THE IMPLICATIONS OF THE EU AI ACT FOR TURKISH COMPANIES

On 2 August 2026, Regulation (EU) 2024/1689 (the "**EU AI Act**" or "**Act**") became generally applicable.[1] Although Türkiye is not subject to the EU AI Act, the Act's extraterritorial reach covers a broad spectrum of Turkish companies, ranging from software vendors and outsourcing providers to industrial manufacturers that integrate AI into products exported to the EU market.

Compliance Timeline: Provisions Applicable as of 2 August 2026

Date	What applies
2 February 2025	Article 5 prohibitions; AI literacy obligation (Article 4)
2 August 2025	GPAI provider regime
27 July 2026	Governance and penalty framework (Articles 102-110)
2 August 2026	General application of the Act; Article 50 transparency obligations (chatbot disclosure, AI-content marking, deepfake labelling)
2 December 2026	New Article 5 prohibitions on AI-generated intimate imagery/CSAM; transition period for providers whose generative AI systems were already on the market
Due by 1 August 2027	Commission guidance on interplay with sectoral product safety law (Articles 8(2), 9(10), 17(3))
2 December 2027	Annex III standalone high-risk obligations (employment, credit scoring, biometrics, education, law enforcement, migration, justice)
2 August 2028	Annex I embedded high-risk systems (AI in machinery, medical devices and other product-safety-regulated goods)
2 August 2030	Pre-existing high-risk systems used by public authorities must comply regardless of the transitional carve-outs above

Article 5 prohibitions and the regime governing general-purpose AI (GPAI) models are already in force. Likewise, the transparency and labelling obligations under Article 50, together with the Act's enforcement and supervisory framework, became applicable on 2 August 2026.

By contrast, the more extensive compliance obligations applicable to high-risk AI systems under Annex III, including conformity assessment, technical documentation, and human-oversight requirements, have been deferred until December 2027 (and until August 2028 for embedded systems).

[1] The EU AI Act has a flexible implementation timetable. On 27 July 2026, Regulation (EU) 2026/1744 of 8 July 2026 entered into force, amending the compliance schedule. See EU AI Act, Article 113 (https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng); see also European Commission, *Rules for trustworthy artificial intelligence in the EU* (EUR-Lex Summary of Regulation (EU) 2024/1689) (https://eur-lex.europa.eu/EN/legal-content/summary/rules-for-trustworthy-artificial-intelligence-in-the-eu.html); and the Digital Omnibus Regulation on AI (https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng).

The revised implementation timeline provides businesses with additional preparation time. However, it is important that this period not lead companies to postpone implementation efforts. Rather it should be viewed as an opportunity to strengthen governance and compliance frameworks and to advance AI readiness initiatives.

Which Turkish Companies Fall Within the Scope of the EU AI Act

Article 2 of the EU AI Act establishes a market-plus-effects test reminiscent of Article 3 of Regulation (EU) 2016/679 ("**GDPR**"). Under this framework, the Act applies to:

(i) providers placing AI systems or GPAI models on the EU market, irrespective of where they are established;

(ii) deployers established in the EU;

(iii) importers and distributors;

(iv) authorized representatives of providers established outside the EU;

(v) affected persons located within the EU; and

(vi) providers and deployers established in third countries whose AI system output is used within the Union.

Accordingly, a wide range of Turkish businesses may fall within the scope of the Act even if they are established in Türkiye and have no physical presence in the EU. Examples include an HR-screening software provider licensing its solution to a German customer, a call-center managing interactions with customers in the EU, a manufacturer integrating AI into machinery intended for the single market, or a fintech company whose creditworthiness assessment are used as inputs in the decision-making processes of an EU credit institution.

Relevant Penalties

The EU AI Act sets fine ceilings above the GDPR, calculated by reference to global turnover:

- Up to EUR 35 million or 7% of worldwide annual turnover (whichever is higher) for breaches of Article 5 prohibitions;
- Up to EUR 15 million or 3% of worldwide annual turnover (whichever is higher) for non-compliance with core operator obligations (applicable to providers, importers, distributors, deployers, and notified bodies) and the transparency obligations under Article 50;
- Up to EUR 7.5 million or 1% of worldwide annual turnover (whichever is higher) for providing incorrect, incomplete, or misleading information to competent authorities or notified bodies.

SME's and start-ups benefit from a proportionality regime, under which the lower —rather than the higher— of the two applicable thresholds applies.

GPAI providers are subject to a separate supervisory and enforcement framework administered by the European Commission, which can impose fines of up to EUR 15 million or 3% of worldwide annual turnover.

As the Act's governance and sanctions framework forms part of its "general application" wave, the associated enforcement risks have existed since 2 August 2026. This remains the case notwithstanding that certain obligations relating to high-risk AI systems linked to those enforcement mechanisms will only become applicable at a later date.

Developments in Türkiye

As with GDPR before it, the EU AI Act continues to exert a gravitational pull on Türkiye's regulatory reform agenda. Three developments warrant particular attention:

- **Legislative developments:** Following the completion of the Turkish Grand National Assembly's AI Research Commission's work, a draft AI Law was submitted on 24 July 2025, proposing amendments relating to AI-related civil liability, alignment with Law No. 6698 on Personal Data Protection (KVKK), deepfake content, cybersecurity, and administrative sanctions. The proposal is still undergoing the legislative process, and further calibration toward the EU AI Act's risk-based approach is anticipated.
- **Institutional framework:** Türkiye's cyber and digital governance framework has generally evolved into a more integrated structure through successive legislative reforms. The

Cybersecurity Presidency was established by Presidential Decree No. 177, published on 8 January 2025. Its duties, powers, and enforcement authority were subsequently codified at the statutory level through Cybersecurity Law No. 7545. In addition, Presidential Decree No. 191 of 25 December 2025 renamed the General Directorate of National Technology, operating under the Ministry of Industry and Technology, as the General Directorate of National Technology and Artificial Intelligence, and expanded its remit to encompass the development of AI technologies, national AI policy, and data infrastructure. Taken together, these developments have contributed to the emergence of an increasingly significant institutional framework for AI oversight and governance.

- **Guidelines Issued by the Turkish Data Protection Authority:** The Personal Data Protection Authority has signaled its intent to treat AI as a governance issue, not merely a technological one, through its Generative AI and Personal Data Protection Guide published in 2025 and its 2026 publication on the Use of Generative AI Tools in the Workplace.

Roadmap for Turkish Companies

For many Turkish businesses, the immediate priority is not whether they build AI systems themselves, but rather identifying where AI is already being used across their products, services, supply chains, and customer-facing operations. Where a customer, distributor, affiliate, or end-user is located in the EU, the EU AI Act should generally be presumed applicable unless a specific assessment indicates otherwise.

Priority steps include the following:

- **Create an inventory and assigning responsibility:** Establishing an organisation-wide inventory of AI-systems, GPAI models, automated decision-making tools, and AI-enabled products, while clearly identifying the individuals or functions responsible for each of them.

- **Assessing and classifying EU AI Act exposure:** Evaluating whether specific AI-use cases fall within the scope of the Act and determining their regulatory classification. In light of the implementation timeline, particular attention should be paid to recruitment, employee monitoring, credit assessment, customer profiling, insurance risk assessment, biometric systems, critical infrastructure, healthcare, and industrial safety applications.

- **Ensuring compliance with Article 50:** Before the 2 December 2026 transitional cut-off for pre-existing systems, implementing measures to comply with requirements concerning chatbot disclosures, generative-AI output labelling, and deepfake disclosure obligations.

- **Reviewing contracts and supply chains:** Examining contractual representations and warranties, rights of access to technical documentation rights, audit and incident reporting obligations, and provisions related to cooperation with EU notified bodies.

- **Integrating AI compliance with privacy and cybersecurity processes:** AI-related risks are closely linked to existing obligations concerning personal data protection and cybersecurity. Addressing these areas in isolation may lead to duplication efforts and gaps in compliance programmes.

- **Monitoring regulatory developments:** Guidance issues by the European Commission, harmonized standards, and implementing measures will play a key role in shaping compliance expectations ahead of the high-risk AI transition date of December 2027. The Turkish legislative proposal is likewise expected to evolve in light of these developments.

Author

Derya Durlu Gürzumar
ddgurzumar@kolcuoglu.av.tr