.

02 **L'exemption « Délivrabilité »**

La mesure individuelle du taux d'ouverture des courriels à des fins de délivrabilité.

Évaluer et adapter le canal de communication pour, le cas échéant, choisir des modalités alternatives de contact.

Contribuer à la démonstration du respect d'une obligation légale relative à la transmission d'informations au destinataire en conservant la trace de l'ouverture du courriel (exemple : la délivrance des informations requises par des dispositions légales et règlementaires en amont, pendant ou en aval de la contractualisation, etc).

Dans ce cadre, l'usage de pixel de suivi poursuit l'unique finalité de participer à la sécurisation d'une authentification (en s'assurant, par exemple, que le courriel contenant un code utilisé dans le cadre

du processus d'authentification est bien ouvert sur un terminal connu pour appartenir à l'utilisateur visé).

5.2. L'exemption « délivrabilité »

La gestion d'une liste de diffusion requiert presque systématiquement l'utilisation de statistiques d'ouverture des courriels afin d'identifier d'éventuelles problématiques de délivrabilité. Pour que les pixels puissent être exemptés au titre de cette finalité, le responsable du traitement devra démontrer que les opérations effectuées ont vocation à se limiter à ce qui est strictement nécessaire (principe de minimisation) pour adapter la fréquence ou arrêter l'envoi des courriels aux destinataires dits « inactifs » (nettoyage des bases) et les données collectées ne doivent servir à aucune autre fin.

> **Piège fréquent**
>
> *Beaucoup de praticiens considéraient que les courriels transactionnels échappaient à l'ensemble des contraintes pesant sur l'email marketing. La CNIL retient une lecture plus rigoureuse : un courriel transactionnel peut être adressé sans consentement, mais le pixel qu'il contient relève d'un régime indépendant. Si ce pixel sert à autre chose qu'à une finalité strictement nécessaire (par exemple à du scoring comportemental ou à de la personnalisation marketing), le consentement redevient exigible.*

6. Modalités pratiques de recueil et de retrait du consentement

6.1. Le moment du recueil

La CNIL recommande de recueillir le consentement au moment de la collecte de l'adresse électronique, par exemple lors de l'inscription à une lettre d'information ou de la création d'un compte. À défaut, le consentement peut être recueilli ultérieurement par un courriel dédié, sans pixel de suivi, renvoyant vers une page d'action explicite. Cette seconde option s'impose notamment lorsque l'adresse n'a pas été collectée directement (listes acquises auprès de tiers).

6.2. La granularité

Chaque finalité distincte appelle, en principe, un opt-in spécifique. La CNIL admet deux assouplissements. D'une part, lorsque les finalités sont « connexes », un consentement unique peut suffire : ainsi, le consentement à une prospection personnalisée peut couvrir les pixels qui y concourent directement. D'autre part, une interface à deux niveaux est admise : un consentement global au premier niveau, à condition que les finalités y soient clairement exposées et que le second niveau permette à l'utilisateur d'exprimer des choix finalité par finalité.

6.3. L'information préalable

L'information délivrée doit être conforme aux articles 12, 13 et 14 du RGPD et présentée dans un langage clair et adapté, avant l'activation des pixels. La CNIL propose un format en deux niveaux : un intitulé court mis en évidence, accompagné d'un bref descriptif, complété par un lien vers une information plus détaillée (notamment via la politique de confidentialité). Le destinataire doit pouvoir identifier l'adresse concernée et comprendre que les pixels seront déployés sur l'ensemble des terminaux qu'il utilise pour consulter ses courriels.

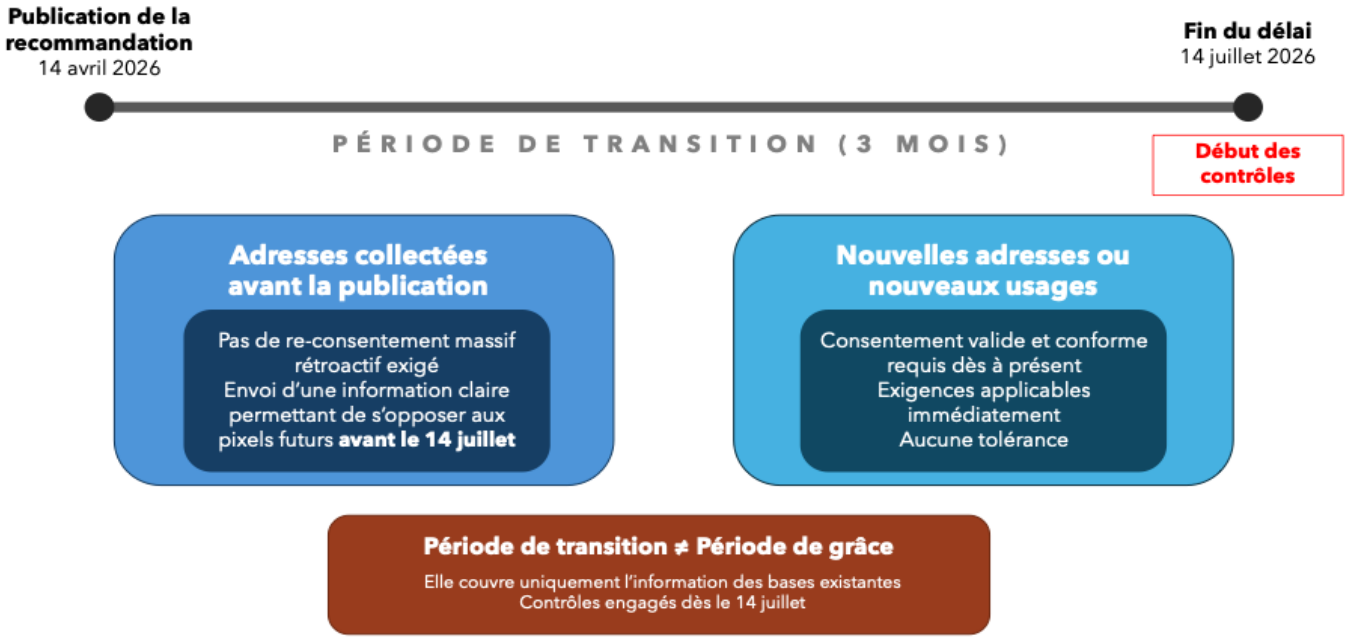
6.4. Le retrait

Le retrait du consentement doit être aussi simple que son recueil. La CNIL recommande l'insertion d'un lien dédié dans chaque courriel, distinct du lien de désinscription, avec effet immédiat sur les envois futurs. Le responsable du traitement doit en outre mettre en place les mesures techniques nécessaires pour garantir que les pixels des courriels déjà envoyés ne soient plus exploités si le destinataire les ouvre à nouveau après avoir retiré son consentement.

6.5. La preuve

Le responsable du traitement doit pouvoir démontrer à tout moment que le consentement a été valablement recueilli — son contenu, sa date et le canal employé. Cette obligation, classique en matière de consentement RGPD, prend ici une importance particulière compte tenu de la promesse de contrôles annoncée par la CNIL.

7. Régime transitoire : l'échéance du 14 juillet 2026



8. Risques juridiques et contentieux à anticiper

8.1. Risque administratif

L'article 83 du RGPD, combiné aux articles 20 et suivants de la loi Informatique et Libertés, autorise la CNIL à prononcer des amendes administratives pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial. Pour les manquements à l'article 82 de ladite loi spécifiquement, le plafond se situe à 2 % du chiffre d'affaires annuel mondial. La sanction de 150 millions d'euros prononcée en septembre 2025 contre la filiale irlandaise de Shein pour non-respect des règles cookies illustre la fermeté que la CNIL est susceptible d'adopter en matière de traçage.[2]

8.2. Risque contentieux civil

Les actions individuelles fondées sur l'article 82 de la loi Informatique et Libertés ou sur l'article 9 du Code civil (atteinte à la vie privée) sont susceptibles d'être engagées par les destinataires. Les actions de groupe en matière de protection des données (article 16 de la loi n° 2025-391 du 30 avril 2025 portant diverses dispositions d'adaptation au droit de l'Union européenne) constituent également un vecteur contentieux à anticiper, particulièrement dans les secteurs B2C à forte volumétrie.

8.3. Risque réputationnel et commercial

Les contrôles de la CNIL et leurs sanctions font l'objet d'une publicité importante. Au-delà de la sanction pécuniaire, la communication sur les manquements expose les organismes à un préjudice réputationnel significatif et à des conséquences commerciales, particulièrement dans les relations avec les clients grands comptes, qui auditent désormais systématiquement les pratiques de leurs fournisseurs en matière de traitement des données personnelles.

8.4. Risque de recours contre la délibération

La recommandation a fait l'objet de critiques importantes de la part des fédérations professionnelles, qui pointent l'absence d'outils de conformité adaptés (il n'existe pas, à ce jour, de plateforme de gestion du consentement spécifiquement conçue pour l'environnement courriel) et un risque de décalage concurrentiel avec les acteurs implantés dans d'autres États membres. Un recours contentieux devant le Conseil d'État, fondé notamment sur la qualification technique retenue, ne peut être exclu. Cette éventualité ne dispense pas, toutefois, de la mise en conformité immédiate : la délibération est exécutoire et un éventuel recours n'a pas, en principe, d'effet suspensif.

[2] Délibération SAN-2025-005 du 1er septembre 2025.

9. Recommandations d'actions

Compte tenu de l'échéance du 14 juillet 2026, il vous appartient avec votre conseil habituel/DPO d'engager sans délai une démarche structurée en trois phases.

PHASE 1 : Cartographie (à engager immédiatement)

1. Recenser l'ensemble des courriels émis par l'organisme : prospection commerciale, lettres d'information, notifications transactionnelles, communications de service, courriels de relation client.
2. Identifier les pixels effectivement déployés dans chacun de ces flux, ainsi que les prestataires techniques impliqués.
3. Cartographier les finalités poursuivies : mesure de performance, personnalisation, profilage, détection de fraude, mesure de délivrabilité, sécurité de l'authentification.
4. Qualifier chaque flux au regard de la grille consentement / exemption établie par la CNIL.

PHASE 2 : Conformité documentaire et contractuelle

5. Réviser la politique de confidentialité afin d'y intégrer une information détaillée sur les pixels de suivi et leurs finalités.
6. Auditer les contrats de sous-traitance avec les prestataires d'emailing et identifier les éventuelles situations de coresponsabilité ; conclure, le cas échéant, des accords (art. 26 ou 28 RGPD).
7. Mettre à jour les formulaires de collecte (inscription à la newsletter, création de compte, formulaires de contact) afin de prévoir un opt-in spécifique pour les pixels de suivi.
8. Mettre à jour le registre des activités de traitement (art. 30 RGPD) pour y intégrer les traitements liés aux pixels et, le cas échéant, mettre à jour les AIPD relatives au marketing et au profilage (art. 35 RGPD).

PHASE 3 : Déploiement opérationnel

9. Adresser, avant le 14 juillet 2026, l'information aux bases existantes leur permettant de s'opposer aux opérations futures de pixels de suivi.
10. Vérifier avec le fournisseur du système d'emailing si la granularité est possible.
11. Documenter les choix d'architecture et les décisions de conformité afin de préparer une éventuelle demande d'information de la CNIL.
12. Former les équipes marketing et CRM aux nouvelles règles applicables.

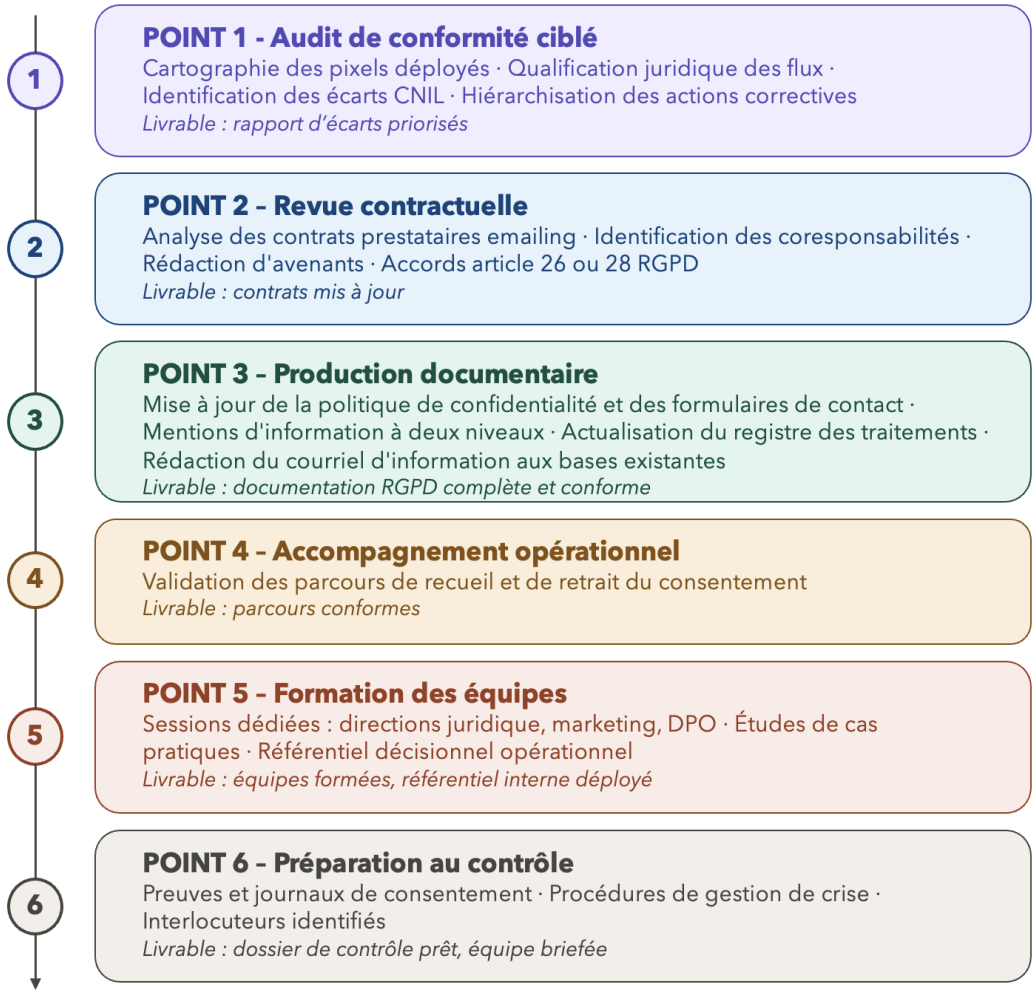
Synthèse opérationnelle

La priorité est double : (i) adresser le message d'information aux bases existantes avant le 14 juillet 2026 ; (ii) reconfigurer les formulaires de collecte pour les nouveaux contacts. Ces deux actions, à elles seules, permettent de neutraliser l'essentiel du risque immédiat de contrôle.

10. Points fondamentaux

Notre association vous présente l'ensemble des points d'attention soulevés par la délibération du 12 mars 2026.

À retenir



Point d'attention :

Le présent livre blanc constitue une note d'information générale rédigée à partir de la délibération CNIL n° 2026-042 du 12 mars 2026, publiée au Journal officiel du 14 avril 2026, et de la documentation associée publiée par la CNIL. Il ne saurait constituer une consultation juridique adaptée à une situation particulière. Les recommandations présentées doivent être ajustées en fonction des spécificités de chaque organisation, qu'il s'agisse de ses flux de courriels, de ses dispositifs techniques ou de la nature de ses relations avec ses destinataires.