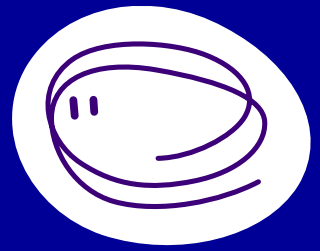
Cross-Border AI sandbox

Ott Velsberg
15.12.2025



REPUBLIC OF ESTONIA
MINISTRY OF JUSTICE
AND DIGITAL AFFAIRS

Next-generation governance infrastructure, not just compliance

+ Supporting innovation while safeguarding rights, safety, and trust
+ Regulatory & technical sandbox aligned with the EU AI Act
+ A strategic competitiveness instrument for Estonia

Why an AI sandbox?

The strategic problem

- AI enables major productivity and economic gains
- High-risk AI introduces new systemic, legal, and societal risks
- Trust is a prerequisite for large-scale AI adoption

Estonian context

- 425 M€ public sector efficiency potential by 2030
- ~8% GDP growth potential from generative AI
- Strong public demand for transparency & lawful data use

Why cross-border?

AI Systems Are Inherently Cross-Border

- AI models, data pipelines, cloud infrastructure, and vendors rarely stay within one jurisdiction
- Training, inference, deployment, and supervision often occur in **different Member States**
- National-only sandboxes cannot reflect **real operational conditions**

- Shared interpretation of high-risk AI requirements
- Early convergence of supervisory practices
- Reduced regulatory fragmentation
- “Test once, deploy many” logic

EU AI Act: What changes?

EU AI Act objectives

- Harmonised internal market for AI
- Human-centric, trustworthy AI
- Innovation-friendly regulation

For high-risk AI systems

- Mandatory risk management
- Testing & validation
- Documentation & transparency
- Ongoing oversight

What Is the AI Sandbox?

A **controlled regulatory and technical environment** where organisations can:

- Develop and test AI systems
- Receive regulatory guidance
- Validate compliance and safety
- Test (when justified) in real-world conditions

Core value

- Legal certainty + technical quality assurance
- Learning loop for regulators and policymakers

Dual Structure: Regulatory & Technical

Regulatory track
- Legal & compliance guidance
- Risk and impact assessments
- AI Act requirement interpretation
- Coordination with supervisory authorities
- Real-world testing

Technical track
- System testing & validation
- Robustness, bias, explainability checks
- Secure data processing environments
- HPC & compute access

Key Sandbox Components

Regulatory components

- Legal compliance support
- Fundamental rights & data protection impact assessments
- Risk management frameworks
- Data governance and data science best practices
- Algorithm transparency & registry
- Trusted AI toolbox

Technical components

- Testing & validation
- Cybersecurity & logging
- Development support
- Data governance & quality support
- Secure data environments (ERIKA)
- HPC via ETAIS & LUMI

Governance and roles

Coordinator

Ministry of Justice and Digital Affairs (JDM)

Core partners

Supervisory authorities (TTJA, DPA, FI, etc.)

AIRE (pre-assessment & guidance)

Statistics Estonia (data governance, secure data)

RIA (cybersecurity)

ETAIS (HPC)

AI Centre of Excellence

Participants

Public sector

SMEs & private sector

Research institutions

Sandbox process

End-to-end flow

Pre-consultation via AIRE

Sandbox application

Joint testing plan (risks, scope, safeguards)

Controlled testing (incl. real-world, if approved)

Monitoring & incident handling

Exit report

Timeframe

Real-world testing: up to 6 months

Exit Report & Regulatory Learning

Exit report provides

- Evidence of AI Act compliance
- Summary of risks & mitigation measures
- Technical & legal findings
- Best practices and lessons learned

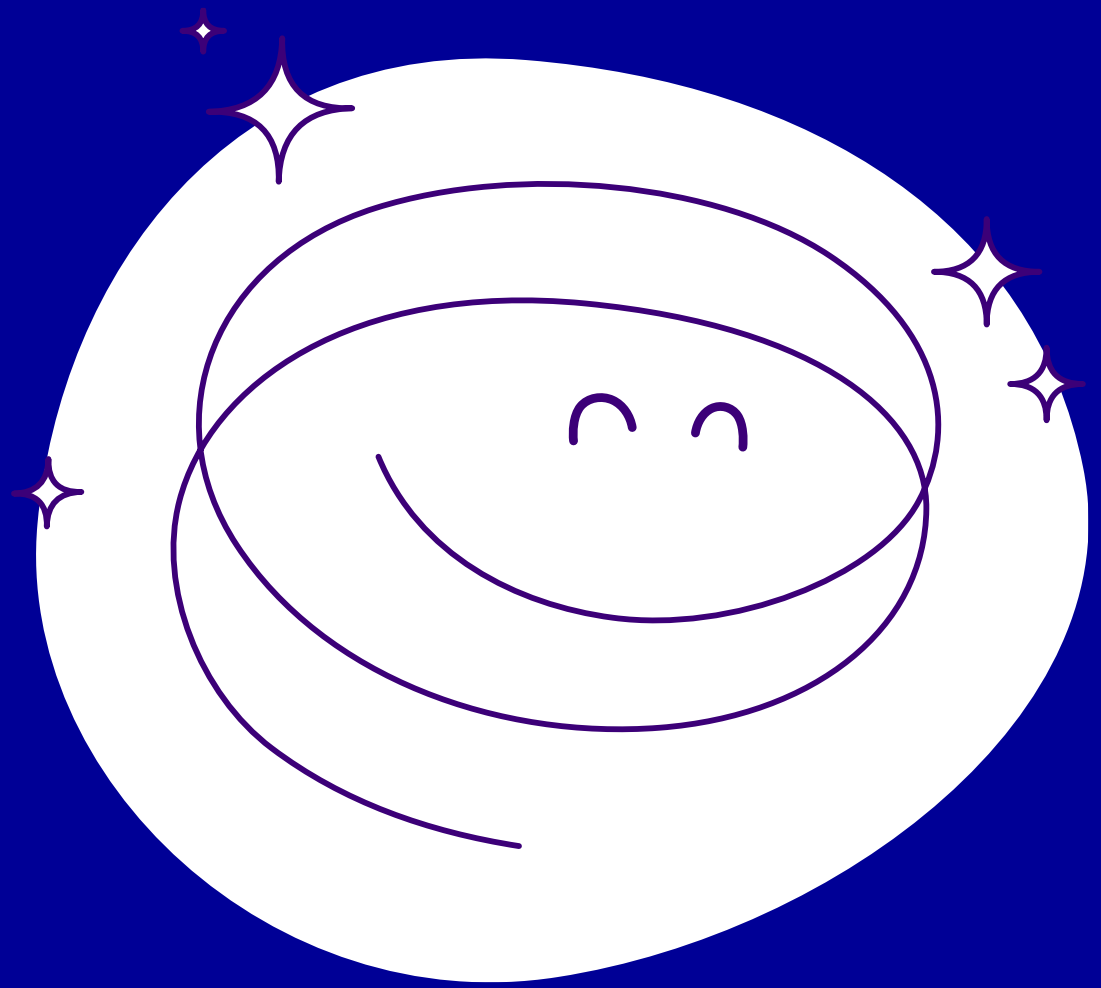
Public value

- Non-confidential results published
- Input for legal updates, standards, guidance
- Strengthens national AI governance capacity

Next steps

Jan: Sandbox advisory & technical support starts
Feb: Trusted AI Toolbox launch
Feb–Jul: Data governance pilot
Feb end: HPC access available
Mar: Algorithm Registry launch
Jun: AI Act national implementation amendments
End Jun: Full sandbox service live

Thank you!



ott.velsberg@justdigi.ee
www.kratid.ee