Recommendation on tracking pixels in electronic mail

Suppliers and providers of the "pixel" ecosystem: how to implement the CNIL recommendation?

Webinar of 4 June 2026

Speakers:

- Alice Darmon, lawyer with the Digital Economy and Financial Sector Department.
- Benjamin Poilvé, engineer with the Technological Expertise Department.

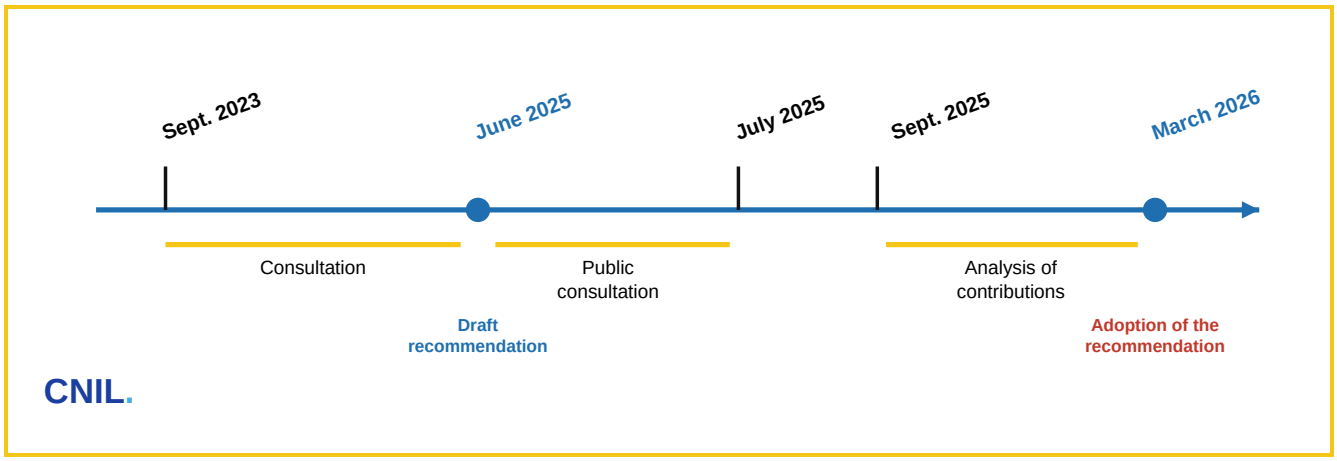
Introduction & context:

Purpose of the webinar:

This webinar complements a previous webinar held on 28 May 2026. Unlike the first, this one focuses on the implications of the recommendation for solution providers. The subject is therefore approached from a more technical angle.

Historical background:

The recommendation is the result of work that began in September 2023 and unfolded in two phases: an initial consultation phase, followed by a public consultation phase. These phases enabled the CNIL to engage with numerous stakeholders (professional associations, civil society actors) and to better understand the issues, including technical ones, related to the use of pixels. This work led to the publication of a draft recommendation, then a final version adopted by the CNIL in March 2026 and published in the Official Journal on 14 April 2026.



Reminder of the issues at stake

Even today, few people are aware that opening a simple email can generate the collection of information about them, since pixels are generally barely visible. The aim of the recommendation is therefore to enable individuals to understand and control how their data is used. This is all the more essential given that pixels are used in the email environment, a confidential environment in which people have high expectations regarding respect for their privacy, knowing that pixels are also fairly often associated with advertising uses. For all these reasons, the CNIL, which had also received a significant number of complaints from 2020 onwards, decided to work on the subject of pixels in order to clarify the legal context.

- Particular issues arise in the **context of an email service**, a personal space intended for the consultation of private content, accessible after an authentication procedure.
- Barely visible mechanisms lead to the **collection of data without people's knowledge**, leaving them unable to understand or control how their data is used.
- Pixels are frequently associated with **advertising uses involving behavioural analysis** (feeding a profile, more relevant targeting based on email send times / more enticing subject lines / adaptation of emails / targeted advertising).

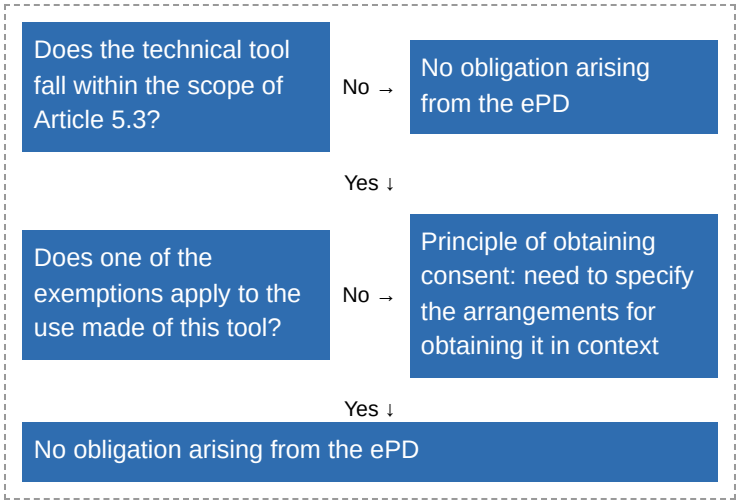
CNIL.

Legal context

The recommendation clarifies the arrangements for applying Article 82 of the French Data Protection Act (Loi Informatique et Libertés) to tracking pixels in electronic mail. This article stems from the transposition into French law of Article 5.3 of the ePrivacy Directive. The fact that pixel technology falls within the scope of this text was confirmed at European level by the European Data Protection Board (EDPB) in its guidelines. As a reminder, Article 82 of the Data Protection Act concerns only read and write operations and sets out, as a principle, the requirement of prior consent to these operations, save in two cases falling within the scope of the exemptions.

The recommendation on pixels is in line with the work previously published by the CNIL on cookies and other trackers, and supplements the recommendation and guidelines on cookies and other trackers.

Article 5.3 of the ePrivacy Directive (ePD) transposed into Article 82 of the Data Protection Act:



Guidelines on the technical scope of Article 5, paragraph 3 (2024)
Analyse the various technologies that may be concerned by this obligation, notably tracking pixels.

Guidelines and recommendations on "cookies and other trackers" (2020)
Explain how to comply with the read/write obligations on the user's terminal in the general case.

Guidelines on tracking pixels (2026)
Builds on the pre-existing texts and specifies their application in a particular context (emails) and for a particular technology (pixels).

CNIL.

What is not in the recommendation (two subjects are not addressed):

- The subject of other tracking methods, including tracking links.
- The subject of proof of consent is not addressed specifically in the recommendation on pixels, as the CNIL is currently carrying out work on this question.

✗ What is not in the "pixels" recommendation

The use of other tracking methods (tracking links, unique identifiers, etc.), whether or not used within emails

- *The need to collect consent depends on the purpose and not on the technology.*
- *Thus, reading the "cookies and other trackers" and "pixels" recommendations together should enable controllers to analyse their practices without a need being identified to publish specific documents at this stage.*

Proof of consent in general

- *The recommendation restates the principle.*
- *The CNIL's departments are currently carrying out work on this question to clarify the obligations arising from the texts.*

CNIL.

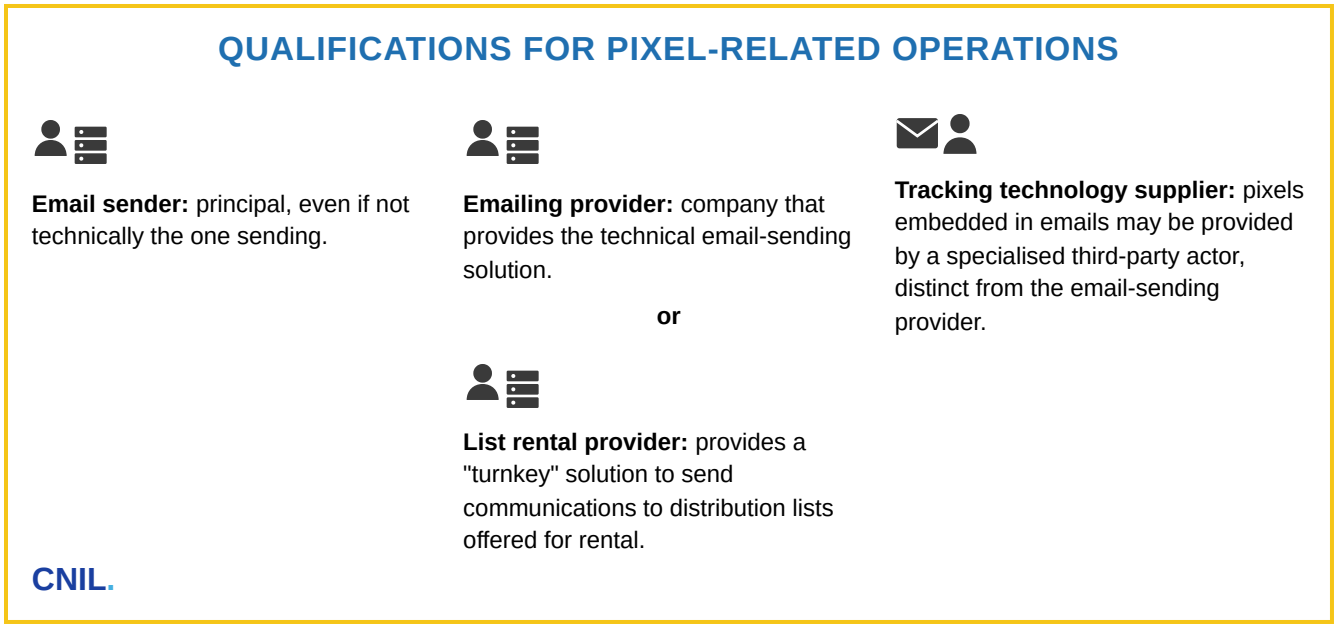
Why a supplier webinar?

The recommendation identifies several actors with responsibilities regarding pixel operations: the sender of the email, the emailing provider, the list rental provider (which, in addition to handling sends, rents out its distribution lists), and the tracking technology supplier.

Qualifications for pixel-related operations

As regards qualification in relation to pixel operations, the recommendation adopts **two schemes.**

1. The provider (solution supplier) does not use the pixel on its own behalf. It carries out the read and write operations exclusively on behalf of the email sender and under its instructions. In this scheme, the provider has the status of processor and the sender that of controller.



2. The solution supplier also uses the pixel, and therefore the data collected through this technology, for its own purposes (for example, improving its solution). In this case, the provider that uses the pixel with the contractual agreement of its client for its own purposes has the status of joint controller with the sender for the read/write operation. The parties (sender and provider) must then allocate and define their respective obligations in a contract, in accordance with Article 26 of the GDPR. The provider will in particular be obliged to be able to demonstrate that consent was validly obtained on its behalf for the use of the pixel, if the purpose of the pixel requires consent.

QUALIFICATIONS FOR PIXEL-RELATED OPERATIONS

Email sender: **Controller**

Emailing provider: **Processor**

or

List rental provider: **Processor (in principle)**

Tracking technology supplier: **Processor (in principle)**

CNIL.

JOINT CONTROLLERSHIP

Emailing provider

or

List rental provider

Joint controllership over the read/write operation

CNIL.

Where the data collected via the pixel is also used for the provider's own purposes, the sender who contractually accepts these processing operations is a **joint controller for the data collection operations** (namely, the read/write operations on information).

However, this **joint controllership does not necessarily extend to subsequent processing** resulting from that collection, for which the supplier and publisher may be separate controllers.

Point of attention

Where the supplier has the status of processor, it retains responsibilities under the regulations. Its obligations are listed in Article 28 of the GDPR and, in the event of a breach, its liability may be engaged. Among these obligations is that of ensuring that it offers its clients the necessary guarantees so that the processing

carried out on their behalf complies with the regulations. This means in particular that, from the design stage, the tools offered must effectively incorporate the principles relating to data protection (privacy by design). A supplier that makes available a non-compliant tool, in addition to failing in its own obligations, exposes its clients to potential penalties, since the latter, as controllers, must also comply with obligations. Making available a non-compliant tool may also constitute grounds for invalidity of the contract binding the supplier to its clients.

POINT OF ATTENTION

A solution that does not enable its clients to achieve compliance puts them in difficulty:

- In the absence of an adequate software solution, it may be impossible for a client to use a solution while remaining compliant.
- The company's clients are then liable to be held responsible for non-compliance with the applicable legislation.
- The compliance of the service with the GDPR/ePD may constitute an **essential quality of the contract justifying its rescission.**

CNIL.

The measures presented below are functionalities suggested by the CNIL. They are not exhaustive and depend on the business expertise of each supplier as well as on the functionalities offered to clients. They should be regarded as a working basis for identifying the relevant measures.

The table below makes it possible to identify the various measures according to the functionalities offered by the supplier.

MEASURES

	Sending emails to distribution lists	Embedding pixels within sent emails	Management of distribution bases
Differentiated management of recipients within lists	✓		✓
Advanced management of distribution lists based on a consent signal	(✓)		(✓)
Identification of purposes		✓	
Analysis of the applicability of the consent exemption		(✓)	
Provision of a collection interface and consent functionalities		(✓)	✓
Consent-withdrawal functionality		(✓)	✓
Transition functionality for bases already collected			(✓)

✓: necessary (✓): optional

CNIL.

• So that your clients can meet their obligations, **the CNIL recommends offering certain functionalities.**

• These functionalities are not exhaustive and **depend on the services you offer to your clients.** Alternative functionalities could also enable them to meet their obligations.

Measure: Differentiated management

Explanation of why these measures are necessary or useful for clients' compliance:

- Differentiated management of bases: if clients use pixels subject to consent, it is essential to have, within a distribution list, a signal enabling the consent status of each recipient to be distinguished. Indeed, within a single distribution list, some people will have consented and others not. As consent must be freely given, it is necessary to retain at least a binary signal (consented / not consented) within the bases managed for clients. Without this signal, it is impossible for clients to be compliant, because they will not know whether the person has consented or not. Moreover, certain subsequent technical measures, such as the generation of differentiated

templates depending on consent status, depend on the existence of this signal. It is therefore the very first step towards compliance.

MEASURE: DIFFERENTIATED MANAGEMENT

• If your clients use pixels subject to consent, **it is essential that they can, within a single distribution list, distinguish the consent status.**

• To this end, adding a binary field storing this information, usable by the client via an API and the use of different templates, constitutes a **minimal technical measure** enabling compliance.

• It remains, however, very limited: **it can only work where consent relates to a single purpose.**

CNIL.

Email	Consent	Consent date	Attribute
prospect81@...	True	12/05/2026	...
client22@...	False	15/05/2026	...
prospect700@...	True	18/05/2026	...
client20@...	True	18/05/2026	...

Doctrine: Purpose

However, this step remains limited. A point of doctrine on the notion of purpose helps to understand why.

The notion of purpose is at the heart of obtaining consent under Article 82 of the Data Protection Act. Indeed, when obtaining consent, it is necessary to inform the person of the purposes pursued and, where applicable, to offer them the possibility of consenting in a granular manner. Moreover, the purpose makes it possible to determine whether consent is necessary or not: Article 82 does not provide for systematic consent, since certain situations benefit from an exemption. In its recommendation, the CNIL identified a number of purposes, with a level of precision aimed both at usefully informing individuals and at avoiding overloading them with an excessive number of purposes. Among the purposes subject to consent, the CNIL identified in particular: analysing the email open rate to measure and optimise campaign performance, as well as creating recipient profiles based on their preferences and interests in order to target them in other contexts. The difference between these two purposes lies in the fact that, in one case, targeting takes place within the emails and, in the other, in other contexts (typically on the web). As regards purposes that may benefit from an exemption, the CNIL identified: the detection and analysis of suspected fraud, as well as the implementation of security measures contributing to user authentication. On this last point, in accordance with the EDPB's work, security measures may be exempted where they are "user centric", that is to say where they directly benefit the user. Thus, the use of pixels to protect user authentication (for example, in the context of password-update functionalities) may be exempted. By contrast, functionalities that do not benefit the user but aim to protect the supplier

of services cannot be exempted. Lastly, the individual measurement of the open rate for deliverability purposes is subject to differentiated treatment depending on whether or not the criteria presented by the CNIL are met.

DOCTRINE: PURPOSES

- The notion of purpose is at the heart of obtaining consent under Article 82 of the Data Protection Act:
  - On the one hand, it makes it possible to determine whether consent is necessary.
  - On the other hand, it affects the obtaining of consent itself.

Analysing the email open rate to measure and optimise campaign performance by personalising the content of messages or adapting the frequency or channel of communication.

Creating recipient profiles based on preferences and interests shown, in order to target them in other contexts (on websites, mobile applications or via other communication channels).

Detecting and analysing suspected fraud, such as identifying unusual or mass email opens likely to indicate automated behaviour (for example, mass sign-ups to a prize draw, attempted data exfiltration, etc.).

Individual measurement of the email open rate for deliverability purposes where carried out outside the cases covered by point 3.2 of this recommendation.

Implementing security measures contributing to user authentication. In this context, the use of the tracking pixel pursues the sole purpose of contributing to the securing of an authentication (user-centric).

Individual measurement of the email open rate for deliverability purposes. Subject to compliance with a number of criteria (see next slide).

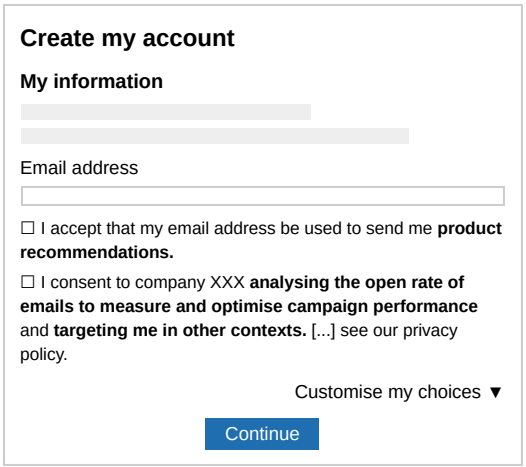
Requiring consent | **Exempt from consent for certain emails**

CNIL.

It is important to understand that determining the purposes is essential when obtaining consent. On the one hand, it makes it possible to know whether consent is necessary. On the other hand, it determines the interface presented to the person: depending on the purposes actually pursued, the text presented to the user must describe them from the first level of consent collection. Consequently, the binary signal is often insufficient where the client pursues more than one purpose, because it does not make it possible to reflect all the granularity needed around consent.

Analysing the open rate to measure and optimise campaign performance by personalising content or adapting the send frequency / communication channel.

Creating recipient profiles based on preferences and interests in order to target them in other contexts (websites, mobile apps or other channels).



CNIL.

In this respect, one suggested measure is the management of a consent signal (by analogy with what exists in the context of cookies on the web). This involves having a more expressive piece of data enabling the consent of individuals to be stored in its granularity. This signal is only truly useful for clients if the supplier offers an interface enabling its exploitation and the generation of dynamic templates, so as to allow clients to interface easily with the tools offered. This is an important measure to consider.

• Where your clients use pixels pursuing several purposes, it is recommended **to enable the storage of a consent signal.**

• This signal should be accessible to the client via an API and enable the generation of dynamic templates so as to allow the client to **interface easily with third-party tools.**

CNIL.

Email	Consent signal	Signal date
prospect81@...	{"advert_mail":false,"deliverability":true,"security":true}	12/05/2026
client22@...	{"advert_mail":true,"deliverability":true,"security":true}	13/05/2026
prospect700@...	{"advert_mail":false,"deliverability":false,"security":false}	18/05/2026
client20@...	{"advert_mail":false,"deliverability":true,"security":true}	18/05/2026

Another measure concerns the situation where the supplier offers pixels to its clients, whether as a provider specialising in pixels or as a sending provider offering this functionality in its catalogue of offers. In this case, it is important to make available to clients all the information enabling them to identify the purposes pursued by these pixels. Clients must have this information in order to be able to implement their own compliance. Failing this, they will not be able to use the solution lawfully. In particular, if the supplier pursues purposes of its own, it must discuss the potential joint controllership with its clients so that this is clearly identified and understood by all parties.

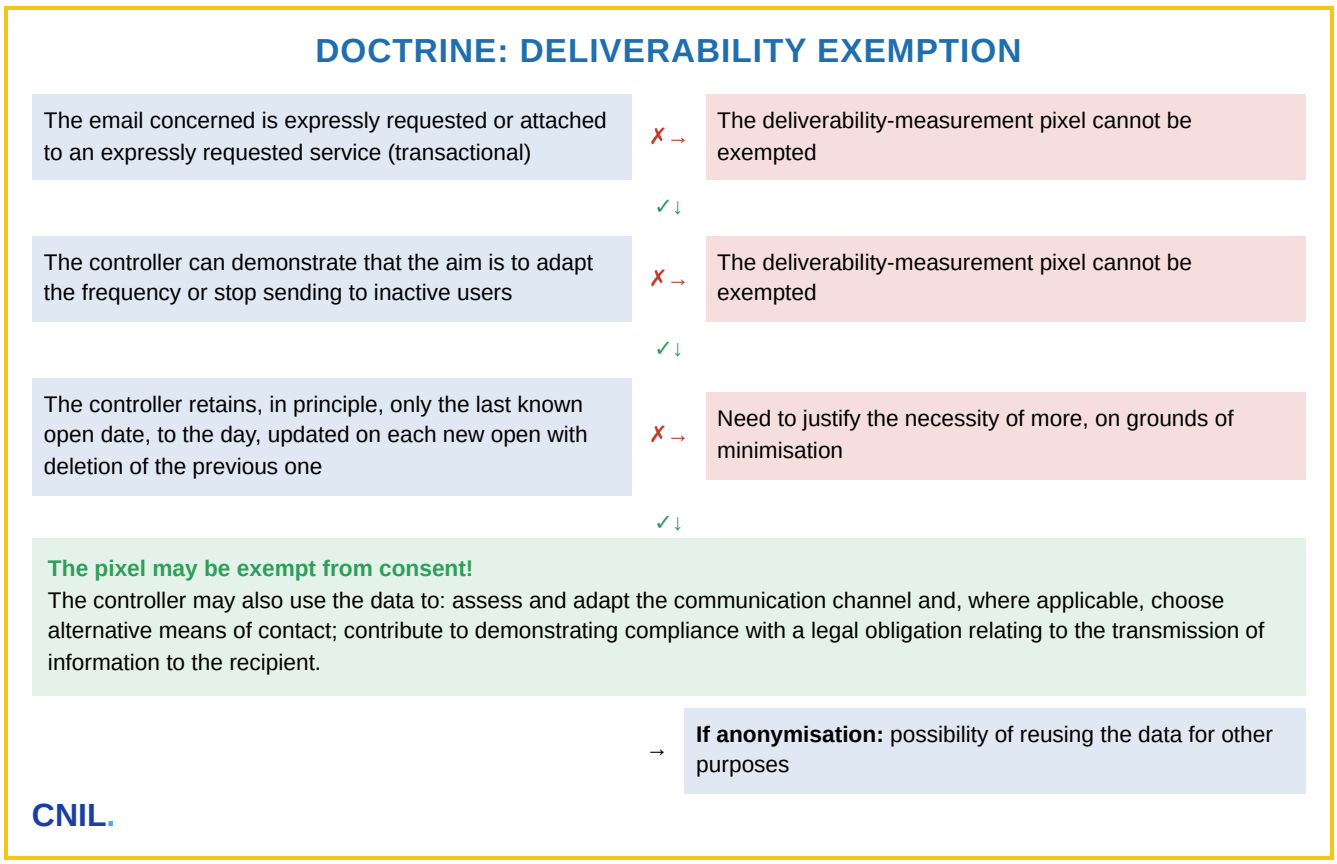
A particular case of this identification of purposes concerns the conditions under which pixels may be implemented without consent for deliverability purposes. The CNIL's recommendation identifies these conditions. If the supplier considers that certain of its functionalities fall within this framework, it must make available to the controller (its client) the information enabling it to corroborate this analysis. The client cannot rely solely on the supplier's declaration, because compliance also concerns it and it is required to carry out its own verification.

Doctrine: Deliverability exemption

To benefit from the deliverability exemption, several conditions must be met. First, the email concerned must be **expressly requested or attached to an expressly requested service.** This criterion does not concern the provider as such, but the sender of the email. Failing to meet this condition, the deliverability-measurement pixel cannot be exempted, whatever its technical characteristics. Next, the controller must be able to demonstrate that the aim is to **adapt the send frequency or to stop sending to inactive users.** This is the primary criterion: this exemption is only possible insofar as it benefits users by limiting sending pressure. If this condition is met, the implementation arrangements recommended by the CNIL are as follows: retention only of the last known open date, to the day, updated on each new open with deletion of the previous one. The aim is to minimise the data collected to what is strictly necessary to pursue this purpose.

Once this step has been completed, the data may also be used to assess and adapt the communication channel and, where applicable, to choose alternative means of contact, as well as to demonstrate compliance with any legal obligations.

By contrast, the data must not be reused for other purposes. If the supplier offers technical means enabling its clients to implement this exemption, it must provide the elements enabling the client to satisfy each of the steps of this analysis.



Point of attention:

The application of the exemption depends on the type of email sent and not solely on the characteristics of the pixel. In this respect, the CNIL advises suppliers against telling their clients that their pixels are "always exempt". The appropriate wording is as follows: the pixels offered may be exempted insofar as the emails sent by clients are eligible for the deliverability exemption. This concerns expressly requested emails and transactional emails. By contrast, emails sent as part of commercial canvassing not subject to consent cannot benefit from this exemption.

✓ Emails eligible for the deliverability exemption

Expressly requested emails:

- Newsletters sent upon the user's sign-up
- Prospecting emails sent with the user's consent

Transactional emails:

- Welcome emails
- Notification emails linked to events such as parcel shipment, purchase invoices

To the extent that it is attached to a requested service

✗ Emails not eligible for the deliverability exemption

- Email sent as part of commercial canvassing not subject to consent, because not expressly requested (B2B or similar products or services).

Second point of attention:

The notion of cleaning the bases. The aim of the pixel must be, for clients, to maintain the deliverability score and to avoid excessive pressure on recipients. This entails reducing the send frequency or removing inactive users. **In the event of a CNIL inspection, clients would be asked to provide elements demonstrating that they are actually pursuing this purpose, notably: the logic for deleting or reducing sends based on opens, the deletion rate of recipients from the base**, etc.

To offer greater legal certainty to clients, suppliers offering these functionalities may make available to them data enabling them to demonstrate compliance with the applicable framework in the event of an inspection, which will facilitate their compliance.

Measure: Provision of a collection interface

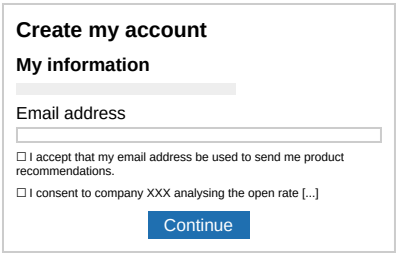
As regards consent-collection interfaces, the CNIL considered that the information provided must in particular enable the recipient to identify the email address concerned by the use of pixels. The CNIL favours obtaining consent for the pixel at the time the email address is collected, by means of a form. This form must enable the person to benefit from a concise description of the purposes of the pixel. If consent was not obtained at the time the email address was collected, it is possible to request it later, in a decorrelated manner, by means of a link embedded in an email sent specifically for that purpose. As regards the

presentation of the consent-collection interface, the CNIL restates in the recommendation the principle of freely given consent, which entails obtaining distinct consent for each purpose.

- If you wish, you can offer your clients **consent-collection functionalities**, or templates to embed.
- In particular, obtaining consent later than the collection of the email address **can be done within an email.**
- Attention, where you offer these functionalities, bear in mind the associated obligations, notably in terms of proof of consent.

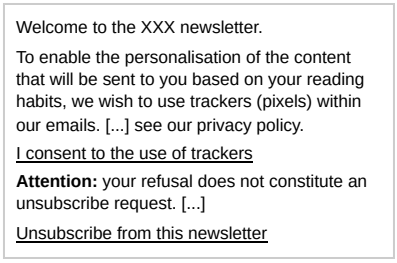
CNIL.

At the time the email address is collected:
Recommended



✓ Easy for the person to understand the address concerned
✓ Interactive interface, easy to implement

Later, via a link in an email:
Possible for later collection



✓ Easy for the person to understand the address concerned
✗ Requires sending an email without a pixel
✗ Requires visiting a page to express one's choice

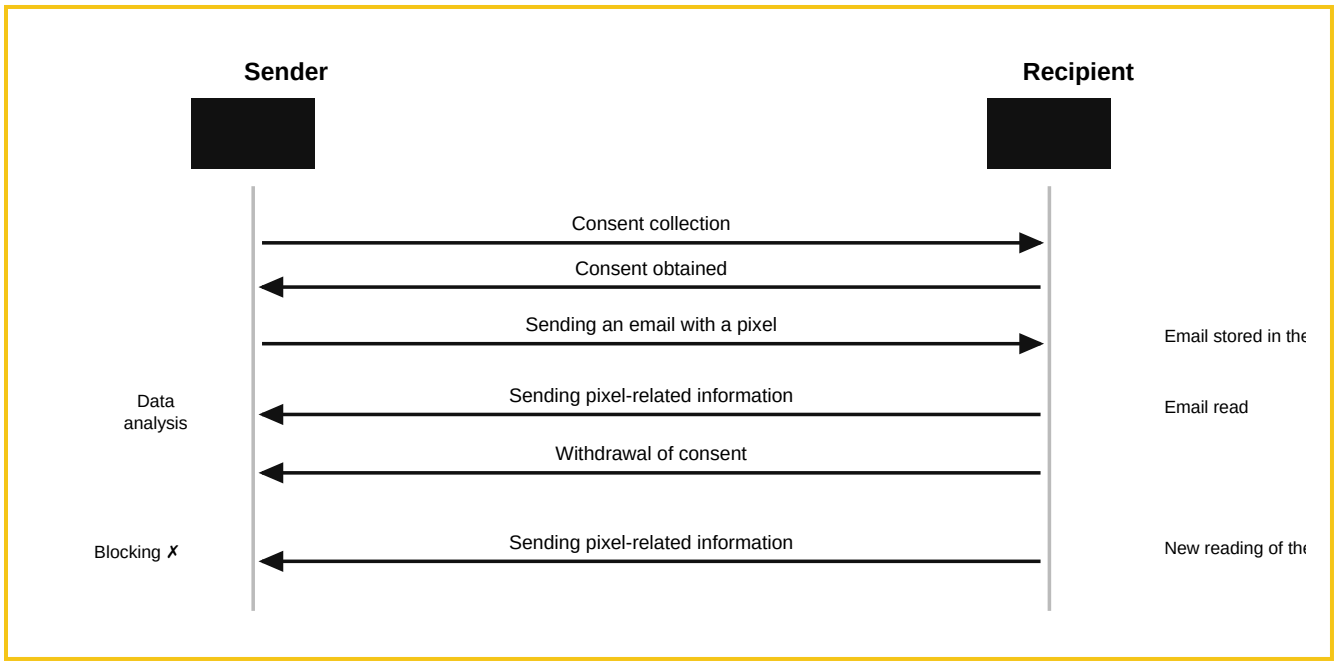
Single consent

However, where the purposes are connected, the recommendation mentions the possibility of obtaining a single consent. Two examples are provided by the CNIL, both concerning the sending of commercial prospecting emails.

One of these examples concerns the **sending of prospecting by email presented as personalised and incorporating a personalisation pixel.** Specifically, in the case of a personalised newsletter sent on a subscription basis (with the person's consent), if the information enables the person to understand that the personalised newsletter incorporates a personalisation pixel, then subscribing constitutes consent for the pixel. The two are linked, which means that a person who does not want pixels in their email does not subscribe and does not receive the email. This is a single consent justified by the connectedness of the purposes. In the absence of connectedness, it is necessary to collect consent for each purpose. For example, in the case of a multi-purpose pixel pursuing several distinct purposes, consent must be obtained for each purpose, which translates into as many checkboxes on the collection interface. However, to facilitate the user journey, the recommendation provides that, if the consent-collection form has two levels of information, it is possible to provide on the first level a single checkbox for consent to pixels (global consent covering all purposes), provided that the user then has the possibility of making a granular choice on a second level of information.

Measure: Consent-withdrawal functionality

Suppliers offering differentiated list-management tools, in which the consent status of individuals is maintained, are intended to make available to their clients functionalities enabling the withdrawal of consent. This functionality is very close to the unsubscribe functionality already offered by most email-sending solution providers. The CNIL recommends embedding a link in the email footer enabling access to a consent-withdrawal page. When withdrawal is exercised, pixels must no longer be included in emails sent thereafter. The use of an intermediate withdrawal page is conceivable and makes it possible to prevent the link from being automatically triggered by certain email clients that scan all the links contained in an email. This intermediate page must not, however, be excessively burdensome for the person, since the withdrawal of consent must remain easy. Moreover, it is acknowledged that it is impossible to delete the trackers contained in emails already sent. When a person who previously consented withdraws their consent, it is not required to delete the emails already present in their inbox. The essential point is to ensure the absence of exploitation of the old pixels. Specifically, if a person who has withdrawn their consent reopens an old email containing a pixel, the HTTP request received by the server must be ignored (dropped) and no processing must be carried out on the data. This approach is considered an acceptable respect for the withdrawal of consent, without it being necessary to go further in terms of technical measures.



Doctrine: Arrangements for applying the recommendations

The recommendation was published in the Official Journal on 14 April 2026, the date corresponding to its entry into application. From that date, a distinction should be drawn between two regimes depending on whether the email addresses were collected before or after publication.

For addresses collected after entry into application, the principle of prior consent applies, save exemption, and this from the publication of the recommendation. By contrast, for addresses collected before publication, a transitional regime applies: the sender must inform the persons concerned and offer them the possibility of exercising a right to object within a period of three months, unless it is necessary to obtain the person's consent for the sending of the email itself.

As regards the regime applicable to bases already constituted, three points of attention are identified for suppliers wishing to offer a functionality for transitioning existing bases. The first point concerns the three-month period, upon the expiry of which the persons must have been informed. However, if the sender demonstrates the need to space out sends owing to volume-related constraints, it may, provided it has documented this, benefit from a limited tolerance permitting a slight overrun of this period.

Addresses collected before publication

- Information + objection
- Three-month period
- Unless it is necessary to obtain consent for the sending of the email

Addresses collected after publication

- Consent, save applicable exemptions
- Applicable from publication of the recommendation

Publication of the recommendation

Measure: Transition functionality for existing bases

As regards the form of the information, it may take the form either of a dedicated email, it being specified that only proof of sending will be required, or of information embedded in another email, for example in an inset. In the latter case, particular attention must be paid to the accessible, clear and comprehensible nature of the information for the recipient.

Lastly, the objection concerns only future read and write operations. In the absence of objection from the person, the sender may continue to use pixels in its emails. In the event of objection, the sender may no longer, going forward, include pixels in emails addressed to the person concerned. However, no obligation

to delete previously collected data is imposed on the sender, subject to compliance with the principle of limiting the data retention period.

• If you wish, it is possible to assist your clients during the transition period provided for by the CNIL (before 14/07/2026) **to enable the continued use of pixels for addresses already collected without formal consent.**

Three-month period

- Period upon the expiry of which persons must have been informed.
- If the sender proves the need to space out sends in view of the send volume and the resulting deliverability constraints: a (limited) tolerance will be granted.

Form of the information

- Either a dedicated email, it being specified that proof of sending will be required.
- Or information embedded in an email (e.g. an inset), but in that case the information remains accessible, clear and comprehensible.

In the event of objection

- No further insertion of pixels in emails.
- No obligation to delete previously collected data (via pixels in emails sent before publication of the recommendation), subject to compliance with the principle of limiting data retention.

CNIL.

Questions and answers session:

1. Can compliance be expected by the end of the three-month period? How does the CNIL anticipate, view and anticipate this subject? What is the official deadline?

The three-month period provided for by the recommendation concerns only compliance for bases already constituted, that is to say the email addresses collected before publication of the recommendation. Generally speaking, the recommendation is applicable from its publication in the Official Journal. However, the CNIL is aware that actors need a certain amount of time to achieve compliance and does not intend to carry out immediate inspections on this subject. The three-month period corresponds to the term upon the expiry of which the information emails relating to the possibility of objecting must have been sent to the persons concerned.

2. What if, operationally, compliance cannot be finalised by July?

As indicated above, if the sender encounters difficulties in sending all the emails necessary to permit objection before the expiry of the period, for example owing to the need to stagger sends because of volume, the CNIL may show a certain tolerance. This overrun must not, however, be excessive. If the sender justifies an objective difficulty in strictly complying with the period, the CNIL will show tolerance on this point.

3. Does the CNIL have a description of a preference centre accessible via a single tracking link in the email footer enabling the management of pixel consents, tracking of clicks and unsubscribes?

The CNIL does not intend to be excessively prescriptive about the means implemented. It is entirely conceivable to group within a single interface the management

of unsubscribes from a distribution list and the management of pixel consents. The essential point is that the person concerned must be able to understand clearly how to exercise their rights in a simple manner. In this respect, if the link enabling one to express one's consent preferences is not clearly identifiable in the email, this poses a difficulty. This would be the case, for example, of a link entitled "See my preference centre" without explicit mention of the possibility of expressing one's preferences regarding trackers. Likewise, redirecting to an interface with multiple levels, difficult to grasp and not enabling the person to easily distinguish the different options, would be problematic. By contrast, if the approach simply aims to simplify the user journey through a single interface, the CNIL sees no objection, provided this facilitates the effective exercise of the rights of the persons concerned.

4. Is it more appropriate to use a CMP (Consent Management Platform) rather than another mechanism to collect consent for pixels?

The CMP is indeed mentioned in the recommendation. However, an important point of attention must be highlighted: where consent is collected by means of a CMP, it must be clear to the user which email is concerned by this consent, that is to say which channel is targeted. Now, this poses significant operational difficulties, insofar as it is necessary to have identified this channel in relation to the user before proceeding to collect consent, which proves very difficult in practice in many cases. This is why the CMP is not a modality favoured by the CNIL. The CNIL considers that collecting consent at the time the email address is collected, or by means of an email sent specifically for that purpose, is much more appropriate for ensuring that the persons concerned are adequately informed.

5. Does the CNIL expect suppliers to restate the applicable obligations, collect consents, and clients to validate by checkbox or re-date upon importing contacts or activating pixels?

On the first point, suppliers do indeed have a duty to advise their clients. In this respect, it is for them to advise the client and to restate its obligations under the regulations, of which the collection of consent forms part, provided that the purpose of the pixel requires consent. As regards the second point, the consent of the persons concerned must be collected at the time the email address is collected, by means of a checkbox. Furthermore, the CNIL raised the scenario in which a client has a pre-existing base that it wishes to import into the supplier's tool. In this scenario, the tool did not manage the collection of consent and has no information on the consent status of this base. The question then arises as to whether the client can indicate to the tool that it has validly collected consent. The CNIL considers that, the client being the controller, it can indeed declare that it has collected consent, provided that it is able to prove this in the event of an inspection. However, this situation raises operational issues, notably where the tool offers a consent-withdrawal functionality: it is necessary that this withdrawal relate to the purposes for

which the person had actually consented, so that the interface is consistent with the consent initially given. This means that, at the time of importing the consents, the formalism must be agreed between the parties in order to identify the purposes for which the persons had consented. The CNIL emphasises that this is not impossible, but that it is advisable to ensure, operationally, that the entire chain relating to consent and its possible withdrawal is compliant. Ultimately, if the client declares that it has collected consent in a compliant manner, in its capacity as controller, the supplier, in its capacity as processor, may rely on this declaration.

6. What are the CNIL's recommendations for avoiding having to respond to abusive or unfounded complaints?

Where a pixel benefits from an exemption regime, it may be difficult for the persons concerned to distinguish authorised pixels from those that are not. The CNIL restates that, including for exempt pixels, information must be provided to the persons concerned by means of the privacy policy. As regards the handling of complaints, when the CNIL receives a complaint, it is subject to an investigation. It is within the framework of this investigation that the CNIL verifies whether the recommendation on pixels has been complied with and, where applicable, whether pixels subject to consent were used without the persons' consent or whether the pixels in question benefited from an exemption. There is no a priori identification of a complaint as abusive or unfounded: every complaint received is investigated in accordance with the applicable procedures.

7. Must the term "tracking pixel" necessarily be mentioned in the information notices intended for users?

As soon as a controller uses pixels and carries out data processing in this respect, it is required to mention this in its privacy policy. As regards the terminology used, the CNIL adopted the term "tracking pixel", which it considers the most appropriate. However, the use of other terms is permitted, on condition that they are not liable to mislead the user as to the nature of the technology implemented. The CNIL does not impose specific terminology, but encourages the entire ecosystem to agree on a clear and uniform term, so as to enable users to build on their knowledge and to avoid the proliferation of different terms from one actor to another.

8. Must the information email regarding the use of pixels be sent to the entire user base or only to the active base usually contacted?

The information email must be sent to all the persons for whom the sender wishes to continue using pixels. If certain persons will never again receive emails containing pixels, it is not necessary to offer them the possibility of exercising their right to object in this respect. However, the question of retaining these bases may be raised: if the sender no longer intends to send emails to these persons, retaining their data raises questions with regard to the data minimisation principle.

9. Will the recommendation be translated into English?

A translated version of the recommendation in English has already been published on the CNIL's website. It is an unofficial translation, likely to help English-speaking actors grasp the content of the text.

10. Could you define the notion of personalisation?

Personalisation refers to the means aimed at differentiating the emails sent depending on the data collected about the persons concerned. By way of example, where a sender has a client base and wishes to send some of them differentiated product recommendations based on the interests they may have shown through the opening of their emails, this constitutes personalisation.

11. Is the recommendation intended to apply to non-European suppliers?

A non-European supplier that targets users located in the European Union, and more specifically in France, is required to apply the recommendation. Its territorial scope is limited to France: it applies to read and write operations that take place in the receiving terminal of the user located in France.

12. Are there similar rules elsewhere in the world concerning tracking pixels in emails?

Rules have been adopted recently in Italy, by means of guidelines. More generally, throughout Europe, tracking pixels within emails are considered to fall within the scope of the ePrivacy Directive. The related obligations therefore apply in all Member States. The CNIL chose to explain how these obligations should be understood, which it did through its recommendation. However, the absence of similar clarifications from other data protection authorities (as in Italy) does not mean that these obligations do not exist in the other European countries. As recalled in the introduction to the webinar, the fact that pixel technology falls within the scope of the ePrivacy Directive was confirmed at European level by the EDPB.

13. Does subscribing to a newsletter constitute an expressly requested service enabling one to benefit from the consent exemption for pixels?

Yes. Subscribing to a newsletter constitutes a sending expressly requested by the person, based on an opt-in mechanism. In this respect, it falls within the notion of an expressly requested service provided for by the ePrivacy regulations and may benefit from the consent exemption for pixels. By contrast, the issue arises in the context of commercial canvassing not subject to consent for similar products or services: in that scenario, the sending is not expressly requested by the person, so that the exemption is not applicable.

14. What elements of proof does the CNIL expect from an ESP solution supplier?

The question of proof of consent is the subject of ongoing work and will therefore not be dealt with exhaustively in this webinar. However, two situations must be distinguished. First, where consent is collected by means of a form or an email redirecting to a page on which the person expresses their consent, the situation is very close to that which exists for cookies: it is possible to collect basic information such as the timestamp or the page presented. The precise specification of this information forms part of the work currently being carried out by the CNIL. Second, as regards the email sent to the persons figuring in pre-existing bases in order to offer them the possibility of exercising their right to object, only a technical trace of the sending of the email by the sender is expected, that is to say the technical logs attesting that the email was indeed sent. It is not necessary to embed a pixel or any other device in this email to demonstrate that it was read by the person. The mere technical traces relating to the sending suffice to demonstrate compliance with the information obligation for the purposes of objection.

15. Where a client activates the tracking functionality without having first obtained the consent of the persons concerned, does the solution supplier (processor) have an obligation to block the functionality or simply to alert the client?

The solution supplier, in its capacity as processor, has an obligation to alert its client. This obligation falls within the scope of the obligations incumbent on the processor under Article 28 of the GDPR. As regards blocking the functionality, the CNIL has no certainty on this aspect. However, it is advisable to alert the client, indicating that its instructions appear to contravene the applicable obligations, and to ask it for express confirmation attesting that, on its side, it has implemented ancillary means enabling it to meet the obligations provided for by the texts. In this scenario, the controller becomes aware that it assumes full responsibility in the event of a breach.

One of the aims of the webinar is precisely to encourage suppliers to be actors of compliance, insofar as senders expect their providers to make available to them the technical developments necessary for achieving compliance.

16. After a withdrawal of consent, can the previously collected data still be exploited, or only retained?

Since the data was collected with the person's consent, the subsequent withdrawal of that consent has no impact on the processing of the data previously obtained. Consequently, this data may continue to be exploited, subject to compliance with the minimisation principle and the applicable rules on data retention periods.

17. Where a controller holds several email addresses of the same person, is it possible to group the collection of consent or objection within a single interface covering all these addresses, notably for bases constituted before 14 April 2026?

This is not a question they had identified until now.

The essential element is that the person concerned, when expressing their consent or objection, is aware of the channels concerned by the expression of their will.

There is no problem in principle in offering a single interface enabling consent or objection to be collected for all the email addresses held by the controller, provided that the person concerned is clearly informed of the addresses covered by their consent or withdrawal.

By contrast, where the grouping of addresses is carried out heuristically and the person is not certain that all the addresses actually correspond to them, they should be offered the possibility of distinguishing the addresses that concern them from those that do not, so that they can express their consent in an informed manner for each address. In practice, it is important not to prevent a user from expressing their consent in relation to an email address that concerns them on the ground that they do not wish to consent for another address.

18. Is the use of a tracking pixel collecting no personal data permitted? Is it possible to offer clients an anonymous tracking functionality to produce performance indicators (KPIs) (open rate, click rate) without collecting consent?

The ePrivacy regulations are not based on the notion of personal data. The anonymous nature of the data collected has no bearing on the applicability of the obligations. The obligations expressed by the CNIL apply irrespective of the nature of the data collected. Consequently, to offer functionalities without consent, it is necessary to fall within the framework of the exemption as defined by the CNIL.

19. How can the last open date be collected without inserting pixels?

There is a misunderstanding on this point. When the recommendation refers to collecting the last open date within the framework of the consent exemption, this exemption relates precisely to the embedding of pixels. The principle is as follows: a pixel exempt from consent is embedded in the email, and only the last open date is collected at server level, overwriting the previous collection on each new open. It is not possible to collect this data without resorting to a pixel. This mechanism is an integral part of the framework proposed by the recommendation.

20. Does the CNIL recommend that all behavioural tracking be disengageable (opens and clicks), or only open tracking?

If the question is whether clicks are also covered within the framework of the recommendation? The answer is no, since tracking links are not covered by the recommendation.

However, reading this recommendation together with the work on cookies leads to the conclusion that tracking links are subject to similar obligations. Actors are invited to take up this question and to offer functionalities

relating to tracking links, even if this did not constitute the aim of the initial recommendation.

21. Can the CNIL specify the operating method implied by the exemption for cleaning bases or adapting the send frequency (retention period of inactive users' data, multiple campaigns, expected proof)?

In the event of an inspection, it is expected that the sender can, through objective data, demonstrate the effective implementation of the base-cleaning practice. The sender must be able to justify the frequency at which it removes from its base the users identified as inactive. The CNIL makes no particular recommendations as to the types of proof expected: the principle of freedom of proof applies, provided that the elements produced make it possible to establish objectively that this condition is met. Compliance with this condition governs the benefit of the exemption.

As regards the retention periods of inactive users' data and, more generally, the retention periods linked to consent in the context of pixels, the CNIL has not formulated precise recommendations. These timescales depend on the relationship maintained with the persons concerned. The CNIL invites actors to act proportionately, in accordance with the accountability principle provided for by the GDPR, by determining relevant and reasonable periods with regard to the timescale of the relationship with the person.

22. Many clients consider that measuring the open rate for campaign-performance purposes is possible within the framework of the consent exemption or via technical approaches based on non-individualised pixels. What is the CNIL's position on this subject?

The basis for exempting the pixel rests on measuring deliverability and cleaning bases. This is the primary criterion. In the event of an inspection, if this criterion is not met, the CNIL will consider that the pixel was not exempt, for failure to pursue a purpose benefiting the persons concerned.

Once this first condition is satisfied, it is possible to use the data collected by the pixel for other purposes, on condition that the data is first anonymised. For example, a pixel used for cleaning bases may, after anonymisation by aggregation across the entire base, serve as a performance indicator to measure the overall performance of a campaign. The CNIL envisages in particular the aggregation of data over a sufficiently large base as a mechanism liable to meet these criteria. This reuse is therefore not impossible, but it presupposes strict compliance with the framework defined by the recommendation.

23. Can an exempt pixel coexist with a non-exempt pixel?

Yes, provided that consent has been obtained for the purpose requiring it. In this case it is a multi-purpose pixel pursuing both an exempt purpose and a purpose subject to consent. From the moment consent is validly collected for the purpose that requires it, it is entirely possible to provide for a pixel pursuing simultaneously an exempt purpose and a non-exempt purpose.

This question also relates to the use of a single pixel whose behaviour varies depending on consent status: simple deliverability measures in the absence of consent, and advanced campaign-performance measures in the event of consent. This mechanism, comparable to the use of mixed cookies on the web, is not subject to any technical limitation on the part of the CNIL. The CNIL will simply verify that, in the absence of consent, the pixel falls within the framework of the exemption, and that, in the event of consent, broader measures may be implemented.

24. Is the retainable data different depending on the exemption relied upon (deliverability versus authentication)?

Yes. In the context of securing authentication, it may be necessary to collect more precise technical data, such as the User-Agent or the IP address, in order to carry out a comparison with the user's behaviour in other contexts and to identify any attempts to take control of the mailbox. This data is more detailed than that acceptable within the framework of the deliverability exemption, for which the CNIL expects simple, binary processing, limited to the last open date to the day.

25. As regards the exemptions, are the conditions of minimisation and of a service requested by the user specific to the deliverability exemption, or do they also apply to the exemption linked to security and authentication?

These conditions also apply to the security-related exemption. The minimisation conditions are common to both exemptions. The condition of a service expressly requested by the user is explicitly laid down by Article 82 of the Data Protection Act, which provides for exempting trackers necessary for the provision of a service expressly requested by the user. This condition flows directly from the text.

26. Is minimisation relative to the purpose pursued?

Yes. Minimisation in the context of deliverability and minimisation in the context of authentication do not result in the same data set, but the same principle applies in both cases.

27. What is your position on using the pixel to demonstrate the delivery of emails subject to a legal obligation?

The legal obligation relied upon must be clearly defined. The CNIL cautions against the tendency of certain actors to characterise as legal obligations intentions that do not amount to such. It is necessary to be able to identify a text imposing this obligation specifically. In the context of measuring deliverability, once the first criterion is satisfied (namely the purpose of avoiding excessive sending of emails to persons), the data collected may be reused for questions of demonstrating compliance with legal obligations (see slide).

28. What are the criteria for determining whether purposes are connected?

Connectedness is a notion that has no legal definition strictly speaking. It was notably raised by the public rapporteur in the context of a decision handed down by the Conseil d'État relating to the guidelines applicable to cookies and other trackers. In essence, connectedness is the inverse of the distinction between purposes: there is connectedness where the purposes are strongly dependent on one another. This assessment must be documented on a case-by-case basis. Actors may refer to the examples provided in the recommendation, which identifies two cases in which the purposes were considered connected.

The pixel purposes identified in the recommendation as requiring consent are not connected to one another. They are objectively distinct purposes, and the reflection work carried out by the CNIL did not make it possible to identify any connectedness between these different purposes.

29. What exemption arrangements should be put in place in the context of a B2B newsletter and opt-out rather than opt-in consent?

The exemption does not apply in this context. B2B newsletters do not constitute expressly requested emails within the meaning of the ePrivacy regulations; it is therefore not possible to benefit from the consent exemption for pixels. The CNIL notes a lack of alignment between the ePrivacy regulations on the one hand and the regulations arising from Article L. 34-5 of the French Post and Electronic Communications Code on the other: these types of emails, which fall under opt-out for B2B prospecting, cannot fall within the framework of the consent exemption for pixels.

Furthermore, as regards the charitable sector, the same non-alignment issue arises. The ePrivacy regulations do not provide for a specific exemption for this sector. Consequently, there is no exception to obtaining consent for the use of pixels in this context.

30. Does the CNIL consider that processing linked to cybersecurity and the detection of abnormal behaviour should benefit from an explicit exemption?

The answer is nuanced. Reference should be made to the slide on purposes. The recommendation provides that so-called "user centric" security operations are exempted, that is to say those that directly benefit the user (securing their account, their authentication). In this framework, cybersecurity processing aimed at detecting abnormal behaviour is exempted. By contrast, if the aim is to detect the use of bots for the purposes of combating advertising fraud or fraudulent sign-ups to prize draws, these are not measures aimed at protecting the user. In that case, in the light of the applicable texts, it is considered that an exemption cannot be retained.

31. Where one or more exemptions apply, must the persons systematically be offered the possibility of exercising their right to object? Must the exercise of this right put an end to all processing, including that carried out in the context of a legal obligation?

The answer to this question has been provided in connection with the guidelines on cookies and other trackers. The FAQ available on the CNIL's website relating to cookies

addresses this point. There is a need to permit a right to object, but this will be linked to the GDPR processing based on the data collected by means of the exempt pixel. As regards the arrangements for objection, this would be information figuring at the level of the privacy policy. On this aspect, the CNIL's intention is not to overload the consent-collection interfaces with an additional objection. It is accepted that this objection be mentioned in the privacy policy and not in the consent-collection interfaces, which avoids creating further confusion for the persons concerned.