ALERT MEMORANDUM

Italy AI Regulation: New Rules and Risks for Businesses

November 10, 2026

Two recent legislative decrees have added to Italy's regulatory framework for artificial intelligence (AI). Legislative Decree No. 179 of October 7, 2026 (Decree 179/2026) came into force on October 23, 2026, following Legislative Decree No. 160 of September 9, 2026 (Decree 160/2026), which came into force on September 30, 2026. Both decrees were adopted under the powers delegated to the Government by Law No. 132 of September 23, 2025 (the AI Law) to bring Italian legislation into line with Regulation (EU) 2024/1689 (the AI Act).

Although the new provisions are already in force, their application must be considered in light of the AI Act's phased application. Amendments adopted at EU level in July 2026 have further postponed the application of certain rules governing high-risk AI systems[1].

In addition to regulating the use of AI systems in policing and introducing measures relating to testing, education, research, and training, the two decrees introduce significant changes for businesses that develop, supply, or use AI systems:

- Criminal law: Decree 160/2026 introduces a new offence of 'Failure to adopt security measures in artificial intelligence systems and unlawful alteration of systems' (Article *437-bis* of the Criminal Code). It also extends, for the first time, the administrative liability of legal entities under Legislative Decree No. 231/2001 (Decree 231) to cover new AI-related offences.
- Civil proceedings: Decree 160/2026 introduces new mechanisms for seeking compensation for damage caused by the use of AI systems, including orders to produce evidence and direct claims against insurers.
- Regulatory oversight: Decree 179/2026 clarifies the roles and powers of AgID, ACN, and the sectoral authorities, along with the administrative penalties for breaches of the AI Act and the procedures for imposing them. Other significant changes for businesses concern safeguards for workers in AI-driven decision-making and the protection of trade secrets used in AI training.

For any questions relating to the issues discussed in this memorandum, you may contact any lawyer in our firm with whom you are usually in contact or the authors below.

MILAN

Giulia Checcacci
+39 02 7260 8224
gcheccacci@cgsh.com

Marcello Magri
+39 02 7260 8296
mmagri@cgsh.com

ROME

Giuseppe Scassellati-Sforzolini
+39 06 6952 2220
gscassellati@cgsh.com

[1] See Regulation (EU) 2026/1744.

© Cleary Gottlieb Steen & Hamilton LLP,2026 . All rights reserved.
This memorandum, which contains general information and should not be regarded as legal advice, is intended for clients and friends of Cleary Gottlieb to update them on regulatory developments that may be of interest to them. Throughout this memorandum, "Cleary Gottlieb" and the "firm" refer to Cleary Gottlieb Steen & Hamilton LLP and its affiliated entities in certain jurisdictions; the term "offices" includes the offices of such affiliated entities.

I. Decree 160/2026: Key Changes to Criminal Law and Civil Procedure

1. New Criminal Offenses

Decree 160/2026 introduces a new offence under Article 437-*bis* of the Italian Criminal Code: 'Failure to adopt security measures in artificial intelligence systems and unlawful alteration of such systems'. The new offence builds on the AI-related offences already introduced by the AI Act, including the "Unlawful dissemination of content generated or altered using artificial intelligence systems" under Article *612-quater* of the Criminal Code (*deepfakes*) and copyright offences[2].

Article 437-*bis* criminalizes the following conduct if it endangers life, public or individual safety, or national security:

- failure, including through negligence, to implement the technical security measures required for designing, training, producing, or placing a high-risk AI system on the market, or the human monitoring measures needed to detect malfunctions (paragraph 1)[3];
- intentional failure by a professional user of high-risk AI systems to implement human oversight measures (paragraph 4)[4];
- unauthorized tampering with a high-risk AI system[5].

No actual harm is required: it is enough that the conduct puts life, public or individual safety, or national security at risk. A causal link between the conduct and the resulting risk must nevertheless be established. Establishing that link may be particularly challenging in a rapidly evolving field where the underlying technology is not yet fully understood.

2. High-Risk AI Systems

The new provision applies only to AI systems classified as high-risk under Article 6 of the AI Act. Rather than setting out a single definition, Article 6 identifies several categories of high-risk systems.

An AI system is classified as high-risk when both of the following conditions are met:

- the system is intended to be used as a safety component of a product, or is itself a product, covered by the Union harmonization legislation listed in Annex I (which covers, for example, in vitro diagnostic medical devices, lifts, radio equipment, vehicles and civil aviation, etc.);
- the product incorporating the AI system as a safety component, or the AI system itself, is required under that legislation to undergo a third-party conformity assessment before being placed on the market or put into service.

Article 6 also classifies the AI systems used in the sectors listed in Annex III as high-risk, subject to an exception for systems that do not pose a significant risk to individuals' health, safety, or fundamental rights. The following categories are particularly relevant to businesses:

- Human resources management: systems used to recruit and select candidates (including through automated CV *screening* and algorithmic interview assessments), make decisions affecting working conditions (task allocation, promotions, transfers, and dismissals), or monitor and evaluate employee performance.
- Credit and insurance risk assessment: *credit-scoring* systems used by banks and financial intermediaries to make lending decisions, and *risk assessment* systems used by insurers to

[2] For further details, see our alert memorandum "The new Italian law on AI: the first national legislation in the EU to complement the AI Act" dated 29 October 2025 (available at the following link: https://www.clearygottlieb.com/-/media/files/alert-memos-2025/italy-adopts-the-first-national-ai-law-in-europe-complementing-the-eu-ai-act.pdf).

[3] The offence carries a prison sentence of one to five years, rising to two to eight years where national security is endangered. Where the offence is committed through gross negligence, the penalty is reduced by one third to one sixth.

[4] The offence carries a prison sentence of one to five years, rising to two to eight years where national security is endangered.

[5] The offence carries a prison sentence of two to six years, rising to three to ten years where national security is endangered.

underwrite life and health insurance policies and set premiums.

- Other essential services: systems used by public or private entities to assess eligibility for healthcare or social security benefits, and systems used to prioritize emergency responses.

AI systems that profile individuals are always considered high-risk under Annex III.

3. Corporate Liability Under Decree 231: What Risks Do Companies Face?

Decree 160/2026 introduces a new category of predicate offenses under Article *25-vicies* of Decree 231 ('Offences committed through the use of artificial intelligence systems'). The following penalties apply:

- for 'Failure to adopt security measures in artificial intelligence systems and unlawful alteration of systems' (Article *437-bis* of the Criminal Code), a financial penalty ranging from €154,800 to approximately €1.5 million;
- for 'Unlawful dissemination of content generated or altered using artificial intelligence systems' (Article *612-quater* of the Italian Criminal Code), a financial penalty ranging from €51,600 to approximately €1 million;
- in both cases, the disqualification sanctions under Article 9(2)(b), (c), (d) and (e) of Decree 231 apply. These include the suspension or revocation of authorizations, licences, or concessions necessary to commit the offence; a ban on contracting with public authorities; exclusion from benefits, funding, grants and subsidies, and the possible revocation of any already awarded; and a ban on advertising goods and services. These sanctions do not, however, include a ban on conducting business.

4. Practical Implications for Companies

The inclusion of these offenses among the predicate offences under Decree 231 means that companies should review their Model 231, policies, and internal procedures to determine whether updates are needed. This is particularly relevant for companies that develop, produce, place on the market or use them in a professional capacity.

The first step will be to assess whether the AI systems used qualify as 'high-risk' and to keep a clear record of that assessment.

Although Article *437-bis* of the Italian Criminal Code does not expressly refer to the obligations under the AI Act, the delayed application of some of those obligations could affect the practical application of the new offense insofar as it concerns a failure to act (see Annex I). Nevertheless, companies would be well advised to begin identifying and assessing risks now and to adapt their controls progressively.

Practical steps could include:

- identifying all AI systems developed, produced, or used by the company and classifying them according to the AI Act's risk classification framework;
- reviewing and, where necessary, introducing or strengthening technical security measures and human oversight mechanisms for those systems;
- considering specific safeguards to prevent the creation or dissemination of *deepfakes* in business processes most exposed to this risk, including marketing and communications;
- establishing dedicated reporting channels to the Supervisory Body;
- providing targeted training to technical staff involved in system development and to legal, *compliance*, HR, and commercial teams.

5. Civil Procedural Aspects

Articles 16–20 of Decree 160/2026 introduce new civil procedure rules for claims seeking compensation for damage caused by the use of AI. These rules adopt *enforcement* tools already proposed at EU level in the

2022 Proposal for an AI Liability[6] Directive to the new technological context.

The new rules cover:

- the competent venue for such claims (Article 16(4));
- access to evidence (Article 17);
- the allocation of the burden of proof (Articles 18–19);
- the direct action against the insurer of the party identified as liable for damages (Article 20).

6. Scope of Application and Venue

Articles 16–20 of Decree 160/2026 distinguish between two categories of claims:

- under Article 16(1), contractual and non-contractual claims for compensation for damages caused by the use of an AI system;
- under Article 16(2), the narrower category of claims under paragraph 1 where damages result from a breach of one or more obligations under the AI Act.

In particular:

- the rules on access to evidence (Article 17) apply to the broader category of claims set out in paragraph 1 of Article 16;
- the rules introduced by Articles 18–19 of Decree 160/2026 apply to the narrower category under Article 16(2);
- the provisions relating to the competent venue (Article 16(4)) and to actions against the insurer apply both to the actions provided for in paragraph 1 and to those provided for in paragraph 2 of Article 16.

Article 16(4) provides that, in actions for damages governed by Decree 160/2026, the court of the place of residence or domicile of the damaged party also has jurisdiction where the latter is a natural person acting for purposes unrelated to any business, commercial, craft, or professional activity.

This allows a consumer to bring a claim before the court of their place of residence as an exception to the ordinary jurisdiction rules. The provision uses the definition of 'consumer' provided for under the Consumer Code (Article 3(1)(a) of Legislative Decree No. 206/2005).

7. Access to Evidence

Article 17 of Decree 160/2026 gives damaged parties a new way to obtain evidence in proceedings against the entity controlling the AI system. They may seek an order for the disclosure of evidence held by the system's provider.

The court will order disclosure at the request of the party claiming to have suffered damage where:

- the evidence is specifically relevant to the operation of the AI system; and
- the claimant provides sufficient evidence to establish a prima facie case, including a nexus between the AI system's output and the alleged damages. This means that the claim must appear sufficiently well-founded to justify the disclosure order.

The order may be addressed to the opposing party or to a third party holding the relevant evidence, such as the AI system's supplier.

Article 17(2) gives examples of evidence relevant to the operation of the AI system that may be requested:

- event logs automatically generated by AI systems, as referred to in Article 12 of the AI Act;
- the risk management system documentation *referred to* in Article 9 of the AI Act;
- relevant information contained in the technical documentation referred to in Article 11 of the AI Act;
- information on human oversight parameters and methods under Article 14 of the AI Act.

The AI Act already requires this documentation from entities in the *value* chain for high-risk AI systems. In defining the evidence that may be requested, Decree

[6] Proposal for a Directive of the European Parliament and of the Council on the adaptation of the rules on non-contractual civil liability to artificial intelligence, COM(2022) 496 final, 28 September 2022.

160/2026 therefore appears largely to refer to material that must *already* be prepared and retained for regulatory compliance. For high-risk systems, however, these documentation requirements are subject to the delayed application dates mentioned above. Until the relevant date set at EU level, a production order for these systems may therefore cover evidence other than that listed in Article 17(2) (see Annex I).

Under Article 17(3), a disclosure order must be limited to what is necessary and proportionate to the request. The court must consider the interests of all parties, particularly the protection of trade secrets and confidential information. If compliance with the order risks disclosing such information, the court must take appropriate protective measures. Article 17(4) of Decree 160/2026 expressly refers to Article *121-ter* of the Industrial Property Code (Legislative Decree No. 30/2005), which allows the court to:

- prohibit the use or disclosure of confidential information obtained during the proceedings (paragraph 1);
- restrict access to the case files to a limited number of persons (paragraph 3(a));
- order the redaction of sensitive parts in orders made available to third parties (paragraphs 3(b) and 4).

If a party fails, even in part and without good reason, to comply with a production order under Article 17 of Decree 160/2026, the court may draw evidential inferences from that failure under Article 116(2) of the Code of Civil Procedure.

However, where the failure to comply relates to the documentation listed in paragraph 2 of Article 17 (and indicated above), the sanction is more severe, as the Judge, having assessed all other evidence, deems the facts asserted by the applicant to be admissible – and, therefore, proven.

If a third party fails to comply with the order, the sanction is financial only: a fine ranging from €1,500 to €10,000.

This distinction reflects the fact that evidentiary sanctions may only be applicable to parties involved in the proceedings. For third parties, financial sanctions are instead used to encourage cooperation.

8. The Rebuttable Presumption of Causation and the Limits of Regulatory Compliance

Articles 18 and 19 of Decree 160/2026 introduce evidentiary rules that make it easier for claimants to pursue compensation for damages caused by the use of an AI system.

Article 18 introduces a rebuttable legal presumption of causal link between a breach of one or more obligations under the AI Act and the alleged damages. The claimant must prove the breach and the damages, but not the causal link between them. The defendant may rebut the presumption by providing evidence to the contrary.

Article 19 clarifies that compliance with the AI Act does not, by itself, rule out the defendant's liability, even where it has been certified under the assessment procedures in that Regulation. Regulatory certification does not amount to a court finding that the system is actually safe. It may nevertheless have evidentiary value, depending on the specific claims and defenses put forward.

For high-risk systems, the provisions described above are subject to the delayed application dates set at EU level (see Annex I). In particular:

- At present, the presumption under Article 18 can only apply in relation to obligations under the AI Act that are already enforceable;
- as regards conformity certification, Article 19 expressly refers to the rules for high-risk systems in Chapter III, Section 5 of the AI Act. This reference will therefore take practical effect only once the relevant EU rules apply.

9. Direct Action Against the Insurer

Article 20 of Decree 160/2026 allows a claimant alleging damages to bring a claim directly against the defendant's liability insurer, subject to the policy limits.

Before issuing proceedings, the injured party may ask the other party to identify their insurer and provide the policy details. The recipient must respond within 30 days. If the response is incomplete or no response is

given, the court may draw evidentiary inferences from that failure.

In an action brought directly against the insurance company:

- only contractual defenses that existed before the insured event may be raised against the injured party (Article 20(3));
- the party identified as liable for the damages is a necessary co-defendant in the proceedings (Article 20(5));
- the action is subject to the same limitation period as the action against the party identified as liable for the damage (Article 20(6)).

An insurer that pays the injured third party may recover the payment from the insured to the extent that the policy would have entitled the insurer to refuse or reduce payment (Article 20(4)).

* * *

II. New Provisions in Decree 179/2026: Supervisory Authorities and Penalties

1. The Competent Authorities and the Penalty Regime

Decree 179/2026, which applies to the entities referred to in Article 2(1) of the AI Act[7], continues the alignment of national legislation with the AI Act, regulating the powers of national authorities and the use of AI in training.

1.1 The National Notifying Authority

Decree 179/2026 establishes a multi-authority framework led by the National Cybersecurity Agency (ACN) and the Agency for Digital Italy (AgID). Certain sector-specific responsibilities remain with the Bank of Italy, CONSOB, IVASS, and the Data Protection Authority.

In particular, Article 4 designates AgID as the National Notifying Authority, namely responsible for establishing and implementing the procedures necessary for the assessment, designation, and notification of conformity assessment bodies and for their monitoring[8] . Specifically, AgID:

- exercises the powers relating to the notification procedures and the tasks set out in Articles 28, 30, and 36 of the AI Act[9], and may also issue implementing provisions for the latter and for Decree 179/2026 itself in matters falling within its remit (paragraph 1);
- is responsible for defining and carrying out the procedures for the assessment, designation, and notification of conformity assessment bodies (paragraph 2);

[7] By virtue of this reference (Article 2(2)), Decree 179/2026 applies to: *a)* providers of AI systems or general-purpose AI models within the European Union, even if established or located in a third country; *b) deployers* of AI systems established or located within the Union; *c)* suppliers and *operators* of AI systems established or located in a third country, where the output of such systems is used within the Union; *d)* importers and distributors of AI systems; *e)* manufacturers of products who place an AI system on the market or put it into service together with their product and under their name or trade mark; *f)* authorised representatives of suppliers not established in the Union; *g)* other relevant persons located in the Union.

[8] Conformity assessment bodies are entities that carry out, in an impartial capacity, activities such as testing, certification and inspections. Under the AI Act, conformity assessment serves to verify compliance with the requirements relating to high-risk systems (Section II, Chapter III, AI Act).

[9] The three provisions referred to in Article 13(1) of Decree 179/2026 concern, respectively, the notifying authorities, the procedure for notifying bodies to the Commission and other Member States, and amendments to notifications.

- ensures, on an ongoing basis, through periodic and ad hoc audits, that notified bodies and the entities referred to in Article 33[10] of the AI Act continue to meet the required criteria and fulfil their obligations (paragraph 3);
- initiates proceedings to restrict, suspend, or withdraw a notified body's designation if deficiencies or non-compliance are found, after giving the body an opportunity to be heard;
- may seek support from the national accreditation body for its assessment and monitoring work under Regulation (EC) No. 765/2008 on the accreditation of conformity assessment bodies (paragraph 5);
- must cooperate, when performing the tasks under paragraph 1, with the competent national and sectoral authorities, the European Commission, and the notifying authorities of other Member States, including under Union harmonization legislation, subject to the coordination rules in Article 12 of Decree 179/2026 (paragraph 6).

1.2 National Market Surveillance Authorities

For market surveillance, the Decree allocates responsibilities among the following authorities and governs their cooperation, including information sharing (Article 9):

- the ACN as the market surveillance authority for AI systems, pursuant to Article 70 of the AI Act (Article 5, paragraph 1, point (a)).
  In addition to being responsible for the national registration of high-risk AI systems (Article 14), the Agency also acts as the single point of contact[11]: the relevant contact details are therefore published on its official website and in the list of national contact points maintained by the European Commission (Article 6).
  Article 10 applies the national rules on market surveillance and product compliance[12] to ACN's activities, to the extent that they are compatible with the AI Act, but excludes Articles 11 and 12 of those national rules;
- the Bank of Italy, CONSOB and IVASS as the sectoral authorities responsible for the supervision of high-risk AI systems used, respectively, in the specified banking and credit, financial, and insurance activities, in accordance with their respective competences (Article 5(1)(b));
- the Data Protection Authority, within the scope of Article 74(8) of the AI Act[13] (Article 5(1)(c)).

These authorities must cooperate and coordinate their activities where their responsibilities overlap. The Decree allows the Notifying Authority and the market surveillance authorities to enter into agreements on information sharing and cooperation.

1.3 Penalties

Chapter II of Decree 179/2026 sets out the financial and non-financial administrative penalties for breaches of the AI Act and the procedures for imposing them (Articles 19–24).

In particular, unless the act constitutes a criminal offence, Article 23 of Decree 179/2026 provides for the following penalties:

- up to €35 million or, if higher, 7 per cent of annual global turnover for the year preceding the breach, for engaging in practices prohibited by Article 5 of the AI Act[14] (paragraph 1);

[10] That is to say, subsidiaries and subcontractors entrusted with assessment tasks.
[11] Article 70 of the AI Act requires each Member State to designate a market surveillance authority as the national contact point for the Regulation, to notify the Commission of its identity and to make its contact details publicly available.
[12] Legislative Decree No. 157/2022.
[13] This provision refers to high-risk AI systems used for law enforcement, border management, justice and democracy (points 6, 7 and 8, Annex III, AI Act), including biometric systems used in these areas.
[14] Such practices include the placing on the market, putting into service or use of AI systems that employ subliminal, manipulative or deceptive techniques (paragraph 1(a)), exploit vulnerabilities (paragraph 1(b)), assign social scores (paragraph 1(c)), predict criminal offences based

- up to €15 million or, if higher, 3 per cent of annual global turnover for the preceding year, for breaches of operators' and notified bodies' obligations on transparency, incident reporting and system classification (paragraph 2);
- up to €7.5 million or, if higher, 1 per cent of annual global turnover for the preceding year, for providing inaccurate, incomplete or misleading information in response to a request from notified bodies or the competent national authorities (paragraph 3);
- up to €1 million or, if higher, 0.5 per cent of annual global turnover for the preceding year, for breaches of the obligations concerning fundamental rights impact assessments for high-risk systems under Article 27 of the AI Act or the right to an explanation of decision-making under Article 86 (paragraph 4).

For small and medium-sized enterprises, including micro-enterprises and innovative start-ups, the penalty is based on the lower of the fixed amount and the turnover-based amount.

Although formally classified as administrative, these penalties are severe enough that they could be regarded as criminal in nature under the criteria applied for ECHR purposes.

Non-financial sanctions are also available for infringements involving a low level of harm or risk. Under Article 22, the competent authorities may order the infringement to stop and prohibit its repetition, specifying measures and deadlines where appropriate (paragraph 1(a)). If the infringement has already ceased, they may instead issue a public statement identifying it and the person responsible (paragraph 1(b)). Failure to comply with the order triggers the financial penalty for the original infringement, increased by up to one third.

Under Article 24, once the alleged infringements have been notified, any penalty must be imposed by a reasoned decision within a reasonable time (paragraph 1). AgID and ACN set the procedures and deadlines for their proceedings in their respective regulations (paragraphs 2 and 3). The Bank of Italy, CONSOB, IVASS, and the Data Protection Authority follow their respective sector-specific rules.

An extract of the decision must be published promptly on the competent authority's website, together with details of any appeals and their outcome (Article 24(4)[15]).

The timing of national penalties must be read alongside the dates on which the corresponding EU obligations apply. Introducing a national penalty does not bring forward the application of an obligation under the AI Act that has been deferred. Annex II sets out the relevant application dates and the AI Act provisions whose breach may result in a penalty.

2. Safeguards for Employment Decisions and Workplace Safety

Chapter III of Decree 179/2026 (Articles 36–51) governs the use of AI in training programs, professional practice, healthcare, and public administration. Two provisions are particularly relevant to businesses as employers.

Article 41 prohibits final decisions on starting, changing, or ending an employment relationship, including disciplinary measures and performance appraisals, from being based solely on automated processing. A human decision-maker with effective and independent authority must make the decision, and the employee's consent cannot override this prohibition (paragraph 1). A breach renders dismissals

solely on profiling (paragraph 1(d)), indiscriminately extract facial images to create or expand databases (point (e)), recognise emotions in the workplace or at school in the absence of medical or safety grounds (point (f)), biometrically categorise individuals to extract sensitive data (point (g)) or identify them biometrically remotely in real time, in publicly accessible spaces, for law enforcement purposes (point (h)).

[15] Publication must be in anonymised form where ordinary publication would be disproportionate in relation to the personal data concerned (point (a)), could compromise cybersecurity or a criminal investigation (point (b)), or could cause disproportionate and determinable harm to the data subjects (point (c)).

and other employer decisions null and void (paragraph 4).

The use of AI must also respect dignity, confidentiality, and the principle of non-discrimination (paragraph 2). Before processing begins, the employer must provide the information required by Article 1-*bis* of Legislative Decree No. 152/1997. On request, employees may obtain a clear explanation of the decision from a human reviewer, including any algorithmic component and the main parameters considered. The safeguards under Regulation (EU) 2016/679 on personal data protection continue to apply (paragraph 3).

On health and safety, Article 42 requires the risk assessment under Article 28 of Legislative Decree No. 81/2001 to consider AI systems that affect work organization, the pace of work, working methods, or safety-related decision-making (paragraphs 1 and 2). Employers must also give workers adequate information and training on AI-specific risks and the prevention and protection measures adopted (paragraph 3).

3. Protecting Trade Secrets Used in AI Training

AI development also raises questions about protecting companies' information and technical solutions. Articles 52 and 53 of Decree 179/2026 address the protection of these technological assets.

Article 52 adds paragraph 1-*bis* to Article 98 of the Industrial Property Code. It expressly includes data, algorithms, and mathematical methods used to train AI systems among the business information and technical and industrial know-how eligible for protection. Algorithms and mathematical methods also include model architectures, optimization functions, training procedures and configurations, and other technical and computational elements used to develop the systems. Protection is not automatic: the existing requirements under Article 98(1) still apply. The information must (i) be secret, (ii) have economic value because it is secret, and (iii) be subject to reasonably adequate measures to keep it confidential.

Article 53 confirms that disputes over these trade secrets remain within the jurisdiction of the specialized commercial divisions. It does not introduce a separate jurisdiction rule for AI-related information.

* * *

III. Conclusions

Decrees 160/2026 and 179/2026 mark a further step in Italy's regulation of AI. They introduce new criminal offenses, extend liability under Decree 231 and strengthen civil remedies for injured parties. They also establish national rules on supervision and administrative penalties, safeguards for AI use in employment, and protection for trade secrets. Companies that develop, supply or use AI systems, particularly high-risk systems, therefore need to update their *compliance*, technical, and organizational controls promptly and coordinate their response to criminal, administrative, and civil risks.

…

CLEARY GOTTLIEB

Annex I

Overview of the links, not expressly stated, between Regulation (EU) 2024/1689 (AI Act) and the criminal and civil procedure provisions of Legislative Decree No. 160/2026 (Decree 160); application dates and transitional arrangements under Articles 111 and 113 of the AI Act, as amended by Article 1, points 39 and 40 of Regulation (EU) 2026/1744.

Provision (AI Act)	Applicability (AI Act)
Criminal aspects	
Article 6 and Annexes I and III *Classification of high-risk AI systems*	December 2, 2027 (systems under Article 6(2) and Annex III) August 2, 2028 (systems under Article 6(1) and Annex I)*
Articles 9, 14, 15, and 26 *Risk management; security and oversight measures; obligations of* deployers *of high-risk AI systems*	
Civil procedure	
Articles 9, 11, 12, and 14 *Risk management, technical documentation, record-keeping, and human oversight*	December 2, 2027 (systems under Article 6(2) and Annex III) August 2, 2028 (systems under Article 6(1) and Annex I)*
Chapter III, Sections 2 and 3 (Articles 8–27) *Requirements and obligations for high-risk AI systems*	
Articles 5 and 50 *Prohibited practices; transparency obligations for suppliers and* deployers *of certain AI systems*	See Annex II.
Chapter III, Section 5 *Conformity assessment, certificates, and registration*	August 2, 2026 *(to be coordinated with the rules on high-risk systems)*

Annex II

Overview of infringements of Regulation (EU) 2024/1689 (AI Act) punishable under Article 23 of Legislative Decree No 179/2026 (Decree 179/2026) and the relevant maximum fines; effective dates and transitional arrangements pursuant to Articles 111 and 113 of the AI Act, as amended by Article 1, points 39 and 40 of Regulation (EU) 2026/1744.

Provision infringed (AI Act)		Applicability	Maximum fine
Article 23(1) of Decree 179/2026			
Article 5	Prohibited practices	February 2, 2025	€35 million or, if higher, 7 per cent of turnover
Article 5(1)(ba) and (bb)	Prohibitions relating to systems that generate or manipulate intimate or sexually explicit material of identifiable individuals without their consent, or child pornography or pornographic performances involving minors, subject to the conditions set out in paragraphs 1a and 1b	December 2, 2026	
Article 23(2) of Decree 179/2026			
Article 16	Obligations of providers of high-risk AI systems	December 2, 2027 (systems under Article 6(2) and Annex III)	
Article 22	Obligations of authorized representatives of suppliers of high-risk AI systems		

<table>
<tr><th colspan="3">Provision infringed (AI Act)</th><th>Applicability</th><th>Maximum fine</th></tr>
<tr><td>Article 23</td><td colspan="2">Obligations of importers of high-risk AI systems</td><td rowspan="4">August 2, 2028 (systems under Article 6(1) and Annex I) *</td><td rowspan="11">€15 million or, if higher, 3 per cent of turnover</td></tr>
<tr><td>Article 24</td><td colspan="2">Obligations of distributors of high-risk AI systems</td></tr>
<tr><td>Article 25</td><td colspan="2">Responsibilities along the AI value chain</td></tr>
<tr><td>Article 26</td><td colspan="2">Obligations of deployers of high-risk AI systems</td></tr>
<tr><td>Articles 31 and 33, paragraphs 1, 3 and 4</td><td colspan="2">Requirements for notified bodies and obligations of their subcontractors or affiliates</td><td rowspan="2">August 2, 2025 (to be coordinated with the regulations on high-risk systems)</td></tr>
<tr><td>Article 34</td><td colspan="2">Operational obligations of notified bodies</td></tr>
<tr><td rowspan="2">Article 50(2)</td><td rowspan="2">Transparency obligations for suppliers and deployers of certain AI systems</td><td>Labelling and traceability of synthetic outputs by suppliers, in a machine-readable format</td><td>August 2, 2026
December 2, 2026 (AI systems placed on the market before August 2, 2026)</td></tr>
<tr><td>Article 50(1), (3) and (4)</td><td>Information on interaction with AI systems, emotion recognition, and biometric categorization; disclosure that deepfakes and texts on matters of public interest are AI-generated, where applicable.</td><td>August 2, 2026 (to be coordinated with the rules on high-risk systems)</td></tr>
<tr><td>Articles 73 and 80</td><td colspan="2">Reporting of serious incidents
Procedure for AI systems classified as non-high-risk</td><td></td></tr>
<tr><td colspan="4">Article 23(3) of Decree 179/2026</td></tr>
<tr><td>Inaccurate, incomplete, or misleading information</td><td colspan="2">Provision of inaccurate, incomplete, or misleading information in response to a request from notified bodies or the competent national authorities</td><td>August 2, 2025 (imposition of penalties in accordance with the applicable national framework)</td><td>€7.5 million or, if higher, 1 per cent of turnover (Article 99(5) of the AI Act)</td></tr>
<tr><td colspan="4">Article 23(4) of Decree 179/2026</td></tr>
<tr><td>Article 27</td><td colspan="2">Fundamental rights impact assessment for high-risk AI systems</td><td>December 2, 2027 (systems referred to in Article 6(2) and Annex III)
August 2, 2028 (systems pursuant to Article 6(1) and Annex I)</td><td rowspan="2">€1 million or, if higher, 0.5 per cent of turnover</td></tr>
<tr><td>Article 86</td><td colspan="2">Right to an explanation of certain decisions based on the outputs of high-risk systems listed in Annex III, excluding point 2</td><td>August 2, 2026 (to be coordinated with the rules on high-risk systems)</td></tr>
</table>

* With the exception of high-risk systems used by public authorities, for AI systems placed on the market or put into service prior to the respective effective date, the application is subject to significant design changes made from that date onwards, without a general obligation to adapt systems that have remained unchanged (Article 111(2) of the AI Act).