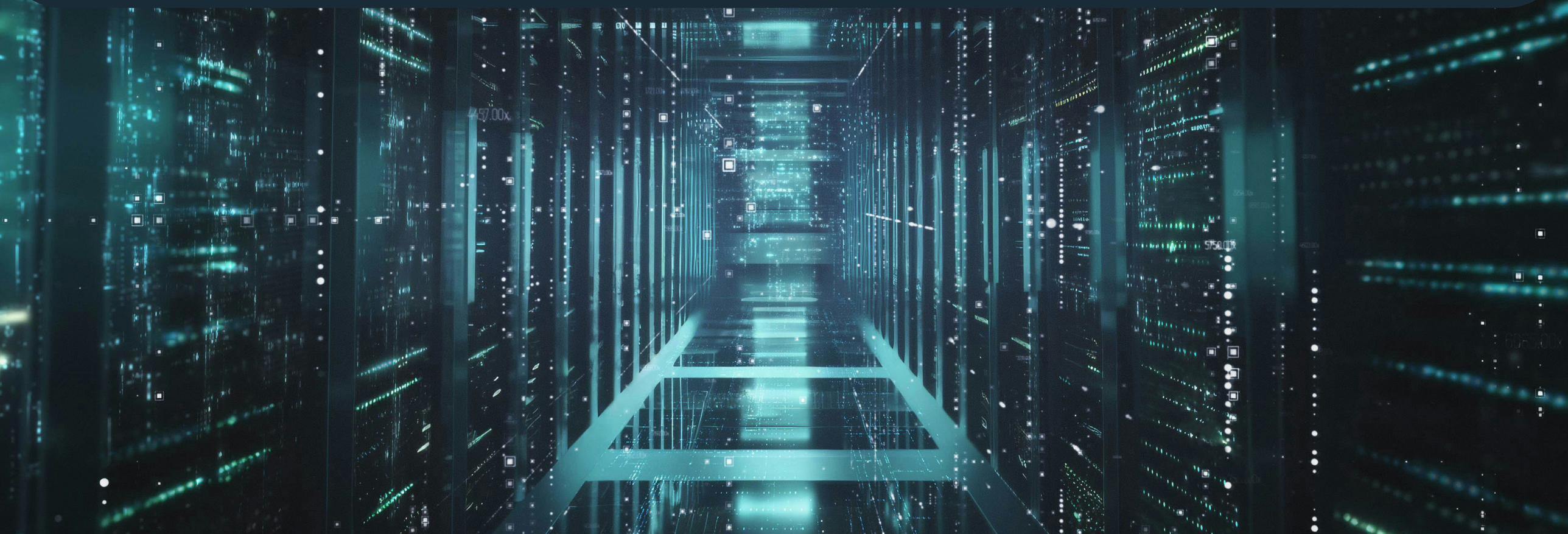
16 Issue 2026

Legance

Privacy & Cybersecurity Update: GDPR Enforcement and the First CRA Compliance Deadline



Data brokers and the limits of legitimate interest: EUR 2,000,000 fine from the IDPA (1/6)

Through Decision No. 542 of 14 July 2026, the Italian Data Protection Authority ("***IDPA***") imposed a fine of EUR 2,000,000 on a US-based data broker (the "***Company***") that operates a platform providing paying customers with enriched professional contact information (name, email address, telephone number, job title, seniority, role and location) on individuals who are not users of the service and have not consented to their data being made available.

The investigation was triggered in April 2025 by press reports signaling the presence on the platform of telephone numbers belonging to senior Italian institutional officials, including the President of the Republic, members of the Government, commissioners of regulatory authorities, and members of parliament, as well as foreign leaders. The IDPA also received complaints from individuals who, after receiving unsolicited commercial communications, had traced the source of their contact details back to the Company.

Data brokers and the limits of legitimate interest: EUR 2,000,000 fine from the IDPA (2/6)

As a preliminary matter, the IDPA rejected the Company's argument that the GDPR did not apply on the ground that it had no EU establishment. On the substance, the **IDPA found the GDPR applicable on the basis of the behavioral monitoring criterion under Article 3(2)(b)**: the Company does not merely collect professional contact data but continuously organizes, enriches, and updates it to track changes in the personal and professional positions of the individuals in its database. The IDPA clarified that this constitutes monitoring within the meaning of Recital 24 of the GDPR, irrespective of whether profiling in the technical sense under Article 4(4) is carried out.

On the merits, the IDPA identified three categories of violation. First, the Company **lacked a valid legal basis for the collection of contacts' data and communication to customers**.

Data brokers and the limits of legitimate interest: EUR 2,000,000 fine from the IDPA (3/6)

The Company relied on legitimate interest under Article 6(1)(f) GDPR, but the IDPA found that none of the three cumulative conditions of the applicable test was satisfied: the interest in making personal data available to third parties for direct marketing purposes is not legitimate under the GDPR, given that Italian law requires prior consent for such transfers; the data collected (including for example calendar entries, email account data, and contact details reconstructed via algorithms or purchased from third-party vendors) exceeded what was strictly necessary; and the balancing exercise had not been genuinely carried out, contacts having no reasonable expectation that their data would be aggregated from multiple sources outside their knowledge and control and made available to an indefinite number of subscribing companies.

Data brokers and the limits of legitimate interest: EUR 2,000,000 fine from the IDPA (4/6)

Second, **the transparency obligations were breached**: the privacy notice did not specify the legal basis for the initial collection of contacts' data, and the privacy information notice was inaccessible from the Company's homepage, requiring multiple navigation steps to reach. Third, despite having adopted voluntary technical filters to exclude data on public officials, the Company **lacked effective technical controls** to implement that objective, a failure the IDPA characterized as a violation of the data protection by design and by default obligation under Article 25 GDPR. The IDPA ordered the immediate cessation of all further processing of personal data of individuals located in Italy collected without a valid legal basis, their deletion, and the communication of compliance within 60 days.

Data brokers and the limits of legitimate interest: EUR 2,000,000 fine from the IDPA (5/6)

The fine of EUR 2,000,000 reflects, as aggravating factors, the structural nature of the unlawful data collection and the high number of Italian individuals affected, and, as attenuating factors, the absence of prior sanctions, the Company's cooperation during the proceedings, and the absence of special categories of data.
The decision confirms that the **GDPR can reach non-EU controllers through the behavioral monitoring criterion under Article 3(2)(b) even in the absence of profiling within the meaning of Article 4(4)**, thereby extending the GDPR's territorial scope to a wide range of data intelligence and lead generation platforms.

Data brokers and the limits of legitimate interest: EUR 2,000,000 fine from the IDPA (6/6)

At the same time, it reinforces that legitimate interest under Article 6(1)(f) cannot serve as the legal basis for making personal data available to third parties for direct marketing purposes, and that the obligation to verify the lawful origin of the data lies with the operator of the contact database regardless of whether the unsolicited commercial communications are ultimately sent by its downstream customers.

The decision also applies the **reasonable expectation standard** in the balancing test strictly, making clear that the mere creation of a profile on a professional networking platform does not, in itself, give rise to a reasonable expectation that one’s contact details will be aggregated from multiple sources and made available to an indefinite number of third parties for commercial purposes outside the platform.

Cyber Resilience Act: the September 11, 2026 deadline and what manufacturers need to do (1/4)

Regulation (EU) 2024/2847 (the "***CRA***") entered into force on December 10, 2024 and will become fully applicable on December 11, 2027. However, Article 14 (which governs manufacturer reporting obligations) will apply from September 11, 2026 and, by virtue of Article 69(3), will extend to products with digital elements already placed on the market before the full application date.

The early application of Article 14 means that manufacturers will be subject to notification obligations well ahead of the broader compliance deadline. Two distinct events trigger those obligations: an actively exploited vulnerability (i.e. one for which reliable evidence of actual exploitation in a real system exists) and a severe incident affecting the security of the product.

Cyber Resilience Act: the September 11, 2026 deadline and what manufacturers need to do (2/4)

For **actively exploited vulnerabilities**, the manufacturer of products with digital elements already placed on the market must transmit an early warning within 24 hours, a more detailed notification within 72 hours, and a final report within 14 days of a corrective measure becoming available; for **severe incidents affecting product security**, a final report is due within one month of the 72-hour notification. Notifications must be transmitted simultaneously to the designated CSIRT coordinator and to ENISA through the single reporting platform under Article 16. Under Article 14(8), manufacturers must also inform the affected users of the vulnerability or incident and of the mitigation measures available to them.

Cyber Resilience Act: the September 11, 2026 deadline and what manufacturers need to do (3/4)

Article 64 places non-compliance with Article 14 in the highest penalty bracket, alongside failure to meet the essential requirements of Annex I: up to EUR 15,000,000 or, for undertakings, up to 2.5% of total worldwide annual turnover for the preceding financial year, whichever is higher. Micro and small enterprises are exempt only from the 24-hour early warning deadline; the remainder of the notification regime applies to them in full.

Article 14 CRA imposes no active monitoring obligation on manufacturers: that obligation, together with vulnerability management and the maintenance of a software bill of materials, does not apply until December 2027. This means that, in the window between September 2026 and December 2027, the 24-hour notification to ENISA via the single reporting platform will typically be triggered by an external signal: a researcher, a customer, a third-party CERT, or an authority reporting an actively exploited vulnerability to the manufacturer.

Cyber Resilience Act: the September 11, 2026 deadline and what manufacturers need to do (4/4)

It is on reception, not on independent discovery, that the organization must be prepared to act.
Before that signal arrives, the manufacturer must already have made a set of organizational decisions: it must know which products remain on the EU market and which units are already in use by European customers, and who, within its group, qualifies as manufacturer under Article 3(13) CRA; it must have a dedicated channel through which an external alert can reach, within hours, someone with the authority to assess it and sign the notification; and it must have identified the single reporting platform through which the notification to ENISA is made.
None of these decisions is technical, but none can be made after the clock has already started running.

For further information, please contact:

Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it

Martina Balzani
mbalzani@legance.it