

Tracking pixels in e-mails: the Italian Data Protection Authority's Guidelines define transparency and consent requirements

July 31, 2026

AUTHORS

Aurora Agostini

Partner



Francesca Costarelli

Associate



*By Measure No. 284 of 17 April 2026 (the “**Measure**”), the Italian Data Protection Authority, for the first time, has regulated in a comprehensive manner, through the adoption of Guidelines, the use of tracking pixels in electronic mail communications, with the aim of specifying the proper manner for providing the privacy notice and obtaining data subjects’ consent. The addressees of the measure, including, inter alia, sending service providers, marketing automation platforms and tracking technology providers, have six months from publication in the Official Gazette to comply. The deadline is 29 October 2026.*



A TRACKING PIXEL CONSTITUTES ACCESS TO A TERMINAL DEVICE

The Measure stems from the need to curb the use of “concealed” tracking technologies in electronic mail communications, particularly those used in newsletters, *direct e-mail marketing* (DEM), transactional e-mails, service communications or institutional messages.

Tracking pixels are transparent images of minimal size, often amounting to a single pixel and therefore imperceptible to the recipient. They are embedded in e-mails but hosted on remote servers and have no content-related function. When the message is opened, an HTML code inserted in the text automatically generates a request to the sender’s server: the pixel is downloaded by the recipient’s e-mail *client* and stored in the memory of the recipient’s terminal device. This process, which is invisible to the user, enables the sender to obtain information regarding the opening of the communication and, in some cases, additional information that can be inferred from the recipient’s IP address, such as the type of device used, the time spent viewing the message and the number of subsequent openings of the same e-mail.

The Authority characterizes this operational sequence as a case of access to a terminal device pursuant to Article 122 of Legislative Decree No. 196/2003 (the “**Privacy Code**”), the provision that transposes into the national legal order Article 5(3) of Directive 2002/58/EC (the “**e-Privacy Directive**”). This classification is also consistent with EDPB Guidelines 2/2023 on the technical scope of application of the same European provision, which the Guidelines



expressly reference. Loading the pixel constitutes the “storage of information in the user’s terminal equipment,” and the recording of the opening constitutes the subsequent “access to information already stored,” both operations falling within the scope of Article 122 of the Privacy Code.

THE PRIVACY NOTICE: AN OBLIGATION ACROSS ALL CATEGORIES OF COMMUNICATION

The Guidelines clarify that any use of tracking pixels in e-mails requires the transmission of an appropriate privacy notice to the recipient, irrespective of the type of message (commercial, service-related or institutional) and the nature of the sender (private or public). According to the Authority, failure to provide such notice renders the processing unlawful under the principle of fairness set out in Article 5(1)(a) GDPR, given the concealed nature of tracking pixels.

In this respect, the Authority follows the same simplification logic already adopted for cookies in the Guidelines of 10 June 2021 (web doc. No. 9677876): the privacy notice may be structured on multiple levels, with a concise statement in the form used to collect the e-mail address and a reference to a more detailed version, which may be incorporated into the existing *cookie policy*. Multichannel methods are permitted, such as *pop-up* windows, videos, virtual assistants and chatbots, provided that the overall system ensures completeness, clarity and usability, in accordance with the principle of *accountability* pursuant to Article 5(2) GDPR.

For processing activities already under way on the date the Guidelines entered into force, the Authority considers it appropriate to discharge the information obligation by means of the first subsequent communication or the first available point of discontinuity in the relationship with the data subject.

CONSENT IS ALMOST ALWAYS REQUIRED

Article 122(2-bis) of the Privacy Code imposes a general prohibition on accessing the user’s terminal device, from which derogations are permitted only where specific conditions are met. The Guidelines identify the situations in which consent is not required and those in which it is mandatory.



Consent is mandatory where measurement of the open rate is carried out on an individual basis in order to assess and optimize promotional campaigns and thus modify the subject line, frequency or relevance of messages based on the behavior of the individual recipient; or where the open data are used to infer the user's tastes, interests and preferences in order to build commercial profiles that may also be used for other initiatives. The Measure clarifies that, for processing activities subsequent to the Guidelines, consent should preferably be collected at the time the e-mail address is obtained. The Authority accepts that consent to the tracking pixel may be incorporated into the more general consent to receive promotional communications, thereby avoiding redundant multiple requests that generate *consent fatigue*, provided that the request is framed neutrally and that the user is fully informed.

Consent may, however, be omitted where:

- (i) The pixel is used for aggregate and anonymized statistical measurement of e-mail opens, provided that the data do not allow personalized measurement. The Authority suggests the use of campaign-specific pixels (rather than pixels for each individual recipient) and the anonymization of the related technical identifiers (IP address, client).
- (ii) The pixel serves security measures relating to the user authentication process (e.g., confirmation of account activation, password reset), by verifying that the message is opened on a terminal device attributable to the data subject. In this case, security needs and the provision of the requested service converge in justifying the derogation.
- (iii) The pixel is embedded in institutional or service messages that the controller is under a legal obligation to send and as to which the recipient's actual awareness is material, including, *inter alia*, anti-fraud and anti-phishing alerts, communications regarding contractual amendments, notifications of security incidents and institutional campaigns.

WITHDRAWAL OF CONSENT MUST BE GRANULAR

A user who has consented to the processing must be able to withdraw that choice in a differentiated manner and therefore opt either to stop all communications or to continue receiving e-mails without tracking pixels. This second option is a functionality that platforms must be capable of ensuring from a technical perspective.

The mechanism suggested by the Authority provides for the inclusion in every e-mail of a standardized icon or a link in the footer leading the user to an area dedicated to the exercise of rights, from which it is possible both to request full unsubscription and to selectively disable tracking only. Refusal of tracking may not entail any limitation of the service, in accordance with the principle that consent must not be conditional, as already affirmed in relation to *cookies*.



All choices made by the data subject must be recorded by the controller and be capable of being demonstrated in the event of a challenge. From a *privacy by design* perspective, the Authority suggests a concrete technical measure: generating, for each recipient, a non-intelligible and non-sequential identifier to be associated with the e-mail address in an internal and separate *layer* of the platform, so that the count of openings is carried out by means of the identifier without exposing the e-mail address in the technical request generated by loading the pixel.

OPERATIONAL IMPLICATIONS

The Guidelines, for the first time, define in a comprehensive manner the framework of obligations applicable to the use of tracking pixels in electronic mail communications, clarifying the conditions for lawful processing and the operational methods for compliance. The addressees of the measure have until 29 October 2026 to comply by updating their privacy notices, supplementing the record of processing activities and technically implementing granular withdrawal mechanisms.

TEAM



Aurora Agostini
Partner



Giulietta Minucci
Partner



Marco Grechi
Senior Associate



Giovanni Lombardi
Associate



Alessandro Carlini
Associate



Francesca Costarelli
Associate



This document is provided for general informational purposes only and is not intended to provide legal advice on the matters addressed. Recipients of this document may not rely on its contents. LEXIA and/or the firm's professionals shall not be held liable in any manner whatsoever for the contents of this document, whether on the basis of a professional engagement or for any other reason.