Crypto, TradFi & Digital

Tracking-pixel special: the email compliance question

Decoding financial, AI and data regulation to anticipate, comply and decide

Tracking pixels in emails: Europe tightens the rules

Previous editions of the Regulatory Brief have covered the major European regulatory workstreams: the AI Act and its Omnibus (Editions #7 and #18), its interplay with the GDPR (Edition #8), the post-quantum transition (Edition #9), technological sovereignty (Edition #10), the convergence of AI and cybersecurity (Edition #11), market abuse and AML/CFT (Editions #12 and #14), the end of the MiCA grandfather clause (Edition #13), the global acceleration of AI regulation (Edition #15), the European Parliament's vote on stablecoins (Edition #16) and the protection of retail investors against crypto scams (Edition #17). This nineteenth edition opens up a new dimension: European data protection rules applied to a practice as commonplace as it is invisible, tracking pixels in emails.

On 14 April 2026, following a public consultation held in June 2025, the CNIL published the final version of its recommendation on tracking pixels in emails, adopted by Deliberation No. 2026-042 of 12 March 2026. This publication does not stand alone. It forms part of a convergent European movement: the Italian Garante published its own guidelines on the subject barely three days later, on 17 April 2026, and the UK's ICO (Information Commissioner's Office) followed on 29 April 2026 with final guidance on pixels under the PECR (The Privacy and Electronic Communications (EC Directive) Regulations 2003). The common European foundation is anchored in the EDPB (European Data Protection Board) Guidelines 2/2023, adopted in their final version on 7 October 2024, which consider that inserting pixels into emails constitutes a storage of, and access to, information on the terminal equipment falling within Article 5(3) of the ePrivacy Directive.

For all organisations subject to the GDPR, and financial institutions in particular, the stakes are direct and operational. Commercial newsletters, client alerts, account-related communications, prospecting campaigns and marketing emails frequently rely on tools that activate open- and click-measurement functions. Opens are generally measured by means of an invisible pixel, whilst clicks are tracked through tracking links or individualised redirects. Both techniques may fall within Article 5(3) of the ePrivacy Directive, but they do not rest on the same technical mechanism. The

question raised by the CNIL and its counterparts is therefore the following: under what conditions may the recipient's behaviour be observed without consent, and under what conditions is prior consent required?

One operational deadline deserves to be flagged from the outset. For addresses collected before 14 April 2026, organisations had, in principle, three months to inform recipients clearly of the use of pixels and to offer them a simple means of objecting. That baseline period expired on 14 July 2026. The FAQ published by the CNIL on 22 July nevertheless states that a reasonable extension may be accepted where objective difficulties relating to database volume or deliverability are justified and documented. In the absence of such information within the applicable period, pixels subject to consent must be deactivated or covered by valid consent. In Italy, the general compliance period runs until the end of October 2026.

The weak signal

Compliance for electronic communications is no longer limited to the question: “Are we entitled to send this email?” It now imposes a second question: “Are we entitled to observe what the recipient does with it?”

This shift is more structural than it appears. Until now, operational compliance for electronic direct marketing has focused mainly on the lawfulness of sending: prior consent under Article L. 34-5 of the French Postal and Electronic Communications Code for individuals, the regime applicable to B2B prospecting and the exception for similar products or services offered to existing customers. Compliance frameworks have therefore been organised around the distinction between transactional and promotional communications. That distinction remains relevant, but it is no longer sufficient.

The second question concerns the technical tracking operation. The regime applicable to pixels is legally distinct from the one permitting the email to be sent. A transactional email, a B2B prospecting message or a communication addressed to an existing customer may lawfully be sent without prior consent to sending, whereas the individualised tracking it contains remains, in principle, subject to consent unless an exemption applies. This distinction calls for a review of email-marketing and CRM arrangements, together with configurations enabling messages to be sent without tracking where such tracking is neither consented to nor exempt.

Focus 1: The CNIL recommendation of 14 April 2026

The CNIL's recommendation, adopted by Deliberation No. 2026-042 of 12 March 2026 and released to the public on 14 April 2026 following a consultation opened in June 2025, is addressed to all organisations, whether private or public (companies, associations, public administrations, local authorities), that use tracking pixels in their emails, as well as to the technical service providers they may engage. It complements the EDPB Guidelines 2/2023 on the technical scope of the ePrivacy Directive and the CNIL's recommendation on cookies and other trackers.

The legal regime is clear: inserting a pixel constitutes a read or write operation on the recipient's terminal equipment falling within Article 82 of the French Data Protection Act (loi Informatique et Libertés), which transposes Article 5(3) of the ePrivacy Directive. Prior consent, freely given, specific, informed and unambiguous, therefore becomes the rule where the pixel is used to measure a campaign's open rate on an individual basis, personalise the content or frequency of messages, adapt the communication channel, build interest profiles, subsequently target the person on other sites or applications, or detect certain types of fraud by analysing opens individually. The CNIL specifies that a single consent may cover both the sending of a promotional communication and the use of pixels with a directly related purpose, for instance where marketing is clearly presented as personalised. Purposes without a direct link must, by contrast, remain separate.

Consent may nevertheless not be required where the pixel is used exclusively for an exempt purpose, in particular a security measure contributing to authentication or a strictly necessary deliverability measure concerning an email requested by the user or connected to a service the user has expressly requested. The transactional nature of the message is not, however, sufficient on its own to justify the exemption: the email must remain exclusively informational or functional in nature, with no promotional element, and all the other conditions set out in the recommendation must be met.

The exemption may also cover, under strict conditions, the identification of inactive recipients in order to adjust the frequency of, or stop, mailings, as well as demonstrating compliance with certain statutory information obligations. For individual deliverability measurement, the CNIL recommends retaining only the date of the last open, without the time, replacing the previous entry with each new open.

What to watch

- The CNIL's support cycle: following an initial general webinar held on 28 May 2026, a webinar aimed at vendors and service providers was held on 4 June. The replay of this second webinar and a detailed FAQ were published on 22 July 2026.
- The **CNIL's first inspections** of pixel practices: the CNIL has announced that it will monitor compliance with the rules as part of its forthcoming inspection activities.

- The interplay with **existing cookie frameworks** and the need to align CRM and emailing practices with the CNIL's cookies recommendation already in force.

Focus 2: Coordinated European convergence

The CNIL's publication forms part of a marked European convergence: between 14 and 29 April 2026, three national authorities published texts devoted to pixels or to storage-and-access technologies. These positions rest on the common foundation of Guidelines 2/2023 of the European Data Protection Board, adopted in their final version on 7 October 2024. The convergence concerns the application of the ePrivacy rules and the need for consent for individualised tracking. The exemptions and the practical arrangements for achieving compliance nevertheless differ across jurisdictions.

The Italian Garante published guidelines on 17 April 2026 that are very close to the French position. The Italian authority requires prior consent for the individual measurement of opens, behavioural campaign optimisation and the creation of commercial profiles. It does, however, permit certain processing operations without consent: calculating an overall open rate, provided the results are anonymous and no pixel makes it possible to distinguish between recipients; certain security and authentication measures; institutional or service communications whose sending is legally required; and certain security, fraud or phishing alerts. Users must be able to withdraw their consent to tracking separately whilst continuing, if they so wish, to receive the emails. The Garante also recommends using unintelligible, non-sequential identifiers stored separately from email addresses. Organisations have six months from the publication of the guidelines in the Italian Official Journal on 29 April 2026, that is, until the end of October 2026, to achieve compliance.

In the United Kingdom, the ICO published final guidance on 29 April 2026 clarifying that pixels embedded in emails fall within the PECR rules on the storage of, and access to, information held on terminal equipment, and not solely within the rules applicable to the sending of commercial communications. Strictly statistical processing may benefit from an exemption where the results are aggregated, do not make it possible to identify or track an individual and are used exclusively to improve the service, with clear information and a simple, free means of objecting still being required. Individual tracking, profiling, advertising targeting or the use of data to take decisions about a person, by contrast, continue to require consent.

One significant divergence should be noted. In France, the fact that a pixel directly collects anonymous or aggregated data is not sufficient to exempt that collection from consent, since Article 82 of the French Data Protection Act applies regardless of whether the data is personal. By contrast, data lawfully collected on the basis of consent or an exemption may subsequently be anonymised

and reused to produce overall statistics. Italy and the United Kingdom recognise, under conditions specific to their national law, more direct possibilities for using aggregated statistics without consent.

This movement does not stand alone. It follows a doctrine already expressed by other authorities: as early as 3 February 2023, the Danish authority Datatilsynet issued severe criticism of an organisation that had analysed the opens and clicks of its newsletters without valid consent or sufficient information. The German BfDI reiterates that consent to receive a newsletter does not automatically cover the use of pixels: if the recipient refuses tracking, it must be possible to send them the newsletter without a pixel. The Irish DPC likewise considers that pixels, web beacons and similar technologies generally require consent whenever they access information held on the terminal equipment.

What to watch

- The **forthcoming guidelines or communications from other European authorities** (the BfDI, the DPC, Spain's AEPD, and the Dutch and Belgian authorities), which could complete the mosaic and harmonise practices.
- Clarification of the divergences on aggregated statistics between the CNIL, the Garante and the ICO, in particular on the distinction between the initial collection via the pixel and the subsequent reuse of anonymised data.
- The **first enforcement decisions** on pixel practices in 2026-2027, which will clarify the practical reach of the recommendations and the operational points requiring vigilance.

Focus 3 - What to check: the operational points

Data controllers, DPOs, marketing departments, CIOs and legal departments should now undertake a systematic review of their emailing and CRM practices. Ten operational points emerge from a combined reading of the CNIL, Garante and ICO publications.

- Take stock of the **open-tracking and click-tracking functions** activated in sending tools and the CRM, distinguishing the pixels used to measure opens from the tracking links or redirects used to measure clicks, and aggregated statistics from individual tracking.
- Identify **the data actually collected** via these pixels (recipient identifier, date, time, device, IP address, approximate geolocation), its precision and its recipients (in-house, service provider, partner).

- Clearly distinguish **aggregated statistics from individual tracking**: a conceptual boundary that is becoming a legal one.
- Document **each purpose separately** (audience measurement, personalisation, profiling, advertising targeting, fraud detection, deliverability measurement, security).
- Check that the **exemptions relied upon are genuinely necessary and proportionate** to the purposes pursued; the exemption must be documented and reasoned.
- Obtain **consent at the point the address is collected** where consent is required, with the characteristics demanded by the GDPR and Article 82 of the French Data Protection Act (freely given, specific, informed, unambiguous).
- Offer a **simple mechanism for refusing or withdrawing tracking alone**, without compromising the ability to continue receiving the communication itself where that communication is lawful.
- Review the **controller, processor or joint-controller qualifications** agreed with emailing providers; a point often dealt with summarily in standard contracts.
- Keep **individualised proof of consent** and of the conditions under which it was obtained, in line with the CNIL's settled doctrine on the burden of proof.
- Deactivate **tracking features by default** where they are not necessary; the minimisation principle is becoming an operational principle for configuring tools.

Focus 4: A structural workstream for financial institutions

The financial sector occupies a particular place in this new landscape. Banks, insurers, asset managers, brokers, investment platforms, fintechs and crypto-asset service providers send numerous emails to their clients and prospects: account movements, order confirmations, margin calls, contractual deadlines, security alerts, financial-information newsletters, and prospecting or loyalty campaigns. These communications often rely on emailing tools and CRMs offering open- and click-tracking features, sometimes activated by default.

Three use cases must be analysed separately.

First, strictly transactional or regulatory communications may benefit from an exemption where the message is requested by the user or directly connected to a requested service, contains no promotional elements, and the pixel is limited to a purpose that is itself exempt.

Second, where a user expressly consents to receiving a personalised newsletter, a single consent may cover both the sending and the pixels directly necessary for that personalisation, subject to clear information. By contrast, where a communication is sent without consent on the basis of the exception for similar products or services, the deliverability pixel does not, on that ground alone, benefit from an exemption and remains, in principle, subject to consent.

Third, B2B prospecting communications may not require consent to be sent, but their individualised tracking remains, in principle, subject to consent unless a duly documented exemption applies.

One important point of interplay deserves to be flagged for organisations subject to the GDPR as well as to MiFID II, MiCA or the French Monetary and Financial Code. Certain communications required by a legal or regulatory obligation, such as pre-contractual information, contractual amendments, or certain mandatory notifications, may benefit from an exemption where measuring the open is strictly necessary to demonstrate that the information was transmitted and the other conditions laid down by the CNIL are met. This analysis must be carried out and documented on a case-by-case basis. It cannot automatically cover all of a regulated firm's communications. A technical and contractual review of emailing solutions is therefore a priority and may lead, where necessary, to adapting or renegotiating contracts with providers.

What to watch

- Any **AMF and ACPR communications** on the interplay between sector-specific client-information obligations (MiFID II, MiCA, PRIIPs) and the pixels regime, a subject that could give rise to sector-specific clarifications.
- The **adaptations proposed by the main emailing providers** over the coming months, in particular default configurations, deactivation options and differentiated consent management.
- The **consistency of the French supervisory reading** across the AMF, the ACPR and the CNIL on regulated communications, in line with the supervisory-interplay logic already described in Edition #8.

Key takeaways

Five structural points to take on board:

- The CNIL's recommendation forms part of a European convergence with the positions of the Italian Garante and the UK's ICO, built on the foundation of the EDPB guidelines. The exemptions and practical arrangements nevertheless still differ from country to country.
- Prior consent is required as a matter of principle for the individualised tracking of opens and clicks. The tracking regime is distinct from the one authorising the sending of the email, even though a single consent may sometimes cover clearly related purposes.
- Exemptions are interpreted strictly and must be documented case by case. The merely transactional or regulatory nature of an email is not enough: the message must in particular be requested, or linked to a requested service, and the tracking must be strictly necessary for an exempt purpose.
- In France, the three-month baseline period expired on 14 July 2026. A reasonable extension may nevertheless be accepted where objective difficulties are justified and documented. In Italy, the general period runs until the end of October 2026.
- Financial institutions must analyse separately transactional or regulatory communications, consented personalised newsletters, communications to existing customers and B2B prospecting. A technical and contractual review of emailing tools is necessary.

Conclusion

The CNIL's recommendation of 14 April 2026 amounts to more than a technical clarification. It formalises a second dimension of email compliance: after the question of the lawfulness of sending comes that of the lawfulness of observing the recipient's behaviour.

The recent convergence between the French, Italian and British authorities, grounded in the EDPB's doctrine and in the earlier positions of other national authorities, confirms that invisible email tracking is becoming a self-standing compliance topic. For financial institutions and other organisations sending large volumes of emails, the challenge is immediate: it calls for a systematic review of practices, a technical and contractual adaptation of emailing tools, and close collaboration between legal departments, DPOs and marketing teams.

Main sources

- CNIL, *« Pixels de suivi dans les courriers électroniques : la CNIL publie ses recommandations pour mieux protéger la vie privée » ("Tracking pixels in emails: the CNIL publishes its recommendations to better protect privacy")*, published 14 April 2026; *Délibération n° 2026-042 du 12 mars 2026 portant adoption d'une recommandation relative aux pixels de suivi dans les courriers électroniques* (JORF, ref. JORFTEXT000053876850); recommendation available for download at cnil.fr.
- CNIL, *Synthèse des contributions à la consultation publique* and *Synthèse des contributions à la consultation sur les enjeux économiques*, published 14 April 2026 (cnil.fr).
- CNIL, *webinar of 22 July 2026 on tracking pixels (vendors and service providers)* and *FAQ – Questions and answers on the tracking-pixels recommendation*, published 22 July 2026.
- EDPB (European Data Protection Board), *Guidelines 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive*, final version adopted 7 October 2024 (edpb.europa.eu).
- Italian Garante (Garante per la Protezione dei Dati Personali), *guidelines on tracking pixels in emails*, published 17 April 2026, entering into force upon publication in the Italian Official Journal on 29 April 2026.
- ICO (Information Commissioner's Office, United Kingdom), *Guidance on tracking pixels under PECR*, final version published 29 April 2026 (ico.org.uk).
- Datatilsynet (Denmark), *decision of 3 February 2023* on the use of pixels in newsletters without valid consent.
- BfDI (Germany), *recommendations on newsletters and tracking pixels*; DPC (Ireland), *guidance on cookies and tracking technologies*.
- Directive 2002/58/EC (ePrivacy), Article 5(3); French Act No. 78-17 of 6 January 1978 (loi Informatique et Libertés), Article 82.
- Regulation (EU) 2016/679 (GDPR); general framework for the processing of personal data.

***

The Seqlense Regulatory Brief - Crypto & TradFi · Edition #19

This publication is provided for information purposes only and constitutes neither investment advice, nor a personal recommendation, nor an inducement to buy or sell financial instruments or crypto-assets.

The information presented reflects a general analysis of market dynamics and regulatory developments as at the date of publication. It does not take account of any reader's personal situation, investment objectives or risk profile.

Despite the care taken in selecting and verifying sources, no guarantee is given as to the accuracy, completeness or currency of the information. Financial markets and crypto-assets carry high risks, including volatility and loss of capital.

Consequently, any investment decision is the sole responsibility of the reader and should, where appropriate, be taken with the support of qualified professional advisers.