**The Norwegian perspective: Policy input for a secure and competitive European tech sector**

**ICT Norway’s recommendations to EU policymakers – April 2025**

As the geopolitical landscape is shifting, it has become clear that Europe must strengthen its own technological capabilities. **Public-private collaboration** is essential to build a more secure, competitive, and digitally sovereign Union.

Europe’s digital resilience and strategic autonomy depend on strong **cooperation with close partners**. Norwegian and Nordic technology companies are key contributors to Europe’s cybersecurity, digital infrastructure, and innovation capacity. Through the EEA framework, we align closely with EU priorities — from secure AI to critical infrastructure protection.

In light of the ongoing implementation of the AI Act and the AI Continent Action Plan, in addition to coming policy initiatives that includes an International Digital Strategy, a Start-up and Scale-up Strategy, and new omnibus legislative packages, these are ICT Norway’s key recommendations for EU policymakers:

### **1. Smarter Regulation of AI**

Ensure that the AI Act and future AI rules **promote innovation and competitiveness**. The EU must prioritise innovation incentives and regulatory clarity over bureaucratic overreach. AI innovation in Europe is being held back by uncertainty, compliance costs, and fragmented implementation. Regulators should guide and enable — not merely enforce.

The EU should:

* Promote regulatory sandboxes and testing zones.
* Accelerate conformity assessments for low-risk applications.
* Incentivise ethical AI development through R&D support schemes.

### **2. Simplify Privacy and Data Sharing Rules**

Ensure that data protection rules — including the General Data Protection Regulation (GDPR) — enable, rather than hinder, **responsible innovation and data sharing**. Clear, consistent guidance and legal certainty are essential to unlock the value of data across sectors, including health, mobility, and critical infrastructure. These issues should be addressed in potential upcoming omnibus initiatives and legislative reviews.

### **3. Strengthen Digital Security and Resilience**

As highlighted in the European Preparedness Union Strategy, **public-private cooperation must be scaled in strategic sectors** such as cybersecurity. Norwegian and Nordic tech actors should be integrated into current and future EU-level cooperations to support cross-border surveillance and cyberdefence capabilities.

### **4. Build Joint Reserves for Critical Tech**

Establish joint European **reserves of critical technology components** to strengthen supply chain resilience and digital crisis preparedness. This should be part of implementing both the European Preparedness Union Strategy and the White Paper on European Defence.

### **5. Align Security Clearance Procedures**

Promote **mutual recognition and alignment of security clearance procedures** for technology providers involved in critical infrastructure and defence. This includes enhanced public-private cooperation and the development of interoperable frameworks across EU and associated countries. Mutual clearance frameworks would reduce delays in deploying trusted vendors in EU critical infrastructure projects.

**About ICT Norway**

ICT Norway is an independent member organization for companies within the digital tech sector. Our members include large and small companies from various digital industries with a common foundation in technology and digital solutions. With over 300 members, ICT Norway offers Norway’s largest network across the digital industry.

**Contact:**   
Mr Øyvind Huseby  
CEO  
husby@ikt-norge.no

Mr Jarle Roheim Håkonsen  
Director of Communication and Business Policy  
jarle@ikt-norge.no

www.ikt-norge.no  
Transparency register: 136147697147-80