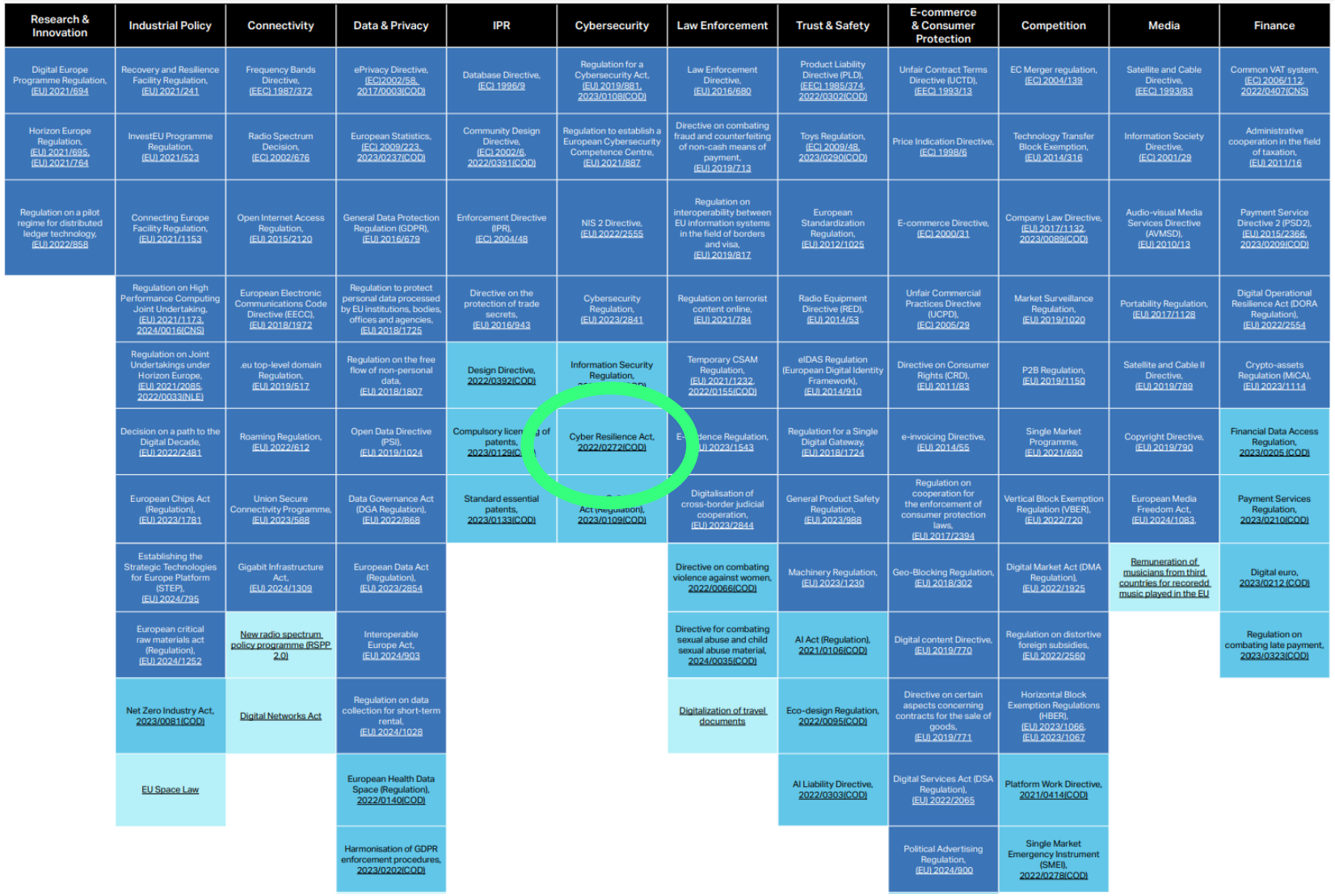
MUNI

CRA and its ?Problematic? Impacts on F/OSS

Pavel Loutocký

The overall context of EU data legislation



Research & Innovation	Industrial Policy	Connectivity	Data & Privacy	IPR	Cybersecurity	Law Enforcement	Trust & Safety	E-commerce & Consumer Protection	Competition	Media	Finance
Digital Europe Programme Regulation, (EU) 2021/694	Recovery and Resilience Facility Regulation, (EU) 2021/241	Frequency Bands Directive, (EEC) 1987/372	ePrivacy Directive, (EC)2002/58, 2017/0003(COD)	Database Directive, (EC) 1996/9	Regulation for a Cybersecurity Act, (EU) 2019/881, 2023/0108(COD)	Law Enforcement Directive, (EU) 2016/680	Product Liability Directive (PLD), (EEC) 1985/374, 2022/0302(COD)	Unfair Contract Terms Directive (UCTD), (EEC) 1993/13	EC Merger regulation, (EC) 2004/139	Satellite and Cable Directive, (EEC) 1993/83	Common VAT system, (EC) 2006/112, 2022/0407(CNS)
Horizon Europe Regulation, (EU) 2021/695, (EU) 2021/764	InvestEU Programme Regulation, (EU) 2021/523	Radio Spectrum Decision, (EC) 2002/676	European Statistics, (EC) 2009/223, 2023/0237(COD)	Community Design Directive, (EC) 2002/6, 2022/0391(COD)	Regulation to establish a European Cybersecurity Competence Centre, (EU) 2021/887	Directive on combating fraud and counterfeiting of non-cash means of payment, (EU) 2019/713	Toys Regulation, (EC) 2009/48, 2023/0290(COD)	Price Indication Directive, (EC) 1998/6	Technology Transfer Block Exemption, (EU) 2014/316	Information Society Directive, (EC) 2001/29	Administrative cooperation in the field of taxation, (EU) 2011/16
Regulation on a pilot regime for distributed ledger technology, (EU) 2022/858	Connecting Europe Facility Regulation, (EU) 2021/1153	Open Internet Access Regulation, (EU) 2015/2120	General Data Protection Regulation (GDPR), (EU) 2016/679	Enforcement Directive (IPR), (EC) 2004/48	NIS 2 Directive, (EU) 2022/2555	Regulation on interoperability between EU information systems in the field of borders and visa, (EU) 2019/817	European Standardization Regulation, (EU) 2012/1025	E-commerce Directive, (EC) 2000/31	Company Law Directive, (EU) 2017/1132, 2023/0089(COD)	Audio-visual Media Services Directive (AVMSD), (EU) 2010/13	Payment Service Directive 2 (PSD2), (EU) 2015/2366, 2023/0209(COD)
	Regulation on High Performance Computing Joint Undertaking, (EU) 2021/1173, 2024/0016(CNS)	European Electronic Communications Code Directive (EECC), (EU) 2018/1972	Regulation to protect personal data processed by EU institutions, bodies, offices and agencies, (EU) 2018/1725	Directive on the protection of trade secrets, (EU) 2016/943	Cybersecurity Regulation, (EU) 2023/2841	Regulation on terrorist content online, (EU) 2021/784	Radio Equipment Directive (RED), (EU) 2014/53	Unfair Commercial Practices Directive (UCPD), (EC) 2005/29	Market Surveillance Regulation, (EU) 2019/1020	Portability Regulation, (EU) 2017/1128	Digital Operational Resilience Act (DORA Regulation), (EU) 2022/2554
	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	.eu top-level domain Regulation, (EU) 2019/517	Regulation on the free flow of non-personal data, (EU) 2018/1807	Design Directive, 2022/0392(COD)	Information Security Regulation,	Temporary CSAM Regulation, (EU) 2021/1232, 2022/0155(COD)	eIDAS Regulation (European Digital Identity Framework), (EU) 2014/910	Directive on Consumer Rights (CRD), (EU) 2011/83	P2B Regulation, (EU) 2019/1150	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MiCA), (EU) 2023/1114
	Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	Open Data Directive (PSI), (EU) 2019/1024	Compulsory licen of patents, 2023/0129(C	Cyber Resilience Act, 2022/0272(COD)	E- dence Regulation, U) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/55	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205 (COD)
	European Chips Act (Regulation), (EU) 2023/1781	Union Secure Connectivity Programme, (EU) 2023/588	Data Governance Act (DGA Regulation), (EU) 2022/868	Standard essential patents, 2023/0133(COD)	Act (Regulation), 2023/0109(COD)	Digitalisation of cross-border judicial cooperation, (EU) 2023/2844	General Product Safety Regulation, (EU) 2023/988	Regulation on cooperation for the enforcement of consumer protection laws, (EU) 2017/2394	Vertical Block Exemption Regulation (VBER), (EU) 2022/720	European Media Freedom Act, (EU) 2024/1083,	Payment Services Regulation, 2023/0210(COD)
	Establishing the Strategic Technologies for Europe Platform (STEP), (EU) 2024/795	Gigabit Infrastructure Act, (EU) 2024/1309	European Data Act (Regulation), (EU) 2023/2854			Directive on combating violence against women, 2022/0066(COD)	Machinery Regulation, (EU) 2023/1230	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	Remuneration of musicians from third countries for recoredd music played in the EU	Digital euro, 2023/0212 (COD)
	European critical raw materials act (Regulation), (EU) 2024/1252	New radio spectrum policy programme (RSPP 2.0)	Interoperable Europe Act, (EU) 2024/903			Directive for combating sexual abuse and child sexual abuse material, 2024/0035(COD)	AI Act (Regulation), 2021/0106(COD)	Digital content Directive, (EU) 2019/770	Regulation on distortive foreign subsidies, (EU) 2022/2560		Regulation on combating late payment, 2023/0323(COD)
	Net Zero Industry Act, 2023/0081(COD)	Digital Networks Act	Regulation on data collection for short-term rental, (EU) 2024/1028			Digitalization of travel documents	Eco-design Regulation, 2022/0095(COD)	Directive on certain aspects concerning contracts for the sale of goods, (EU) 2019/771	Horizontal Block Exemption Regulations (HBER), (EU) 2023/1066, (EU) 2023/1067		
	EU Space Law		European Health Data Space (Regulation), 2022/0140(COD)				AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Platform Work Directive, 2021/0414(COD)		
			Harmonisation of GDPR enforcement procedures, 2023/0202(COD)					Political Advertising Regulation, (EU) 2024/900	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		

MUNI

Why was the CRA adopted?

- A constantly growing number of connected / interconnected devices
- Experience from earlier ransomware attacks that stemmed from insufficient product security – affecting the entire supply chain (WannaCry, Kaseya, Verkada, etc.)
- Insufficient or non-existent incentives to build secure hardware and software products by design, particularly for everyday devices, and no coverage by the legal framework
- The EU legal framework only addressed service providers and networks

X

- Product security is a radically different approach to cybersecurity regulation as a whole
- The same logic as ensuring the (physical) safety of products placed on the market / consumer protection

MUNI

Why the CRA?

- Some partial aspects were regulated only at the level of directives (product quality, durability over time, complaints, quality of software / digital content, etc.)
- Direct effect -> a regulation – the Cyber Resilience Act (CRA)
- Objectives:

1. **Increasing product security** – by introducing security requirements for the software and hardware parts of a product and support throughout the whole lifecycle (5 years, or the expected lifetime of the product)
2. **Ensuring security across the supply chain**
3. **A risk-based approach**
4. **Better information for users** (not only consumers) about (cyber)security

Why the CRA?

- Reducing the potential for damage and other harm caused by cyberattacks, and reducing the costs of compensating for that damage
- The main objective is to support the development of secure digital products, so that products reaching the market contain fewer vulnerabilities and manufacturers take security into account throughout the whole product lifecycle
- Raising user awareness in general, in order to create conditions in which users can take cybersecurity into account when choosing and using products with digital elements
- Increasing transparency about the properties of products with digital elements
- An obligation on manufacturers to report to ENISA every actively exploited vulnerability contained in a digital product

Scope of the CRA

1. Sets the **conditions for placing products** with digital elements on the EU market
2. Sets **rules for the design**, development and production of products with digital elements
3. Lays down requirements for **handling vulnerabilities** in products with digital elements
4. Lays down requirements for **market surveillance** and for supervisory authorities at Member State level

Relationship to other cybersecurity regulation? (overlaps with NIS 2, CSA, AI Act?)

Which products does the CRA apply to?

- **Products with digital elements**
  - **(1)** a **software or hardware product and its remote data processing solutions**, including software or hardware components placed on the market separately
  - (2) made **available on the market** (x the obligations also cover the design, development and production of such a product)
  - (3) the intended purpose or reasonably foreseeable use includes a **direct or indirect logical or physical data connection** to a device or network

X unless…

X Which products does the CRA not apply to?

- NO – purely offline products
- NO – medical devices under the MDR / motor vehicles / items certified for civil aviation / marine equipment / unmodified spare parts placed on the market before the CRA applies
- NO – products developed or modified exclusively for national security or defence purposes
- NO – products specifically designed to process classified information

- Only partly
  - **products covered by stricter or conflicting sectoral rules, where a Commission decision so provides (it sets the scope of the limitation and specifies the products and rules concerned)**
  - cloud solutions

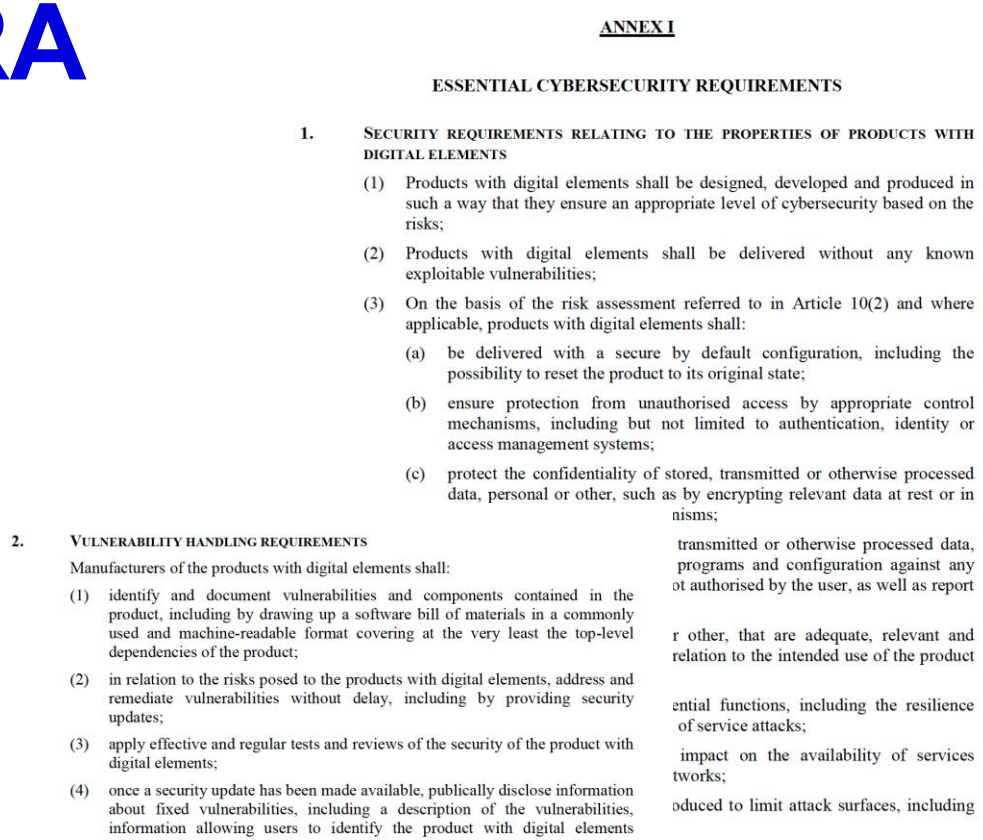
Cloud solutions?

- *R(12) Cloud solutions constitute remote data processing solutions within the meaning of this Regulation only where they meet the definition laid down in it.*
- **YES – e.g. cloud functions provided by the manufacturer of a smart home device that let the user control the device remotely.**

- **NO – e.g. websites that do not support the functionality of a product with digital elements, or cloud services for whose design and development the manufacturer of the product with digital elements is not responsible**
- cloud computing services, SaaS, PaaS, IaaS – NIS 2 applies instead (medium and large enterprises)

Obligations under the CRA

- Conditions for placing on the market:
  - ensuring compliance with the essential cybersecurity requirements
  - ensuring that vulnerabilities are handled
  - preparing the product documentation
- Demonstrating that the conditions are met:
  - self-assessment (declaration of conformity)
  - certification
  - confirmation of compliance with a relevant standard



ANNEX I

ESSENTIAL CYBERSECURITY REQUIREMENTS

1. SECURITY REQUIREMENTS RELATING TO THE PROPERTIES OF PRODUCTS WITH DIGITAL ELEMENTS

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;

(2) Products with digital elements shall be delivered without any known exploitable vulnerabilities;

(3) On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:

(a) be delivered with a secure by default configuration, including the possibility to reset the product to its original state;

(b) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;

(c) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in

nisms;

2. VULNERABILITY HANDLING REQUIREMENTS

Manufacturers of the products with digital elements shall:

(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product;

(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and information helping users to remediate the vulnerabilities;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;

(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

transmitted or otherwise processed data, programs and configuration against any ot authorised by the user, as well as report

r other, that are adequate, relevant and relation to the intended use of the product

ential functions, including the resilience of service attacks;

impact on the availability of services tworks;

oduced to limit attack surfaces, including

MUNI LAW

Categories of products & the market?

Where the requirements are met – CE marking

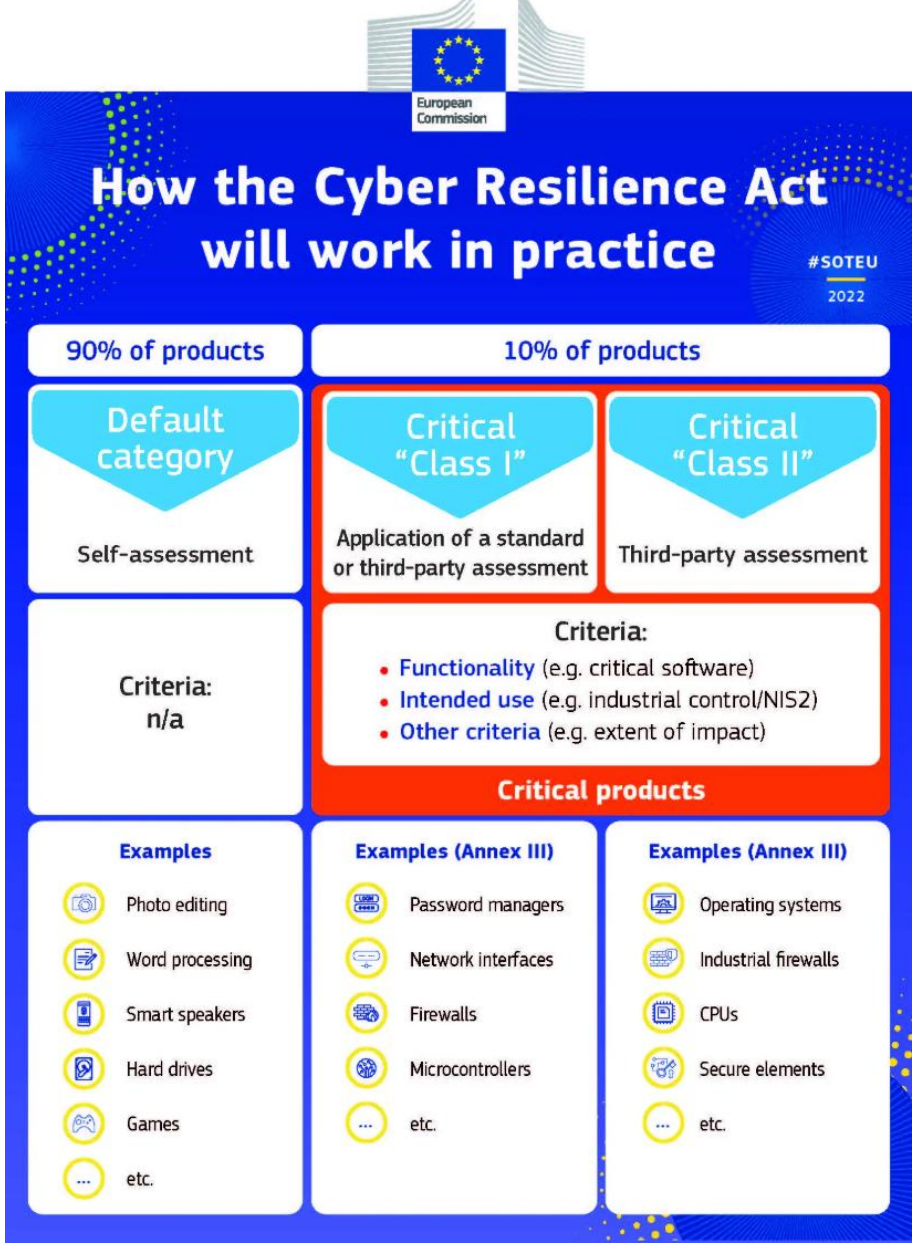
1. products with digital elements – internal control procedure

+ special regime:

2. important products with digital elements:
   - Class I: a harmonised standard, or third-party conformity assessment plus control mechanisms ensuring production control
   - Class II: third-party assessment of the complete security system

---

3. critical products with digital elements
   - CSA or a European cybersecurity certificate



MUNI LAW

Who bears the obligations?

- Manufacturer (Art. 3(13))
  - develops or manufactures a PDE, or has it designed, developed or manufactured, and markets it under its own name or trademark – for payment, for other monetisation, or free of charge
- Importer (Art. 3(16)) and distributor (Art. 3(17))
  - importer: established in the Union, places on the market a PDE bearing the name or trademark of a person established outside the Union
  - distributor: makes a PDE available on the Union market without affecting its properties
  - in a number of situations they take over the full set of manufacturer obligations (Arts. 21–22)
- Open-source software steward (Art. 3(14), Art. 24) – a new category
  - a legal person other than a manufacturer that systematically and on a sustained basis supports the development of specific PDEs qualifying as free and open-source software intended for commercial activities, and ensures their viability
  - typically foundations, industry consortia, entities publishing F/OSS in a business context
  - light-touch regime: a documented cybersecurity policy, cooperation with market surveillance authorities, reporting duties under Art. 14 to the extent they are involved
  - no CE marking, no conformity assessment, no technical documentation – and no administrative fines (Art. 64(10)(b))

Essential requirements under the CRA

- Place the product on the market without known exploitable vulnerabilities and with a secure-by-default configuration
- Set security updates to be installed automatically
- Document, identify and test the vulnerabilities of the product
- Minimise the processing of (personal) data
- Address and remediate discovered vulnerabilities without delay and publish information about fixed vulnerabilities
- Put in place a CVD policy and provide a contact point for reporting vulnerabilities
- Inform users about the measures or steps they have to take if a security problem occurs

Vulnerability handling (Annex I, Part II)

- Notification of vulnerabilities and incidents (CSIRT, ENISA)
- Documentation of vulnerabilities and components (SBOM)
- Remediation of vulnerabilities (risk-based; separate updates)
- Regular and effective security testing and review of the PDE
- Publication of information on updates and vulnerabilities
- A coordinated vulnerability disclosure policy
- Requirements on sharing vulnerability information
- Mechanisms for the secure distribution of updates
- Updates: without delay, free of charge, with advisories

Technical documentation

- Drawn up before placing on the market; part of the Declaration of Conformity (DoC)
- Content:
  - description of the product with digital elements (purpose, version, architecture, user documentation)
  - description of the design and architecture of the product with digital elements
  - description of the vulnerability handling mechanism
  - risk analysis
  - determination of the support period (usually 5 years)
  - list of the relevant standards
  - description of the technical measures applied
  - reports from testing and from vulnerability handling
  - Declaration of Conformity
  - SBOM

Information and instructions for users

- Identification of and contact details for the manufacturer
- SPoC for vulnerabilities (Single Point of Contact)
- Identification of the product with digital elements
- The intended purpose of the product with digital elements
- Identification of misuse risks with cybersecurity impacts
- Reference to the Declaration of Conformity
- Technical support contact
- Information about the support period
- User instructions (operation, configuration, security implications, updates, integration, decommissioning)

Conformity assessment

- Carried out in line with Decision No 768/2008/EC on a common framework for the marketing of products
- 4 routes:
  1. **Self-assessment (Module A)** – the manufacturer assesses conformity and draws up the documentation itself (it may mandate someone else to do so)
  2. **Third-party assessment (Module B)** – an independent body (CAB) carries out the assessment on the basis of the technical documentation and testing (type examination), combined with conformity to type (Module C) – the manufacturer itself checks that the PDE conforms to the type certificate under Module B
  3. **Quality system (Module H)** – a CAB assesses the quality system put in place by the manufacturer, which then assesses the PDE within its own quality management system (the CAB carries out surveillance)
  4. **Certification under the CSA –** EUCC etc.

Conformity assessment by type of PDE

Default	Important Class I	Important Class II	Critical

• **Self-assessment**
• Conformity may be assessed under:
  • Module A
  • Module B+C
  • Module H
	• **Use of a harmonised standard or specification**
	• Declaration of conformity with a harmonised standard, or Module B+C or H (where no standard exists or it is not sufficient)
		• **Third-party assessment**
		• Under Module B+C or H
			• **Certification under the CSA**
			• EUCC
			• Conditional on a presumption of conformity, otherwise as Important Class II

Harmonised European standards

- Standards developed by the European standardisation organisations:
  - **CEN (general standards)**
  - **CENELEC (electrotechnology)**
  - **ETSI (telecommunications, ICT)**
- Issued on the basis of a mandate from the European Commission
- Applying hENs gives the manufacturer a "presumption of conformity" = the product is presumed to meet the CRA requirements
- Not published yet – mandated by the Commission, expected towards the end of 2026
- They will draw on existing standards; the model is the IEC 62443 family (cybersecurity of industrial control systems)

Substantial modification of a product

- Products placed on the market before 11 December 2027 are caught only if they undergo a substantial modification (Art. 69(2))

- If the product is modified, the original assessment or certification may no longer match it

?Substantial modification?

- A substantial modification requires a new assessment or certification
- **"a change to the product with digital elements following its placing on the market, which affects the compliance of the product with digital elements with the essential requirements set out in Part I of Annex I, or which results in a modification to the intended purpose for which the product with digital elements has been assessed"**
- *"a software update modifies the original intended functions, type or performance of the product and these changes were not foreseen in the initial risk assessment, or the nature of the hazard has changed, or the level of risk has increased as a result of the software update"*

Information and reporting duties

Towards consumers:

- CE marking
- Declaration of conformity
- Information and instructions about the product, supplied electronically or in physical form, which must be clear, understandable and intelligible (details in Annex II to the CRA)

Towards supervisory authorities:

- Where needed, all information allowing the authority to verify that an appropriate conformity assessment was carried out
- An actively exploited vulnerability must be reported to ENISA within 24 hours – a vulnerability for which there is reliable evidence of exploitation by a malicious actor, i.e. without the permission of the system owner; the same applies to severe incidents having an impact on the security of the product with digital elements
- A single reporting platform (ENISA)
- Reporting on a voluntary basis is also possible (not only by the manufacturer, but by anyone X NIS 2)

Market surveillance and enforcement

- New authorities may have to be set up
- Cooperation between Member States is possible (CSoIA?) – EU-CyCLONe

- Fines of up to EUR 15 million (or 2.5% of worldwide turnover for the preceding year, whichever is higher) for Annex I and Arts. 13–14;
- EUR 10 million / 2% and EUR 5 million / 1% for other breaches – open-source software stewards are exempt from administrative fines

How to start preparing?

Get leadership on board

- Brief management on the impacts of the CRA
- Start planning budget, capacity and responsibilities

Run an initial impact analysis

- Which of our products fall under the CRA?
- What roles do we play in the supply chain (manufacturer, importer, etc.)?

Map the CRA requirements against the current state

- Assess how well you cover:
  - Technical requirements (Annex I)
  - The vulnerability handling process (Annex I, Part II)
  - Identify the gaps (a GAP analysis)

Introduce an SDL process (Secure Development Lifecycle)

- Following EN IEC 62443-4-1
- Focus on:
  - Secure design and development
  - Testing
  - Updates and vulnerabilities

Verify the technical requirements for the products

- Compare against EN IEC 62443-4-2
- Prepare mechanisms for:
  - Updates
  - Logging
  - Data erasure
  - Access control

Start building the technical documentation

- Create a template for the technical file
- Start recording the SBOM, security decisions and tests

Train your people

- Developers, product managers, compliance
- Explain what the CRA means for their day-to-day work

MUNI

Certification – overlaps?

- CRA / CSA
  - CRA is mandatory / CSA is voluntary
  - CSA – it will depend on the certification schemes, which may also cover services and processes
  - CSA – only a few schemes are in preparation (EUCC, 5G?, cloud?, smart metering, …)
  - CRA / CSA overlaps – potentially a duplicated system of two certification regimes

- CRA / AI Act
  - The AI Act also introduces a potential certification route (self-assessment, documentation X CSA)

Timeline

- The CRA (Reg. (EU) 2024/2847) applies in stages:
  - 11 June 2026: notification of the conformity assessment bodies
  - 11 September 2026: vulnerability and incident reporting + the single reporting platform
  - 11 December 2027: full applicability (earlier products only on a substantial modification)

CRA and F/OSS – the earlier (heavily criticised) version

Recital (10) CRA (Commission proposal of 15 September 2022 – the version that prompted the open letter from Eclipse, OSI, Linux Foundation Europe and others)

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.

CRA and F/OSS – the wording that made it through

Recital (17) (text adopted on 12 March 2024; now Recitals (18)–(20) of Regulation (EU) 2024/2847)

Software and data that are openly shared and where users can freely access, use, modify and redistribute them or modified versions thereof, can contribute to research and innovation in the market. To foster the development and deployment of free and open-source software, in particular by microenterprises and small and medium-sized enterprises, including start-ups, individuals, not-for-profit organisations, and academic research organisations, the application of this Regulation to products with digital elements qualifying as free and open-source software supplied for distribution or use in the course of a commercial activity should take into account the nature of the different development models of software distributed and developed under free and open-source software licences.

…impacts (AKA what does not fall under the CRA)

- the provision of **free and open-source software products that are not monetised** by their manufacturers is not considered a commercial activity
- the **mere fact that an open-source software product receives financial support from manufacturers**, or that manufacturers contribute to its development, should not in itself determine that the activity is commercial
- the CRA does not apply to natural or legal persons who **contribute source code to free and open-source products that are not under their responsibility**
- the development of F/OSS products by not-for-profit organisations is not a commercial activity, provided all earnings after cost go to not-for-profit objectives
- the sole act of hosting products on open repositories, including package managers or collaboration platforms, is not making a product available on the market

- / commercial products are a different situation entirely / most F/OSS projects stay outside the CRA

MUNI

CRA and F/OSS – three tiers of exposure

- 1) Outside the scope – no obligations
  - individuals and genuinely non-commercial projects; contributors to a product that is not under their responsibility (Recital 18)
  - e.g. a hobby project on GitHub, a university prototype, a patch sent upstream to curl
- 2) Open-source software steward – light-touch regime (Art. 24)
  - foundations and industry consortia (Eclipse, Apache, OpenSSL Foundation), or a company publishing a community edition next to a paid one
  - cybersecurity policy + cooperation with authorities – no CE marking, no conformity assessment, no fines
- 3) Manufacturer – the full regime (Art. 13, Annex I)
  - anyone who monetises the product, or markets a product built on F/OSS under their own name
  - e.g. Red Hat Enterprise Linux, an IoT device running Linux, a paid enterprise edition of an open-core product
  - Annex I, documentation, conformity assessment, CE marking, 24h reporting, due diligence on components (Art. 13(5))

Types of F/OSS projects and their tier

There is no single F/OSS development model

- Hobby project, academic experiment → outside the scope
  - a weekend tool on GitHub, a PhD prototype; nobody is monetising it
- Volunteer-maintained project that ends up inside commercial products → outside the scope
  - libraries and tools such as curl, OpenSSH, zlib, sqlite; contributors may be paid by companies
  - sponsored CI, hosting or donated hardware do not make it commercial – the integrator downstream is the manufacturer
- Maintained on a commercial basis but distributed as F/OSS → usually a steward
  - foundation + separate paid support and certification; e.g. OpenSSL (Foundation + Corporation)
- F/OSS integrators → manufacturer
  - a commercial product assembled from F/OSS components: Red Hat, Canonical, SUSE, cloud providers, IoT vendors
- Special cases
  - the Linux kernel – its own vulnerability-handling model; distributions, not the kernel itself, are placed on the market

Where is the line? Five cases

The test: is the software itself monetised – not the only condition

- A paid developer contributes to another project in their free time → outside the scope
  - the CRA follows responsibility for the product, not who pays the person (Recital 18)
- A company funds a foundation → outside the scope
  - money flowing in does not make the activity commercial (Recital 18), selling the product does
- A vendor sells a device running F/OSS → manufacturer of the device
  - the device is placed on the market; the upstream project it builds on is not
- A foundation sustains a library that companies build products on → steward (Art. 24)
  - light-touch duties only: security policy, cooperation, reporting – no CE marking
- Open core: free community edition + paid enterprise edition → both at once
  - steward for the community edition, manufacturer for the paid one

What do you actually have to do?

1. Outside the scope → the CRA asks nothing of you
   - but your downstream integrators will: an SBOM, a security policy, a contact for reports
   - good practice already pays off: OpenSSF Scorecard, Best Practices Badge, a SECURITY.md file

2. Steward (Art. 24) → one core duty: a documented cybersecurity policy
   - plus cooperation with market surveillance authorities and reporting under Art. 14
   - no CE marking, no conformity assessment, no technical documentation, no fines

3. Manufacturer (Art. 13) → the full set of duties
   - reporting from 11 September 2026; CE marking and conformity assessment from 11 December 2027
   - due diligence on every F/OSS component you ship (Art. 13(5))

4. Still unsettled
   - an internal fork that later gets published; a volunteer selling support for their own project
   - harmonised standards, the ENISA platform and the Art. 25 attestation schemes do not exist yet

MUNI

Thank you for your attention!

loutocky@muni.cz