onetrust

Operationalizing the EU AI Act

28 January, 2025

Today’s Speakers

Anastasia Konova
Privacy Analyst

Adomas Siudika
Senior Privacy Counsel
Research

Bex Evans
GTM Strategy – Data & AI
Governance

Poll:
Which best describes your role within your organization?

A. Privacy
B. Legal
C. IT
D. GRC
E. Infosec
F. AI Governance
G. Data
H. Other

Today's Agenda

1. Classifying & managing AI in accordance with the EU AI Act
2. A practitioner's perspective
3. How OneTrust helps

Classifying & managing AI in accordance with the EU AI Act

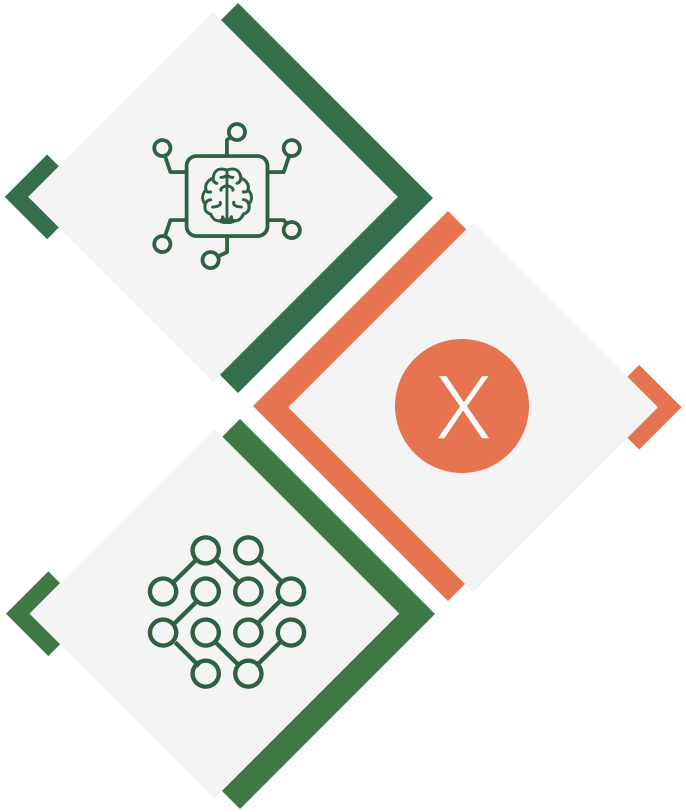
Scope of EU AI Act (1) - systems and models

AI systems

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

General-purpose AI models

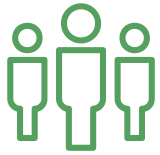
AI model displaying **generality**, capable of performing **distinct tasks**, and that can be **integrated** into downstream systems



Exceptions

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

Scope of the EU AI Act(2) - operators



Providers

Develops an AI 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 AI system under **its authority**

Importers

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

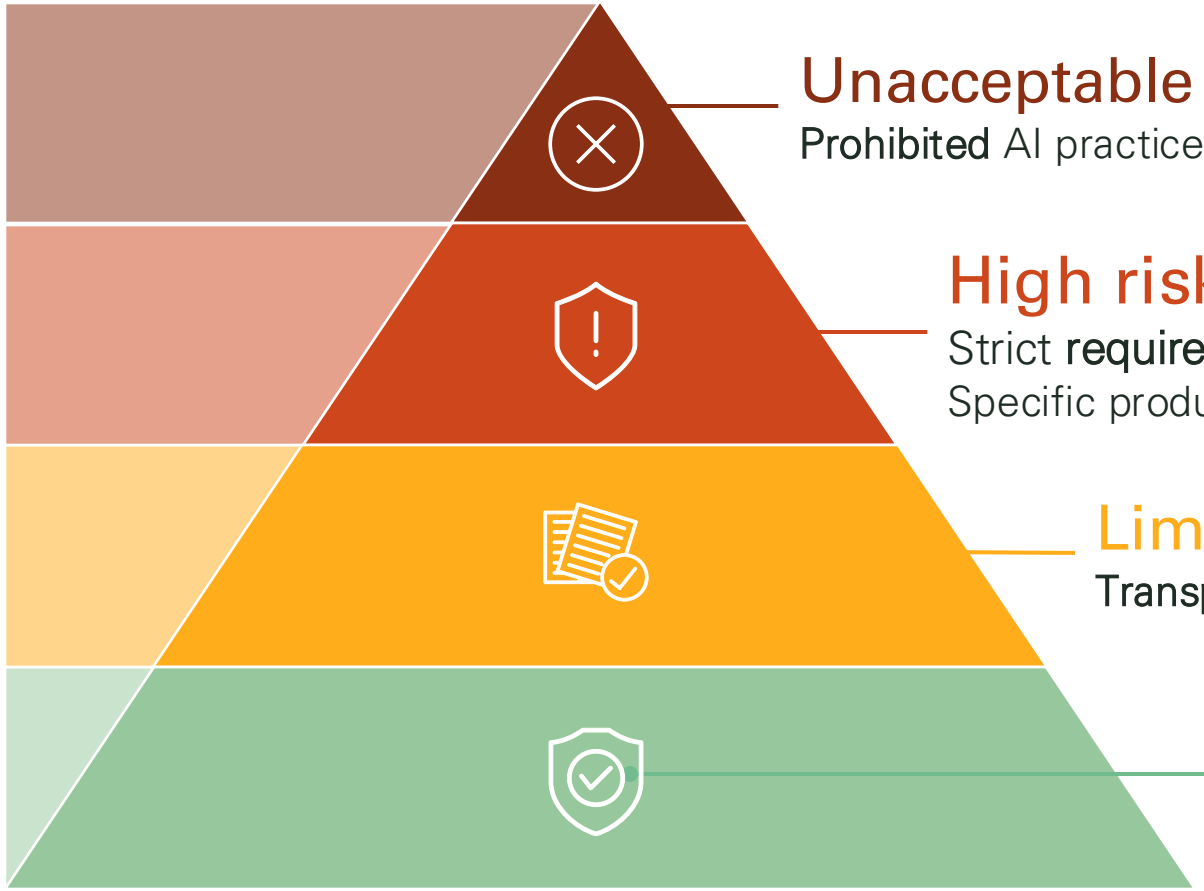
Distributors

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

Poll:
Which best describes your organization's relationship to AI & ML technologies? (Select all that apply)

A. We are a provider
B. We are a deployer
C. We are a distributor
D. We are an importer

Risk-based approach



Unacceptable risk

Prohibited AI practices

E.g. social scoring, facial recognition

High risk

Strict **requirements**
Specific products and areas

E.g., education, employment, immigration, critical infrastructure, toys

Limited risk

Transparency obligations

E.g., genAI applications, chatbots, deepfakes

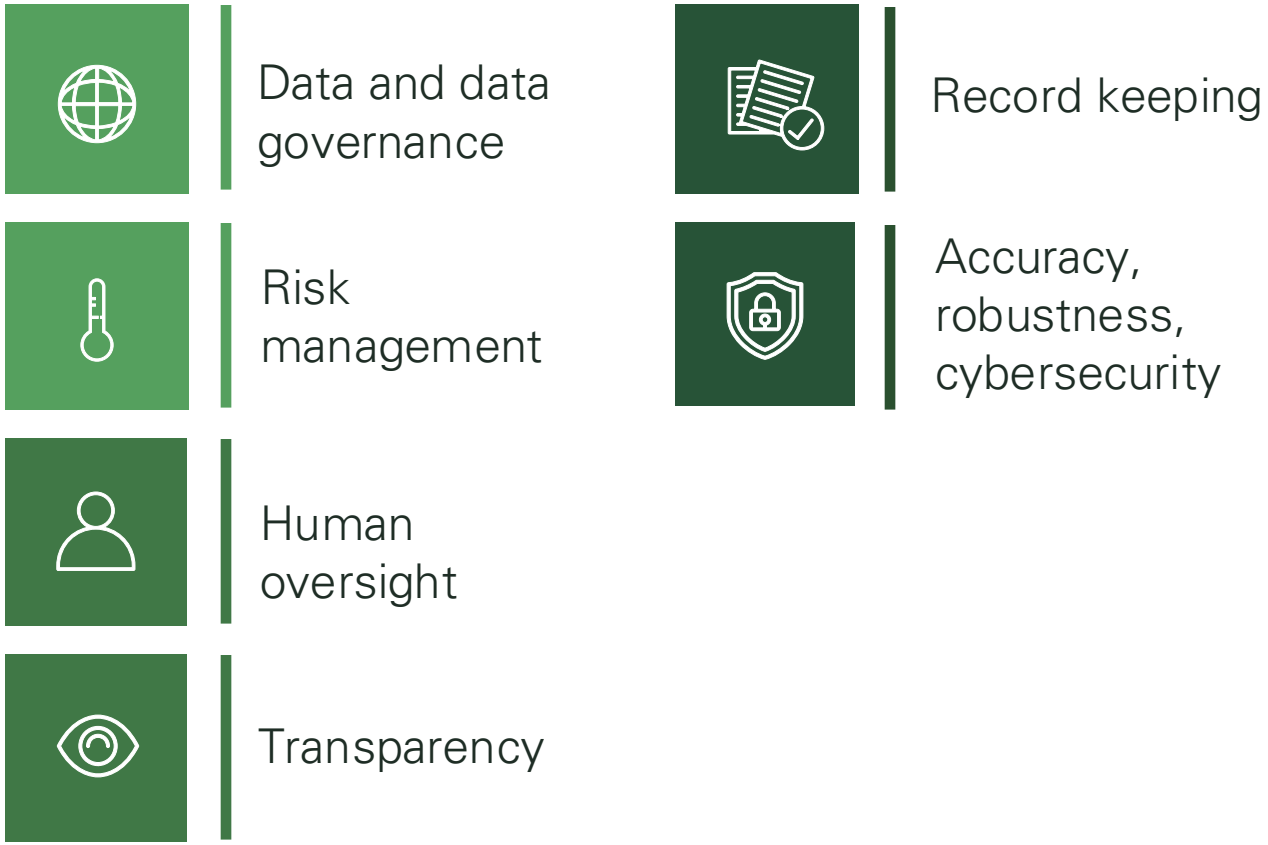
Minimal risk

Majority of AI systems
Voluntary **codes of conduct**

E.g., spam filters, video games

High-risk AI systems – requirements providers (1)

Before placement on the market



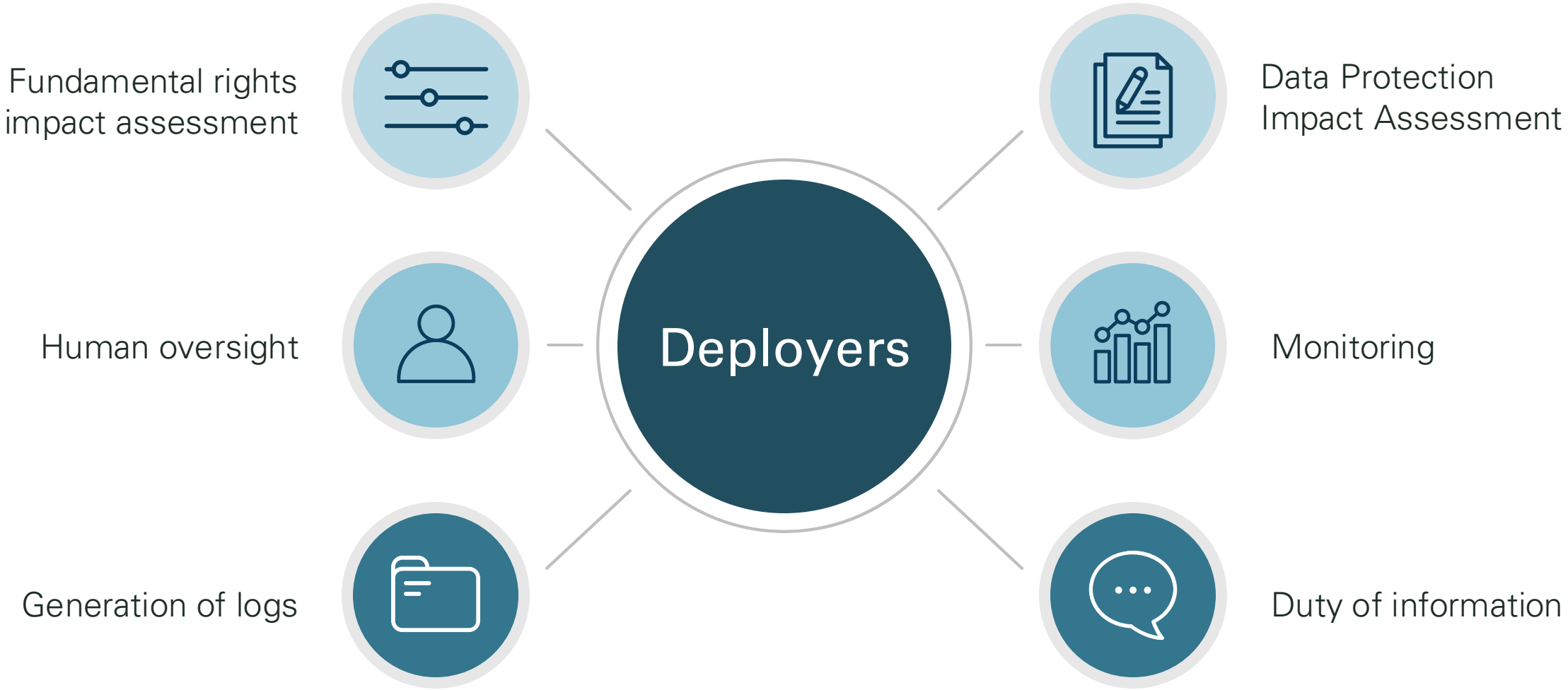
High-risk AI systems – requirements providers (2)

After placement on the market

Post-market monitoring

Incident reporting

High-risk AI 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

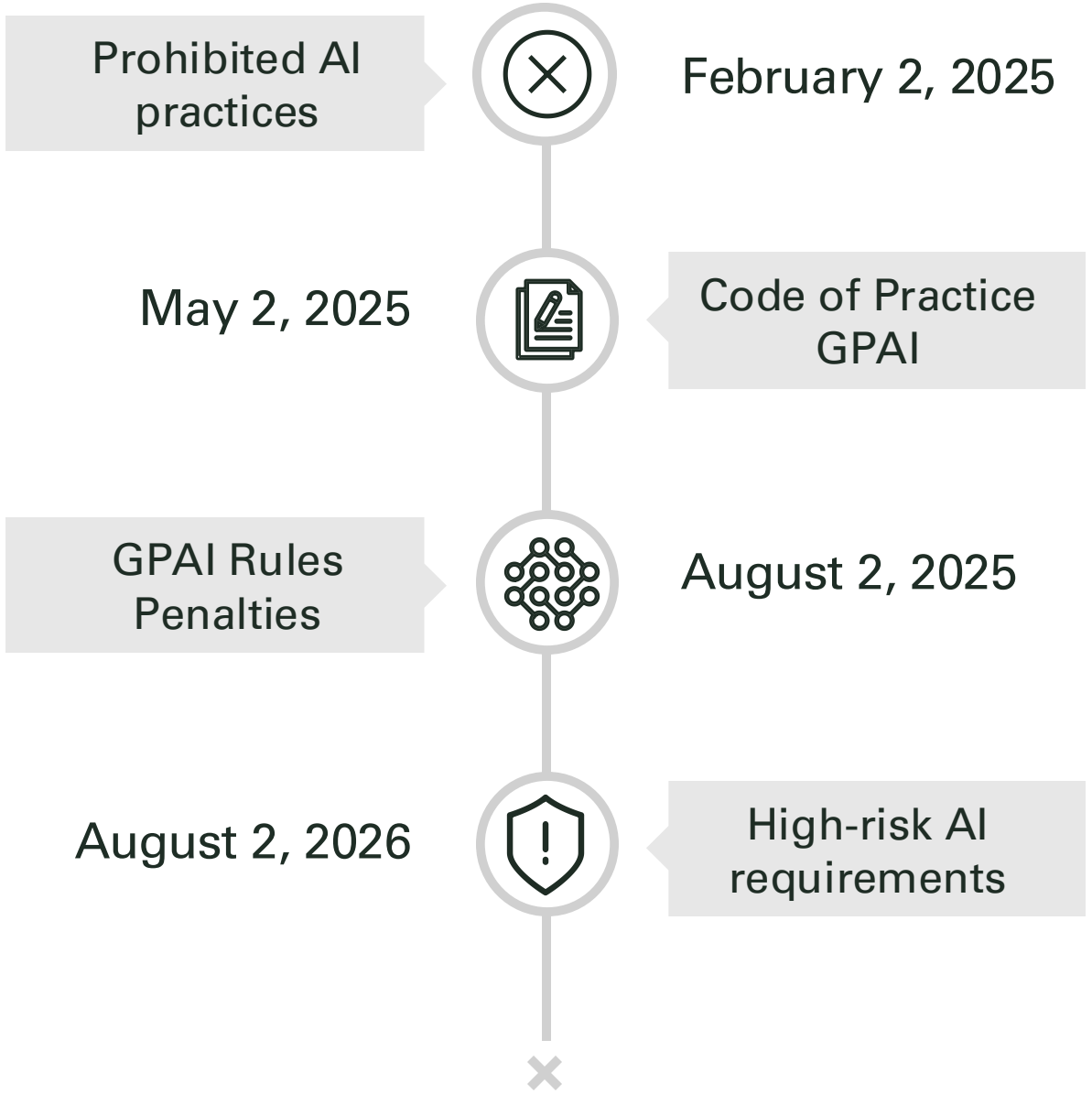
Enforcement and compliance timeline

Fines

Prohibited AI 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)



A practitioner’s perspective

AI governance roadmap

AI use strategy	Responsible AI use parameters	Setting up compliance infrastructure
Defining business problem, discovering AI opportunities	How to embed your organization's values into AI governance?	Assessing the existing infrastructure, AI requirements, operationalizing AI governance.

Responsible AI use parameters

AI with controlled impact

AI that solves something

Human-centric ethics built-in AI

Robust data protection practices embedded in AI

AI with human in the loop

OneTrust Responsible AI use principles

Operationalizing AI Governance

AI Compliance Infrastructure

Establish governance structure	AI Gov committee, roles/tasks/projects
AI Policy development	Global AI Use Policy
AI Transparency	AI Transparency report, interaction with AI banners
Assessing AI risk	OT AIGov risk assessment framework
AI Literacy	Company wide and role/team-based training

AI governance challenges

- Responsible data governance
- Compliant data flows
- Regulatory requirements

Key data governance risks in AI systems:

Risk descriptions & possible solutions

Uncertainty about data residency

Reversal of deidentification and anonymization of data

No control over input data

Repurposing of data

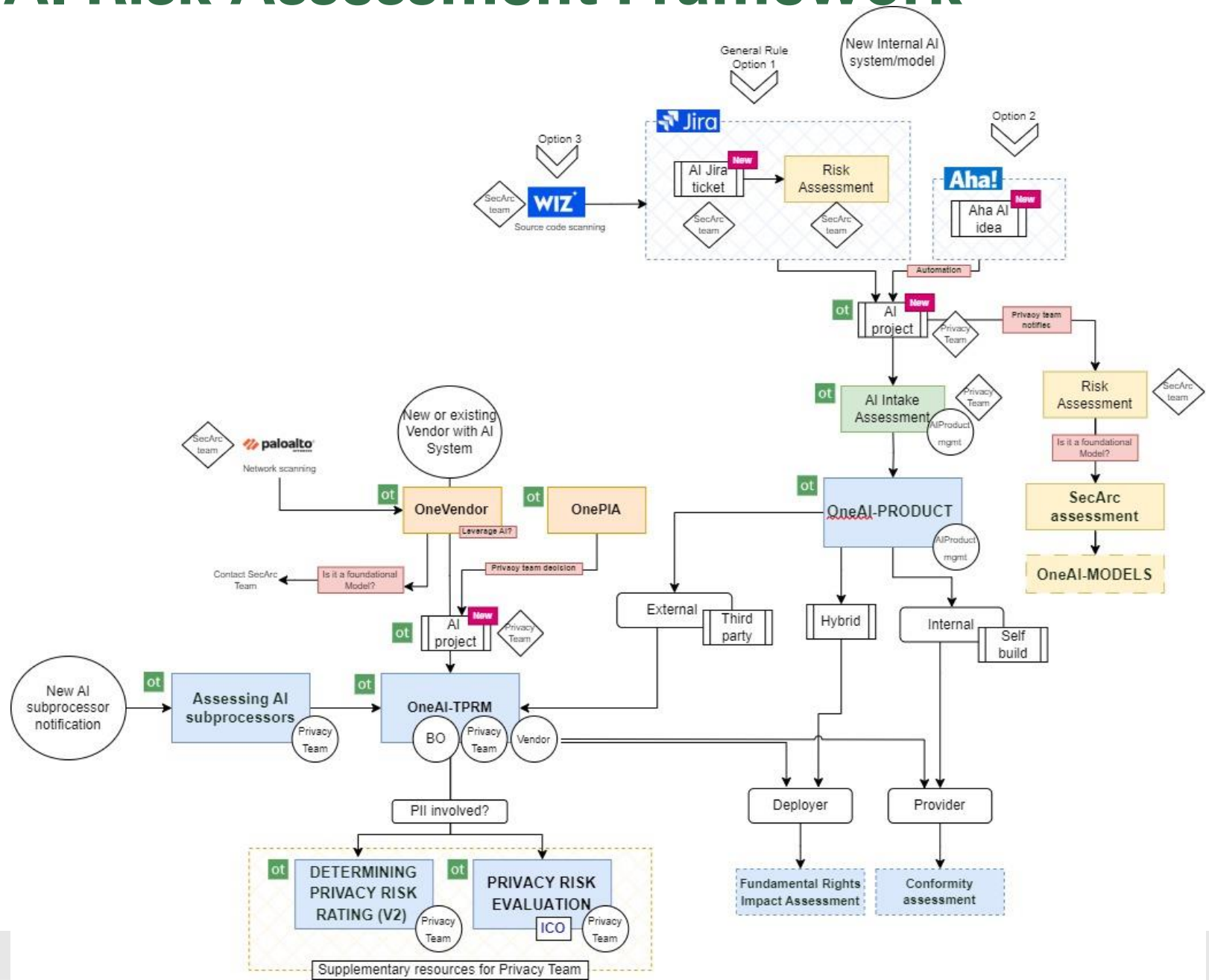
Quality of Training/Testing data

External AI vendor using ingested data to train/improve its services

OneTrust OneAI risk assessment program

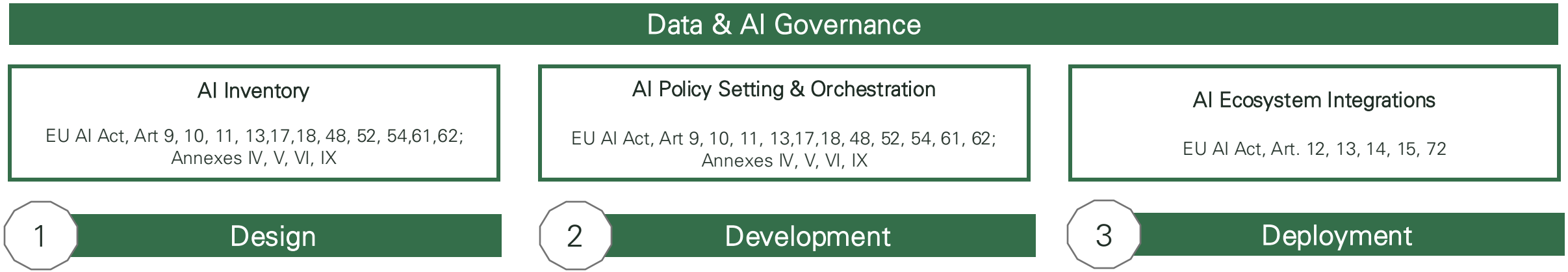
- Visibility into data governance
- Holistic approach to AI risk assessments
- Central depository for all information
- Collaboration
- Promoting AI literacy
- Documentation for audits
- Assessment lifecycle: faster turn around

OneTrust AI Risk Assessment Framework



How OneTrust helps

Helping customers meet EU AI Act compliance



Helping customers meet EU AI Act compliance

Data & AI Governance

Privacy Management

Data & AI Governance

AI Inventory

EU AI Act, Art 9, 10, 11, 13,17,18, 48, 52, 54,61,62; Annexes IV, V, VI, IX

AI Policy Setting & Orchestration

EU AI Act, Art 9, 10, 11, 13,17,18, 48, 52, 54, 61, 62; Annexes IV, V, VI, IX

AI Ecosystem Integrations

EU AI Act, Art. 12, 13, 14, 15, 72

1 Design

Strategy & planning

Identify AI systems & evaluate AI risk per EU AI Act levels

Conduct risk assessments (FRIA, PIA, DPIA)

Data management

Scan and classify data and set governance policies

Map data transfers
Manage consent for training data sets

2 Development

3 Deployment

Helping customers meet EU AI Act compliance

Data & AI Governance

Privacy Management

Data & AI Governance

AI Inventory

EU AI Act, Art 9, 10, 11, 13,17,18, 48, 52, 54,61,62; Annexes IV, V, VI, IX

AI Policy Setting & Orchestration

EU AI Act, Art 9, 10, 11, 13,17,18, 48, 52, 54, 61, 62; Annexes IV, V, VI, IX

AI Ecosystem Integrations

EU AI Act, Art. 12, 13, 14, 15, 72

1 Design

Strategy & planning

Data management

Identify AI systems & evaluate AI risk per EU AI Act levels

Scan and classify data and set governance policies

Conduct risk assessments (FRIA, PIA, DPIA)

Map data transfers
Manage consent for training data sets

2 Development

Model development & selection

Evaluation & validation

Evaluate & manage proprietary and open-source AI/ML models

Centralize technical documentation

Manage third-risk for AI vendors & suppliers

Conduct conformity assessment

3 Deployment

Helping customers meet EU AI Act compliance

Data & AI Governance

Privacy Management

Data & AI Governance

AI Inventory

EU AI Act, Art 9, 10, 11, 13,17,18, 48, 52, 54,61,62; Annexes IV, V, VI, IX

AI Policy Setting & Orchestration

EU AI Act, Art 9, 10, 11, 13,17,18, 48, 52, 54, 61, 62; Annexes IV, V, VI, IX

AI Ecosystem Integrations

EU AI Act, Art. 12, 13, 14, 15, 72

1 Design

Strategy & planning

Identify AI systems & evaluate AI risk per EU AI Act levels

Conduct risk assessments (FRIA, PIA, DPIA)

Data management

Scan and classify data and set governance policies

Map data transfers
Manage consent for training data sets

2 Development

Model development & selection

Evaluate & manage proprietary and open-source AI/ML models

Manage third-risk for AI vendors & suppliers

Evaluation & validation

Centralize technical documentation

Conduct conformity assessment

3 Deployment

Notice

Summarize key model details

Provide notice & choice to end users

Monitoring

Monitor model KPIs

Manage AI incidents

Questions?