



DIGITALEUROPE

UNECE WP.6 How to target
continuous compliance

Omar Daher, Associate Technical Director

Geneva, November 24

UNECE Disclaimer

- The author and the speaker of this presentation confirm that they have authorization to use all photos and visual elements.
- The material is either copyright-free or the author / speaker holds the necessary copyright.
- The UNECE will remove any material from its events and supporting websites if there is unlawful use of copyrighted material.
- The author / speaker takes responsibility for any infringements on copyright and holds the UNECE harmless to this effect.

1

Our membership

We represent over 45,000 businesses across Europe

The voice of digitally transforming industries

1010
1010



- platform services
- data analytics
- software & hardware
- cybersecurity
- telecoms
- semiconductors
- cloud technology
- Healthcare
- Manufacturing
- Finance
- Buildings
- Mobility

Stakeholder access & EU setting digital agenda

Policy development & influence

EU Projects

DIGITALEUROPE 



41

NATIONAL ASSOCIATIONS

106

COMPANIES



Our members



45,000

companies represented



41

NATIONAL ASSOCIATIONS

106

COMPANIES

Cybersecurity
AI software & hardware
Data analytics
Telecoms
Semiconductors
Cloud technology
International trade

Resilience and the Ukraine war
Healthcare
Manufacturing
Finance
Buildings
Mobility

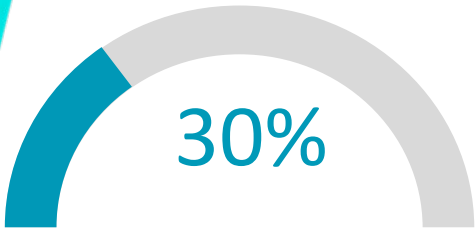


20 solutions to boost European tech leadership and resilience

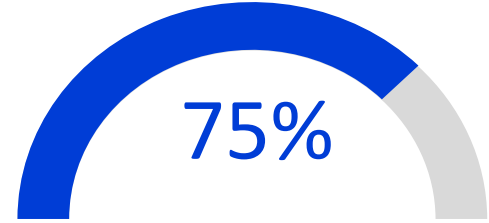


Scan to read the full report

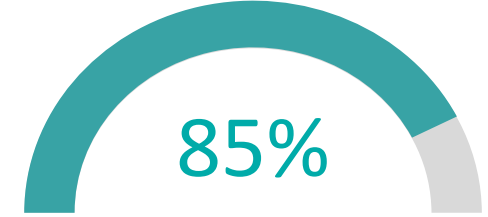
DIGITALEUROPE 



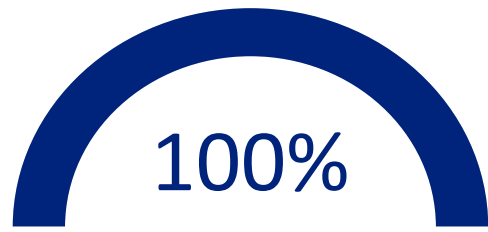
of European SMEs trade across European borders (8%)



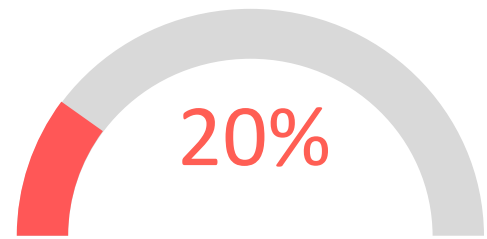
of EU companies use cloud computing Services (34%), big data (14%), and AI (8%)



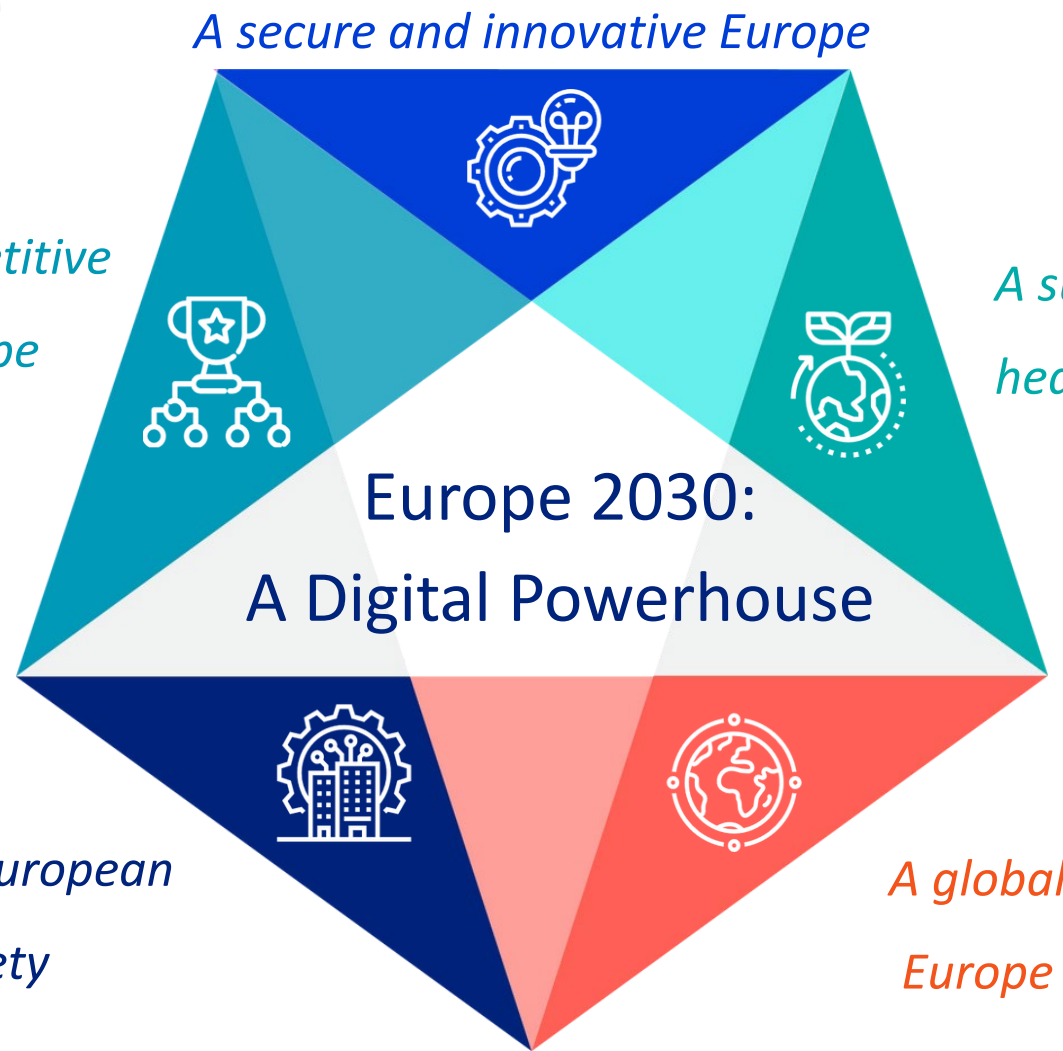
of EU companies use ICT to reduce their environmental impact (66%)



of key public services being available online (73%)



of biggest world's tech companies are European (11%)





Masters of Digital 2024

Europe 2030: A Digital Powerhouse

21 FEBRUARY 2024 | BRUSSELS & ONLINE

DIGITALEUROPE 



Alexander de Croo
Prime Minister
Belgium



Valdis Dombrovskis
Executive Vice-President
European Commission



Marie Bjerre
Minister for Digital
Government
and Gender Equality
Denmark



Dimitris Papastergiou
Minister of Digital
Governance, Greece



Iliana Ivanova
European Commissioner
for Innovation, Research,
Culture, Education and
Youth



Florian Tursky
State Secretary for
Digitalization,
Austria

2

DIGITALEUROPE work on standardisation

External

- ▶▶ Members of the **EU High-Level Forum on Standardisation (HLF)**
- ▶▶ Members of **Multistakeholder Platform on ICT Standardisation (MSP)**
- ▶▶ **Members of the Rolling Plan on ICT Standardisation**
- ▶▶ Members of EC EG RED

Work with **CEN-CENELEC/ETSI**

- AI
- Cybersecurity and Data
- DPP
- Compliance & market access

Internal

- ▶▶ **Advisory board for standardisation**
- ▶▶ **Digital Technology and Innovation Policy Group**
- ▶▶ **Standards and Interoperability WG**
- ▶▶ **Product Compliance and Market Access WG**

Sectoral Workstreams

▶▶ Green

- Clean hydrogen (work in Clean Hydrogen Alliance)
- Sustainable Cities
- Low Carbon Cement
- Wind
- Green Electricity Systems
- Photovoltaics

• Digital

- Artificial Intelligence
- Digital Product Passport
- Data interoperability

▶▶ Resilience

- Critical Raw Materials

Horizontal Workstreams

- ▶▶ Education and skills
- ▶▶ Fundamental rights and standards
- ▶▶ Greater civil society inclusion in standardisation at international level (ECOS)
- ▶▶ National standardisation bodies – peer review
- ▶▶ Alignment between European and International standards

Leading/actively contributing
Monitoring

For information

Members consulted in relevant PGs/WGs across the association

▶▶ Lasting liaison status:

- TC 13: Electrical energy measurement and control
- TC 210: Electromagnetic Compatibility (EMC)
- TC 209: Cable networks for television signals, sound signals and interactive services
- TC 205: Home and Building Electronic Systems (HBES)
- TC 108X: Safety of electronic equipment within the fields of Audio/Video, Information Technology and Communication Technology
- TC 106X: Electromagnetic fields in the human environment
- CEN/CLC/ETSI/JWG eAccessibility
- CEN/CLC/JTC 21 - Artificial Intelligence
- CEN/CLC/JTC 13 - Cybersecurity and Data Protection



3

The NLF and continuous compliance

Intro / NLF training

- ▶▶ **Training on the New Legislative Framework (NLF)** to our national trade associations and corporate members
- ▶▶ Promote **exchange of knowledge** between experts and better understand the **interplay between the NLF and horizontal legislation** defining product compliance
- ▶▶ Analyse interaction between NLF provisions and horizontal legislation: **AI Act, Cyber Resilience Act, Eco-Design for Sustainable Products Reg.** (including Digital Product Passport)
- ▶▶ Alignment / misalignment? **Solutions** for the upcoming revised NLF?

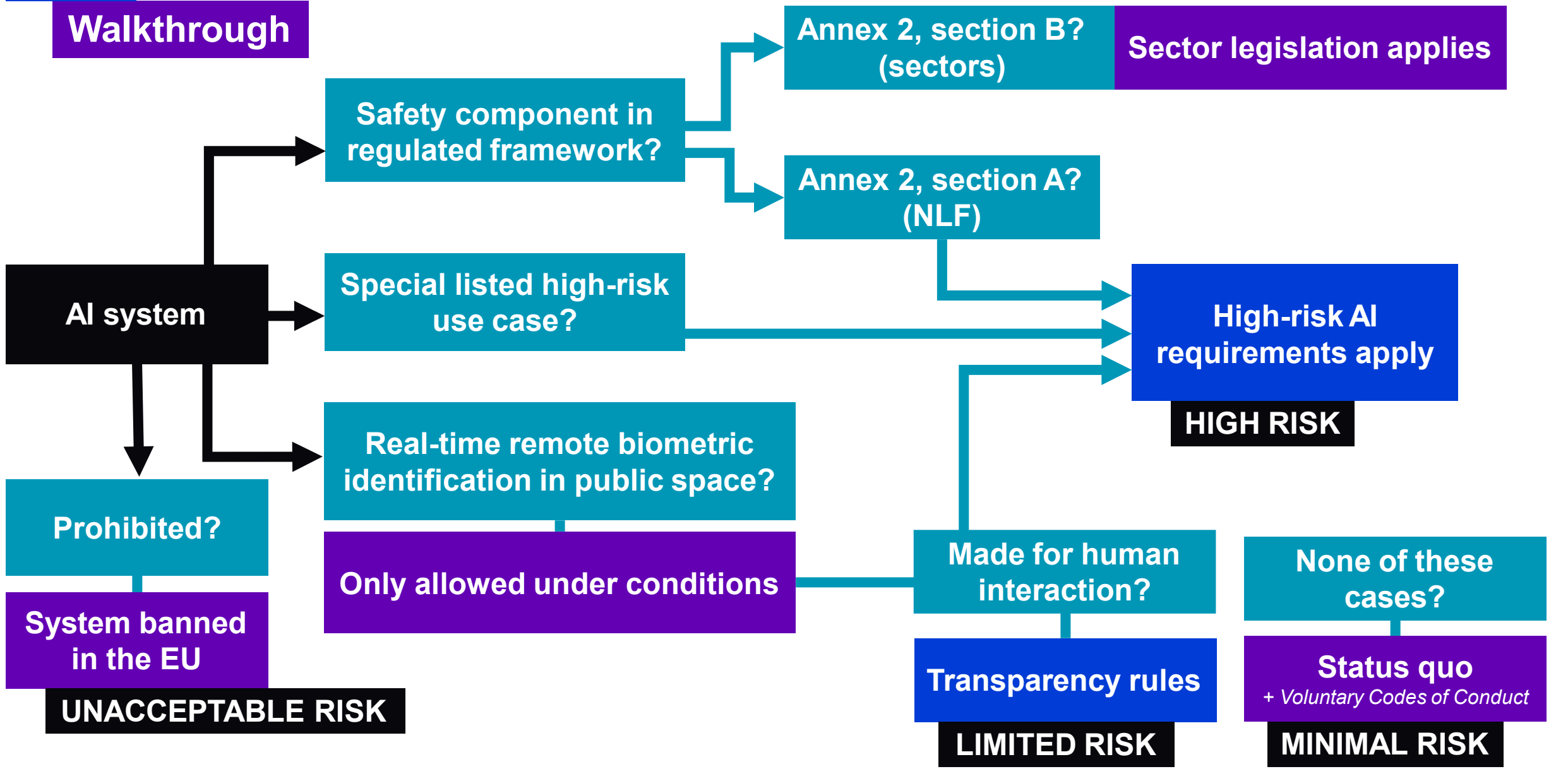


AI Act - compliance

- ▶▶ Lack of understanding of how to use the NLF definitions for non-tangible products and value chain integration.
- ▶▶ **Putting into service:** Inconsistent definitions in sectorial legislation (Medical Devices Regulation, AI Act).
- ▶▶ **CE marking:** Practicality issues of putting it on all digital products and with the value chain integration.
- ▶▶ **Presumption of Conformity:** Processing capabilities of notified bodies.
- ▶▶ **User documentation, declaration of conformity:** Need for more alignment.
- ▶▶ **Conformity assessment:** New provisions for Foundation Models don't fit existing conformity assessment procedures.

AI Act

Walkthrough



AI Act

Scope – High-risk AI

Article 6

8 categories of intended use of AI

1. Biometric identification of persons
2. Critical infrastructure management
3. Education (admission tests & selection processes)
4. Employment (HR/recruitment processes)
5. Essential services (access to social benefits or credit, emergency first response)
6. Crime prediction & response
7. Migration, asylum & border control
8. Justice

Annex 3

AI as safety component to products under New Legislative Framework

Including:

- Machinery Regulation
- Radio Equipment Directive
- Toys Safety Directive
- Medical Devices Regulation
- In-Vitro Diagnostics Regulation

Annex 2 part A

Update possible within 8 categories if risk for health & safety or impact on fundamental rights

Article 7

Cyber Resilience Act (CRA) - compliance

- ▶▶ **Making available and placing on the market, and substantial modification:** Concepts to be adapted to software (solutions in MDR).
- ▶▶ **CE marking** for digital products may differ from traditional hardware products.
- ▶▶ **Vulnerability reporting:** Obligation of the manufacturer to report vulnerabilities and incidents is a new kind of obligation.
- ▶▶ **Presumption of conformity:** The complexity of ensuring continuity of conformity after software updates.

- ▶▶ **Toy Directive**
 - Issues on privacy and cybersecurity started before the CRA (in the Radio Equipment Directive – RED)
 - The TSR allows the data carrier to be affixed on the product packaging only, if the toy is too small. The ESPR was arguably vague on this possibility.
 - The TSR allows voluntary data to be added to the DPP, provided it is clearly distinguished from mandatory DPP compliance data. This wasn't foreseen in the ESPR, although it's mentioned in the draft sReq.
 - The TSR gives a concrete 10-year timeline for DPP maintenance for product placing on the market (even if the operator is insolvent or there's liquidation or cessation of activity).

Provision	ESPR	Toy Safety Regulation
DPP Granularity	<ul style="list-style-type: none"> Model, batch or item-level 	<ul style="list-style-type: none"> Model-level
Declaration of Conformity	<ul style="list-style-type: none"> To be determined if rolled into DPP or not 	<ul style="list-style-type: none"> Fully replaced by DPP
Data access via data carrier	<ul style="list-style-type: none"> Explicitly differentiated by stakeholder type 	<ul style="list-style-type: none"> Undifferentiated by stakeholder type
Information scalability in DPP system	<ul style="list-style-type: none"> Yes to some extent: DPP should be adaptable to incorporate sustainability aspects as mandated by Union legislation 	<ul style="list-style-type: none"> Yes: operators will have a single data carrier and a single product passport only if other EU legislation will in future require info provision via a data carrier
Modalities	<ul style="list-style-type: none"> Data carrier physically present on the product Exceptions possible based nature, size or use of the product 	<ul style="list-style-type: none"> Data carrier physically present on the product Alternatively, if product too small, present on its packaging
Voluntary data in the passport	<ul style="list-style-type: none"> Unspecified (but sReq text introduces possibility) 	<ul style="list-style-type: none"> Yes, provided it is clearly distinguished from mandatory compliance data
Passport time-frame	<ul style="list-style-type: none"> Unspecified 	<ul style="list-style-type: none"> Until 10 years after moment of product placing on the market (even if operator is insolvent, liquidation, cessation of activity)
Usage data	<ul style="list-style-type: none"> No in EC proposal (but Council supports inclusion) 	<ul style="list-style-type: none"> No, unless for what is needed in order to provide info on the product passport online.
Language availability	<ul style="list-style-type: none"> Unspecified 	<ul style="list-style-type: none"> Languages required by the Member State where the toy is made available on the market
Information in central registry	<ul style="list-style-type: none"> List of data carriers and unique product identifiers at a minimum (but Council supports unique product, facility and operator identifiers at a minimum) 	<ul style="list-style-type: none"> Unique product identifier and unique operator identifier at a minimum

Ecodesign Regulation (ESPR) - Compliance

- ▶▶ **Making available and placing on the market:** Uncertainty on how to handle second hand and spare parts, as limited exemptions are granted for spare parts in the ESPR.
- ▶▶ **Repair** as produced vs placing a new product on the market (Ex. hardware changes and software updates might change conformity of a product). The ESPR does not guarantee the repair as produced principle.
- ▶▶ **CE marking:** ESPR Art. 40 allows EC to define rules.
- ▶▶ **Harmonised standards:**
 - Test method in Regulations and EC Communications as presumption of conformity.
 - Reference to common specification rather than standards.
 - Different test methods developed in different geographical areas as a consequence.
- ▶▶ **Conformity assessment procedure Module A:** ESPR reference to all modules.

Digital Product Passport (DPP) - Compliance

- ▶▶ Linear economy legislation (e.g. NLF) vs circular economy legislation (e.g. ESPR).
- ▶▶ Uncertainty on what are the product categories in scope: Risk of different sectorial DPPs (battery regulation).
- ▶▶ Misalignment with sectorial legislation.
- ▶▶ **Declaration of conformity:** Lack of notified bodies.
- ▶▶ **Conformity assessment:** Should it be added to the DPP?
- ▶▶ **CE marking:** Will DPP replace the CE mark itself?

4

Requests to regulators

Main Asks

- ▶▶ **Alignment between sectorial legislation and horizontal legislation**
- ▶▶ **Harmonised standards instead of common specifications**
- ▶▶ **Clarity on how to apply product provisions to software**
- ▶▶ **Compliance based on circular lifecycle of products instead of linear**

Main Asks – AI ACT & NLF

- ▶▶ **New: recital 29a - avoid different or overlapping requirements and reduce the burden on manufacturers.**
- ▶▶ **Amendment: Article 8.2a - Align with NLF, bringing non-equivalent requirements under the union harmonization legislation**
 - **Conformity assessment based on Union Harmonisation Legislation by relevant notified bodies.**
- ▶▶ **New: Article 85c - Date of application of requirement shall be specified**
- ▶▶ **New: Article 71.1a, fines should be dealt in case-by-case basis.**
- ▶▶ **Art. 5: Prohibited practices need precise definition** and clarity to avoid unintended restrictions. Prohibitions of social scoring, biometric identification and emotion recognition should be targeted, to permit controlled high-risk applications.

#AStrongerDigitalEurope



@DIGITALEUROPE



linkedin.com/digitaleurope

**Thank you for
your attention!**

DIGITALEUROPE

