



# DIGITALEUROPE

## Cybersecurity Standardisation Conference 2021

Alberto Di Felice  
Director for Infrastructure, Privacy and Security

# Can't wait for IoT security



# But mind the gaps – and the overlaps

Disclaimer: This "working" document has been built on the base of technical solutions, received by the ESOs, that may apply to Articles 3(3)(d/e/f/l) and 4 of the RED if/when appropriate delegated acts are adopted. It is a "draft" and, as such, the information herein are not conclusive. It does not prejudice any future Commission's legal act, policy decision, standardization request and/or discussions in Expert/Working Groups or with the stakeholders. It does not prejudice further independent analysis, hence the information herein contained can change, following inputs from the stakeholders. It is not an acknowledgement of the state-of-the-art and it does not prejudice any other technical solution that may be relevant and added in a second moment.

Does the clause

ESO	Docu-ment type	Reference	Version	Year	Title	Status	Scope, as related to the RED	Horizontal legislation	Requirement(s)?	Related test method(s)?	(new) (if yes to the previous question) contain a test method whose results can and should be self-assessed?	(new) needs to be adapted/modified/specified so to be inserted in harmonised standards?	apply or can apply to other categories or classes of radio equipment? (if yes, please specify)	
ETSI	EN	303 645	2.0.0	2019	Securing consumer IoT	Draft	IoT devices	5.6	Minimize exposed attack surfaces	N	May be assessed through ETSI TS 103701	TBC	TBC	under assessment
								5.7	Ensure software integrity	N	May be assessed through ETSI TS 103701	TBC	TBC	under assessment
								5.8	Ensure that personal data is secure	N	May be assessed through ETSI TS 103701	TBC	TBC	under assessment
								5.9	Make systems resilient to outages	N	May be assessed through ETSI TS 103701	TBC	TBC	under assessment
								5.10	Examine system telemetry data	N	May be assessed through ETSI TS 103701	TBC	TBC	under assessment
								5.11	Make it easy for users to delete user data	N	May be assessed through ETSI TS 103701	TBC	TBC	under assessment

Vertical legislation

RED et al. NLF

IMMINENT

Horizontal legislation

FUTURE

Certification schemes

FUTURE

Standards

# Mapping the gaps



■ Fully addressed\* 
 ■ Partially addressed\* 
 ■ Not addressed

\* Requirements might be placed on the service provider

Source: European Commission, Study on the need of Cybersecurity requirements for ICT products, Workshop #1 – Problem Definition

# How does the RED perform?

Protection against accidental or unauthorised against storage, processing, access and disclosure	Protection against accidental or unauthorised destruction, loss or alteration or lack of availability	Authorisation to access data and services	Identification of dependencies and vulnerabilities	Record of access
Art 3 - Essential requirements - Manufacturers	Art 3 - Essential requirements - Manufacturers	Art 3 - Essential requirements - Manufacturers	Not addressed	Not addressed
Verification of access	Verification of the absence of vulnerabilities	Restoration of availability	Security by default and design	Secure update of software and hardware
Not addressed	Not addressed	Not addressed	Not addressed	Not addressed

Fully addressed\*
  Partially addressed
  Not addressed

\* Requirements might be placed on the service provider

Source: European Commission, Study on the need of Cybersecurity requirements for ICT products, Workshop #1 – Problem Definition

# What industry needs

- ▶▶ Legal certainty and consistency – things standards can't take care of  
*Measures to address IoT cybersecurity should aim to avoid multiple and diverging requirements*
- ▶▶ Common baseline, with a differentiated approach to IoT per domain  
*Cybersecurity requirements should always be based on risk and intended use – the higher the risk, the more stringent the requirements*
- ▶▶ Standards must be ready before any legislation is implemented  
*The development of appropriate IoT security standards and criteria should be allowed before enforcing or making applicable legislative measures*



**Thank you**

**DIGITALEUROPE** 