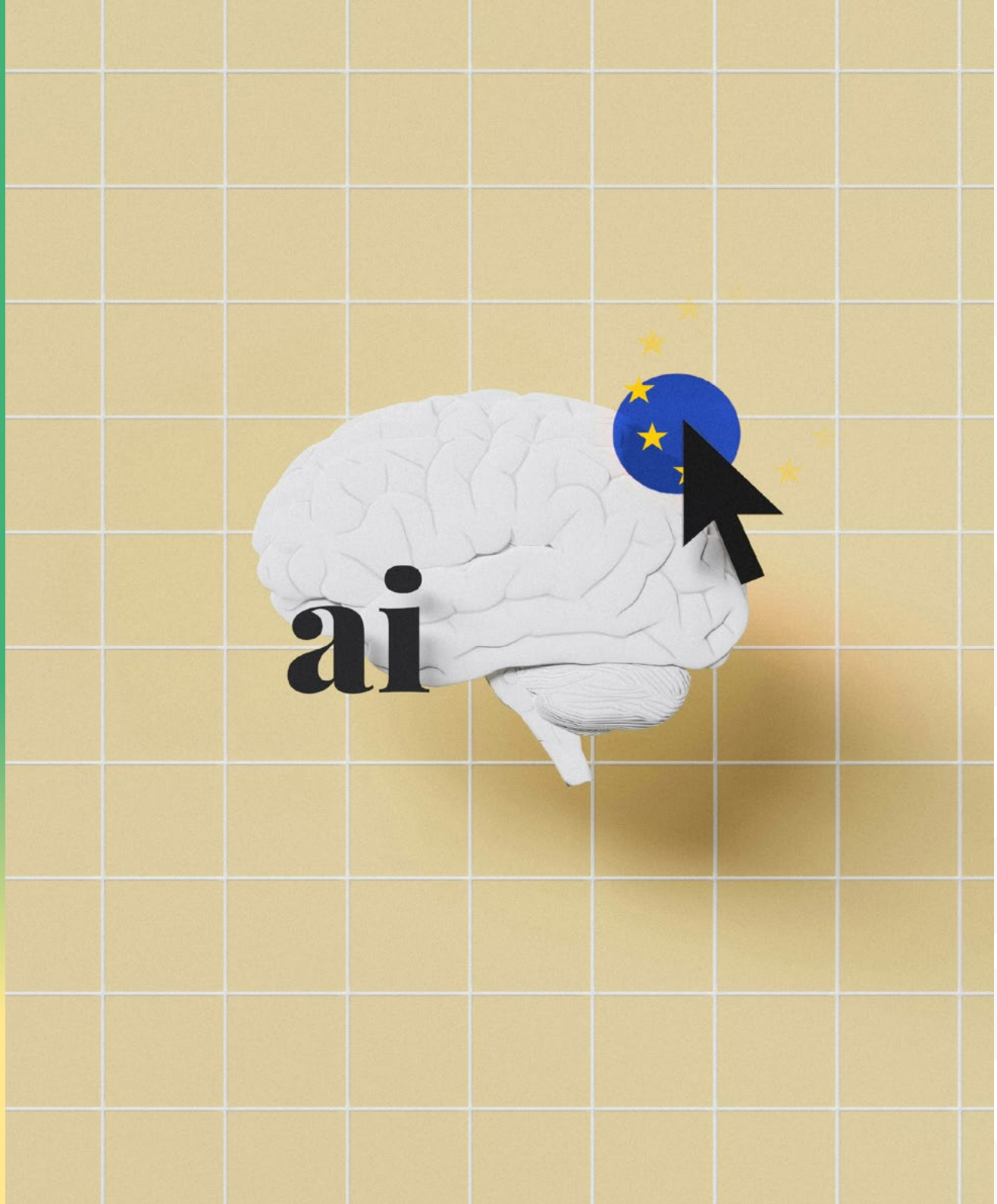


The EU Digital Framework:

A Compliance Guide to DSA, DMA, Data Act and AI Act

Ecem Süsoy Uygun
Sevgi Ünsal Özden
Tilbe Birengel
Ozan Akman
Gülnur Çakmak Ergene
İlayda Salkım

ERDEM & ERDEM
40 YEARS

Introduction

The Digital Transformation of European Regulation

The European Union ("EU") is reshaping the digital economy through groundbreaking regulations that govern how digital services, platforms, data, and artificial intelligence systems operate. **The Digital Services Act** ("DSA"), **Digital Markets Act** ("DMA"), **EU Data Act** ("Data Act"), **EU AI Act** ("AI Act"), EU Data Governance Act, Cyber Resilience Act, Digital Operational Resilience Act, and EU Cybersecurity Act form the cornerstone of the EU's digital policy framework, collectively known as the "European Digital Strategy".

Unlike traditional sector-specific regulations, these instruments adopt a horizontal approach affecting businesses across all industries. Whether you operate an e-commerce platform, provide cloud services, develop artificial intelligence ("AI") applications or manufacture connected devices, compliance is a fundamental requirement for doing business in or with the EU.

Why Non-EU Companies Must Pay Attention

A critical feature of the EU's digital regulations is their extraterritorial scope. These laws apply not only to companies established within the EU but also to any business, regardless of where it is headquartered, that offers goods or services to users in the EU or whose activities affect EU users. This means that Turkish companies, even those without a physical presence in Europe, may fall within the scope of these regulations under certain conditions.

For Turkish businesses engaged in cross-border digital commerce, software development, data processing or technology services, compliance is not merely a legal obligation, it is a competitive necessity and a gateway to one of the world's largest markets.

The Cost of Non-Compliance

Administrative fines can reach up to **3-10% of worldwide annual turnover**, with higher penalties for repeated infringements. EU regulators have demonstrated their willingness to enforce these rules against both EU and non-EU companies.

A Proactive Approach to Compliance

Early engagement with these requirements offers significant advantages:

- **Market access:** Demonstrating compliance builds trust with EU customers and partners
- **Risk mitigation:** Identifying gaps early avoids costly fines and operational disruptions
- **Operational efficiency:** Compliance requirements align with best practices that improve business operations
- **Future-proofing:** Mastering EU compliance positions you for similar requirements in other jurisdictions

What This Guide Covers

This guide provides a practical overview of four major EU digital regulations. For each, we outline the scope, key obligations, enforcement mechanisms and practical compliance steps.

Digital Services Act

Who is Subject to the DSA Compliance Process?

The DSA applies to intermediary service providers (mere conduit, caching, hosting) offering services including: (i) **online platforms** and **marketplaces**, (ii) **online search engines** and (iii) **cloud** and **web hosting services** to users having their place of establishment or that are located in the EU. Non-EU providers are covered when services are offered to EU Member States users, and a substantial connection exists (significant user numbers or activities targeting EU).

What are the Key Obligations under the DSA?

The obligations under the DSA vary, following a tiered approach with escalating obligations based on service type and size:

Obligations for All Intermediary Service Providers	• Designate and publish a single point of contact for authorities and service users. • Non-EU providers must appoint a legal representative in one of the EU Member States where the service is offered. • Publish clear terms and conditions and annual transparency reports.
Additional Obligations for Online Platforms and Online Search Engines	• Establish internal complaint-handling with human oversight and access to out-of-court dispute settlement. • Prohibit dark patterns in interface design and targeted advertising based on special categories of personal data. • Implement measures against misuse.
Additional Obligations for Hosting Services	• Establish easy-to-use electronic notice-and-action mechanisms allowing individuals or entities to notify illegal content. • Provide statements of reasons to affected users when restricting content or suspending accounts, including information on redress possibilities.
Specific Obligations for Online Marketplaces	• Trader traceability (KYBC): collect and verify trader identity, contact details, payment information and trade register data; suspend non-compliant traders. • Inform consumers when illegal products/services are identified.
Obligations for Very Large Online Platforms/Search Engines (VLOPs/VLOSEs) *(Having 45 million or more monthly active users on average in the EU)*	• Conduct annual systemic risk assessments and implement proportionate risk mitigation measures. • Undergo independent annual audits and implement audit recommendations. • Provide at least one recommender system option not based on profiling. • Maintain publicly accessible advertising repositories with content, advertiser details, targeting parameters and reach metrics.

What happens if you do not comply?

Failure to comply may result in administrative fines of up to **6% of worldwide annual turnover** and periodic penalties of up to **5% of average daily turnover**.

Digital Market Act

What is DMA?

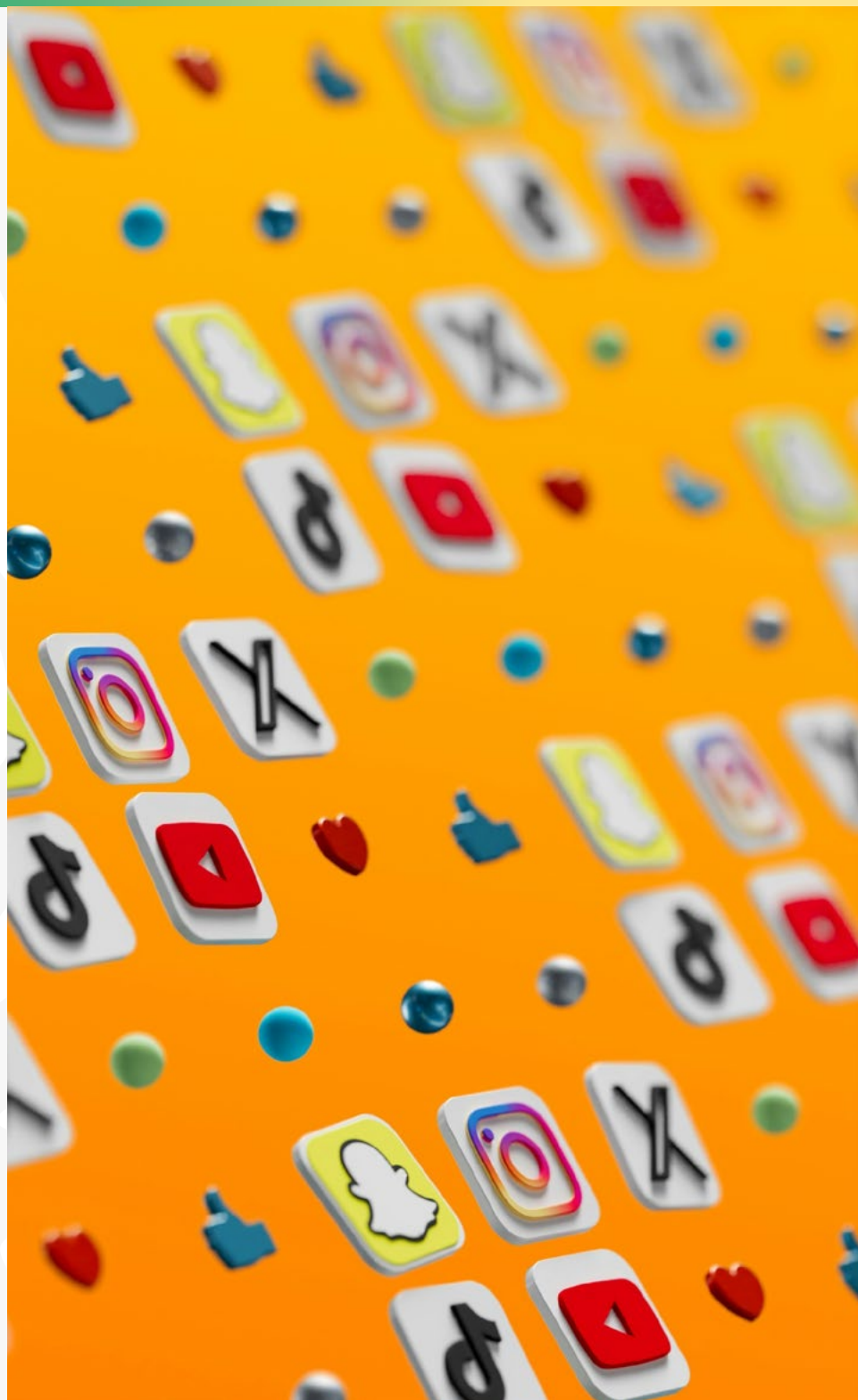
The DMA regulates the gatekeeper power of the largest digital platforms providing core platform services *(e.g., search engines, app stores, messaging, social networks)* that serve as key gateways between business users and end users.

Who is subject to the DMA Compliance Process?

Platforms meeting the following thresholds are designated as gatekeepers by the European Commission:

- €7.5 billion annual EU turnover or EUR 75 billion market capitalization
- 45 million monthly active end users in the EU
- 10,000 yearly active business users in the EU

Designated gatekeepers as of the date of this Guide: 7 companies covering 23 core platform services (*Alphabet/Google, Amazon, Apple, ByteDance/TikTok, Meta, Microsoft, Booking*).[*]



* European Union Official Website, Digital Markets Act, https://digital-markets-act.ec.europa.eu/gatekeepers_en.

Key Do’s and Don’ts:

- ✔ Ensure interoperability with third-party services
- ✔ Prohibit self-preferencing of own services over competitors
- ✔ Allow users to uninstall pre-installed apps
- ✔ Provide business users with access to their own data generated on the platform
- ✔ Refrain from combining personal data across services without explicit user consent
- ✔ Provide transparent ranking parameters and fair access to app stores

What happens if you do not comply?

- Fines up to 10% of worldwide annual turnover (20% for repeated infringements)
- Periodic penalty payments up to 5% of average daily worldwide turnover
- Structural remedies including forced divestiture for systematic non-compliance

EU Data Act

Who is Subject to the Data Act?

The Data Act applies to: (i) manufacturers of connected products *(e.g., smart home devices, industrial machines, vehicles, sensors)* and providers of related digital services interacting with such products or processing user-generated data *(e.g., mobile applications, cloud dashboards/platforms)*, (ii) data holders controlling access to generated data, *(e.g., manufacturers/platform operators deciding who may access usage, performance, or sensor data)*, (iii) providers of data processing services, in particular cloud and edge service providers, (iv) participants in data spaces and smart-contract-based data sharing arrangements, including platforms that enable multiple parties to share data through smart contracts and (v) users of connected products and digital services interacting with such products or data generated by users.

Businesses relying on access to generated data, such as repair and maintenance providers, logistics and mobility operators, data analytics and AI-driven companies, are also directly affected, as the Data Act grants new rights to request and receive such data under defined conditions.

Turkish companies may fall within scope where their connected products or digital services are offered to EU users or where they act as data holders or cloud service providers.

What are the Key Obligations under the Data Act?

Data Holders	• Ensure users can access their generated data and request that their data is shared with designated third parties. • Apply fair, reasonable and non-discriminatory (FRAND) terms when making data available to third parties. • Provide data to public bodies in cases of exceptional need. • Do not use data to derive insights into the user's economic situation or undermine the user's commercial position.
Data Recipients (and, where applicable, Users)	• Use data only for purposes agreed with the user. Do not develop, train or improve a competing connected product/related digital service using obtained data. • Respect security and integrity of products and services. • Do not share data onward without contractual authorization, where such sharing could undermine market fairness. • Do not share data with DMA-designated gatekeepers.
Data Processing Service Providers	• Enable switching and data portability between providers. Remove contractual, technical or financial lock-in mechanisms that restrict customer mobility and market competition. • Implement safeguards against unlawful third-country access to EU-held non-personal data.

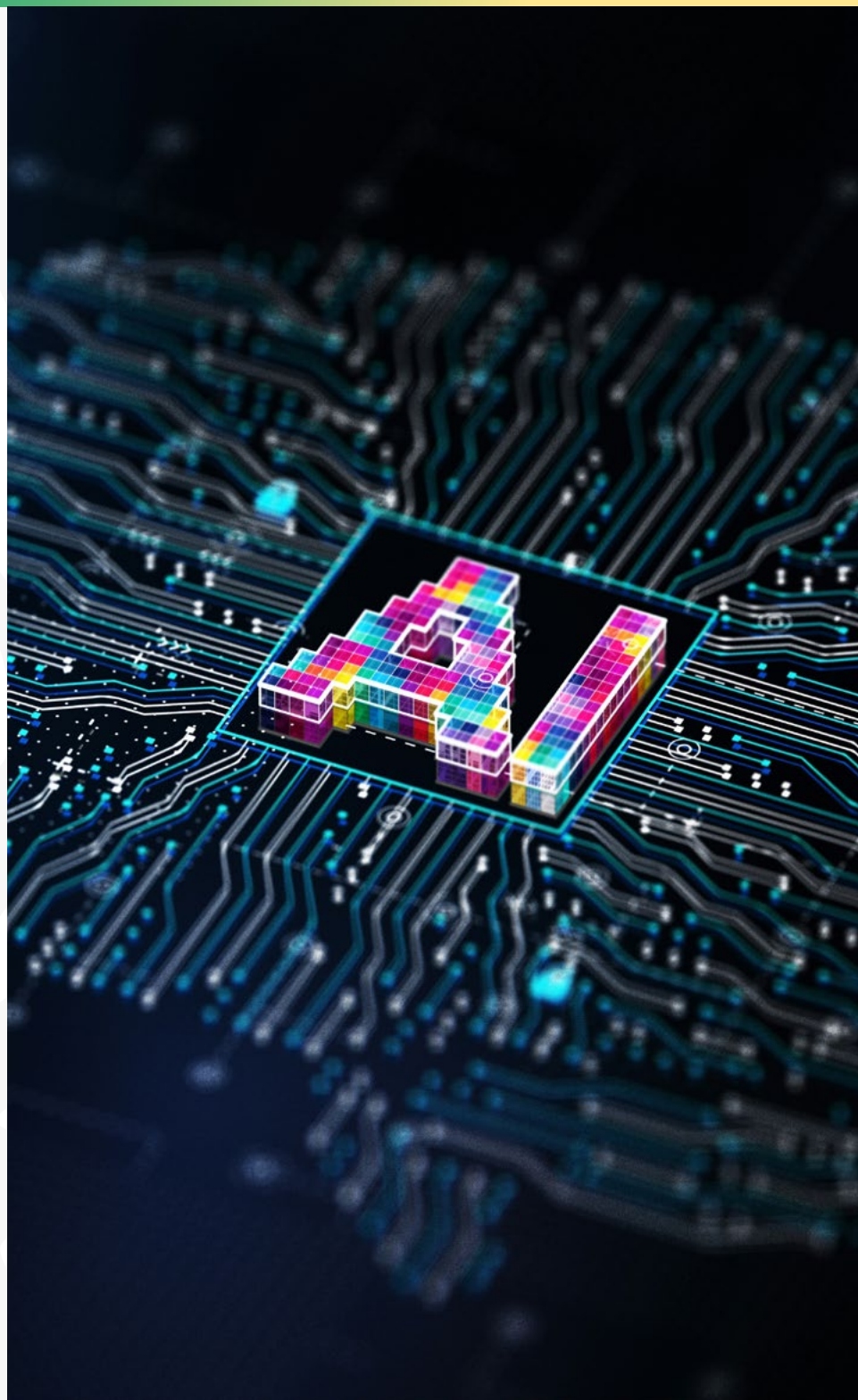
What happens if you do not comply?

- Administrative fines are determined under national law, which must be effective, proportionate and dissuasive.
- For certain infringements involving personal data, data protection authorities may impose administrative fines using the penalty framework and maximum levels set out in the General Data Protection Regulation (GDPR).

EU AI Act

Who is subject to the AI Act?

The EU AI Act applies to providers, deployers, importers and distributors of AI systems placed on the EU market or put into service in the EU, regardless of where they are established. Turkish companies fall within scope where their AI systems are placed on the EU market, put into service in the EU, or their outputs are used in the EU.



What are the Key Obligations under the AI Act?

The AI Act follows a risk-based approach, under which different obligations apply depending on the risk level of AI systems.

Unacceptable

AI practices that pose an unacceptable risk to fundamental rights are strictly prohibited. This category covers a range of practices, including manipulative or exploitative AI techniques, social scoring, real-time biometric identification in public spaces (with limited exceptions), emotion recognition systems in workplaces and schools, and particular forms of predictive policing, as well as untargeted scraping of internet or CCTV footage for facial images to build databases.

High Risk

AI systems used in economically and sensitive areas such as *employment, education, critical infrastructure, self-employment, essential private and public services, law enforcement, migration, asylum, border control* etc. or AI systems subject to EU product safety legislation are classified as high-risk. These systems are subject to enhanced obligations, including pre-market conformity assessment, risk management, data governance, technical and compliance documentation, transparency documentation and human oversight arrangements. Additionally, providers outside the EU are obligated to appoint a representative in the EU.

Limited Risk

Certain AI systems, particularly those interacting directly with individuals or generating synthetic or manipulated content, are classified as limited-risk and are subject to transparency obligations. Examples include chatbots and conversational AI tools (such as *ChatGPT, Gemini* etc.), voice-based virtual assistants, and tools generating AI-created text, images etc. Users must be clearly informed that they are interacting with an AI system or that the content has been generated/manipulated by AI. This requires the preparation of transparency notices.

No / Minimal Risk

AI systems that pose no or minimal risk are not subject to additional obligations under the AI Act. This category covers the majority of AI applications, such as *AI-enabled productivity tools, spam filters, recommendations systems*, for which compliance remains voluntary.

Providers of **General Purpose AI (GPAI)** models must meet additional documentation and governance obligations, with enhanced duties for systemic risk models. GPAI models are broadly trained AI models, such as large language or foundation models, that can be adapted for many different tasks and integrated into various AI systems, including chatbots, search tools, and content generation systems (e.g., *ChatGPT*). Their cross-sector reuse triggers specific documentation and governance obligations under the AI Act, including maintaining technical documentation, providing relevant information and documentation to downstream providers integrating these models into AI systems, publishing a sufficiently detailed training data summary, and ensuring compliance with EU copyright law. Additionally, providers of GPAI models established outside the EU are obligated to appoint a representative in the EU.

What happens if you do not comply?

- Fines up to:
  - EUR 35 million or 7% of worldwide annual turnover for prohibited AI practices.
  - EUR 15 million or 3% for other infringements.
  - EUR 7.5 million or 1.5% of annual turnover for incorrect reports.
- Corrective measures *(e.g. bringing AI system into compliance or withdrawing it from the EU market)*.

Legal Services Provided by Erdem & Erdem

As Erdem & Erdem, we provide comprehensive legal advisory to businesses seeking to comply with the EU's digital regulatory framework. Our practice areas include:

Regulatory Compliance Assessment and Strategy

We conduct comprehensive assessments to determine which EU digital regulations apply to your business, identify compliance gaps and develop tailored implementation strategies to ensure full regulatory compliance.

Legal Documentation and Contractual Support

We draft and review all necessary documentation including terms and conditions, privacy policies, reports, platform agreements, data sharing arrangements and trader contracts to meet regulatory requirements.

Training and Ongoing Advisory

We deliver compliance training programs for your teams, provide regular updates on evolving EU digital legislation and offer strategic advice on regulatory risk management.

Key Contacts

Compliance with EU digital regulations, which impose distinct obligations for each type of business, requires a meticulous and sensitive process. In this process, as Erdem & Erdem, we provide legal support to local and foreign companies to continue their activities in the EU market in compliance with the new digital legislation and aim to find answers to all questions that may arise.

Key Individuals

Ecem Süsoy Uygun
Managing Associate
ecemsusoy@erdem-erdem.av.tr

Sevgi Ünsal Özden
Managing Associate and Mediator
sevgiunsal@erdem-erdem.com

Tilbe Birengel
Managing Associate
tilbebirengel@erdem-erdem.nl

Ozan Akman
Senior Associate
ozanakman@erdem-erdem.av.tr

Offices

Istanbul
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

Izmir
1476 Sokak, No. 2, D. 27, Aksoy Plaza
Alsancak, İzmir
+90 232 464 66 76 / +90 232 466 01 21
izmir@erdem-erdem.com

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