BCLP. Client Intelligent

Insights

TRACKING PIXELS IN EMAILS

THE CNIL PUBLISHES ITS RECOMMENDATION AND REQUIRES CONSENT

Apr 23, 2026

On April 14, 2026, the CNIL published its long-awaited recommendation on tracking pixels in emails (Decision No. 2026-042). Tracking pixels are invisible images hosted on remote servers whose display within an email triggers a network request, allowing the sender or one of its partners to know whether, when and from which device the email was opened. Their use falls under Article 82 of the French Data Protection Act, the French provision transposing the ePrivacy Directive, the applicability of which to tracking pixels was reiterated by the EDPB in its Guidelines 2/2023. The CNIL goes further than its European counterparts: it requires the recipient's prior consent as a general rule, subject to two strictly defined exceptions. It follows that this regime imposes immediate obligations on any organisation using email as a communication or marketing channel.

THE NEW LEGAL FRAMEWORK APPLICABLE TO TRACKING PIXELS

Consent is the rule. The insertion of tracking pixels in emails requires the prior collection of the recipient's free, specific, informed and unambiguous consent, unless such operations are intended solely to enable or facilitate electronic communication or are strictly necessary for the provision of an online communication service at the user's express request. The CNIL specifies certain cases where consent is required (email open rates, creation of recipient profiles, detection and analysis of suspected fraud).

Consent must be obtained at the time the email address is collected. The CNIL recommends that consent be obtained at the time the email address is collected, by including clear information on the purposes of tracking pixels within the form. Where simultaneous collection of consent and email address is not possible (e.g. where the email address is collected by a third party without proof of consent, or where it is collected in circumstances making valid consent difficult to obtain, such as verbally) consent may be sought via a dedicated email containing no tracking pixels. Also, as consent must be given through a positive action, the recipient's inactivity must be interpreted as a refusal to consent.

THE CNIL SETS OUT TWO EXCEPTIONS

- The first covers pixels used for authentication and security purposes;
- The second covers those used to measure deliverability in order to identify and remove inactive recipients.

These exceptions apply only to emails requested by the recipient and must be justified on a case-by-case basis. These are typically transactional emails such as order confirmations, account alerts or password resets. Therefore, they do not apply to promotional messages (marketing emails).

Withdrawal of consent must be simple and effective. The CNIL recommends that a tracking link be included in the footer of every email, allowing withdrawal without further action. Tracking operations must cease for future emails, and proof of consent must be retained on an individual basis.

The impact on the B2B opt-out regime. The recommendation does not abolish the opt-out regime applicable to B2B marketing, a commercial email may still be sent to a business contact without prior consent. However, if that email contains a pixel, that pixel is subject to consent, regardless of the regime applicable to the email itself. Companies that used the opt-out to avoid obtaining consent will now have to obtain separate consent for pixels. Therefore, the operational benefit of the regime is considerably reduced.

WHAT YOU MUST DO AND BY WHEN

The CNIL is adopting a phased approach.

- **For addresses already collected**, tracking may continue provided that recipients are informed within three months to allow them to object. This does not involve obtaining new consent, but rather providing information. This simultaneous obligation for all organisations creates a real risk of confusion for recipients and of malicious exploitation by third parties (phishing risk).
- **For addresses collected after the publication of the recommendation**, consent must be obtained at the time the email address is collected, by including in the collection form the information necessary to obtain informed consent.

An update to the privacy policy is strongly recommended for all organisations using tracking pixels. Whilst Article 82 of the French Data Protection Act does not require entities to inform individuals about the use of pixels that do not require their consent, the CNIL recommends, as a matter of good practice, that they be informed of their existence in order to ensure full transparency.

In conclusion, this new regime calls into question practices that have so far been compliant, including opt-out B2B emailing. Organisations have three months from the publication of the recommendation to inform their existing recipients, i.e. until 14 July 2026. Given the complexity of

the requirements and the absence of ready-made compliance solutions on the market, early legal and technical advice will be essential.

Our BCLP team is available to support you throughout the compliance process.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Pierre-Emmanuel Frogé

Counsel, Paris

pierreemmanuel.froge@bclplaw.com
+33 (0) 1 44 17 76 21
