The EU approach to AI Governance

Laura Caroli, former AI Act negotiator

AI Act: a risk-based approach

- Product safety framework
- Prohibited practices
- High-risk classification – high risk systems face the bulk of requirements
- AI systems requiring transparency (chatbots, deepfakes, genAI)
- GPAI models and models with systemic risk (specific regime)

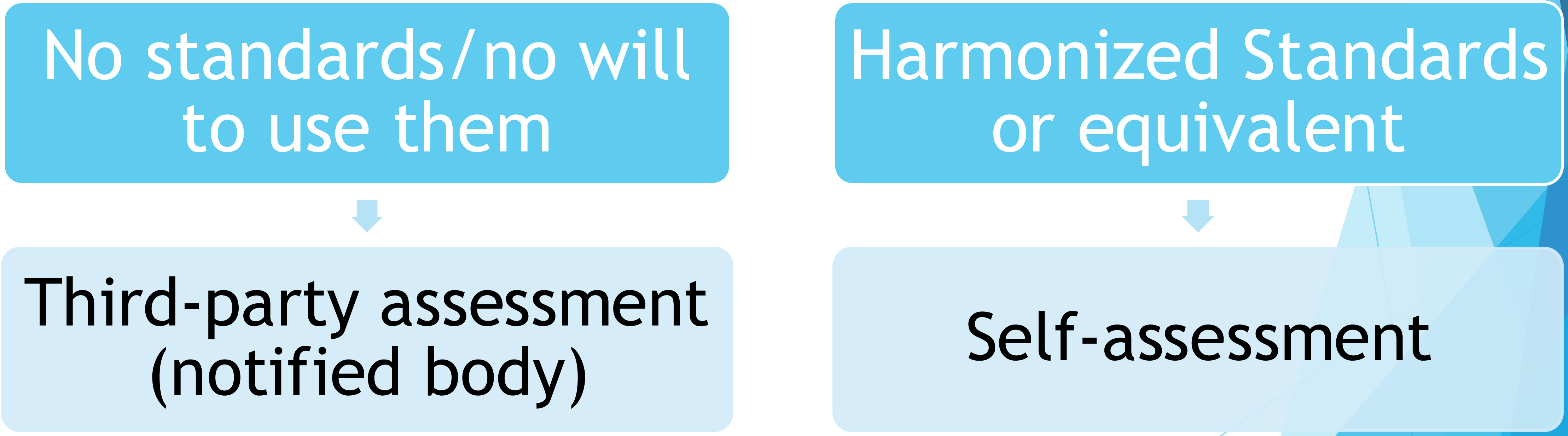
What are the high-risk use-cases?

- AI embedded into regulated product as a safety component (i.e. medical devices, autonomous vehicles, machinery)
- OR
- Critical infrastructure
- AI susceptible of impacting fundamental rights
  - Biometrics
  - Education
  - Employment
  - provision of essential public and private services
  - Migration
  - Law enforcement
  - Democracy/justice

Requirements for high-risk AI systems

- risk management system
- data governance
- technical documentation
- automatically generated logs
- transparency (towards deployer): instructions etc.
- human oversight
- accuracy, robustness, cybersecurity

Role of standards for high-risk AI systems (currently being drafted by CEN-CENELEC’s JTC21)



No standards/no will to use them

Third-party assessment (notified body)

Harmonized Standards or equivalent

Self-assessment

GPAI models (rules operationalized through Code of Practice, not standards yet)

- Technical documentation
- Copyright policy

- For models with systemic risk (above 10^25 FLOPs):
  - Risk assessment
  - Risk mitigation
  - Model evaluation
  - cybersecurity

EU Digital Omnibus – simplification to enhance EU competitiveness?

- One on data (including GDPR)
- One on AI Act
  - TIMELINE
  - AI literacy
  - Training using sensitive data
  - Expanding SME-dedicated provisions to small mid-caps
  - Real-world testing also for regulated products
  - EU-level sandbox
  - Further centralization of powers towards EU AI Office

EU’s approach not only about regulation!

- EU AI Office units
  - “Excellence in AI and Robotics” unit
  - “Regulation and Compliance” unit
  - “AI Safety” unit
  - “AI Innovation and Policy Coordination” unit
  - “AI for Societal Good” unit
  - "AI in Health and Life Science" unit
- EU AI Continent Action Plan
  - AI factories and gigafactories
  - ApplyAI Strategy
  - Data Union Strategy