ometria

# Email tracking pixels: changes in France and Italy

## What is a tracking pixel?

A tracking pixel is a tiny, invisible image embedded in an email. When the email is opened and the image is loaded, the recipient's device makes a request to the server hosting the image. That request allows the sender to record that the email has been opened. The resulting information can be useful. Apart from showing an overall campaign open rate, an individual open can be used to understand whether a customer remains engaged, decide when or how frequently to contact them, trigger an automation, contribute to a customer profile or help determine which marketing channel to use next. Tracking pixels are not new. They have been a standard feature of email marketing platforms for many years.

## Consent to email and consent to tracking

There are two separate activities here: sending the marketing email and tracking what the recipient does with it. That distinction is not new. In the UK, PECR has regulated both electronic marketing and the use of cookies and similar technologies since 2003. The equivalent rules across the EU derive from the ePrivacy Directive.

A recipient who has consented to receive your newsletter has therefore not necessarily consented to everything that might happen once the email arrives. In particular, consent to receive marketing emails does not, by itself, amount to consent to the use of a tracking pixel to determine whether that individual has opened the email or to use that information to measure their engagement, personalise future marketing or build their customer profile. Nor is the requirement for consent to tracking something created by the GDPR. The underlying ePrivacy rules requiring consent to the storage of, or access to, information on a person's device pre-date the GDPR by many years. What the GDPR did was clarify and strengthen what valid consent looks like. Where consent is required, it must be freely given, specific, informed and unambiguous, and demonstrated by a clear affirmative action.

In simple terms, there have always been two questions: are you entitled to send this person the email, and are you entitled to track what they do with it? The answer to the first question does not determine the answer to the second.

## How have retailers previously obtained consent?

Historically, retailers have generally dealt with email tracking through their privacy notices rather than by asking customers a separate question when they sign up for marketing. A privacy notice might explain that the retailer uses "pixels", "web beacons", "tracking technologies" or similar technologies in emails and on its website to understand whether messages have been opened or clicked and to measure and improve its marketing.

The difficulty is not necessarily that the pixel was never mentioned. It is that the customer's agreement to tracking was often bundled into something wider. A customer might tick a box saying "Yes, I would like to receive news and offers", with the privacy notice explaining elsewhere that emails contained pixels, web beacons or other tracking technologies. Alternatively, a privacy notice might group email pixels together with website cookies, analytics and other technologies under a general heading such as "cookies and similar technologies". That approach provided transparency about the existence of the

technology, but it did not necessarily obtain a separate, specific choice about whether the individual agreed to be tracked.

For many years that distinction attracted relatively little regulatory attention. Retailers disclosed the technology, customers consented to marketing and email platforms continued to provide the open data on which marketers had come to rely.

## What has changed?

The technology has not changed and the underlying ePrivacy rules are not new. What has changed is the regulatory focus on email tracking and, in particular, whether the way retailers have traditionally obtained consent is sufficient.

In April 2026, the French data protection authority, the CNIL, published a recommendation dealing specifically with tracking pixels in emails with the Italian Garante published its own guidelines three days later.

Historically, retailers principally used open rates to understand how an email campaign had performed. Ometria and other modern marketing platforms can do considerably more with that information. An individual open can form part of the customer's profile and be used for segmentation, engagement scoring, send-time optimisation, automation triggers or to determine the content, frequency or channel of future marketing.

The regulators are therefore looking not simply at the pixel itself, but at why it is there and what happens to the information it produces. Although France and Italy start from broadly the same ePrivacy rules, they have not reached precisely the same position on what requires consent and what may be done without it.

## France – the CNIL recommendation

The CNIL's recommendation was adopted on 12 March 2026 and published on 14 April 2026. It rests on Article 82 of the French Data Protection Act, which implements the ePrivacy rules on accessing information stored on a person's device. It is therefore not a question of which GDPR lawful basis you rely on to send the email. In the CNIL's view, consent is required where a pixel is used to measure open rates, optimise campaigns, personalise content, profile recipients, detect fraud or measure deliverability for individual recipients. The exemptions are narrow: pixels used for authentication security, and a deliverability pixel limited to recording the day of the last open in an email the recipient asked to receive.

The practical consequence is that consent to receive marketing emails and consent to be tracked are two different things. A recipient who has opted in to your newsletter has not, by doing so, agreed to open-tracking. Where tracking consent is required, it must be specific, informed and freely given. Refusing tracking must not prevent the recipient from receiving marketing which you are otherwise lawfully entitled to send. That refusal must also be respected: the CNIL identifies not asking again for six months as good practice, although the appropriate period will depend on the relationship with the recipient.

## What about anonymous open rates?

Making a pixel "anonymous" does not take it outside the rule. The CNIL's FAQ is clear that Article 82 applies whether or not the information collected is personal data. You cannot therefore fire a pixel for everyone and avoid the consent requirement simply by stripping out the identity afterwards.

There is a narrower route. Information lawfully collected through an exempt pixel may subsequently be effectively anonymised and aggregated, for example to produce an overall campaign open rate. That does not, however, provide a general route to fire an anonymous pixel across the whole audience.

## What about clicks?

Links in emails are not directly covered by the recommendation. The CNIL's FAQ nevertheless says that Article 82 still applies to tracking links and that the principles in the recommendation can be used when assessing them. We would therefore be cautious about using a click to recreate something which could not lawfully be obtained from an open. For example, treating a click as an "open" for the purpose of an engagement score, customer profile or automation could simply recreate through a different technology the processing for which the customer has not consented. Ometria's open-tracking consent setting controls the tracking pixel only. Click tracking stays on for every contact, including those who have refused open tracking, and cannot be switched off for individual contacts. Any consent wording you use should say so.

## Existing French customers

For addresses collected before 14 April 2026, the CNIL allowed a transition: notice to the recipient and an opportunity to object, to be completed by 14 July 2026, with a limited and documented extension available where there were genuine operational difficulties. That date has now passed.

If you relied on the transition, you should be able to show that you gave the notice and offered the objection route. Importantly, silence during the transition was not converted into consent. It was non-objection which allowed the existing tracking to continue, and it does not extend to new purposes or materially different processing. Addresses collected on or after 14 April 2026 did not benefit from the transition. In Ometria, the account setting for contacts acquired before the effective date (14 April 2026) treats those contacts as consented for every open-based use, including segmentation, send-time optimisation and automations, and the preference centre shows the tracking box ticked for them. Ometria does not check that you gave notice or offered an objection route, and treating these contacts as consented may go beyond what the transition permits. Unless you can show both, and that your uses fall within what you notified, we recommend the alternative setting, under which contacts in an enabled country are treated as not consenting until they opt in.

## Italy

The Garante published its provision (no. 284) on 17 April 2026. Like the CNIL, it treats an email tracking pixel as a technology that accesses information on the recipient's device. Consent is therefore required for individual open measurement used to assess and improve promotional campaigns, adjust the frequency of sending according to the recipient's engagement, or infer interests and preferences for commercial profiling.

There is, however, an important difference. The Garante permits aggregate measurement of the overall percentage of emails opened without consent, provided that the information is anonymised so that individual recipients cannot be measured. It suggests using the same pixel for all recipients of a campaign, rather than an individual pixel for each recipient, together with anonymisation of associated technical information such as IP address and email client. France expressly rejects an anonymous pixel as a way around the consent requirement. Italy therefore gives retailers a more straightforward route to retaining campaign-level open statistics without tracking the behaviour of individual recipients. Ometria cannot currently offer this aggregate-only approach: disabling open tracking through our email delivery provider disables the open event altogether, so no aggregate open rate is returned to Ometria.

The guidelines were published in the Italian Official Gazette on 29 April 2026 and give organisations six months from publication to bring their practices into line. The implementation deadline is therefore 29 October 2026. Unlike France, there is no effective date for Italy: Italian contacts are treated as not consenting until they opt in.

## Where is this heading?

We do not expect this to stop with France and Italy. The rule the CNIL and the Garante are applying is not a French or Italian invention. It comes from Article 5(3) of the ePrivacy Directive, which every EU Member State has transposed (in France as Article 82 of the Data Protection Act and in Italy as Article 122 of the Privacy Code), and the European Data Protection Board's guidelines on the technical scope of that Article already treat pixel tracking, including in emails, as within it. That gives other national authorities a ready basis to follow, and we think it likely that more of them will publish their own positions, through guidance, enforcement or both. We cannot predict when. The detail will also differ from country to country: the Garante's allowance for aggregate pixels is already more accommodating than the CNIL's approach. Harmonisation across the EU is therefore likely to be gradual and partial rather than a single rule arriving at once.

For clients with audiences across Europe, the sensible planning assumption is that consent-based open-tracking will become the norm rather than a French exception. That is why the functionality described above is organised country by country and lets you apply the stricter standard wherever you choose to, rather than building to a single territory's rules. We will update this note as the position develops.

## What does this mean for Ometria clients?

If you email recipients in France or Italy, you should assume that tracking whether those recipients open your emails needs their consent, unless you have concluded, with your own advisers, that an exemption applies. The practical consequences are these.

First, you will need a way of asking recipients for that consent, separately from their consent to receive marketing, and of recording the answer.

Second, open rates will fall, because you will only be measuring recipients who have agreed to be measured. They will also be less representative of your audience as a whole.

Third, features that depend on opens, such as engagement-based segments, send-time optimisation and A/B test winners selected on opens, will work on a smaller group, and you may therefore wish to place greater weight on genuine click and conversion activity, rather than using clicks to infer opens. Contacts who are not tracked cannot meet an open-based condition, and if you exclude unengaged contacts from your sends, contacts whose only engagement is opening emails may drop out of your broadcasts.

Finally, the rules for each country apply by reference to where the recipient is, Ometria applies these controls only to contacts whose country is on record and is one you have enabled. Contacts with no recorded country are always tracked. The decisions about whether to track, where, and on what basis are yours as the controller. So are the wording of your consent requests, the notices you give, the evidence you keep, and the accuracy of the country information you hold about your contacts.

## What is Ometria doing?

We have added functionality to the platform so that you can comply with these rules in the way that suits your business. In broad terms, it allows you to:

- record consent to open-tracking as a choice that is separate from consent to receive marketing;
- decide, country by country, how contacts in the countries you enable (currently France, including its overseas territories, and, from 26 October 2026, Italy) are treated, including how to treat contacts who have not yet been asked;
- collect that consent in the places your customers already interact with you: in overlays and sign-up forms, in the preference centre (including by clicking through to it from links in your emails), through one-click opt-in and opt-out links in emails, and by importing consent you already hold by API or CSV;
- send in a way that does not track contacts who have not consented, so that the tracking pixel is not used for them;
- see the answer each contact has given on their profile (a contact kept tracked by the effective date setting shows “No preference”) and use the status Ometria applies to build segments and exports; and
- report on opens, and use open-based features, on the basis of the contacts who have consented, with an open no longer being inferred from a click.

This functionality is available on all accounts, but nothing changes until you enable a country in your channel settings. Overlays, forms and preference centre pages also need updating before consent can be collected: forms need new code added for your site, and your customer success manager can help arrange the preference centre. The technical documentation is available at support.ometria.com/hc/en-gb, which is the place to look for how each feature works and how to set it up.

These are tools, and the settings are yours to choose. The defaults we provide are configuration choices and not legal conclusions, and using the functionality does not by itself make a particular campaign compliant. As set out in our Data Processing Agreement, you are the controller of your contacts' personal data and Ometria is your processor. It is for you to decide whether and how to track recipients, to give them the right information, to word your consent requests, and to keep the records that demonstrate consent. We will process data on your documented instructions, and we will support you in doing so.

## Finally

This is a fast-moving area, and regulators in other countries may follow. We will update this note as the position develops and as the functionality is rolled out. If you have questions about how the functionality works, please speak to your customer success manager. If you have questions about this note, please contact dpo@ometria.com.

---

**Julian Palmer, DPO, October 2026**

Please note that Julian is Ometria's legal counsel and as such cannot give our clients legal advice. Nothing in this note constitutes legal advice nor gives rise to a lawyer/client relationship.