


# Provisions on Prohibited Artificial Intelligence Systems Subject to the EU Artificial Intelligence Law Entered into Force

Sevgi Ünsal Özden  
Gölnur Çakmak  
İpek Ertem

ERDEM  
&  
ERDEM



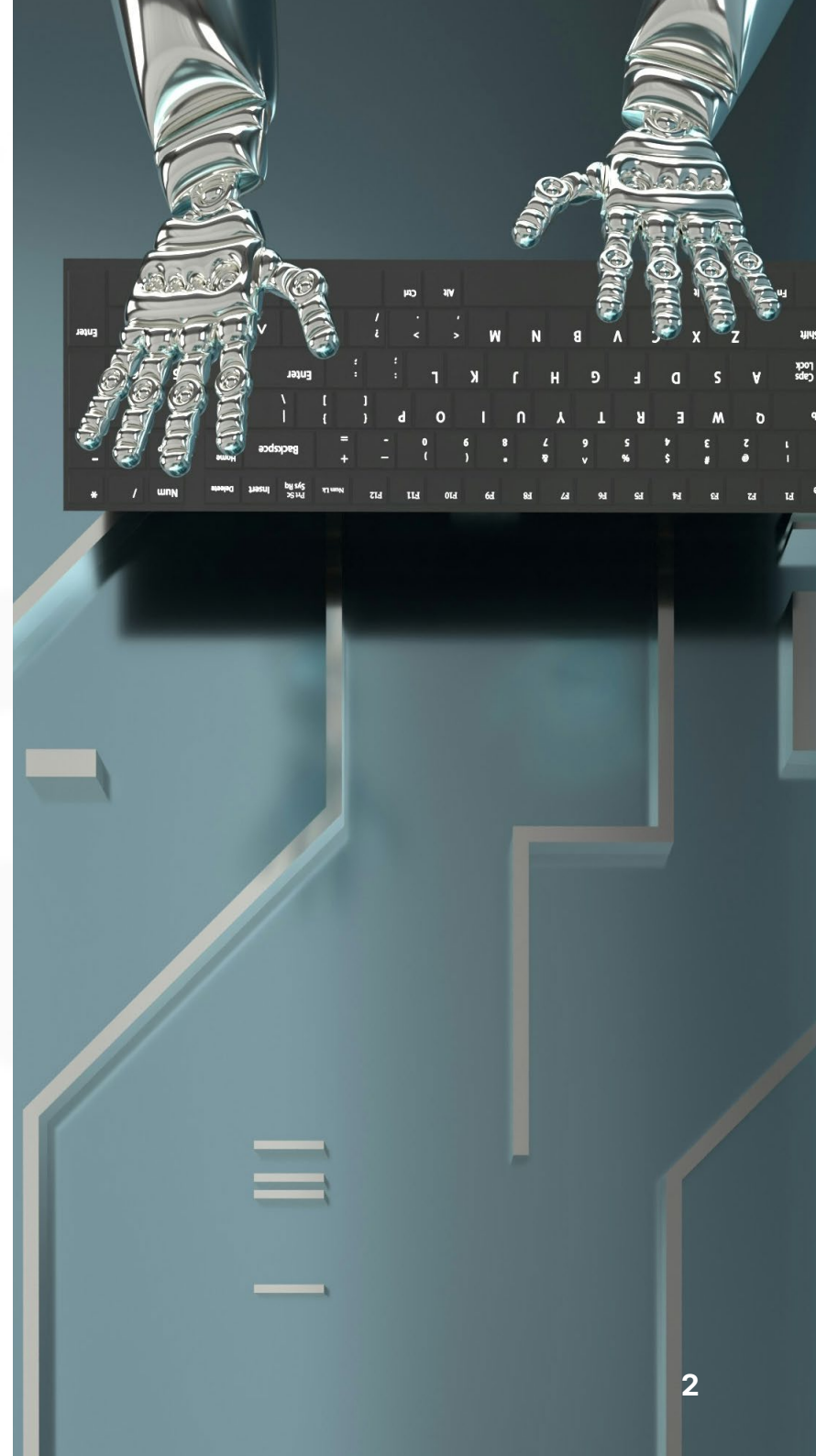
## Provisions on Prohibited Artificial Intelligence Systems Subject to the EU Artificial Intelligence Law Entered into Force

Under the European Union (EU) Artificial Intelligence Act (AI Act or the Act), the prohibitions concerning artificial intelligence (AI) systems that pose an unacceptable risk and threaten human safety, as outlined in “*Chapters I and II (general provisions and prohibited AI practices)*”, entered into force as of February 2, 2025.

The Act classifies AI systems based on risk levels and imposes a complete ban on those who pose an unacceptable risk.

# AI Literacy Requirement

Article 4 of the Act mandates that organizations providing or utilizing AI systems must ensure that their employees and other relevant individuals engaging with AI systems possess adequate AI literacy. This requirement must be fulfilled by considering the technical knowledge, experience, training, and the context in which AI systems are deployed. AI literacy encompasses the ability to use AI systems informally, understand both the opportunities and risks associated with AI, and recognize potential harms.





# Prohibited AI Systems

As of February 2, 2025, the following AI applications are strictly prohibited:

**Social Scoring Systems:** AI applications used by public authorities, private companies, or other entities that assess individuals based on their social behavior or personality traits, leading to discriminatory or disadvantageous outcomes.

**Emotion Recognition Systems:** AI technologies that analyze individuals' emotions in workplaces and educational institutions.

**Biometric Identification and Facial Recognition Systems:** AI systems that create biometric databases by collecting large-scale facial data from the internet or CCTV footage.

**Crime Prediction Profiling:** AI systems that predict the likelihood of individuals committing crimes based on personality profiling.

**Use of Sensitive Biometric Data:** AI systems that engage in discriminatory categorization based on sensitive personal data, such as race, political views, trade union membership, religious beliefs, or sexual orientation.

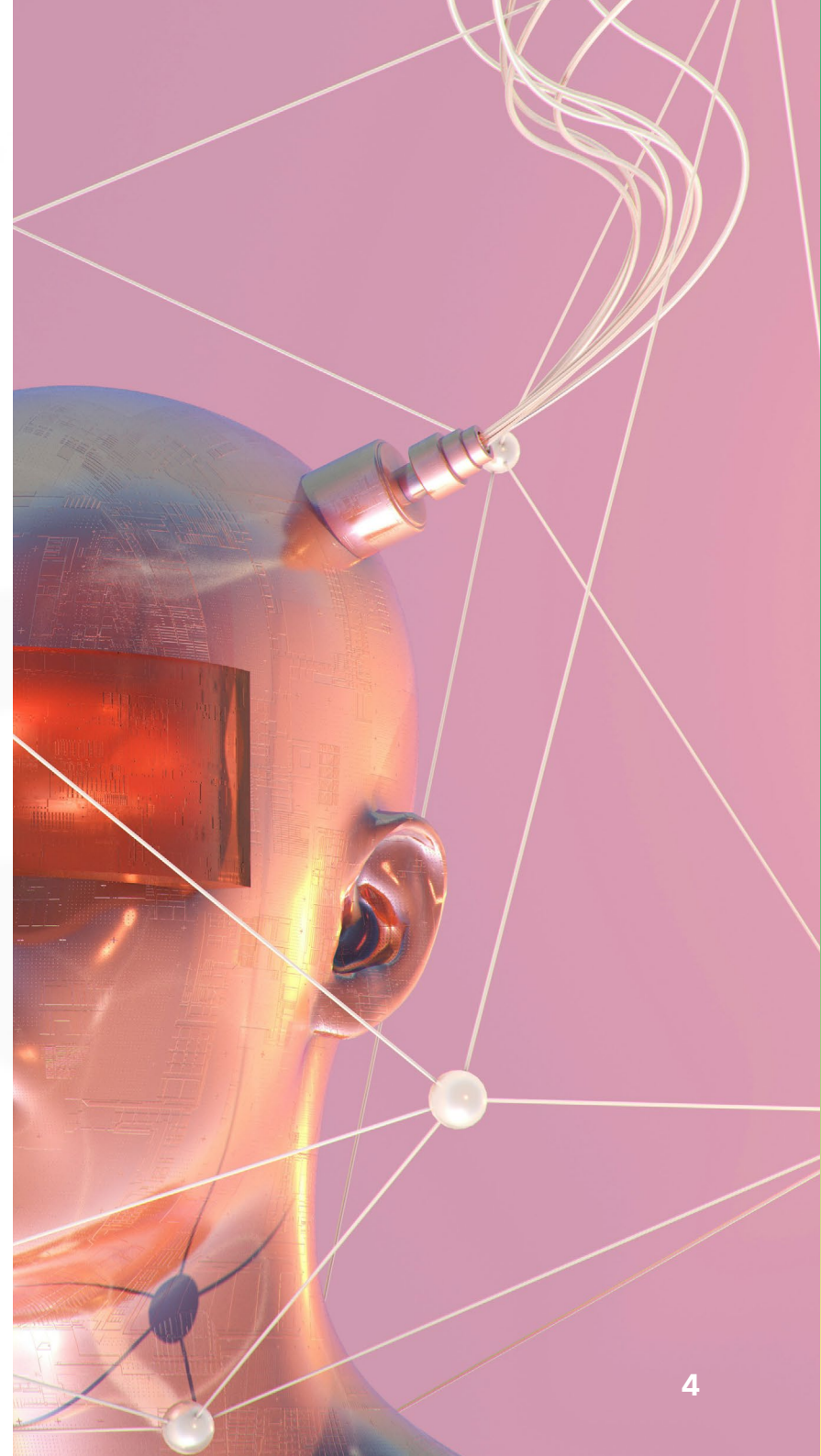
**Subliminal Manipulation and Exploitation of Vulnerabilities:** AI applications that impair individuals' ability to make conscious decisions or exploit personal vulnerabilities such as age or disability.

**Real-Time Biometric Surveillance:** AI systems that collect biometric data in publicly accessible spaces in real time, except in specific law enforcement exceptions.

## Sanctions

Non-compliance with the enforceable provisions of the AI Act carries the risk of severe administrative fines. The applicable sanctions are set to be implemented as of **August 2, 2025**.

A maximum fine of *EUR 35 million* or up to *7% of the company's total worldwide annual turnover for the preceding financial year*, whichever is higher.



# Key Contacts



**Özgür Kocabaşođlu**  
Partner and Head of Corporate  
[ozgurkocabasoglu@erdem-erdem.av.tr](mailto:ozgurkocabasoglu@erdem-erdem.av.tr)



**Sevgi Ünsal Özden**  
Managing Associate and Mediator  
[sevgiunsal@erdem-erdem.com](mailto:sevgiunsal@erdem-erdem.com)



**İstanbul**  
Ferko Signature  
Büyükdere Caddesi, No. 175 Kat. 3, 34394, Esentepe - Şişli, İstanbul  
+90 212 291 73 83 / +90 212 291 73 82  
[istanbul@erdem-erdem.av.tr](mailto:istanbul@erdem-erdem.av.tr)

**İzmir**  
1476 Sokak, No. 2, D. 27, Aksoy Plaza Alsancak, İzmir  
+90 232 464 66 76 / +90 232 466 01 21  
[izmir@erdem-erdem.com](mailto:izmir@erdem-erdem.com)

**Amsterdam**  
Office 4.31, Strawinskylaan 457, 1077 XX Amsterdam  
+31 (0)20 747 1113  
[amsterdam@erdem-erdem.nl](mailto:amsterdam@erdem-erdem.nl)