Scope of EU Al Act (1) - systems and models

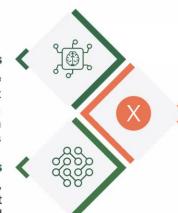


Al systems

Autonomous and adaptive machine-based system that generates output (e.g., predictions, content, recommendations) from the input it receives

General-purpose AI models

Al model displaying generality, capable of performing distinct tasks, and that can be integrated into downstream systems



Exceptions

- Military, defense, or national security purposes
- Scientific research and development
- Al systems or models research, testing, or development
- Personal non-professional activity
- Free and open-source licenses

Scope of the EU Al Act(2) - operators





Providers

Develops an Al system, places it on the market or puts it into service under its own name or trademark, whether for payment or free of charge



Deployers

Natural or legal person, public authority, or agency using an Al system under its authority



Importers

EU established, placing on the market an Al system with name/trademark of person in a third country



Distributors

Present in the **supply chain**, other than the provider or the importer, makes AI system available in EU

Risk-based approach

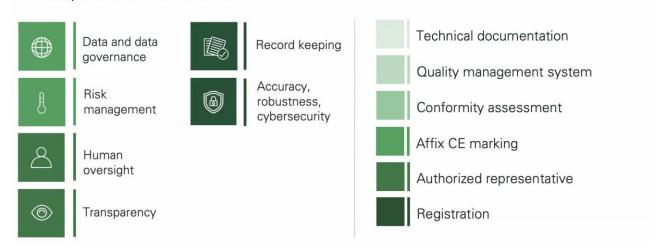




High-risk AI systems - requirements providers (1)



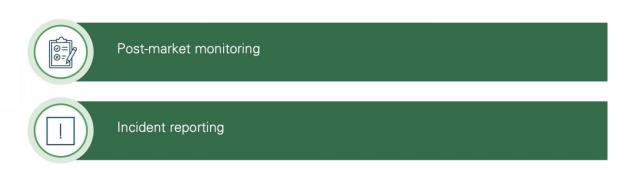
Before placement on the market



High-risk AI systems – requirements providers (2)



After placement on the market



High-risk Al systems - requirements deployers



General-purpose AI (GPAI) models



Requirements for providers



Up-to-date documentation



Detailed summary



Copyright law



Authorized representative

GPAI with systemic risk (high impact capabilities)



Model evaluation



Assess and mitigate systemic risks



Document and report serious incidents



Adequate level of cybersecurity

Enforcement and compliance timeline

Fines



Prohibited Al practices €35 million (or 7% of global revenue)

Most other requirements €15 million (or 3% of global revenue)

Supplying incorrect information €7.5 million (or 1% of global revenue)

Prohibited Al practices



February 2, 2025



May 2, 2025



Code of Practice GPAI

GPAI Rules Penalties



August 2, 2025

August 2, 2026



High-risk Al requirements

Al governance roadmap



Al use strategy



Defining business problem, discovering AI opportunities

Responsible Al use parameters



How to embed your organization's values into Al governance?

Setting up compliance infrastructure



Assessing the existing infrastructure, AI requirements, operationalizing AI governance.

Responsible AI use parameters





Al that solves something

Human-centric ethics built-in Al

Robust data protection practices embedded in Al

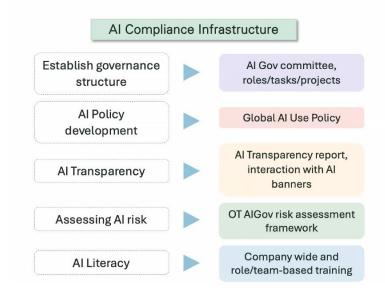
Al with human in the loop

OneTrust Responsible AI use principles





Operationalizing Al Governance



Al governance challenges



Responsible data governance



Compliant data flows



Regulatory requirements

Key data governance risks in Al systems:

Risk descriptions & possible solutions

Uncertainty about data residency

Reversal of deidentification and anonymization of data

No control over input data

Repurposing of data

Quality of Training/Testing data External AI vendor using ingested data to train/improve its services

OneTrust OneAl risk assessment program

Visibility into data governance

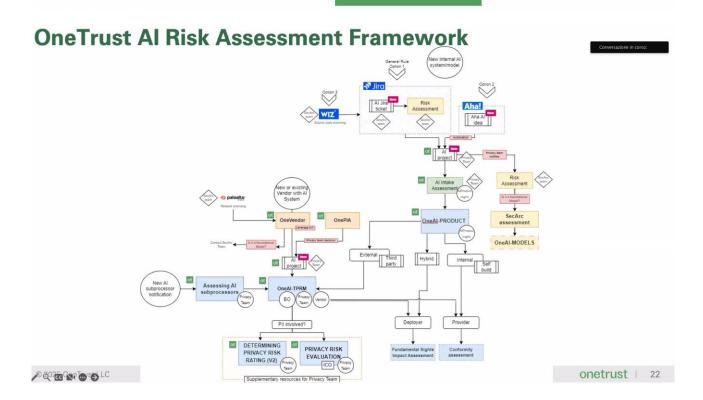
Holistic approach to Al risk assessments Central depository for all information

Collaboration

Promoting Al literacy

Documentation for audits

Assessment lifecycle: faster turn around



Helping customers meet EU Al Act compliance



Data & Al Governance Al Policy Setting & Orchestration Al Inventory Al Ecosystem Integrations EU Al Act, Art 9, 10, 11, 13,17,18, 48, 52, 54,61,62; Annexes IV, V, VI, IX EU Al Act, Art 9, 10, 11, 13,17,18, 48, 52, 54, 61, 62; Annexes IV, V, VI, IX EU Al Act, Art. 12, 13, 14, 15, 72 3 2 Design Deployment Development Strategy & planning Data management Evaluation & validation Notice Identify AI systems & evaluate AI risk per EU AI Act levels Evaluate & manage proprietary and open-source AI/ML models Scan and classify data and set governance policies Summarize key model Monitor model KPIs documentation details Map data transfers Manage consent for training data sets Conduct risk assessments (FRIA, PIA, DPIA) Manage third-risk for Al vendors & suppliers Manage Al incidents end users