Prepared by DigitalTrade4.EU

Call for Evidence for a Digital Networks Act

June 2025

About Us

The **DigitalTrade4.EU consortium** envisions a **seamlessly interconnected Europe** and **neighbouring regions** powered by harmonized standards for the digitalisation of trade documents and processes. By fostering the digital transformation of trade, we aim to promote economic integration, enhance cooperation, and ensure long-term trade facilitation across borders.

Our consortium is made up of **experts in their field**, including **107 full partners**—trade associations, logistics providers, shipping lines, banks and insurances, technology innovators, etc.—**from 17 European Union countries** (*France, Belgium, Netherlands, Austria, Estonia, Finland, Italy, Latvia, Spain, Germany, Sweden, Poland, Luxembourg, Lithuania, Slovenia, Denmark, Bulgaria*) and **22 non-EU countries** (*United Kingdom, Switzerland, Montenegro, Japan, Singapore, Hong Kong, Australia, New Zealand, India, Nepal, Canada, United States of America, Cameroon, Morocco, Egypt, Kenya, Pakistan, Nigeria, Brazil, Uzbekistan, Turkey, Ukraine*).

Our consortium is already **aligned with the fundamentals** of the **EU Competitiveness Compass**. Learn more:

- How DigitalTrade4.EU Can Help Achieve the Objectives of the EU Competitiveness Compass (February 2025) https://www.digitaltrade4.eu/how-digitaltrade4-eu-can-help-achieve-the-objectives-of-the-eu-competitiveness-compass/

Web page: www.digitaltrade4.eu

EU Transparency Register: 355266197389-94

Contact person: Riho Vedler

Email: riho.vedler@ramena.ee

Executive Summary

This document presents the consolidated feedback of the **DigitalTrade4.EU** consortium in response to the European Commission's strategic initiatives concerning the Single Market, digital networks, a European Data Union, and Defence Readiness. We commend the Commission for its ambitious vision but assert that these strategic pillars—**economic competitiveness**, **data sovereignty**, and **defence capability**—are deeply interconnected and can only be fully realised through a **unified and integrated digital transformation strategy**.

DigitalTrade4.EU advocates for an approach centred on **interoperability**, **decentralisation**, and **harmonised international standards**. The **digital solutions** vital for a **modern** and **efficient single market**—such as those compliant with the **UNCITRAL Model Law on Electronic Transferable Records (MLETR)**[1], which enables **legally binding electronic trade documents**; the **eIDAS 2.0 Regulation**[2], which establishes a framework for **secure digital identities** across the EU; and the **Digital Product Passport (DPP) framework**[3], which provides **traceability for products** throughout their **lifecycle**—possess **significant dual-use potential**. These tools can simultaneously enhance economic competitiveness and bolster European defence readiness by enabling **secure cross-border logistics, trusted digital identities, and traceable, secure supply chains** for both civilian and military applications. The **integrity and security of the data** underpinning these systems are paramount, as **insecure data can compromise both economic and national security**.

Our key recommendations are to:

- **Champion Harmonised Digital Standards for Dual-Use:** Actively promote and mandate the EU-wide adoption of **MLETR** and **eIDAS 2.0** to serve as the backbone for both commercial and defence logistics, ensuring seamless and secure data exchange.

[1] UNCITRAL. Model Law on Electronic Transferable Records
https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records
[2] European Commission. Discover eIDAS
https://digital-strategy.ec.europa.eu/en/policies/discover-eidas
[3] European Commission. EU's Digital Product Passport: Advancing transparency and sustainability (September 2024)
https://data.europa.eu/en/news-events/news/eus-digital-product-passport-advancing-transparency-and-sustainability

- **Extend the Digital Product Passport (DPP) Framework:** Adapt and extend the DPP framework to critical **defence and dual-use components** to enhance traceability, prevent counterfeit parts, and secure the **European Defence Technological and Industrial Base (EDTIB) supply chain**.
- **Foster a Unified and Secure Data Infrastructure:** Ensure the European Data Union and the Digital Networks Act explicitly provide for **dual-use data spaces** and invest in resilient infrastructure that supports both seamless trade and military mobility, built on **security-by-design principles**.
- **Prioritise Data Integrity and Security:** Embed robust data security best practices, including **provenance tracking, cryptographic verification, and secure data supply chain management**, as a foundational requirement for all digital initiatives to protect against data poisoning and manipulation.

By strategically aligning these initiatives, the EU can create powerful synergies, transforming its regulatory leadership in the green and digital transitions into a cornerstone of its **strategic autonomy** and global leadership.

Introduction

DigitalTrade4.EU is a multi-stakeholder consortium of trade associations, logistics providers, financial institutions, technology innovators, and other experts from 17 EU and 22 non-EU countries. Our mission is to promote the digital transformation of trade to enhance economic integration, facilitate cross-border cooperation, and ensure long-term trade resilience.

Our work is directly aligned with the **EU's strategic objectives**, including the **EU Competitiveness Compass**[4], which prioritises **economic resilience** through **technological leadership**, and the **Digital Decade Policy Programme 2030**[5], which aims to ensure Europe leads in **digital innovation** and **infrastructure**. We believe that the digitalisation of trade documents and processes is a cornerstone of a more competitive and sustainable European economy. This submission provides our perspective on how the proposed **Digital Networks Act (DNA)** can serve as a foundational element for achieving this vision.

This initiative is not occurring in a vacuum. It aligns directly with the urgent strategic vision presented in the Commission's **Joint White Paper for European Defence Readiness 2030**[6]. The White Paper correctly identifies that Europe faces a new geopolitical reality and must bolster its strategic autonomy and resilience. It emphasizes that **technological leadership** and **secure, dual-use infrastructure** are paramount. The cutting-edge, secure, and resilient networks the DNA aims to create are the quintessential **dual-use infrastructure of the 21st century**—as critical for military mobility and defence as they are for a competitive single market and secure digital trade.

Moreover, our approach directly supports and operationalizes the Commission's 2024 White Paper, "How to master Europe's digital infrastructure needs?"[7]". This White Paper

[4] European Commission. Competitiveness compass (January 2025) https://commission.europa.eu/topics/eu-competitiveness/competitiveness-compass_en

[5] European Commission. Europe's Digital Decade https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

[6] European Commission, Internal Market, Industry, Entrepreneurship and SMEs. The Single Market: our European home market in an uncertain world (May 2025) https://single-market-economy.ec.europa.eu/publications/single-market-our-european-home-market-uncertain-world_en

[7] European Commission. White Paper - How to master Europe's digital infrastructure needs? (February 2024) https://digital-strategy.ec.europa.eu/en/library/white-paper-how-master-europes-digital-infrastructure-needs

outlines the importance of building a **"Connected Collaborative Computing" (3C) environment**, deploying **quantum-secure infrastructure**, and completing the **Digital Single Market**[8] to boost the EU's competitiveness, sustainability, and resilience. **DigitalTrade4.EU addresses these exact priorities through its focus on global standards, secure supply chains, interoperable legal frameworks, and scalable infrastructure for both civil and defence use.** Our recommendations are thus designed not only to boost economic performance but also to reinforce the resilience and strategic autonomy that the Commission rightly identifies as a top priority.

We draw upon our recent analysis, **Strengthening EU Leadership in Green-Digital Trade: Key Developments and Strategic Recommendations**[9] (May 2025), to offer concrete, actionable feedback that bridges these economic and security imperatives.

[8] European Commission, Internal Market, Industry, Entrepreneurship and SMEs. The Single Market: our European home market in an uncertain world (May 2025) https://single-market-economy.ec.europa.eu/publications/single-market-our-european-home-market-uncertain-world_en

[99] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14589-International-Digital-Strategy/F3552794_en

Expectations from the Commission's Side: The Objectives

DigitalTrade4.EU acknowledges and supports the ambitious objectives set forth by the European Commission. We have synthesized the core goals from the strategic documents, which form the basis of our responsive recommendations.

From the Single Market Strategy (COM(2025) 500 final):

- **Fewer Barriers:** A focused effort to eliminate the most harmful Single Market barriers, the **'Terrible Ten'**, to unlock trade and investment.
- **More Ambition:** A new, sectoral approach to invigorate the underdeveloped Single Market for **services**.
- **More Simplification:** A commitment to **reduce red tape** and move from a document-based to a **data-based Single Market**.
- **More Effective Digitalisation:** A paradigm shift towards **digital-by-default** solutions, including the Digital Product Passport (DPP) and eInvoicing.

From the Digital Networks Act & European Data Union Strategy:

- **Incentivise Investment:** Drive innovation and investment in **advanced connectivity** and computing infrastructures to enable the **"AI continent."**
- **Simplify the Legal Framework:** Reduce regulatory burdens, streamline data rules (Data Act, Data Governance Act), and merge related legislative instruments to create **legal certainty**.
- **Further Harmonisation:** Move towards a more integrated single market by reducing fragmentation caused by **divergent national practices** in spectrum management, authorisation regimes, and end-user protection.
- **Strengthen Governance:** Strengthen the roles of EU bodies such as the Body of European Regulators for Electronic Communications (BEREC) and the Radio Spectrum Policy Group (RSPG) to better address pan-European challenges and drive the advancement of the **digital single market**.

From the European Defence Readiness 2030 White Paper:

- **Re-arm Europe:** Achieve sufficient **military readiness** and capabilities by 2030 to credibly deter aggression.
- **Strengthen the Defence Industrial Base (EDTIB):** Foster a strong, resilient, and innovative EDTIB with **secure supply chains** and reduced external dependencies.
- **Enhance Military Mobility:** Develop **dual-use transport infrastructure** and digital systems to ensure the rapid and seamless movement of troops and equipment.
- **Foster Collaboration and Interoperability:** Generate economies of scale and improve the **effectiveness and interchangeability** of Member States' defence efforts.

Approach and Recommendations

Our approach is founded on a core principle: the creation of a **secure, interoperable, and decentralised digital backbone** for Europe. This infrastructure, built on harmonised international standards, must serve both **civilian and defence purposes**, creating powerful synergies between economic competitiveness and security.

1. Champion Harmonised Digital Standards for Dual-Use

The **fragmentation of digital rules** is a **critical barrier** to both a **seamless single market** and **interoperable defence capabilities**. For example, **inconsistent digital documentation standards** across **EU member states** can **delay cross-border military asset transfers**, undermining **rapid deployment** during **crises**.

- **Recommendation:** Actively promote and mandate the EU-wide adoption of **UNCITRAL MLETR** for electronic transferable records. This legal framework, essential for streamlining commercial logistics, must be extended to **military logistics** to enable the secure, legally-recognized, and paperless movement of defence assets across borders.
- **Recommendation:** Fully leverage the **eIDAS 2.0 framework** and the European Digital Identity Wallet as a universal standard for secure identification. This is crucial not only for citizen and business services but also for creating **trusted digital identities for defence personnel and contractors**, ensuring secure access to sensitive systems.

2. Extend Digital Product Passports (DPPs) for Enhanced Security

The DPP is a revolutionary tool for transparency, and its potential for enhancing security is equally significant.

- **Recommendation:** Adapt and extend the **DPP framework** to cover critical components in the **defence and dual-use sectors**. A **DPP** for a **missile guidance system**, a **turbine engine**, or a **critical microchip** could securely track its **entire lifecycle**—from **raw material origin** and **manufacturing data** to **maintenance history** and **chain of custody**. By embedding **cryptographic verification** into each stage, DPPs

ensure that **unauthorised modifications** or **counterfeit components** are **immediately detectable.**

- **Benefit:** This provides **unprecedented traceability**, helping to **prevent counterfeit parts** from entering the supply chain, manage strategic stockpiles, verify compliance with security standards, and ensure the **security of supply** for the EDTIB.

3. Foster a Unified and Secure Data and Digital Infrastructure

A **siloed approach** to data spaces—one for industry, another for defence—is inefficient and insecure.

- **Recommendation:** Ensure the European Data Union strategy and Digital Networks Act explicitly include provisions for **dual-use data spaces**. These **secure, federated environments**—such as **cross-sector data hubs** governed by **strict access controls**—can facilitate **R&D collaboration** between **civilian** and **defence industries** and enable **secure information sharing** during **crises**.
- **Recommendation:** Invest a significant portion of the **Connecting Europe Facility (CEF)** and **Digital Europe Programme** funding into **dual-use digital infrastructure**. This includes **quantum-secure fibre optic networks** along military mobility corridors and sovereign cloud infrastructure that meets the high-security requirements of both modern industry and defence operations.

4. Bolstering Security and Trust: The Data Integrity Imperative

The effectiveness of the recommended digital infrastructure is entirely dependent on the **security and integrity of the data** that flows through it. **Insecure data** not only **jeopardises national security** but also **undermines economic competitiveness**. For instance, **supply chain disruptions** caused by **counterfeit components** or **data breaches** can cost **EU businesses billions annually**. By mandating **robust data integrity measures**, the **EU** can protect both its **industrial base** and its **citizens' trust in digital systems**.

As highlighted in the "**CSI on AI Data Security**[10]", a **compromised data supply chain can undermine any system** built upon it, whether for commercial or defence purposes. Therefore, **data security cannot be an afterthought**; it must be a **foundational, non-negotiable principle**.

- **Recommendation: Secure the Data Supply Chain.** The EU must establish **robust verification protocols** for all data, especially data ingested from third-party or web-scale sources. This includes mandating the use of **cryptographic hashes and digital signatures** to verify data integrity upon collection and throughout its lifecycle. For both commercial products and defence systems, **data provenance must be meticulously tracked** to ensure its origin and history are auditable.
- **Recommendation: Protect Against Malicious Data Modification.** The digital frameworks for trade and defence must be designed to detect and mitigate the risks of **data "poisoning"** and tampering. This requires implementing **anomaly detection algorithms**, regular data sanitization, and adopting a **Zero Trust architecture** for all data processing environments. Bad data, whether from unintentional error or malicious intent, poses a direct threat to the Single Market's fairness and the defence sector's operational reliability.
- **Recommendation: Mandate Security-by-Design.** The principles of data security—**encryption at rest and in transit, strict access controls, and regular risk assessments**—must be embedded in the legal and technical frameworks of the Digital Networks Act, the European Data Union, the DPP, and all related initiatives from their inception. A secure digital Europe requires a **proactive, not reactive, approach to cybersecurity**.

[10] U.S. National Security Agency/Central Security Service. AI Data Security - Best Practices for Securing Data Used to Train & Operate AI Systems (May 2025)
https://media.defense.gov/2025/May/22/2003720601/-1/-1/0/CSI_AI_DATA_SECURITY.PDF

Conclusion and Next Steps

The European Union stands at a critical juncture. The path to a more competitive, resilient, and secure future requires **breaking down the silos** between economic, digital, and defence policy. Digital transformation, guided by the principles of **interoperability, security, and harmonised standards**, is the most powerful tool at the Commission's disposal to achieve this integration.

The recommendations outlined by DigitalTrade4.EU are not separate initiatives but parts of a **single, coherent vision**. A traceable supply chain for a consumer product uses the same core technology as one for a critical military component. A secure data infrastructure benefits both start-ups and strategic defence planners.

DigitalTrade4.EU is committed to this vision and proposes the following **next steps for collaboration**, which will **reduce long-term costs** by avoiding **redundant infrastructure development** and **maximising resource efficiency** across **sectors**:

1. **Engage in a structured dialogue** with DG TRADE, DG CNECT, DG MOVE and DG DEFIS to create a **cross-directorate task force** focused on implementing **dual-use digital standards and infrastructure**.
2. **Launch pilot projects** that demonstrate these concepts, such as a **DPP for a dual-use component** or the use of **MLETR-compliant documents** in a joint military-civilian logistics exercise.
3. **Collaborate on developing the legal and technical frameworks** to ensure the European Data Union and other digital initiatives are designed from the outset with dual-use potential and **security-by-design principles**.

By embracing this unified approach, the EU can ensure that its investments in the digital and green transitions directly contribute to its **strategic autonomy and security**, creating a **virtuous cycle where economic strength and defence readiness reinforce one another**.

EU Green-Digital Trade Leadership Roadmap (DigitalTrade4.EU, 2025)

activity	objective	indicative metrics	tools/enablers
1. EU-Singapore DTA & Expand DEPA Partnerships	Strengthen digital trade diplomacy in Asia through high-standard agreements.	- 5+ new digital trade agreements with key Asian partners (e.g., Japan, India, ASEAN) by 2030 - 15% increase in EU-Asia digital services trade by 2028	DEPA framework, EU-Singapore DTA, Global Gateway Initiative, eIDAS 2.0
2. Implement Digital Product Passports (DPPs)	Ensure traceable, sustainable supply chains aligned with EU Green Deal.	- 50% adoption of DPPs by 2030 - 20% reduction in supply-chain carbon intensity by 2030	EU Sustainable Products Initiative, CBAM incentives, UNECE Recommendation 49
3. Fund Secure Digital Corridors in Asia	Build interoperable digital infrastructure for EU-Asia trade.	- ~€2B allocated via NDICI-Global Europe - 10+ blockchain-based traceability pilots by 2027	NDICI-Global Europe, ASEAN digital customs systems, EU Customs Data Hub
4. Harmonize Digital Standards (MLETR/eIDAS 2.0)	Enable cross-border recognition of e-documents and digital identities.	- 90% mutual recognition of e-signatures by 2028 - 70% SME adoption of eIDAS wallets	MLETR framework, eIDAS 2.0, EU Transport Law updates, UN/UNECE protocols
5. Launch Green-Digital Trade Academy	Upskill SMEs and officials on DPPs and carbon accounting.	- 40% increase in SME participation by 2027 - 60% cost savings for SMEs	Erasmus+ grants, COSME programme, tiered compliance thresholds
6. Integrate ESG into Trade Finance	Link trade finance to sustainability metrics for cheaper capital access.	- €10B/year unlocked for green trade finance - 30% lower Scope 3 emissions by 2030	InvestEU guarantees, CSRD-aligned reporting, FinTech platforms
7. Enforce Platform Interoperability	Prevent vendor lock-in and empower SMEs.	- 100% compliance with CJEU rulings by 2026 - 50% reduction in platform dominance	Court of Justice of the European Union (CJEU) Case C-233/23, DEPA, eIDAS 2.0, Digital Markets Act (DMA)
8. Global Digitalisation Projects with EU Standards	Extend EU digital infrastructure and norms globally.	- 20+ co-funded projects by 2030 - 80% interoperability with EU systems	Digital Europe Programme, CEF funding, EU-Asia Digital Standards Taskforce
9. Advance UNECE Transparency Protocols	Globalize EU sustainability standards for supply chains.	- 100% alignment with UNECE Rec. 49 by 2028 - 30% reduction in greenwashing claims	UNECE CEFACT, W3C Verifiable Credentials, EU CBAM registry
10. Pilot CBAM-DPP Corridors	Link trade finance to verifiable ESG metrics for tariff incentives.	- 20% CBAM compliance cost reduction - 50% DPP adoption by 2030	IoT carbon trackers, CBAM rebate schemes, EU Customs Single Window

Table 1. The roadmap above, DigitalTrade4.EU's input to the European Commission's "International Digital Strategy" operationalises the recommendations outlined in this document. For instance, Activity 1 (EU-Singapore DTA & Expand DEPA Partnerships) directly supports the harmonisation of international digital standards, while Activity 8 (Global Digitalisation Projects with EU Standards) aligns with efforts to promote dual-use infrastructure globally. These activities collectively reinforce the EU's ability to leverage digital trade diplomacy as a tool for both economic growth and strategic security.