

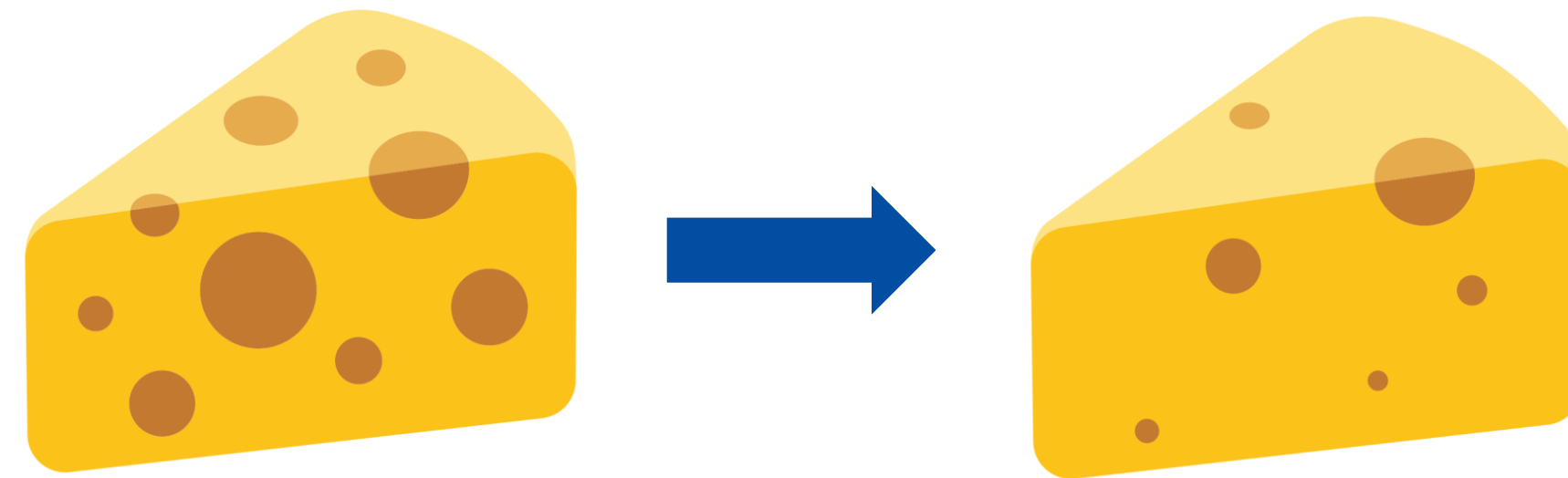
# The EU regulating (open source) software

*the proposed Cyber Resilience Act and  
Product Liability Directive*

Benno Overeinder, Bastiaan Goslings and Robert Carolina

proposal text: <https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act>

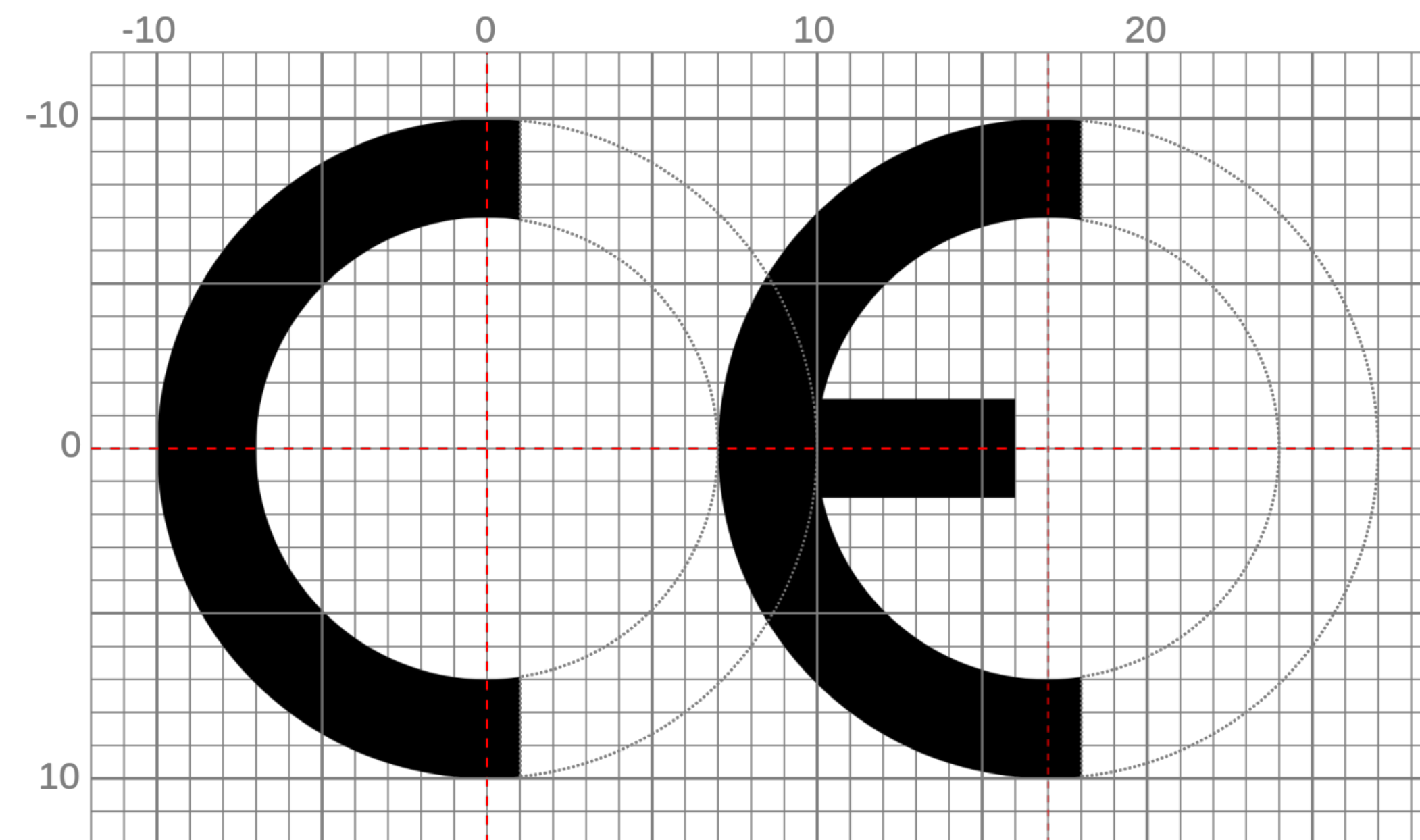
CRA in a nutshell



**European Commission intends to regulate**  
*products with digital elements*  
**( $\approx$  all hardware & software)**

Slide image source: [CONNECT University](#), CC BY 4.0

# CE marking



**TL;DR: this affects FOSS too**

1  
What?

2  
How?

3  
now  
what?

# Scope

## Products with digital elements:

- + **Hardware products** and components placed on the market separately, such as laptops, smart appliances, mobile phones, network equipment or CPUs
- + **Software products** and components placed on the market separately, such as operating systems, word processing, games or mobile apps
- ① The definition of “**products with digital elements**” also includes **remote data processing solutions**.

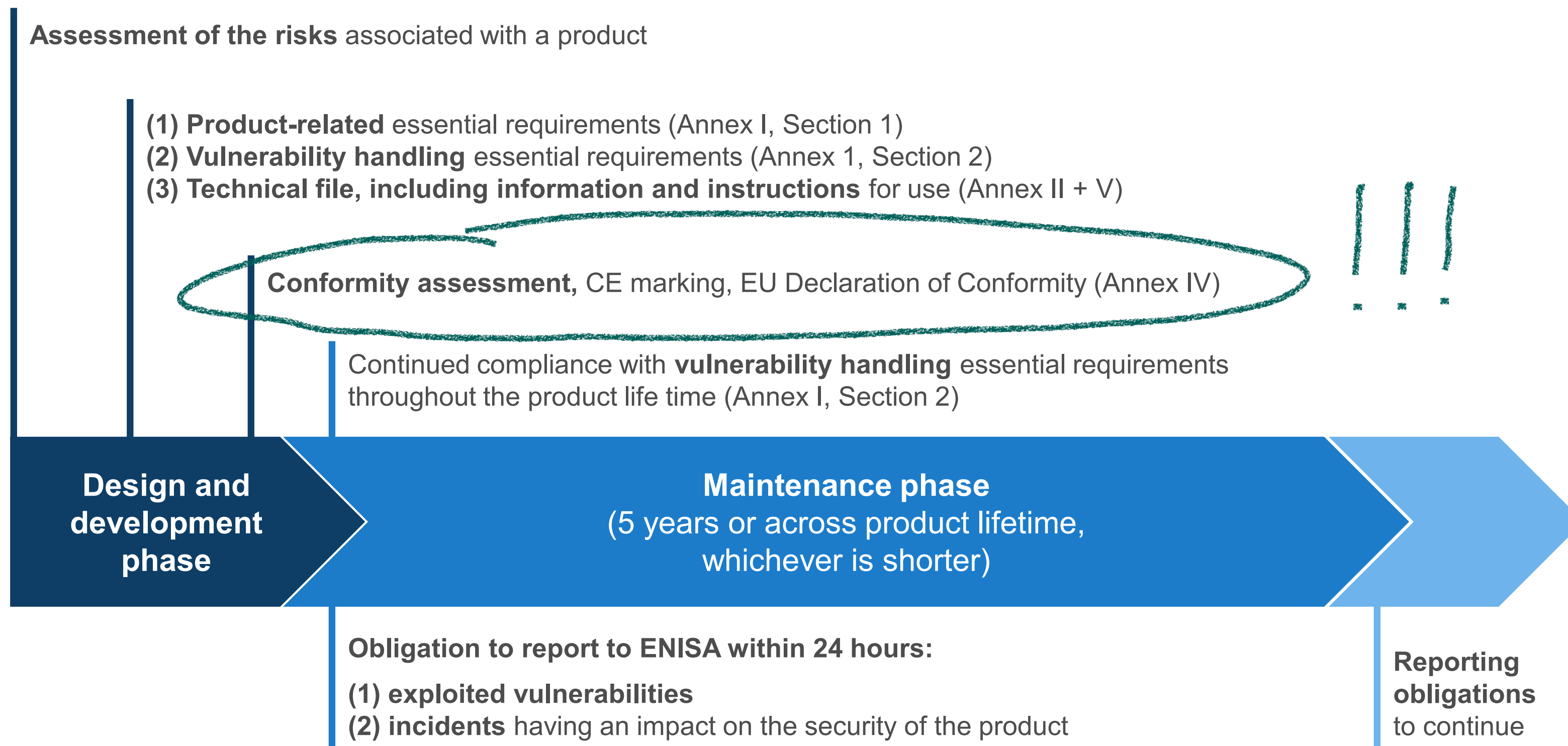
## Not covered:

- ✘ **Non-commercial projects, including open source** in so far as a project is not part of a commercial activity
- ✘ **Services, in particular cloud/Software-as-a-Service** – covered by NIS2

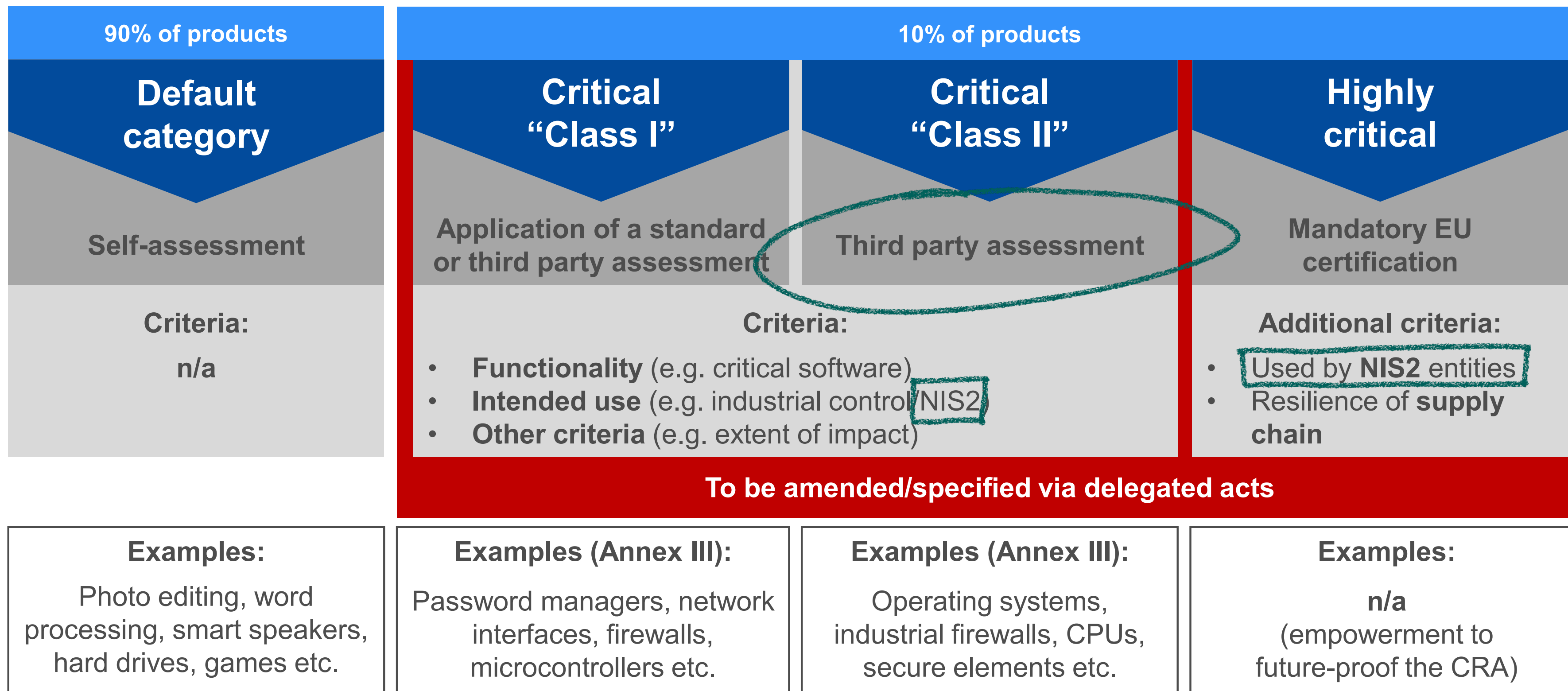
## Outright exclusions:

- ✘ **Certain products sufficiently regulated on cybersecurity** (cars, medical devices, *in vitro*, certified aeronautical equipment) under the new and old approach

# Obligations of manufacturers



# Which conformity assessment to follow?



# New Legislative Framework

- Manufacturers, authorised representatives, distributors and importers

- Notified bodies

→ third party assessment

(e.g. NL: RDI?)

- Notifying authorities

- National accreditation bodies

- Market surveillance authorities

appoint,  
monitor

"Liftinstituut"

"TUV"

"DEKRA"

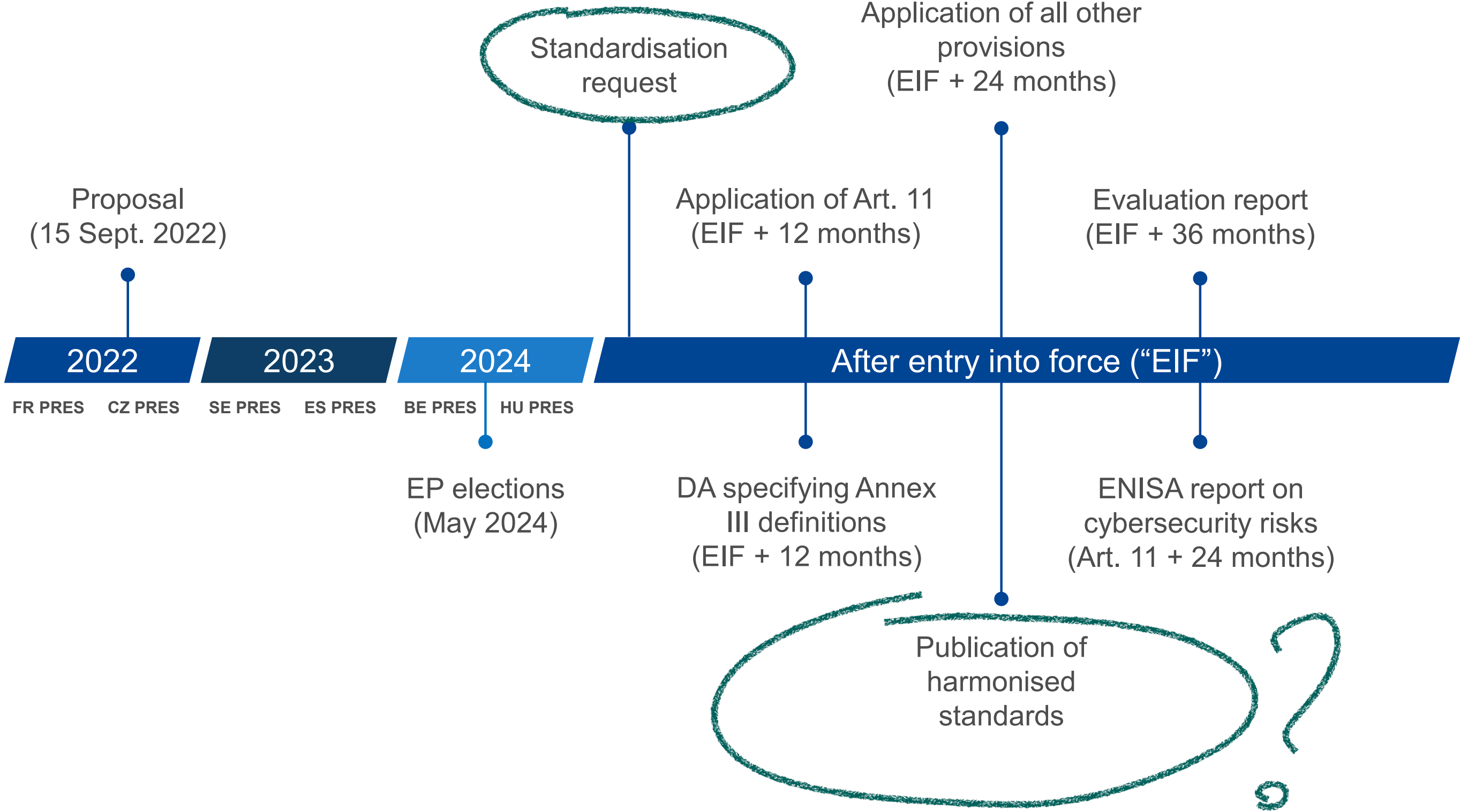
...

(your favorite here)





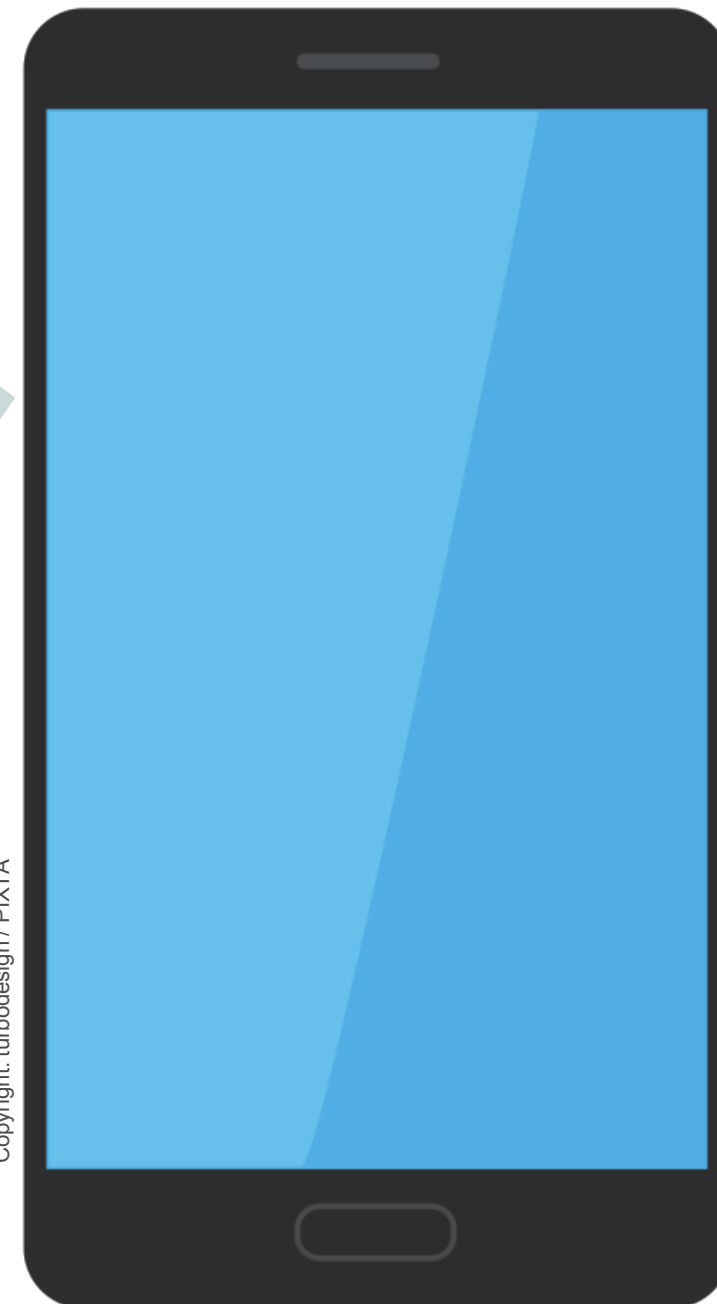
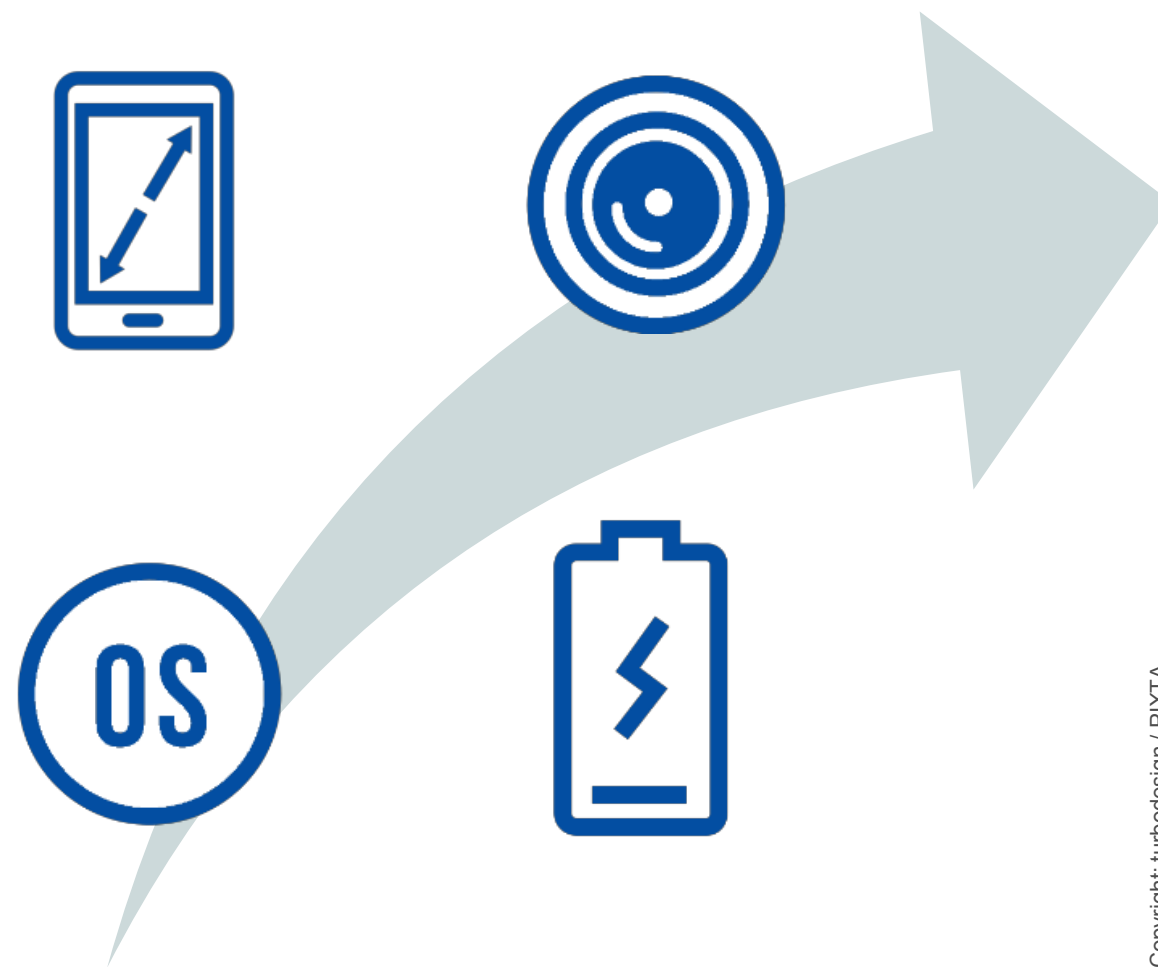
# Tentative timeline



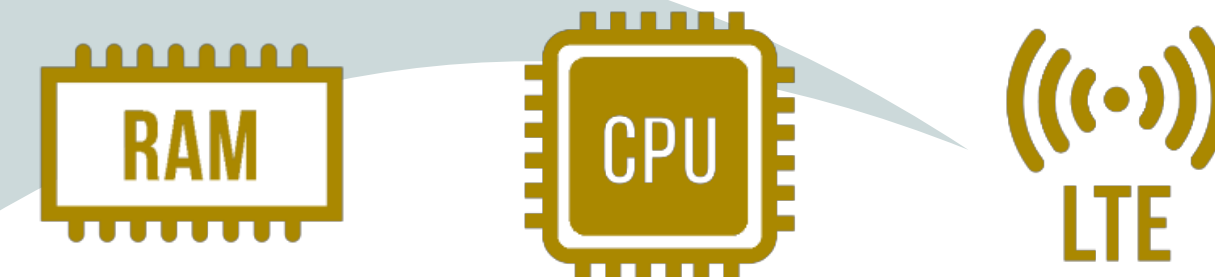
# A simplified example of smartphones (hardware)

As a rule, whoever places on the market a “final” product or a component is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking**.

Developed by the manufacturer placing the smartphone on the market:



Developed by upstream manufacturers for integration into the “final” product:



Placed on the market separately for users to buy and integrate:



# A simplified example of ~~smartphones~~ Linux kernels

As a rule, whoever places on the market a “final” product or a component is required to comply with the **essential requirements**, undergo **conformity assessment** and affix the **CE marking**.

Developed by the manufacturer



Developed <sup>by 1971 developers</sup> by upstream ~~manufacturers~~ for integration into the “final” product:  
employed by (some indicative companies)



source: [LWN.net: Development statistics for 6.3](https://lwn.net/Articles/704000)

**TL;DR: this affects FOSS too**

1  
What?

2  
How?

3  
now  
what?

# FOSS out of scope?

“In order not to hamper innovation or research,  
**free and open-source software**  
developed or supplied  
outside the course of a commercial activity  
**should not be covered by this Regulation. [..]”**

- recital 10

# "Commercial activity"?

"[...] a **commercial activity** **might be characterized** not only

1. by charging a price for a product, but also
2. by charging a price for technical support services,
3. by providing a software platform through which the manufacturer monetises other services, or
4. by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. "

- recital 10



# Risks arising from the proposal's chosen open source exception

Expansive interpretation of "commercial activity" leads to narrow scope of exemption

---

Disincentive to professionalise development and curation


---

Incentive to move away from open source non-profit model

---

Harming product diversity and reducing innovation

---



# The *Blue Guide* guidance on the NLF from 2022 did not actually consider *standalone software as a product*

See: [2022/C 247/01 The 'Blue Guide' guidance on the implementation of EU product rules](#)

*“Commercial activity is understood as providing goods in a business related context”*

---

*“[...] appreciated on a case by case basis taking into account: [...]”*  
 regularity of supply

---

characteristics of the product

---

intention of the supplier

---



# Further reading

- Content of today's presentation was sourced from the joint response with ISC, CZ.NIC and NetDEF

## **broader FOSS perspectives on the CRA:**

- Responses by Open Source Initiative, Open Forum Europe
- many others! See "the ultimate list of reactions to the CRA" by Simon Phipps

## **on the limitations of "supply chain"-thinking:**

- "I am not a supplier" by Thomas Depierre

## **on the lack of standards and audit capacity required:**

- "The EU's new Cyber Resilience Act is about to tell us how to code" by Bert Hubert

**TL;DR: this affects FOSS too**

1  
What?

2  
How?

3  
now  
what?



**RIPE NCC**

RIPE NETWORK COORDINATION CENTRE

# The EU Cyber Resilience Act

Feedback provided by the RIPE NCC

Bastiaan Goslings | 23 May 2023 | RIPE 86

# Good intentions?



- Improve cybersecurity in the EU
- Harmonisation and legal clarity for manufactures when placing products on the EU market
- Risk-based approach
- Security-by-design principle
- Clear information for users

# Feedback requested by EC



- RIPE NCC submitted a response on 23 January 2023:
  - What does this mean, in terms of scope, definitions, necessity & proportionality?
  - How does it affect RIPE NCC services and infrastructure?
  - What are the concerns within the RIPE community at large?

<https://t.ly/upBI>

## Feedback from: RIPE NCC

[Have your say](#) > [Published initiatives](#) > [Cyber resilience act – new cybersecurity rules for digital products and ancillary services](#) > **Feedback from:**

<b>Feedback reference</b>	F3376593
<b>Submitted on</b>	23 January 2023
<b>User type</b>	Other
<b>Organisation</b>	RIPE NCC
<b>Organisation size</b>	Medium (50 to 249 employees)
<b>Transparency register number</b>	<a href="#">075577725582-66</a>
<b>Country of origin</b>	Netherlands
<b>Initiative</b>	<a href="#">Cyber resilience act – new cybersecurity rules for digital products and ancillary services</a>

As the Regional Internet Registry for Europe, the Middle East and parts of Central Asia, the RIPE NCC welcomes the opportunity to give feedback on the European Commission's proposed Cyber Resilience Act. In the attached document, we explain how we foresee the Cyber Resilience Act impacting the RIPE NCC's own operations and services, and areas in which we believe further clarity is needed. In addition, we include viewpoints from the wider RIPE community, which is made up of technical operators, open-source developers and others responsible for maintaining much of the Internet's technical infrastructure within Europe and beyond.

# Community concerns



- Welcome the exemption for open source software in recital 10, however it is too limited
  - Only when “developed or supplied outside the course of a commercial activity”
  - Terminology of the New Legislative Framework does not fit the way open source software is developed and published (‘manufacturer’, ‘placing on the market’)
  - Potential impact of compliance costs for small entities, individual developers - will harm innovation within the EU
  - Emphasis should be put on usage of the product, not on the type of license

'For the CRA to reach the goal of reducing product vulnerability, it also needs to reduce vulnerability in open-source software – an aim the RIPE NCC strongly supports.

## **The lack of clarity surrounding the notion of “commercial activity” referred to in**

**Recital 10** however, is what creates uncertainty for, and risks placing undue regulatory burden on, those from the community who contribute to open-source software and its security without the intent of making a profit as a result of its later use.'



To: ITRE's (shadow) rapporteurs on the Cyber Resilience Act

Amsterdam, 21 April 2023

Dear Members of the European Parliament,

As the Regional Internet Registry for Europe, the Middle East and parts of Central Asia, the RIPE NCC welcomes the European Commission's efforts to further harmonise and improve cybersecurity in the European Union by setting essential cybersecurity requirements for all products with digital elements that are placed on the EU market. We therefore support the proposed Cyber Resilience Act's (CRA) cybersecurity-by-design approach, as well as the included obligation for manufacturers and other relevant operators to provide end users with clear and understandable information about their products with digital elements. Manufacturers, distributors and other relevant operators can benefit from the legal clarity and certainty created by avoiding fragmentation on the topic between different Member States within the EU's single market.

The RIPE NCC would like to use this opportunity to reiterate<sup>1</sup> the RIPE community's concerns regarding the limited exemption, formulated in Recital 10 of the CRA, for the development and making available of open-source software. We do so in our role as secretariat for RIPE, which is an open, inclusive community that welcomes the participation of anyone with an interest in IP-based networking. We also do so as an organisation that publishes the source code for several of its own products/services, under various public licences, via repositories such as GitHub. This is something we do, not with the intention to make the software available as an independent product for end users, but for transparency and research purposes, outside our standard business context/activities as a Regional Internet Registry.

As we highlighted in our response to the European Commission's proposal, open-source software is often published by one developer and then built upon and modified by many others, some of whom may ultimately incorporate it into a product to be placed on the market. In this sense, there is often not a clear-cut distinction of who can be considered the "manufacturer". As open source veteran and expert Simon Phipps has said, 'Open source is an artefact arising from the interactions of a community of contributors with no contractual binding between them beyond the open source licence itself, which disclaims all warranties and has no conduit for funds'<sup>2</sup>.

For the CRA to reach the goal of reducing product vulnerability, it also needs to reduce vulnerability in open-source software — an aim the RIPE NCC strongly supports. The lack of clarity surrounding the notion of "commercial activity" referred to in Recital 10 however, is what creates uncertainty for, and risks placing undue regulatory burden on, those from the community who contribute to open-source software and its security without the intent of making a profit as a result of its later use. The Blue Guide does not give sufficient clarity as to when open-source

<sup>1</sup> [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3376593\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3376593_en)

<sup>2</sup> <https://the.webm.ink/open-source-is-conceptually-disjoint-from-proprietary-software>

Registered in Amsterdam Chamber of Commerce No. 40539632  
Bank: ABN-Amro EUR Account No. NL 3748N40618139087  
VAT No. NL806268220B01

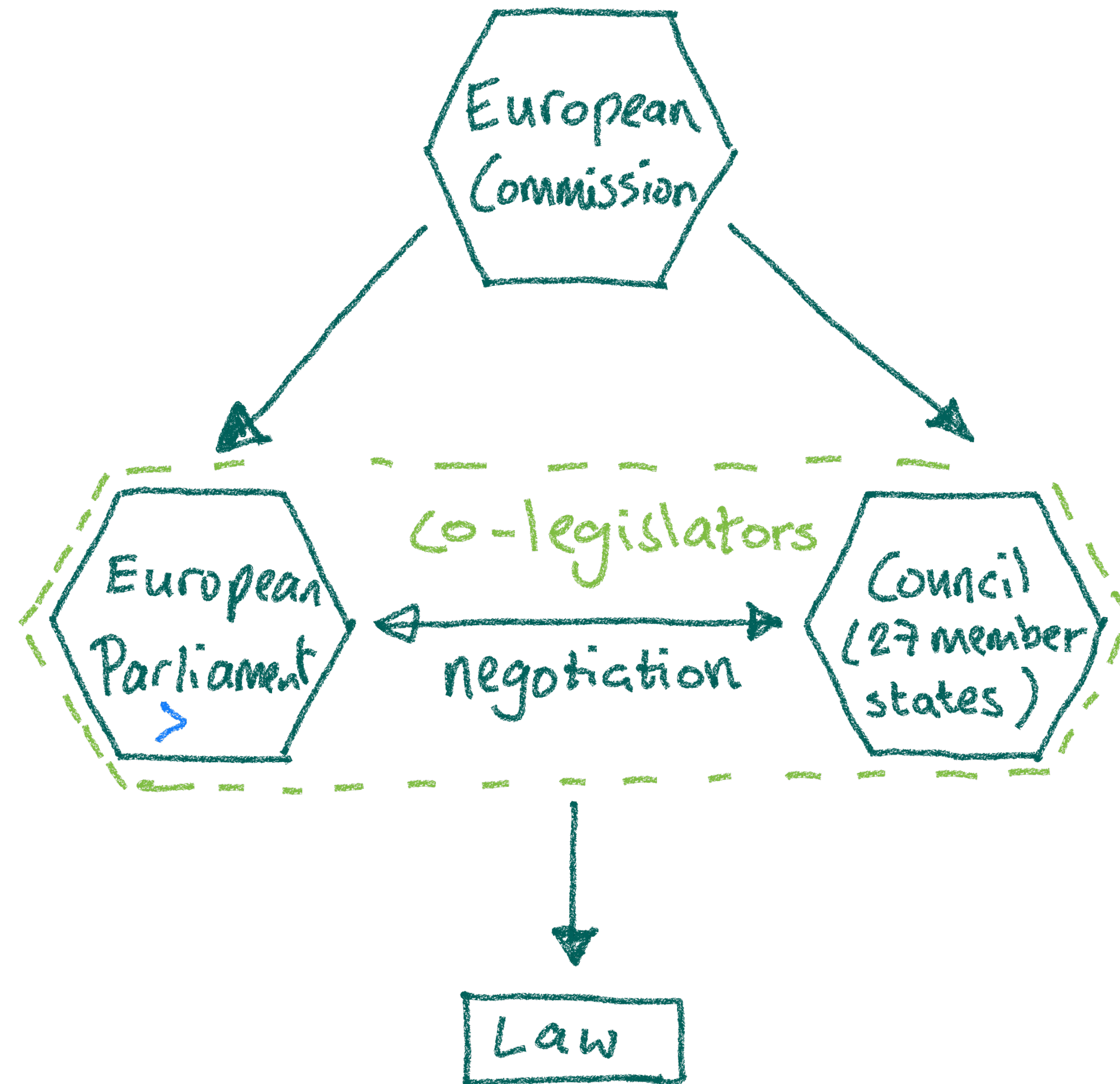
Stationsplein 11  
P.O. Box 10096  
1001 EB Amsterdam  
The Netherlands

T: +31 20 535 4444  
F: +31 20 535 4445  
E: [ncc@ripe.net](mailto:ncc@ripe.net)  
W: [www.ripe.net](http://www.ripe.net)

<https://www.ripe.net/participate/internet-governance/multi-stakeholder-engagement/ripe-ncc-letter-to-itre-on-cra.pdf>



# Now: discussion in council, parliament



# Current status



- Council compromise text for OSS in recital 10 reached - improved text
- European Parliament
  - ITRE (Industry Research Energy) lead committee; draft report strengthens exclusion of OSS for non-commercial purposes
  - ITRE technical meetings to discuss proposed amendments currently ongoing
  - Reach out to MEP's to state concerns



# Questions



[bgoslings@ripe.net](mailto:bgoslings@ripe.net)

# Council: FOSS comprise text 10 March 2023

**This Regulation applies only to products with digital elements made available on the market, hence supplied for distribution or use on the Union market in the course of a commercial activity. The supply in the course of a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise, by providing a software platform through which the manufacturer monetises other services, or by requiring as a condition for use, the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity. Taking account of the above-mentioned elements determining the commercial nature of an activity, only free and open-source software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable, supplied in the course of a commercial activity and therefore placed on the market should be covered by this Regulation. For the same considerations, products provided by public administration**

# EP: from ITRE draft report 31 March 2023

## Amendment 8

### Proposal for a regulation

#### Recital 10

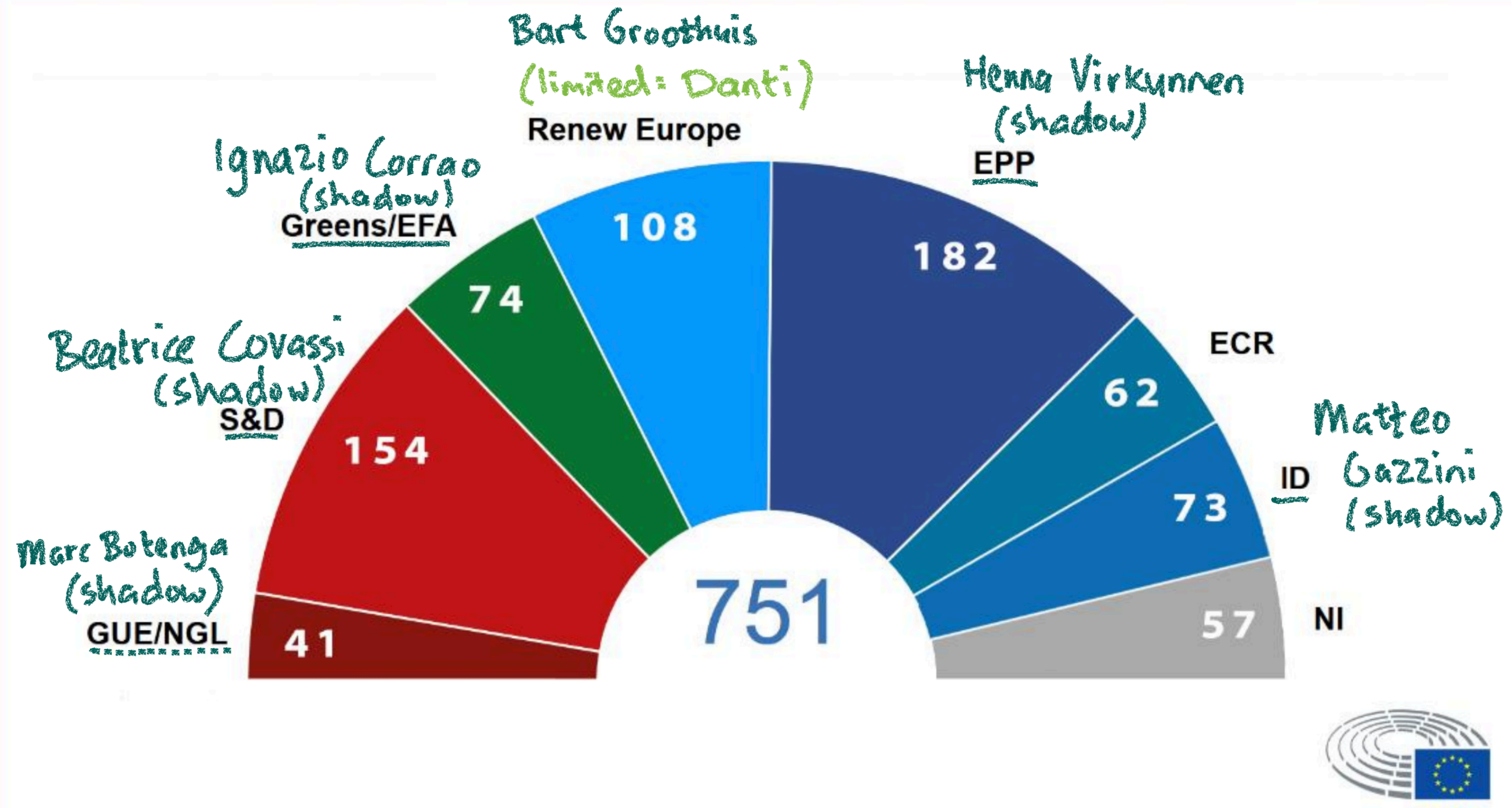
##### *Text proposed by the Commission*

(10) In order not to hamper innovation or research, free and open-source software **developed or** supplied **outside** the course of a commercial activity should **not** be covered by this Regulation. ***This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable.*** In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software.

##### *Amendment*

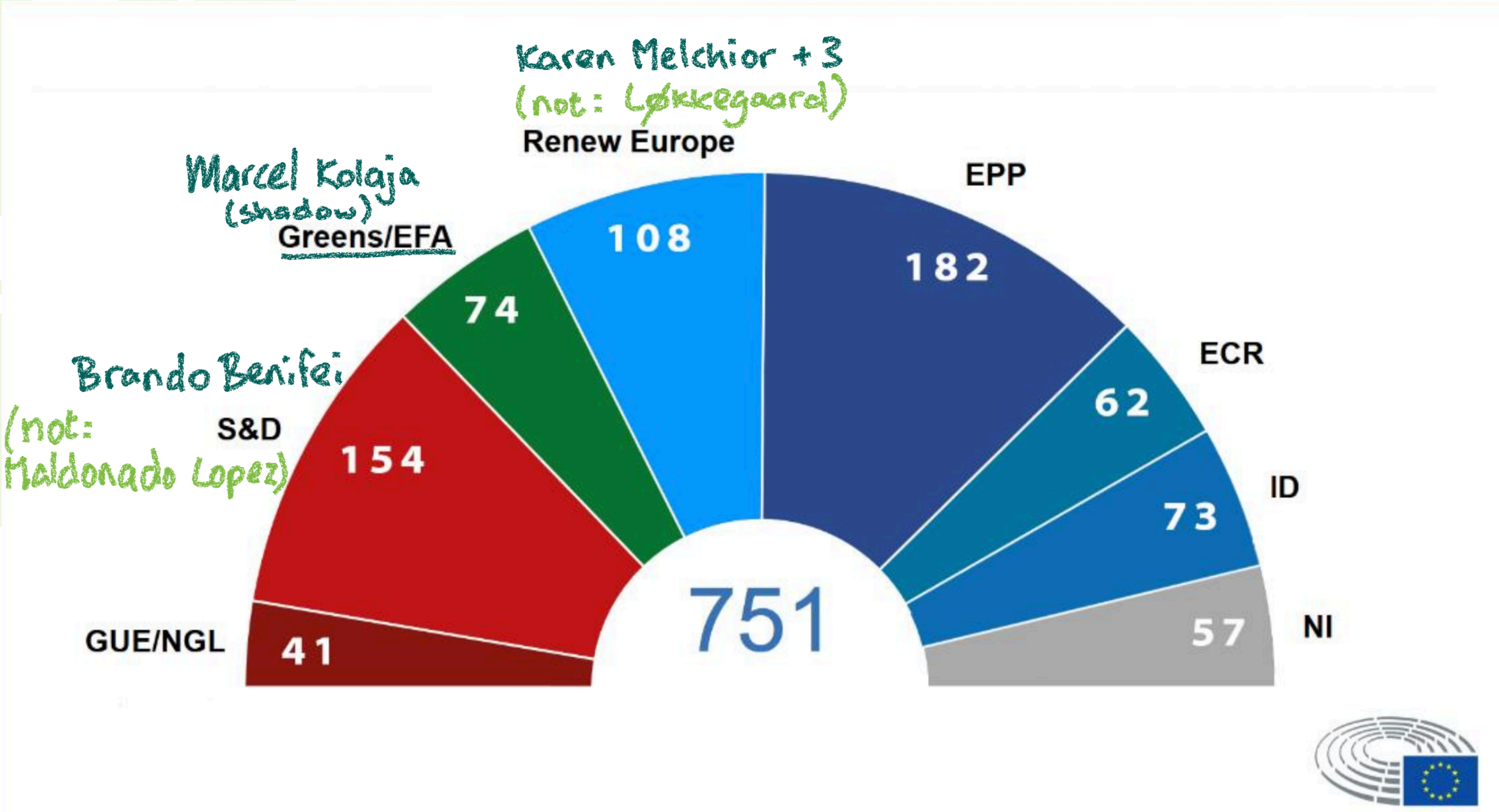
(10) In order not to hamper innovation or research, **only** free and open-source software supplied **in** the course of a commercial activity should be covered by this Regulation. In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. ***Where free and open-source software has been developed or supplied outside the course of a commercial activity, manufacturers that incorporate such software in their products with digital elements should take all the necessary steps to ensure the***

# Last week: FOSS related amendments in ITRE



Slide image source: [European Parliament](#)

# Last week: FOSS related amendments in IMCO



Slide image source: [European Parliament](https://www.europarl.europa.eu)

# The proposed Product Liability Directive (PLD)

## What would it do?

Robert Carolina, General Counsel  
Internet Systems Consortium  
RIPE86, Rotterdam, 22-25 May 2023





# Robert Carolina

- Lawyer (England & US)
  - General Counsel, ISC (2020- )
  - Author, CyBOK Law & Regulation ([www.cybok.org](http://www.cybok.org))
  - Practitioner, law & regulation of ICT; law & ethics in cyber security
  - BA (Dayton, 1988)  
Juris Doctor (Georgetown, 1991)  
LL.M (London School of Economics, 1993)
- Royal Holloway University of London
  - Senior Fellow, Law & Regulation module leader, Information Security Group, (1999- )

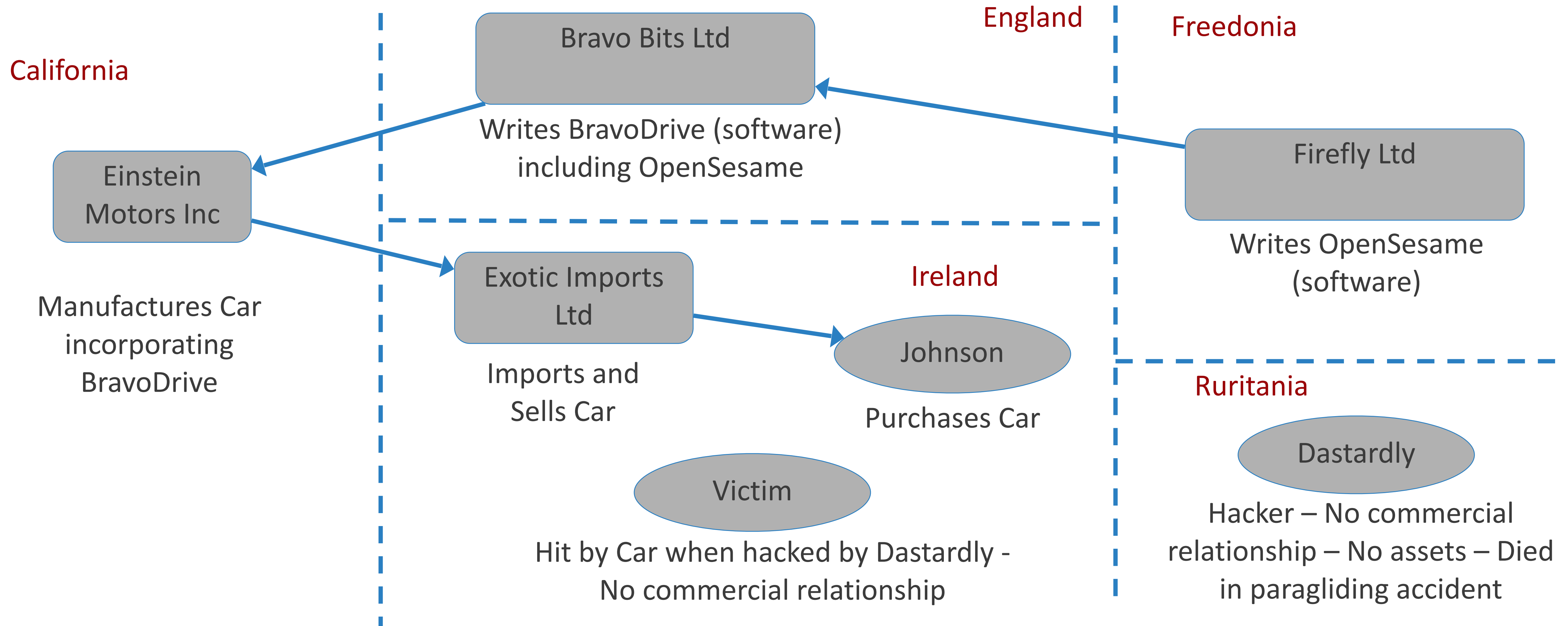


**Hypothetical: 7 persons, 2 pieces of software, 1 car, 1 victim, all fictitious**

# Hypothetical – the story

- Firefly Ltd (Freedonia) develops and supplies "OpenSesame" cryptographic authentication software package.
- Bravo Bits Ltd (England) writes BravoDrive software: human-machine middleware. Incorporates OpenSesame authentication software.
- Einstein Motors Inc (California) adopts BravoDrive as fly-by-wire solution in automobiles they manufacture.
- Exotic Imports Ltd (Ireland) imports Einstein Sedans from California
- Jim Johnson (Ireland) purchases an Einstein Sedan from Exotic Imports.
- Denis Dastardly (Ruritania) exploits a flaw in OpenSesame. He remotely hacks Johnson's sedan and accidentally commands the car (in Ireland) to swerve & crash into Victor Victim.
- Victor Victim suffers life-altering injuries.
- Dastardly has no money. He dies in a paragliding accident.

# Hypothetical – the supply chain



# Hypothetical – the forensic export report

- The vulnerability
  - OpenSesame source code included a subtle coding error – a single misplaced semi-colon. This created a vulnerability in the (otherwise standard) cryptographic authentication protocol.
  - Firefly normally has a strong reputation for secure coding, but this Q/A programme was poorly managed.
  - Dastardly discovered the weakness independently. This was a zero day exploit.

# Legal analysis: the law today

If Victim brings a lawsuit in Ireland against...	Negligence (common law)			Strict Liability Defective Product (EU 85/374)		
	Duty of care to victim (foreseeable, proximity)	Acted unreasonably (negligently)	Liable	Supply of product	Lacks reasonably expected safety	Liable
<b>Johnson</b>	YES	No	n/a	Not a supplier	n/a	n/a
<b>Exotic Imports</b>	YES	No	n/a	YES - car	YES	YES
<b>Einstein Motors</b>	YES	No	n/a	YES - car	YES	YES
<b>Bravo Bits</b>	Probably yes	Probably no	Probably no	No - software	n/a	n/a
<b>Firefly</b>	Maybe?	Maybe??	Maybe???	No - software	n/a	n/a
<b>Dastardly</b>	Who cares? He has no money! If any other person found liable, they could be jointly & severally liable for up to 100% of Victim's damages.					

# Legal analysis: the law today

If Victim brings a lawsuit in Ireland against...	Negligence (common law)			Strict Liability Defective Product (EU 85/374)		
	Duty of care to victim (foreseeable, proximity)	Acted unreasonably (negligently)	Liable	Supply of product	Lacks reasonably expected safety	Liable
Johnson	YES	No	n/a	Not a supplier	n/a	n/a
Exotic Imports	YES	No	n/a	YES - car	YES	YES
Einstein Motors	YES	No	n/a	YES - car	YES	YES
Bravo Bits	Probably yes	Probably no	Probably no	No - software	n/a	n/a
Firefly	Maybe?	Maybe??	Maybe???	No - software	n/a	n/a

Law of strict liability for defective products makes manufactures and component suppliers financially responsible for dangerous products they supply that hurt people – they are efficient cost spreaders.

# Legal analysis: after transposition of PLD in 2024-26?

If Victim brings a lawsuit in Ireland against...	Negligence (common law)			Strict Liability Defective Product (EU PLD?)		
	Duty of care to victim (foreseeable, proximity)	Acted unreasonably (negligently)	Liable	Supply of product	Lacks reasonably expected safety	Liable
<b>Johnson</b>	YES	No	n/a	Not a supplier	n/a	n/a
<b>Exotic Imports</b>	YES	No	n/a	YES - car	YES	YES
<b>Einstein Motors</b>	YES	No	n/a	YES - car	YES	YES
<b>Bravo Bits</b>	Probably yes	Probably no	Probably no	<u>YES-software</u>	<u>YES</u>	<u>YES</u>
<b>Firefly</b>	Maybe?	Maybe??	Maybe???	<u>YES-software</u>	<u>YES</u>	<u>YES</u>
<b>Dastardly</b>	Who cares? He has no money! If any other person found liable, they could be jointly & severally liable for up to 100% of Victim's damages.					