AI Act - Fact Sheet

On 21 May 2024, the AI Act was finally passed by the European Council. It will enter into force 20 days after its publication in the Official Journal. The new regulatory framework may require significant legal and engineering effort to (re-)design affected AI-driven products/services and to ensure compliance when placing such products/services on the market or otherwise use them. Organizations should evaluate their compliance strategies well in advance of the enforcement deadlines, as the new legal obligations may require significant time to plan and implement technical and organizational solutions in connection with any internal or customer-facing use of AI systems.

Scope

The AI Act targets **providers** (entities that develop, place on the market or put into service an AI system) and **deployers** (entities who commercially use AI systems under their authority).The AI Act is in general **risk-driven**, categorizing certain AI practices as prohibited practices as well as high-risk AI systems and general-purpose AI models, depending on the level of risk they pose to health, safety, fundamental rights, etc.

Obligations

The AI Act imposes various obligations on certain AI systems, primarily high-risk systems, including:

- **Transparency** through **traceability** and **explainability**
- **Technical documentation** of the AI model, including its training and testing process,
- **User-awareness** regarding interaction with an AI system communicating or interacting with an AI system
- **Information/documentation obligations for** providers regarding deployers
- **Risk assessments** and **cybersecurity measures**
- **Human oversight**
- **Risk** and **quality management system** and **post market monitoring**
- **Conformity assessment** and **EU declaration of conformity**
- **Registration** of high-risk AI systems in an EU database.

Timeline

After the AI Act enters into force,

- **prohibited AI systems** must be disabled within 6 months (approx. December 2024),
- the AI Act will be **fully applicable** after 24 months (approx. June 2026),
- **obligations regarding high-risk AI systems** are to be fulfilled within 36 months (approx. June 2027).

Compliance risks

Non-compliance with the AI Act may have serious negative consequences for affected organizations, including:

- **Severe administrative fines** (up to EUR 35m or 7% of the total worldwide annual turnover of the preceding financial year, whichever is higher)
- **Actions of competitors** under laws on unfair competition
- **Claims for damages** by affected persons
- **Loss of reputation**
- **Negative impact on ESG ratings**

AI Act – Capability Statement

Drawing on our many years of experience as a market-leading firm in data & tech, we provide our clients with wide-ranging and balanced advice on the robust implementation of regulatory requirements in the fields of artificial intelligence and data law, including the new AI Act:

AI Act Readiness – Scope, Impact, Implementation

- **Scope**: Comprehensive review which of your organization's products/services and business processes are affected by the AI Act
- **Impact:** Assessment of the AI Act's impact for the affected products/services and business processes, including risk classification of AI systems
- **Implementation:** Planning and structuring the practical implementation of the AI Act in your organization considering key compliance risks under the AI Act

AI Compliance by Design and by Default

- **Innovation Support**: Advising on new products/services and business processes to ensure compliance with the AI Act and other applicable (Data & AI) regulatory requirements by design and by default
- **Documentation**: Preparing mandatory documentation and transparency information for providers, deployers and customers

AI Governance

- **Framework & Strategy**: Establishing a robust and efficient AI compliance governance and tailored compliance strategy for effective management of AI compliance requirements in synergy with established data protection governance
- **ACMS**: Implementing practicable AI compliance management systems (ACMS) to plan, implement, monitor and improve risk-based compliance measures for provision or deployment of AI systems
- **Certification**: Providing guidance on obtaining relevant certifications

AI Sourcing

- **Vendor Due Diligence:** Assessment of AI vendors/vendor agreements and contract drafting to ensure compliance with the AI Act and other relevant Data & AI regulation
- **Risk Mitigation**: Drafting and negotiating agreements along the AI value chain to mitigate liability risks
- **Data Separation**: Protection of IP rights and shielding confidential information and personal information in the context of AI training

Our Data, Tech & Telecom and Digital Business teams are happy to support our clients in navigating the complex regulatory framework of European and national legislation.