

Tracking Pixel and Email: New Guidelines Issued by the Italian Data Protection Authority to Be Implemented by 29 October 2026

On 17 April 2026, the Italian Data Protection Authority (*Garante per la protezione dei dati personali*) ("Italian DPA") adopted the "*Guidelines on the Use of Tracking Pixel in email Communications*" (doc. web n. 10241943), which set out the applicable legal framework, transparency obligations and conditions for obtaining consent for all entities using tracking pixels.

These include **information society service providers**, entities offering **publicly accessible online services**, **email providers**, and **mass email distribution platform providers**. However, because the use of tracking pixels in email communications is widespread in business practice, **entities that do not fall within these categories but nevertheless use tracking pixels are also included within the scope of the Guidelines**.

The deadline for compliance is six months from publication in the Official Gazette; accordingly, companies will have until **29 October 2026** to comply.

I Tracking Pixels and the legal framework

How tracking pixels work

Tracking pixels are very small images (1x1 pixel), often transparent, hosted on remote servers and loaded in emails through HTML code. When the recipient opens the message, the code contained in it triggers a request to the sender's server: the pixel is downloaded and the server may receive data such as the IP address, device type, time of opening and number of subsequent openings.

In the Guidelines, the Italian DPA adopts a similar approach to the now consolidated one for the use of cookies: the insertion of the tracking pixel and the subsequent monitoring of the user's behavior constitute **operations involving access to terminal equipment** within the meaning of **Article 122 of Legislative Decree No. 196/2003 ("Italian Privacy Code")**. The provision covers both the storage of information on terminal equipment and access to information already stored: in the case of tracking pixels, both scenarios arise through the loading of the remote image and the consequent transmission of data to the server.

The fact that the Italian DPA has brought the use of tracking pixels within the scope of Article 122 of the Italian Privacy Code is particularly significant, because that provision transposes the European Union's so-called "ePrivacy" Directive and, as such, operates as a *lex specialis* in relation to the provisions of Regulation (EU) 2016/679 ("GDPR"). It follows that the requirement to obtain consent from data subjects, discussed below, leaves no room for alternative solutions based on different legal bases (e.g., legitimate interest) for the processing associated with the use of the tracking pixels covered by the Guidelines.

Scope of application

The Guidelines apply to any public or private entity that uses tracking pixels in electronic communications, regardless of whether the message is commercial, service-related, institutional or informational in nature.

Accordingly, the obligations established by the Guidelines apply not only to the sender, but also to all other parties involved, including, for example, **emailing service providers**, **tracking technology providers**, providers of **mailing-list rental services** and **content creators**, according to their respective roles and responsibilities in relation to the protection of personal data.

II

Transparency obligations: privacy notice and consent

The Italian DPA emphasizes that tracking pixels are **particularly intrusive** tools because of their **hidden nature**, and that their use without adequate information **violates the principle of fairness under Article 5 of the GDPR**. Every controller must therefore inform recipients of the use of these tools, regardless of the purpose of the communication or the nature of the sender.

As it is already the case with cookies, the **privacy notice** may be provided **on several layers**: for example, through a concise notice in the form used to collect the email address and a link to more detailed information, which may also be included in the cookie policy, where one exists. In all cases, the controller must adopt a **complete, clear, effective and user-friendly solution**.

With respect to the new requirements imposed by the Guidelines, it is necessary to distinguish between: **(i) a transitional regime**, applicable to processing carried out using tracking pixels before the Guidelines enter into force; and **(ii) an "ordinary regime,"** applicable to processing commenced after the obligations enter into force.

Transitional regime (processing already under way)

This regime covers all processing already under way on the date the Guidelines enter into force, based on consent or another valid legal basis, that involves sending recipients commercial emails using tracking pixels. Examples include newsletters that are already active or using contact lists already in use. In such cases, the controller may continue to use tracking pixels in relation to data subjects, provided that it satisfies the information obligation with the first relevant message or at the first interruption of the communications, and implements and discloses an **easy-to-use, highly visible and granular** withdrawal mechanism.

This withdrawal mechanism may consist, for example, of a standardized icon or a link in the footer leading to a dedicated area where the data subject can choose either to stop receiving all communications or to continue receiving them without the use of tracking pixels. In

substance, this is an **opt-out approach**: after the information campaign, tracking pixels may continue to be used in relation to **data subjects already included in the database** who have not expressly withdrawn their consent to their use.

However, the data subject must not be prompted or steered towards a particular choice. Refusal of tracking may not in any event limit access to the service in any way, and all choices made by data subjects must be recorded by the controller, including for the purpose of demonstrating consent under Article 7 of the GDPR. The transitional regime is intended to be phased out progressively as new processing activities subject to the ordinary regime are initiated.

Ordinary regime (new processing activities)

The ordinary regime operates according to an **opt-in approach**: the use of tracking pixels in relation to new data subjects is generally prohibited by Article 122 of the Italian Privacy Code, unless informed, freely given, specific and unambiguous **consent has been obtained in advance** from the data subject. Consent should preferably be collected when the email address is obtained, after the privacy notice has been provided.

To avoid the so called “consent fatigue” and simplify the process, the Guidelines permit consent to tracking pixels to be collected **together with general consent to receive marketing communications**, provided that the request is worded neutrally and without pressure, and that it remains possible to withdraw easily and granularly only the consent to tracking pixels while continuing to receive the emails normally.

The collection of consent is necessary, in particular, whenever the controller individually measures the open rate to assess campaign performance, adjusts the frequency or stops sending communications based on the interest shown by the recipient, or uses reading data to derive information about tastes, interests and preferences - in other words, for all **processing activities involving profiling**.

III Exceptions to the consent requirement

The exceptions provided for in Article 122 of the Italian Privacy Code remain applicable in all cases. By virtue of these exceptions, the data subject’s **consent is not required** where the use of tracking pixels is necessary to: **(i)** transmit an electronic communication, or **(ii)** provide an online communications service expressly requested by the user. Consistently with paragraph 5 of the Guidelines, these cases include in particular the following situations:

Aggregated statistical measurement of the overall open rate

Tracking pixels may be used to measure the overall open rate when the result serves to **improve deliverability** of emails and/or to **combat spam**. In such cases, the count must be exclusively aggregated and must not permit personalized measurements: tracking pixels must therefore be identical for all recipients of the same campaign, and the **other related technical data**—e.g., the IP address and the client—must be anonymized using the methods described in WP29 Opinion No. 05/2014 on **anonymization techniques**.

Security measures in authentication processes

The use of tracking pixels may be considered necessary for the implementation, completion or updating of security measures in **user authentication processes**. This includes, for example,

messages concerning confirmation of account activation, password changes and requests to exercise rights relating to the protection of personal data, including data portability, where it is necessary to **verify that the message was actually opened** on a terminal known to belong to the data subject.

Mandatory institutional or service messages

The exception also applies to **institutional** or service messages that the controller is **legally required to send** and in respect of which **actual awareness** by the recipient is relevant, for example in the banking sector or in connection with the institutional activities of a public body. These include, among others, notices to prevent phishing or fraud and indicate the available remedies; communications concerning contractual or logistical and organizational changes, changes to terms of service or privacy notices; security incident notifications; institutional information campaigns; and reminders of contractual and social-security contribution deadlines or obligations. These are cases in which the basis for the exemption from the consent requirement lies in the benefit and protection afforded to recipients through the use of tracking tools.

However, it should be borne in mind that even in the exceptions described above, the **information obligations remain fully applicable**: the data subject must in all cases be informed of the use of tracking pixels and the purposes for which they are used. The exemption relates exclusively to the need to obtain specific consent for the use of tracking pixels and does not affect the other obligations imposed by personal data protection legislation.

IV Compliance requirements for affected companies

The obligations established by the Guidelines will enter into force on **29 October 2026**, namely six months after publication in the Official Gazette. By that date, entities that use tracking pixels must put in place **compliance plans** covering several areas: from **mapping ongoing tracking activities**, to **reviewing and updating privacy documentation**, through to **implementing technical solutions** for managing consent and enabling data subjects to exercise their rights.

The professionals of the *Data Protection & Cybersecurity Practice Area* are available to assist clients in assessing the best strategies and means of complying with the requirements of the Guidelines, while balancing compliance obligations with commercial needs.

Contacts

Pierluigi Perri

Of Counsel - Chiomenti
Data Protection & Cybersecurity
T. +39.02.721.571
pierluigi.perri@chiomenti.net

Matteo Leffi

Senior Associate - Chiomenti
Data Protection & Cybersecurity
T. +39.02.721.571
matteo.leffi@chiomenti.net

Carlo Piva

Associate - Chiomenti
Data Protection & Cybersecurity
T. +39.02.721.571
carlo.piva@chiomenti.net
