# Data Law Alert

Data Law

# Italy & EU Latest Developments on AI and Data Protection

No.17 Issue 2026

Legance

## Italy issues further rules on AI

Legislative Decree No. 160 of 9 September 2026, published in the Official Gazette on 15 September 2026 (the ***"Decree"***), introduces new detailed rules on AI systems, with an impact on criminal and civil law (contracts and torts).

The Decree is divided into three Sections:

I. Section I **governs the use of AI by police forces, requiring qualified human review of the outputs of automated processing before their use, and, for high-risk systems, effective human oversight.**
The most sensitive aspect of this Section concerns real-time remote biometric identification, which is permitted only for the prevention of specific threats or the search for missing persons or victims of kidnapping, trafficking or sexual exploitation, subject to authorisation by the *procuratore della Repubblica* (the head of the local public prosecutor's office) for a **maximum of fifteen days** (which may be extended by the *procuratore della Repubblica*, by means of a decree setting out the reasons, for successive periods of fifteen days where the conditions referred to in Article 8, paragraph 1 continue to apply), with an absolute prohibition to use databases built through untargeted scraping. It also addresses post-event facial recognition, which, as a general rule, requires **authorisation from the preliminary investigations judge following the prosecutor's request within 48 hours of the system's activation**. In all cases, generalised or indiscriminate biometric surveillance is prohibited.

II. Section II **introduces** (i) **the new offence of failure to adopt security measures in, or unlawful alteration of, high-risk AI systems** (Article 437-bis of the Italian Criminal Code), (ii) the new Article 359-ter of the Italian Code of Criminal Procedure on **real-time remote biometric identification in investigations**, (iii) the extension of **corporate criminal liability of legal persons** for offences committed through the use of AI, and (iv) **amendments to civil procedure** intended to facilitate the exercise of rights to parties claiming damages for violations of the AI Act.

III. Section III provides for a **one-year transitional period to bring existing AI systems into compliance** with the new rules, together with a financial neutrality clause.

Amongst the many aspects that are raising interest, we highlight the following.

**Research collaborations** (Article 4): research partners (universities, research bodies, and public or private entities collaborating with the police forces) are prohibited from acquiring or using AI systems trained for police purposes. However, research may proceed using synthetic data or masked/pseudonymised real data as an alternative.

**Regulatory sandboxes** (Article 5): the Decree requires the mandatory involvement of the Italian Data Protection Authority ***(IDPA)*** where the processing involves personal data. Paragraph 4 provides that the coordination between the AI regulatory sandbox under Article 57 of the AI

Regulation and the activities under Article 5 shall be governed by a regulation adopted by decree of the President of the Council of Ministers, on the proposal of the National Authorities for Artificial Intelligence, in consultation with the *Ministro dell'interno*, and after obtaining the opinion of the *Ministro dell'economia e finanza* and of the IDPA.

**Impact assessment for real-time remote biometric identification** (Article 9): the Decree requires both a fundamental rights impact assessment under Article 27 of the AI Regulation and a data protection impact assessment under Articles 23 and 24 of Legislative Decree No. 51/2018 before using real-time remote biometric identification systems.

**Real-time remote biometric identification** (Article 8): the Decree assigns to the public prosecutor (*"procuratore della Repubblica"*, i.e. the head of the local public prosecutor's office) the competence to authorise the use of real-time remote biometric identification systems, to extend such authorisation for further periods of 15 days (renewable once), and to confirm a system deployed by police forces on grounds of urgency for up to 24 hours.

**Retrospective facial recognition** (Article 10): as a general rule, the Decree requires **authorisation from the preliminary investigations judge on the prosecutor's request within 48 hours** before activating retrospective facial recognition. An exception applies where the technology is used solely for the initial identification of a person potentially suspected of an offence, immediately after that offence, based on objective and verifiable elements directly connected to the

offence itself. In that case, use remains under the sole responsibility of the public security officer designated by the *questore* (or, outside that scenario, the investigating judicial police officer).

**New AI-related offence** (Article 437-bis of the Criminal Code): The Decree adds a new criminal offense, aimed at punishing the professional user of a high-risk AI system who intentionally fails to implement human oversight measures, with imprisonment from one to five years, where such omissions give rise to a danger to life or to public or individual safety.

**Corporate liability for AI-related offences** (Article 15): the Decree extends the corporate liability regime under Legislative Decree No. 231/2001 to AI-related offences by introducing a new Article 25-vicies *(Reati commessi con l'uso di sistemi di intelligenza artificiale)*. Injunctions, disqualifications and other non monetary sanctions under Article 9(2) of Legislative Decree No. 231/2001 apply on top of monetary fines.

**Civil actions for the redress of AI-related damages** (Articles 16–20): the Decree introduces procedural instruments to facilitate claims for both contractual and tortious reimbursement of damages arising from the use of AI systems (Article 16). On request of the allegedly injured party, the court may order the opposing party or a third party to produce evidence on the functioning of the AI system — including logs, risk management documentation, technical documentation and information on human oversight parameters — provided that the claimant presents facts making the claim plausible (Article 17). If a party fails to comply with such order

without justified reason, the court shall consider that violation in adjudicating the case; where the regulatory documentation listed in Article 17(2) is not provided despite the Court order (basically the documentation which is mandatory under the AI Act for high-risk systems), the facts alleged by the claimant are deemed proved. More, the third party who fails to comply with the Court order, is also subject to a fine of between EUR 1,500 and EUR 10,000. Where the damage results from a breach of obligations under the AI Act, the causation nexus between the breach and the damage is presumed but the defendant can rebut the presumption and prove otherwise (Article 18). Compliance with the AI Act — including certification under Chapter III, Section 5 of the AI Act — does not *per se* exclude liability (Article 19). The injured party may enquire whether the defendant holds a liability insurance policy and, if so, bring a direct action against the insurer within the limits of the insurance coverage; the alleged tortfeasor is a necessary party to such proceedings (Article 20).

## The CJEU rules that EU law does not require publication of all shareholders' personal data and that the GDPR precludes unconditional public access to it

With its judgment of 3 September 2026 in Case C-798/24 (*Jautiva*), the Court of Justice of the European Union (**"CJEU"**) ruled on a reference from the Latvian Constitutional Court concerning national legislation that requires companies to publish online, without any access restriction and downloadable in bulk, personal data relating to all shareholders of a joint-stock company, including minority shareholders (namely their identity, contact details, and the category, number, value and voting rights of their shares). The reference was raised by 17 minority shareholders challenging the legislation as contrary to the rights to privacy and data protection.

The Court first held that Article 14(d) of Directive (EU) 2017/1132 on certain aspects of company law does not require the publication of information on all shareholders, including minority shareholders. Unlike directors and other persons empowered to bind or represent the company, shareholders derive their status solely from their capital participation, and the publication of their identities does not usefully serve the Directive's underlying purpose of protecting third parties dealing with limited-liability companies.

On the GDPR, the Court held that Articles 5 and 6, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights, preclude national legislation requiring unconditional public access to shareholders' personal data, even where the disclosure pursues an EU-recognised objective of

general interest (such as business transparency, anti-money laundering and counter-terrorist financing, or the implementation of sanctions) where access is not subject to any condition, such as demonstrating a legitimate interest. The Court found that such publication amounts to a serious interference with fundamental rights, since it allows a profile of the shareholder's financial standing to be drawn up and exposes the data, once public, to unlimited access, retention and further dissemination. It further found the measure neither necessary nor proportionate to the stated objectives, given that less intrusive means are available, such as restricting access to persons demonstrating a legitimate interest and, for sanctions purposes, limiting publication to individuals actually listed on sanctions lists.

The decision raises questions for the Italian regime on shareholder disclosure applicable to non-listed S.p.A. and S.r.l. Under Italian law, the identity, tax code, domicile and shareholding of those who set up a company, or who become shareholders through a capital increase or share transfer, are readily available through the Companies' Register (save that, for non-listed S.p.A., a share transfer becomes visible in the Register only once the financial statements reflecting that transfer are filed, so the Register may not always show the current position). While this dataset is narrower than under the Latvian legislation and access requires a log-in, it is not subject to any requirement that the person consulting it demonstrate a legitimate interest, even as regards minority shareholders.

# Data Law Alert

Data Law

For further information, please contact:


Andrea Fedi
afedi@legance.it

Lucio Scudiero
lscudiero@legance.it

Martina Balzani
mbalzani@legance.it