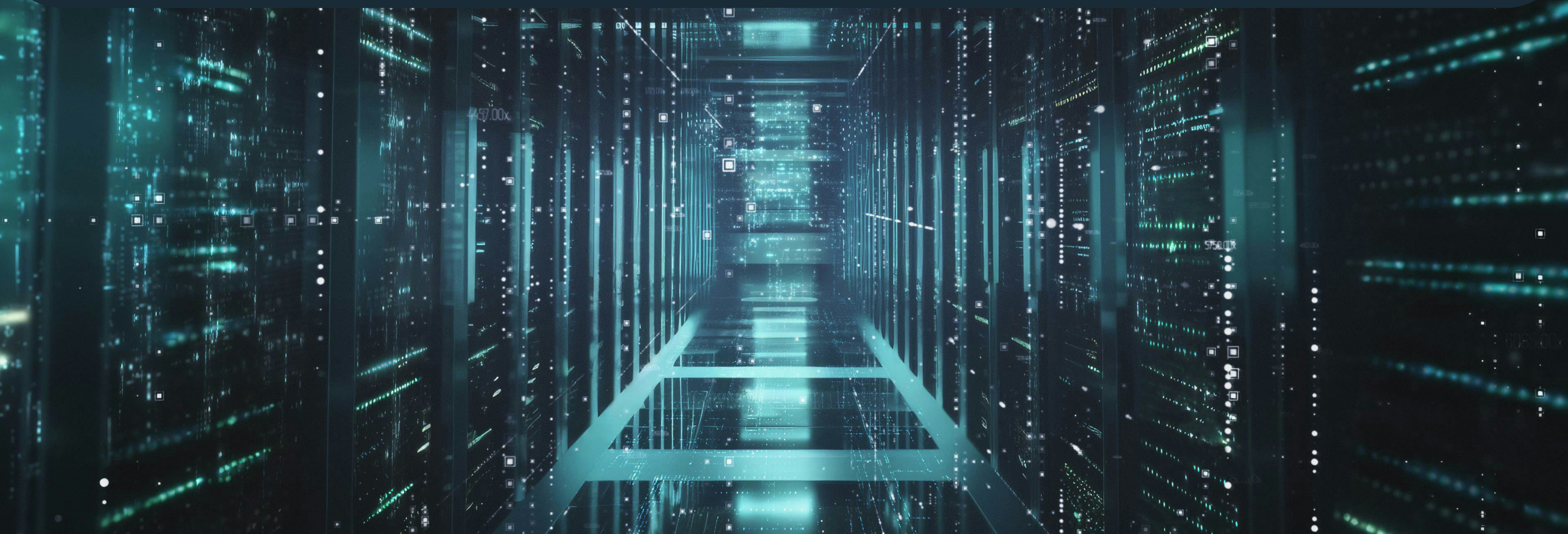
09 Issue 2026

Legance

Italian Data Protection Authority adopts Guidelines on tracking pixels in email communications



On 17 April 2026, the Italian Data Protection Authority (the "**IDPA**") adopted new Guidelines on the use of **tracking pixels in email communications** (the "**Guidelines**"), providing a detailed interpretation of the legal framework applicable to one of the most widespread - yet often opaque - tracking technologies used in digital communications. Tracking pixels are small, often transparent remote images referenced in emails and loaded from external servers when the message is opened by the recipient. According to the IDPA, this **mechanism enables senders or third parties involved in the communication process to collect information relating to the opening of the email**, including, in certain cases, data such as the recipient's IP address, device type, client used, time of consultation and repeated openings of the same message. The IDPA places particular emphasis on the **inherently invasive nature of these tools, noting that tracking typically occurs without the recipient's awareness**. Although tracking pixels do not directly concern the content of the communication, the IDPA considers their hidden character especially problematic in the context of email services, which by their nature are intended to convey private correspondence.

A central aspect of the Guidelines is the **qualification of tracking pixels under Article 122 of the Italian Privacy Code**, implementing the ePrivacy Directive (also known as "cookie law"). According to the IDPA, the insertion of tracking pixels in emails and the subsequent collection of information generated through their loading constitute operations involving both the storage of information on the user's terminal device and access to information already stored therein. As a result, the use of tracking pixels falls within the scope of the ePrivacy regime, which operates as *lex specialis* in relation to the GDPR.

On this basis, the Guidelines reaffirm that the **use of tracking pixels is prohibited unless one of the statutory exceptions under Article 122 applies or**, failing that, **the recipient has provided valid consent**.

The IDPA nevertheless recognizes that **consent may not be required in certain circumstances**, particularly where tracking pixels are used exclusively for aggregated and anonymized statistical measurements aimed at improving email deliverability or preventing spam, for security-related authentication purposes, or in connection with institutional or service communications where proof of receipt is relevant.

Outside these scenarios, prior consent remains necessary, especially where tracking is used to measure individual engagement with emails, optimize marketing campaigns, adapt the frequency or content of communications based on user behavior or derive information relating to preferences and commercial profiling.

The Guidelines also address **transparency obligations**. The IDPA states that **recipients must be adequately informed of the use of tracking pixels** regardless of the nature of the communication or the type of sender involved. Such information may be provided through simplified and layered notices, including via links, multichannel tools or integrated privacy policies, provided that the overall system ensures clarity, accessibility and effectiveness.

Importantly, the IDPA adopts a **pragmatic approach to consent collection in the marketing context. The Guidelines clarify that consent to tracking pixels may, in principle, be incorporated into the broader consent to receive promotional communications, provided that the request is formulated in a clear, neutral and informed manner**. At the same time, users must be able to withdraw consent easily and also on a granular basis, including by opting out of tracking while continuing to receive email communications without tracking functionalities.

Finally, the IDPA strongly emphasizes the importance of privacy by design and by default measures. In particular, the IDPA **recommends the implementation of technical solutions aimed at reducing identifiability risks**, such as the use of unintelligible and non-sequential identifiers separated from the recipient's email address within the platform architecture.

For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it