RECOMMENDATION

ON TRACKING PIXELS IN EMAILS

This content is a courtesy translation of the original publication in French.
In the event of any inconsistencies between the French version and this English translation, please note that the French version shall prevail.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. Introduction

The use of invisible tracking pixels inserted into emails has grown significantly in recent years. These technical tools, which are widely used in electronic communications, are used for a variety of purposes: to ensure the correct receipt of emails (known as 'deliverability'), to measure the audience, to personalise communication according to the interests of users, etc.

This practice raises particular challenges in the context of email, a personal space for consulting private content, accessible after an authentication procedure. The CNIL receives an increasing number of reports and complaints, which show that people are becoming more vigilant about these practices.

The European Data Protection Board[1] (EDPB) published its Guidelines 2/2023 on technical scope of Article 5(3) of ePrivacy Directive, transposed into Article 82 of the Law of 6 January 1978 ('the Data Protection Act'). Those guidelines recall the application of those provisions to pixels inserted in emails.

The principles and obligations laid down in Article 82 of the Data Protection Act with regard to the reading or writing of information have been the subject of guidelines [2] and a recommendation[3]. This Recommendation therefore clarifies the application of all these texts taking into account the technological and operational specificities related to pixels and proposes concrete recommendations to comply with them.

Any processing of personal data produced or collected via a tracker (hereinafter referred to as "subsequent processing") must comply with the provisions of the General Data Protection Regulation (GDPR) and the relevant provisions of the Data Protection Act.

The recommendation applies to reading or writing operations, without prejudice to compliance with the GDPR by subsequent processing operations.

The Recommendation, and in particular the examples proposed therein, is neither regulatory nor exhaustive and its sole purpose is to assist professionals in their compliance process. It was drawn up following consultation with representatives of the professions concerned and civil society. It was also the subject of another public consultation from 12 June to 24 July 2025.

[1] Guidelines 2/2023 on technical scope of Article 5(3) of ePrivacy Directive, Version 2.0, adopted on 7 October 2024

[2] Deliberation No 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Law of 6 January 1978 to reading and writing operations in a user's terminal (in particular 'cookies and other trackers') and repealing Deliberation No 2019-093 of 4 July 2019

[3] Deliberation No 2020-092 of 17 September 2020 adopting a recommendation proposing practical arrangements for compliance in the event of the use of 'cookies and other trackers'.

2. Scope of the recommendation

2.1 Technologies and environments concerned

In the context of emails, tracking pixels are images, usually of very small size, that are not directly contained in the email concerned but are hosted on remote servers. Their display within an email client (either in a specific software or within a browser) requires a query to be made over the network, using the URL provided in the body of the message.

The URL of the image usually has individualised settings relating to the user or context in which the image appears. In response to this call, the image in question is loaded and written to the user's terminal memory for the email client to display. The display of that image does not generally have, in itself, any informative value for the user; the process which leads to that display allows the sender of the message or one of its partners to obtain information relating to the consultation of an email by a specific user or in a specific context. The inclusion of those tracking pixels in emails therefore constitutes an instruction given to the user's terminal to return targeted information (pixel identifier, IP address, etc.) to the actors who deposit them. This information is communicated through the parameters of the request and its collection, by the server hosting the image, constitutes a reading operation on the user's terminal. Therefore, and in line with the position expressed by the EDPB in its Guidelines, Article 82 of the Data Protection Act is applicable to the use of tracking pixels in emails.

The recommendation is limited to the use of tracking pixels in emails. While some captive messaging systems (e.g. secure messaging systems provided by banks) may have formal similarities with emails, they rely on other protocols, which excludes them from the scope of this recommendation.

2.2 Relevant actors and qualifications within the meaning of the GDPR

The Recommendation is addressed to private or public sector bodies involved in reading or writing operations related to tracking pixels in emails. **Each of these actors must determine its role with regard to the treatment carried out.**

The sender of the email

The term 'email sender' refers to the actor (company, public body, association, etc.) who decided to send the email, whether it is technically the sender or not.

It may decide to use solutions that involve the use of tracking pixels and then determine the purposes for which those trackers are used as well as the means. It must therefore be regarded as controller, including when it outsources to third parties (e.g. the emailing service provider) the management of trackers set up at its request.

In principle, it will also be **jointly responsible for the reading or writing operations,** which it accepts contractually, carried out by third parties within the emails which it has requested to be sent[4].

[4] By analogy, in the web environment, the publisher of a website was held responsible for the processing of reading/writing operations carried out by third parties in a decision 'Éditions Croque Futur', No 412589 of 6

The purposes and means of those operations are then determined jointly[5], even though subsequent processing operations may fall within the independent responsibility of one or other of those parties.

The service provider for sending emails (or 'emailing')

This is the company that provides the technical solution for sending emails. It is the actor that most often offers the integration of tracking functionalities via pixel technology. This service provider acts, in general, on behalf of the data controller and according to his instructions. In this context, it will act as a **processor.**

The service provider for the rental of mailing lists and the sending of emails

This is the company that provides its customers with a "turnkey" solution for sending communications to mailing lists offered for rent. A case-by-case analysis is necessary in this case.

When the provider integrates tracking tools via pixel technology to provide information to its customer, controller, **it acts, in principle, as a processor.**

The provider may also use these pixels for its own purposes which are not generally linked to a specific customer (e.g. improving the relevance of its mailing lists or the deliverability of emails to email providers). In those situations, where a customer contractually agrees to the implementation of such operations, **co-responsibility for processing may be retained for** those operations. In accordance with Article 26 of the GDPR, that relationship presupposes a clear and transparent division of the respective obligations, in particular as regards information to data subjects and respect for their rights.

The supplier of tracking technology

Pixels embedded in emails may be provided by a specialised third party, separate from the email provider.

The qualification of this actor depends on the purposes it pursues on the basis of the monitoring data. If the reading or writing operations are carried out exclusively on behalf of the sender, **the technology provider will be a processor.**

On the other hand, if the data collected via pixels is also used for its own purposes (e.g. to improve the solution provided), when a customer contractually agrees to the implementation of such operations, the technology provider and the sender **can be considered co-responsible for the reading or writing operations.**

June 2018, in which the Conseil d'État takes the view that the publisher of a website which authorises the deposit and use of third-party cookies must be regarded as the controller. Similarly, in deliberation No SAN-2021-013 of 27 July 2021, the CNIL considered that the publisher of the site had a certain responsibility (an obligation of means) with regard to the collection of consent on third-party cookies. Thus, the fact that the cookies come from partners does not relieve the publisher of the site of its own responsibility in so far as it has control of its site and its servers.

[5] In this case, a mutual interest emerges from this operation. See, CJEU, 29 July. 2019, Case C-40/17, Fashion ID GmbH & Co. KG v. / Verbraucherzentrale NRW eV.

The email service provider

The email service provider ensures the reception and display of emails addressed to its users. Although it is an essential technical actor for the operation of email, it does not intervene directly in the processing linked to the use of pixels.

However, this provider can technically influence the pixel's ability to trigger a reading operation on the terminal, for example by blocking the automatic loading of images. However, since it does not use the data generated by the pixel, **it is neither a processor nor a controller.**

3. Objectives pursued by the treatment (purposes)

Tracking pixels in emails may be used for several purposes.

In accordance with the provisions of Article 82 of the Data Protection Act, the insertion of tracking pixels in emails requires the prior collection of the recipient's free, specific, informed and unambiguous consent, unless these operations:

- have the exclusive purpose of enabling or facilitating communication by electronic means; or
- are strictly necessary for the provision of an online communication service at the express request of the user.

3.1 Purposes that require the consent of the recipient

In the light of these legislative provisions, the CNIL considers that the use of pixels for the following purposes requires the collection of the recipient's consent:

- **Analysis of the email opening rate to measure and optimise the performance of campaigns** by customising the content of messages or by adapting the frequency of sending or the communication channel (email, SMS, push notification, etc.). This purpose includes the procedures for ensuring the reliability of this measure (e.g. the fight against advertising fraud).

- **The creation of profiles of recipients with regard to the preferences and interests expressed in order to target them in contexts other than emails** (on websites, mobile applications or via other communication channels).

- **Detection and analysis of suspected fraud,** such as the identification of unusual or massive openings of emails, which may indicate automated behaviour (e.g. massive entries to a competition, attempts to exfiltrate information, etc.).

- **The individual measure of the email open rate for deliverability purposes** when performed outside the cases referred to in point 3.2 of this Recommendation.

3.2 Purposes exempted from the collection of consent

In the light of the same provisions of Article 82 of the Data Protection Act, and in the light of the practices brought to its attention, the CNIL considers that pixels used exclusively for the following purposes may be exempted from consent:

- **The implementation of security measures involved in user authentication.** In that context, the use of tracking pixels serves the sole purpose of helping to secure an authentication (by ensuring, for example, that the email containing a code used in the authentication process is indeed open on a terminal known to belong to the intended user).
- **The individual measure of the opening rate of emails for deliverability purposes.** Managing a mailing list almost systematically requires the use of email opening statistics to identify potential deliverability issues. In order for pixels to be exempted for that purpose, the controller will have to demonstrate that the operations carried out are intended to be limited to what is strictly necessary to adjust the frequency or stop the sending of emails to so-called 'inactive' recipients (database cleaning). Subject to this reservation, pixels may also be used for the following purposes:
    - assess and adapt the communication channel in order, if necessary, to choose alternative contact methods;
    - contribute to the demonstration of compliance with a legal obligation relating to the transmission of information to the recipient: keeping track of the opening of the email may help to demonstrate compliance with a legal obligation in the context of certain emails (for example, the delivery of the information required by legal and regulatory provisions before, during or after of the contractualisation, etc.).

In principle, in compliance with the principle of minimisation (Article 5.1.b) of the GDPR, only the date (at the day and without recording the time) of the last known opening of emails, overwritten at each new opening with deletion of the previous one, should be kept.

In so far as Article 82 of the Data Protection Law refers to an 'express request' by the user, those exemptions may relate only to emails requested by the recipient or which relate to a service requested by the recipient. These include, for example, so-called 'transactional' emails (see below) or emails for which the recipients have given their consent.

What is a 'transactional' email?

For the purposes of this recommendation, a transactional email can be understood as a message triggered by a specific action or event of a user. These emails are usually sent to provide users with important information about a requested service, their account, or their transaction. It is not a promotional message, but an informative or functional message, necessary for the contractual relationship or the requested service.

These include, for example, welcome emails, account alerts, notifications related to events such as shipping a package, order confirmations and purchase invoices, reminders and password resets, responses to requests sent to customer service, reminders of appointments or reservations, payment notifications or breach notification emails related to the requested service.

Pixels inserted in **the administration's emails,** when they are sent in the context of an activity directly linked to a public service mission, in particular those sent in the context of proactive steps benefiting the user (information on the possibility of benefiting from a right), also fall within the scope of those exemptions.

The re-use of data actually anonymised is presumed not to create any further infringement of privacy in the light of the protection afforded by Article 82 of the Data Protection Act. It follows that where personal data are collected for an initial purpose – whether it is subject to the consent of the data subjects or exempted – their re-use does not require consent provided that they have been effectively anonymised beforehand. The GDPR remains applicable to the anonymisation processing itself.

4. Information and consent

Consent must be obtained under the conditions set out in article 2 of the guidelines[6] and article 2 of the recommendation[7] 'cookies and other trackers', subject to the specific recommendations set out below, which take account of the technological and operational specificities of the pixel environment.

4.1 Information on the purposes of trackers

In addition to the other information necessary to obtain informed consent (identity of data controllers, categories of data, etc.), it follows from the applicable texts, as interpreted by the case-law, that the purposes of trackers must be presented to the recipients before giving them the opportunity to consent or refuse: they must be formulated in an intelligible manner, in

[6] Deliberation No 2020-091 of 17 September 2020 adopting guidelines on the application of Article 82 of the amended Law of 6 January 1978 to reading and writing operations in a user's terminal (in particular 'cookies and other trackers') and repealing Deliberation No 2019-093 of 4 July 2019 Available here: https://www.cnil.fr/sites/cnil/files/atoms/files/lines_directors_de_la_cnil_sur_les_cookies_et_other_traceurs.pdf.

[7] Deliberation No 2020-092 of 17 September 2020 adopting a recommendation proposing practical arrangements for compliance in the event of the use of 'cookies and other trackers'. Available here: https://www.cnil.fr/sites/cnil/files/atoms/files/recommendation-cookies-and-other-tracers.pdf.

appropriate language and sufficiently clear to enable the persons concerned to understand precisely the scope of their choice.

The CNIL recommends that each purpose be highlighted in a short title and that it be accompanied by a brief description. Examples of how to comply with the applicable rules are given below:

- **Analysis of the email opening rate for deliverability purposes:** *[Name of the sender of the emails] and [third party companies] use trackers (tracking pixels) to find out if and when you open the emails in order to compile diffusion statistics and take the necessary actions (adaptation of the frequency or stop mailings) to manage the mailing lists.*

- **Analysis of the email opening rate to measure and optimise campaign performance:** *[Name of the email sender] and [third-party companies] use trackers (tracking pixels) to find out whether you open the emails, the time at which you do so, and information about the device you use to personalise the content of the messages, adjust the sending frequency or the communication channel used.*

- **Creation of recipient profiles based on observed preferences and interests in order to target you in contexts other than emails:** *[Name of email sender] and [third-party companies] use your preferences (e.g. emails you have opened or topics you are interested in) to provide you with tailored content or advertisements on other sites, applications or communication channels. These trackers allow us to know if you open the emails, the time at which you do so and to obtain information about the terminal you are using.*

- **Detection and analysis of suspected fraud:** *[Name of email sender] and [third party companies] use trackers (tracking pixels) to detect and analyse suspected fraud. These trackers allow us to know if you open the emails, the time at which you do so and to obtain information about the terminal you are using.*

The CNIL also recommends that the detailed description of these purposes be included in a way that is easily accessible from the consent collection interface. This information can, for example, be displayed under a expand button that the user can activate directly at the first level of information. It can also be made available by clicking on a hyperlink at the first level of information.

Finally, while Article 82 of the Data Protection Act does not require individuals to be informed about the use of pixels that do not require their consent, the CNIL recommends, as a good practice, that they be informed of their existence in order to ensure full transparency on those operations. This information can be provided within the privacy policy.

4.2 Practical arrangements for collecting consent

Information on the scope of consent

It follows from the applicable texts, as clarified by the case-law, that the recipient must be aware of the scope of the consent he intends to give. Consequently, the CNIL considers that the information provided must in particular enable the recipient to identify the email address that will be affected by the use of tracking pixels. Similarly, that information must also enable

him to understand that the trackers will be deposited on all the terminals on which he is likely to consult his emails.

Prioritise a collection of consent at the time of collection of the relevant email address

The CNIL recommends that consent to the use of tracking pixels in emails be collected at the time of collection of the email address concerned. Indeed, by informing the user when providing his email address, the controller can, on this occasion, specify in an intelligible way that trackers may be inserted in the emails that will be sent to the address provided, in particular those that require valid consent. The direct link between the email address collected and the subsequent use of trackers is thus explicit and strengthens the user's understanding of the scope of his consent.

Concretely, the CNIL therefore recommends integrating, at the level of the email collection form, the information necessary to collect informed consent, including summary information on the purposes of trackers (see point 4.1) with a link to more detailed information (for example, the 'cookies and other trackers' policy).

Collect consent later via a link embedded in an email without a tracking pixel

Where the collection of consent cannot be carried out concurrently with the collection of the relevant email address, the controller may seek the consent of the person targeted by the sending of an email message which shall not contain a tracking device subject to consent.

The use of this method of collection is appropriate in the following situations:

- To be able to use pixels subject to consent in emails sent to an email address, where that consent was not collected at the time of collection.
- Where the email address is collected by a third party without providing proof of consent for tracking pixels.
- When the email address is collected under conditions that make it difficult to obtain valid consent for tracking pixels (e.g. when the address is collected orally).

Concretely, the email may include a link to collect the choices of the data subject but it should be avoided that consent is collected involuntarily by an automatic pre-loading of the link by some email clients. To this end, the CNIL recommends, for example, providing that the link redirects to a page on which the person will have to take a positive action (click on a button, etc.) to confirm their consent, similar to the mechanisms used for unsubscribe links.

The CNIL recommends the use of a tracking link in order to allow the sole holder of the email address to express his consent.

Tracking links used to participate in the security of the user may be exempted from consent within the meaning of Article 82 of the Data Protection Act'.

As recalled in EDPB Guidelines 2/2023, the use of tracking links is subject to Article 5.3 of the ePrivacy Directive, transposed into national law by Article 82 of the Data Protection Act.

However, the use of a single link per recipient limits the use of a functionality (in this case the expression of choices) to the intended user only and avoids abusive access to that functionality. Consequently, in so far as those tracking links contribute to the protection of the recipient against unauthenticated access to features reserved for them, that use corresponds to a security measure **linked to user authentication** and is exempted from consent, since the trackers are strictly necessary for the service requested by the user.

Where consent to the use of tracking pixels is requested by sending an email containing a link to a consent collection interface, such solicitation must not be designed in such a way as to exercise disproportionate pressure on the data subjects with a view to inducing them to consent, in particular by preventing or hindering the reading of emails.

Since consent must result from a positive act, the recipient's inactivity must be analysed as an expression of a refusal to consent to the use of tracking pixels.

The CNIL recommends that the recipient be offered the possibility of explicitly refusing tracking pixels, as simple as accepting them, and that the recipient's choices be recorded so that he or she is no longer solicited in subsequent emails for a certain period of time. The absence of solicitation for a period of 6 months is a good practice on the part of publishers.

Expression of free consent

Consent can only be valid if the recipients are able to freely exercise their choice.

The simultaneous collection of a single consent for several processing operations serving different purposes (purpose coupling), without the possibility to accept or refuse purpose by purpose, is likely to affect, in certain cases, the freedom of choice and thus the validity of the consent (recital 43 GDPR).

Therefore, in order to ensure the free nature of the consent given, the CNIL recommends asking recipients for their consent independently and specifically for each separate purpose. However, where the means of collecting consent has two levels of information, it is possible to obtain overall consent at the first level of information only if the user is able, at the second level, to give consent by purpose, or by family of purposes where these are related.

It is possible to obtain a single consent – thus without offering the recipient the possibility to choose granularly on the second level of information – for direct commercial marketing by

electronic means (in accordance with Article 34-5 of the Postal and Electronic Communications Code (CPCE)) and for the use of tracking pixels in commercial prospecting emails for related purposes. By way of example:

- Where direct marketing is expressly presented as personalised, consent to such marketing and the use of tracking pixels directly contributing to such personalisation (e.g. for personalising content or adapting the sending frequency) may be covered by a single consent.

- A single consent may be given for direct marketing by electronic means and the use of tracking pixels to combat fraudulent registration in an email contest, in order to ensure a level playing field for participants by excluding participants who would use automated solutions to register multiple times.

In the event that the reading or writing operations pursue separate and non-related purposes (see point 4.1), consent must be obtained independently and specifically for each of them.

The CNIL points out that advertising – personalised or contextual – displayed in online advertising banners (also known as display advertising) and commercial prospecting are two separate purposes. Users must therefore have the possibility to consent independently and specifically to these two purposes.

Attention point

The consent regime for tracking pixels is independent of that applicable to the sending of the email in question: thus consent for tracking pixels may be necessary for emails that do not, in principle, require the consent of the recipients (confirmation of an order, marketing for similar products or services provided by the same company to its customers, charity marketing, prospecting for professionals related to the profession of the person being marketed, etc.).

Collecting consent to pixels via a consent *management platform* (CMP)

Today, CMPs are identified by the public as tools to collect choices about trackers placed on the web or within mobile applications.

In addition, the collection of consent to pixels takes place, in certain cases, in a decorrelated manner from the collection of the email address.

The use of a CMP to collect consent for the insertion of pixels in emails therefore requires particular attention. The 'informed' nature of consent presupposes, in particular, that the person easily understands the scope of his or her consent, in particular that his or her choice also concerns transactions carried out in connection with an (email) environment distinct from that in which he or she expresses his or her consent (web or mobile application) and the email address which would ultimately be affected by those choices.

5. Withdrawal and management of consent

It follows from the applicable texts, as clarified by the case-law, that persons who have given their consent to the use of trackers must be able to withdraw it at any time. It must also be as simple to withdraw consent as it is to give it.

In the context of the use of tracking pixels in emails, the CNIL recommends that the possibility of withdrawing consent be offered by a tracked link in the footer of each email. The controller must implement appropriate technical measures to allow easy withdrawal of consent. In the event that the link directs the user to a web page, it should allow the withdrawal of the consent(s) granted without further action (including without having to enter the relevant email address in a form).

The use of a single link per recipient makes it possible to limit the use of that functionality to the sole recipient targeted by the withdrawal tool and thus to avoid abusive access to that functionality while respecting the criterion of ease of withdrawal of consent.

Therefore, as recalled in the box above ('Tracking *links used to participate in the user's security may be exempted from consent, within the meaning of Article 82 of the Data Protection Act'),* such use corresponds to a security measure for the benefit of the user and is exempted from consent since trackers are then strictly necessary for the service requested by the user, in accordance with Article 82 of the Data Protection Act.

The controller must ensure that the withdrawal of consent is effective: the reading or writing operations concerned by this withdrawal can no longer take place when future emails are sent. As regards emails already sent, given the specific technical context, it may be necessary to put in place solutions to ensure that previously used trackers are not exploited (in particular when the recipient reopens the email) in order for the withdrawal of consent to be effective.

6. Proof of Consent

The controller must be able to demonstrate, at any time, that the users have given their consent (Article 7.1 of the GDPR).

In principle, the mechanisms implemented by the actors must make it possible to keep evidence of consent in an individualised manner, that is to say, a record of each person's consent, as well as the conditions under which that consent was obtained.

In certain situations, the controller does not itself collect the consent of the data subjects. This is the case, in particular, where the data are transmitted by a third party who is also responsible for collecting consent in his or her name and on his or her behalf. The obligation to provide proof of consent cannot be fulfilled by the mere presence of a contractual clause requiring one of the parties to obtain valid consent on behalf of the other party. Such a clause does not enable the body to guarantee, in all circumstances, the existence of valid consent.

The contract may, however, be used to oversee:

- the mechanisms put in place to demonstrate the collection of valid consent;

- the availability of evidence for the benefit of the body wishing to rely on the consent;
- where appropriate, the conditions under which that evidence must be retained, in particular in order to preserve its probative value;
- arrangements for the regular audit of consent-gathering mechanisms.

These contractual commitments do not exempt the controller from liability if it is unable to provide evidence of consent due to the failure of the third party.

7. Application of the CNIL's recommendation

The recommendation clarifies the scope of the provisions applicable to this type of reading or writing operations.

In those circumstances, as regards the email addresses already collected, the reading or writing operations may continue to be carried out, provided that clear and accessible information is sent to the recipients within a period which may not, in principle, exceed 3 months from the publication of the recommendation.
That information must enable those recipients, in the event that their consent has not been obtained in accordance with the detailed rules set out in this recommendation, to be put in a position to oppose such operations for future emails.

However, where the controller is required to seek a new consent for the use of the email address (e.g. for the transmission of data to new controllers for the purpose of electronic prospecting), it will need to obtain a valid consent for the implementation of reading or writing operations that are not exempted.