

**M U N I**

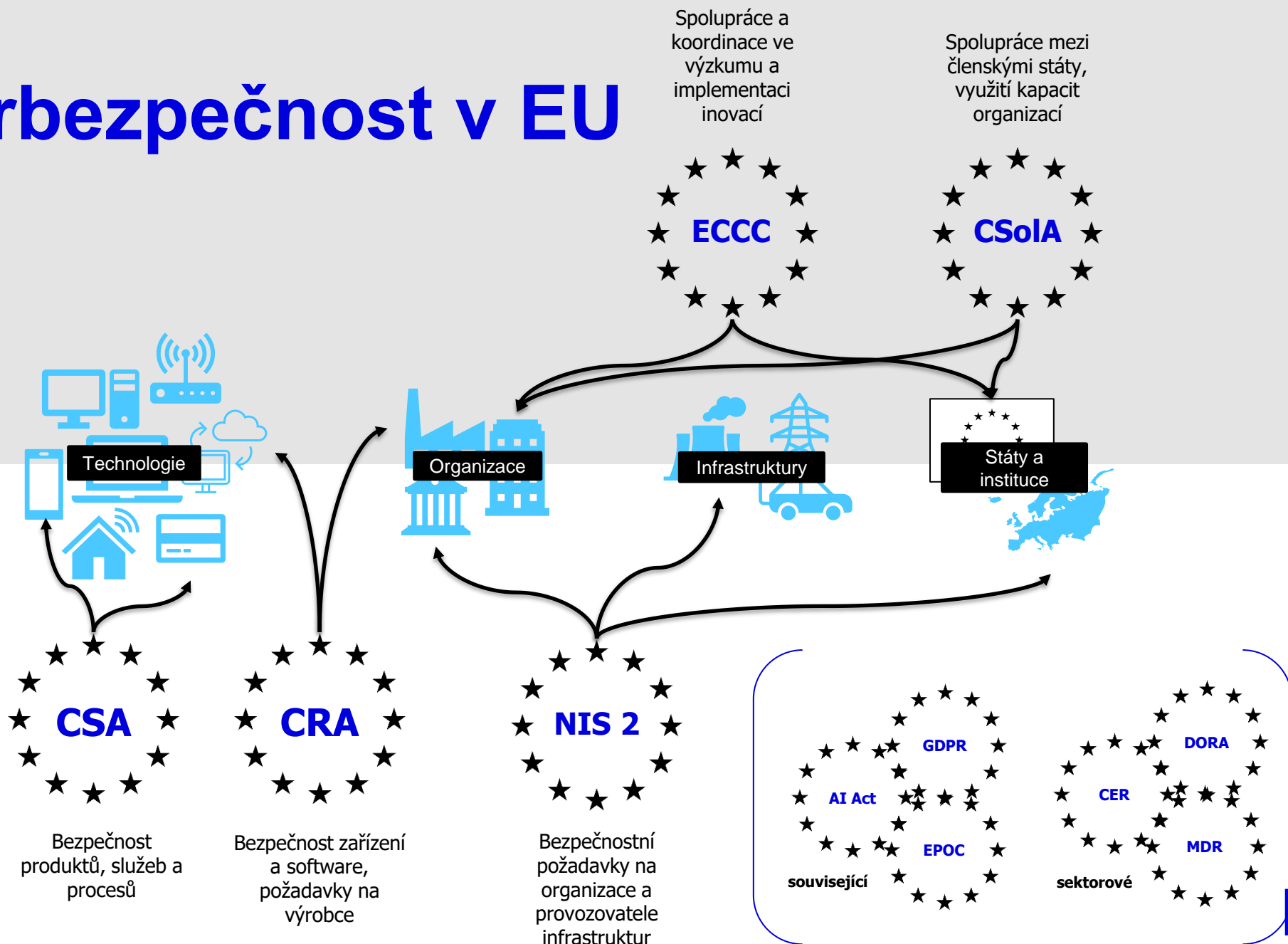
# **Regulatorní prostředí v oblasti kyberbezpečnosti aneb co vše (...) je relevantní?**

Pavel Loutocký

# Celkový kontext datové legislativy!!!

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) 1983/13	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) 2002/223, 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) 2009/18, 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 a 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, 2023/0016(CNS)	Regulation on Joint Undertakings under Horizon Europe, (EU) 2021/2085, 2022/0033(NLE)	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 protection of topographical data, (EU) 2016/917	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
Decision on a path to the Digital Decade, (EU) 2022/2481	Roaming Regulation, (EU) 2022/612	Open Data Directive (PSI), (EU) 2019/1024	Regulation on the free flow of non-personal data, (EU) 2018/1807	Design Directive, 2022/0392(COD)	Information Security Regulation, 2022/0684(COD)	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) 2019/1160	Satellite and Cable II Directive, (EU) 2019/789	Crypto-assets Regulation (MiCA), (EU) 2023/1114
European Chips Act (Regulation), (EU) 2023/1781	Union Secure Connectivity Programme, (EU) 2023/588	Data Governance Act (DSA Regulation), (EU) 2022/868	Standard essential patents, 2023/0128(COD)	Cyber Resilience Act, 2022/0272(COD)	Evidence Regulation, (EU) 2023/1543	Regulation for a Single Digital Gateway, (EU) 2018/1724	e-invoicing Directive, (EU) 2014/65	Single Market Programme, (EU) 2021/690	Copyright Directive, (EU) 2019/790	Financial Data Access Regulation, 2023/0205(COD)	
Establishing the Strategic Technologies for Europe Platform (STEP), (EU) 2023/295	Gigabit Infrastructure Act, (EU) 2024/1309	European Data Act (Regulation), (EU) 2023/2854	Standard essential patents, 2023/0133(COD)	Cyber Solidarity 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) 2022/729	European Media Freedom Act, (EU) 2024/1083	Payment Services Regulation, 2023/0210(COD)	
European critical raw materials act (Regulation), (EU) 2024/1252	<b>New radio spectrum policy programme (RSPP 2.0)</b>	Interoperable Europe Act, (EU) 2024/903	Standard essential patents, 2023/0128(COD)	Cyber Resilience Act, 2022/0272(COD)	Directive on combating violence against women, 2022/0666(COD)	Machinery Regulation, (EU) 2023/1230	Geo-Blocking Regulation, (EU) 2018/302	Digital Market Act (DMA Regulation), (EU) 2022/1925	<b>Remuneration of musicians from third countries for recorded music played in the EU</b>	Digital euro, 2023/0212(COD)	
Net Zero Industry Act, 2023/0081(COD)	<b>Digital Networks Act</b>	Regulation on data collection for short-term rental, (EU) 2024/1028	Standard essential patents, 2023/0128(COD)	Cyber Resilience Act, 2022/0272(COD)	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)		
<b>EU Space Law</b>		European Health Data Space (Regulation), 2022/0140(COD)	Standard essential patents, 2023/0128(COD)	Cyber Resilience Act, 2022/0272(COD)	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	Platform Work Directive, 2021/0414(COD)		
		Harmonisation of GDPR enforcement procedures, 2023/0202(COD)	Standard essential patents, 2023/0128(COD)	Cyber Resilience Act, 2022/0272(COD)		AI Liability Directive, 2022/0303(COD)	Digital Services Act (DSA Regulation), (EU) 2022/2065	Political Advertising Regulation, (EU) 2024/900	Single Market Emergency Instrument (SMEI), 2022/0278(COD)		

# Kyberbezpečnost v EU



Spolupráce

Regulace

## Právo ČR

- Zahrnuje kyberkriminalitu, kyberbezpečnost, kyberobranu
- Ochrana prostředí v ČR
- Zaměření na významné a kritické infrastruktury
- Implementuje právo EU

## Právo EU

- Základ v ochraně prostředí jednotného digitálního trhu
- Oblastí kyberkriminality a kyberobrany jen omezeně řešené
- Stále komplexnější konglomerát obecné a sektorové regulace
- Harmonizace a vliv na podobu právní úpravy členských států

# Strategie kyberbezpečnosti v EU

## Odolnost, technologií suverenita a vedoucí role

- Odolná infrastruktura a kritické služby
- Budování evropského kybernetického štítu
- Ultra-bezpečná komunikační infrastruktura
- Zabezpečení nové generace mobilních sítí
- Internet bezpečných věcí
- Vyšší globální bezpečnost internetu
- Posílení postavení v technologickém dodavatelském řetězci
- Cyber-skilled pracovní síla

## Budování operativních kapacit pro prevenci, odvracení a reakci

- Joint Cyber Unit
- Boj s kyberkriminalitou
- EU toolbox pro kyberdiplomacii
- Posilování kapacit kybernetické obrany

## Podpora globálního a otevřeného kyberprostoru

- Vedoucí role v budování standardů, norem a rámců v kyberprostoru
- Spolupráce s partnery a multi-stakeholder komunitami
- Posilování globálních kapacit pro zvýšení globální odolnosti

# MUNI

## NIS 2

Směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti

# Směrnice NIS2

---

Širší působnost

---

Úprava vztahu k sektorově specifické regulaci

---

Úprava jurisdikce

---

Posílení managementu rizik a incidentů

---

Požadavky na řízení bezpečnosti

---

Vazba na certifikace

---

Vyšší sankce

# Regulované sektory

– Nově není určováno ze strany NS – jen omezení velikosti (mid-caps, large)

## Původně regulované směrnici NIS

- Infrastruktura bankovního a finančního trhu
- Digitální infrastruktura
- Poskytovatelé digitálních služeb
- Energetika
- Zdravotnictví
- Doprava
- Dodávka vody

## Rozšířená působnost NIS2

- *Digitální služby (sítě a datové služby)*
- *Potravinářství*
- *Výrobci vybraných kritických produktů (léčiva, chemické výrobky, zdravotnické prostředky)*
- *Poštovní a kurýrní služby*
- *Orgány veřejné moci*
- *Poskytovatelé veřejných síťových a komunikačních služeb*
- *Poskytovatelé veřejně dostupných služeb elektronických komunikací*
- *Vesmír*
- *Zpracování odpadu a odpadních vod*
- *Výzkumné instituce*



# Sektorově specifická regulace

- EU předpisy by měly být v souladu s NIS2
- *Lex specialis derogat legi generali*
- V aspektech neupravených v sektorově specifické regulaci budou dále účinná ustanovení NIS2
- Budou guidelines
  
- Nově vazba na poskytování služeb, nikoliv sídlo (podobné GDPR)
- Obecně: v místě sídla, případně místo sídla designovaného zástupce

# Management rizik a incidentů

- Harmonizace úprav členských států
- Požadavek na vhodné a proporciální technická, operační a organizační opatření za účelem minimalizace rizik a reakce na hrozby
  - Analytické výstupy (analýza rizik, analýza hrozeb)
  - Opatření a policie (management rizik a hrozeb, incident handling, řízení dodavatelských řetězců, ochrana business continuity, apod.)
  - Technická opatření (šifrování, zálohování, autentizace a autorizace apod.)
- Reportování incidentů s významným dopadem na poskytování služby – stupňovaný přístup:
  - Notifikace
  - Na výzvu průběžná zpráva
  - Finální zpráva ne později než měsíc od incidentu
- Informování uživatelů služby o významných hrozbách a jejich potenciálních dopadech

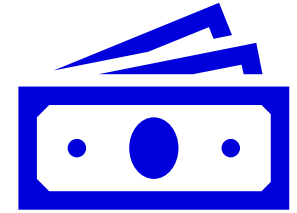
# Bezpečnostní opatření

Analýza rizik a systém informační bezpečnosti
Zvládání incidentů
Nástroje zajištění kontinuity provozu (zálohy, disaster-recovery, krizový management)
Bezpečnost dodavatelského řetězce
Bezpečnost vývoje, údržby a akvizic
Zpracování a oznamování zranitelností
Postupy pro hodnocení opatření k pokrytí kyberbezpečnostních rizik
Školení a kybernetická hygiena
Využití kryptografických prostředků a šifrování
Bezpečnost lidských zdrojů, řízení přístupů a aktiv
Zabezpečení autentizace

# Řízení bezpečnosti

- Organizace musejí zavázat svoje řídicí struktury aby:
  - zavedly systém řízení bezpečnosti informací a systémů,
  - zavedly mechanismy pro dohlížení nad implementací opatření,
  - zavedly mechanismy pro zvyšování kvalifikace.
- Byla rovněž zavedena odpovědnost managementu za neplnění povinností vyplývajících z NIS2
  
- + certifikace

# Sankce



- Ex-ante dozor v případě základních služeb, ex-post v případě významných služeb
- Správní pokuty budou ukládat národní dozorové orgány
- Možnost uvalení sankce v podobě znemožnění výkonu manažerské funkce v rámci regulovaných subjektů

# MUNI

## CSA

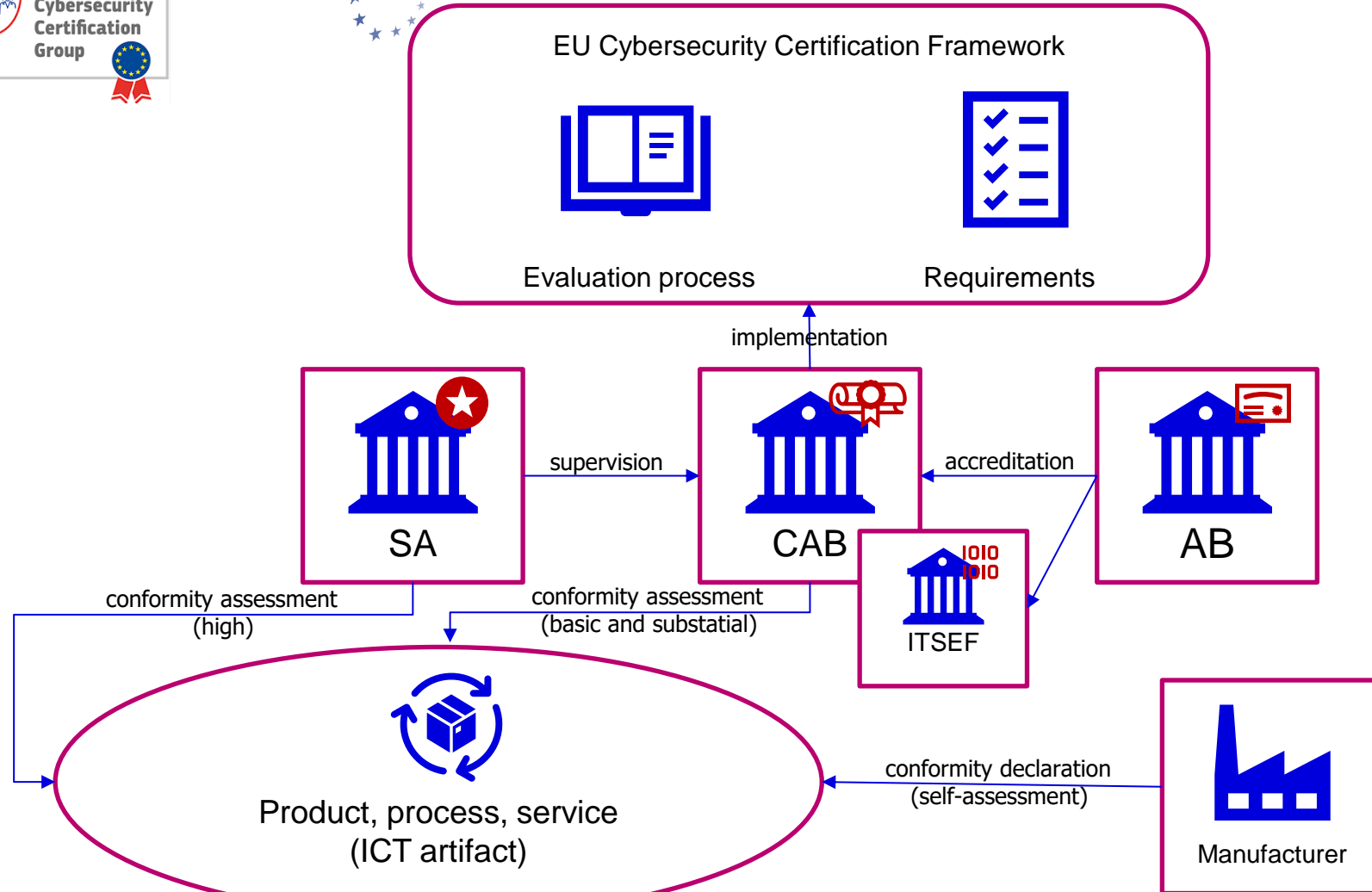
Akt o kybernetické bezpečnosti (nařízení)

# Akt o kybernetické bezpečnosti



- Poskytuje nezávislost a tvalý mandát agentuře ENISA
- Zavádí mechanismus kyberbezpečnostních certifikací
- V současné době se zpracovávají:
  - EUCC – EU Common Criteria
  - EUCS – EU Cloud scheme
  - EU 5G – EU 5G scheme
- Role poradních orgánů ECCG a SCCG
- EURWP – pracovní program – plánování vývoje schémat

# Rámc pro certifikace





# Certifikace

Úroveň	Co se testuje?	Cíle	Minimální posouzení
Vysoká	Compliance a robustnost	Zajištění suverenity, odolnosti klíčových infrastruktur, ochrana dat a informačních systémů	Pentesting State-of-the-art útoky
Významná	Compliance a robustnost	Prevence škálovatelných útoků na středně a vysoce významné infrastruktury a systémy	Absence známých zranitelností Testování compliance
Základní	Compliance	Prevence masivních útoků na low-cost zařízení a služby	Revize dokumentace Self-assessment

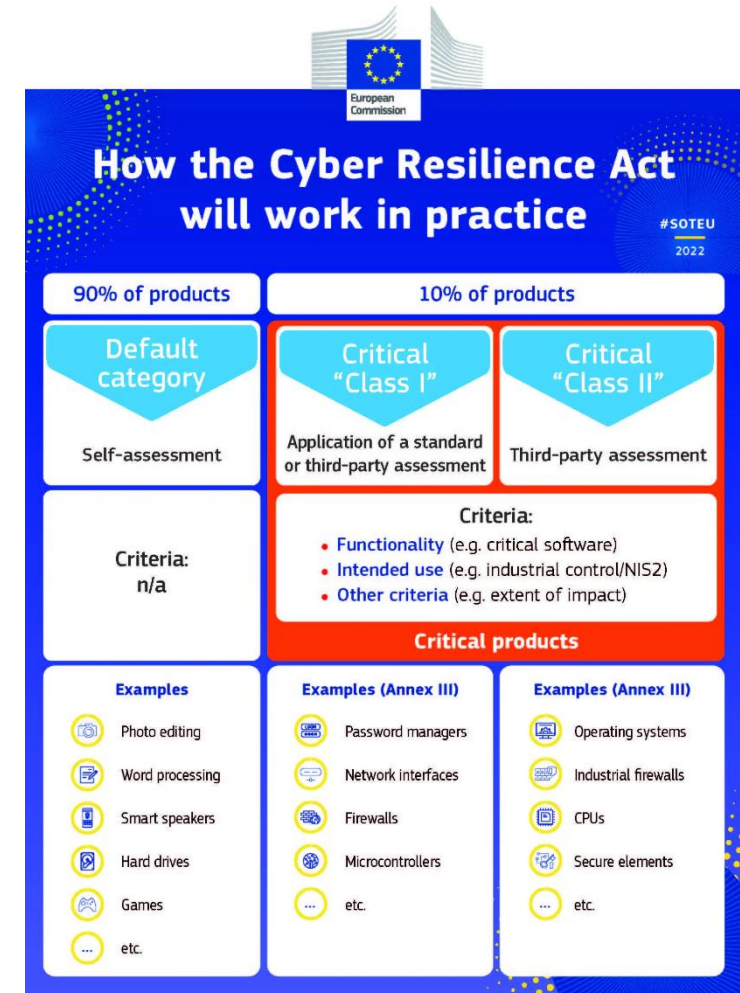
# MUNI

## CRA

Akt o kybernetické odolnosti  
(nařízení)

# Akt o kybernetické odolnosti

- Nastavuje podmínky pro uvádění produktů s digitálním elementem na EU trh
- Nastavuje pravidla pro design, vývoj a produkci produktů s digitálním elementem
- Stanovuje požadavky na nakládání se zranitelnostmi produktů s digitálním elementem
- Produkty s digitálním elementem (jakýkoliv software či hardware umožňující vzdálené zpracování dat):
  - Všeobecné
  - Základní (třída I a II)
- Dohledové orgány na úrovni členských států
- Sankce až 15 mil EUR (2,5% celosvětového obratu)



# Povinnosti podle CRA

- Podmínky zavádění na trh:
  - Povinnost zajištění souladu se základními kyberbezpečnostními požadavky
  - Povinnost zajištění zpracování zranitelností
  - Pořízení dokumentace k produktu
- Zajištění souladu s podmínkami:
  - Self-assessment (declaration of conformity)
  - Certifikace
  - Potvrzení souladu s relevantním standardem

## 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

#### 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;

duced to limit attack surfaces, including

**MUNI**

# **Návrh zákona o kybernetické bezpečnosti**

- Nově jediný typ povinné osoby – tzv „poskytovatel regulované služby“ (jiný přístup než v NIS 2)
- Poskytovatelem regulované služby je kdokoliv, kdo poskytuje alespoň jednu regulovanou službu (dle § 4 obdobně jako NIS 2)
- Poskytovatel regulované služby:
  - režim vyšších povinností (+- 1000 subjektů)
  - režim nižších povinností (+- 5000 subjektů)
- + Strategicky významná služba (§ 25 a násl)

- V režimu **vyšších povinností** je poskytovatel regulované služby, který z důvodu své velikosti, počtu uživatelů, geografického rozšíření služby, dopadu na fungování odvětví nebo jiného poskytovatele regulované služby nebo rizikovosti provozu, je značně ekonomicky, společensky nebo bezpečnostně významný pro Českou republiku.
- V režimu **nižších povinností** je poskytovatel regulované služby, který není v režimu vyšších povinností podle věty první.

# Prověřování dodavatelského řetězce NÚKIB

- Podmínky pro strategicky významnou službu určenou NÚKIBem v rámci poskytovatelů regulovaných služeb
- NÚKIB posuzuje napojení na dodavatele a možnost ohrožení
  - *„Úřad vydá opatření obecné povahy, kterým stanoví poskytovatelům strategicky významných služeb podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li na základě vyhodnocení rizikivosti dodavatele významné ohrožení bezpečnosti České republiky nebo vnitřního pořádku.“ (§ 29)*
  - X výjimky (§ 30) – například ohrožení poskytování strategické služby



# Aktuální stav

V současné verzi došlo k úpravě definic, vhodnějším stanovení zmocnění pro vydání vyhlášek k zákonu, další zjednodušení procesu samoidentifikace a registrace regulované služby, struktura ale zachována

[Aktuální info](#) – návrh zákona schválen vládou, jde do legislativního procesu

**Návrh Zákona o kybernetické bezpečnosti doporučen ke schválení!**

Předseda Legislativní rady vlády svým stanoviskem doporučil vládě návrh zákona o kybernetické bezpečnosti ke schválení.

#nZKB

**Předložili jsme Legislativní radě vlády doplněný návrh Zákona o kybernetické bezpečnosti.**

Cílem nového zákona je především posílit kybernetickou bezpečnost České republiky. Návrh přináší i nové procesy a nástroje a zároveň zjednodušuje a zpřehledňuje právní úpravu.

**I U N I**

11:35 dop. · 29. 5. 2024

**M U N I**

**Sector specific:**

**GDPR**

**AI ACT**

**...**

# Ochrana osobních údajů

Chceme chránit osobní údaje?

profiling / surveillance / [TikTok](#) / [Google](#) / Social Credit System

# Ochrana osobních údajů

- NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (**GDPR**)
- Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů

# Ochrana osobních údajů

- Čl. 4 odst. 1 „osobními údaji (se rozumí) veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby“
  - Přímá v. nepřímá identifikace
  - Kontext!

# Zpracování osobních údajů

## — Čl. 4 odst. 2

- jakákoliv operace nebo soubor operací s osobními údaji
- shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení

# Zpracovávání - zásady

- Platí pro kohokoli, kdo zpracovává (správce, zpracovatel)
  - Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem
  - Zásada limitace účelem
  - Zásada minimalizace údajů (nezbytný rozsah)
  - Zásada přesnosti
  - Zásada omezení uložení (souvisí s minimalizací; právo být zapomenut)
  - Zásada integrity a důvěrnosti
  - Zásada odpovědnosti

# Zákonnost zpracování – právní tituly (čl. 6 odst. 1 GDPR)

- a) Souhlas se zpracováním
- b) Zpracování nezbytné pro plnění smlouvy – **e.g. ehop**
- c) Zpracování nezbytné pro dodržení právní povinnosti správce – **zaměstnavatel předává údaje úřadu práce**
- d) Ochrana životně důležitých zájmů subjektu údajů (souhlas bez zbytečného odkladu) – **zásah doktora**
- e) Zpracování nezbytné pro plnění úkolu ve veřejném zájmu, nebo při výkonu veřejné moci, kterým je pověřen správce – **veřejná bezpečnost**
- f) Nezbytnost zpracování pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby (test proporcionality) – **monitorování sítě, CCTV**



# Práva subjektu údajů (Čl. 13-23)

- Právo být informován o zpracování osobních údajů
  - Čl. 13 (když pochází údaje přímo od subjektu)
  - Čl. 14 (když jsou údaje sesbírané jinde)
- Právo na přístup k údajům (čl. 15)
- Právo na opravu (čl. 16)
- Právo na výmaz („právo být zapomenut“) (čl. 17)
- Právo na omezení zpracování (čl. 18)
- Právo na přenositelnost údajů (čl. 20)
- Právo vznést námitku (čl. 21)
  - Když zpracování z důvodu: oprávněného zájmu NEBO plnění úkolu ve veřejném zájmu NEBO přímý marketing
- Právo na ochranu před automatizovaným individuálním rozhodováním, včetně profilování (čl. 22)

# AI Act

- [Nařízení Evropského parlamentu a Rady \(EU\) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení \(ES\) č. 300/2008, \(EU\) č. 167/2013, \(EU\) č. 168/2013, \(EU\) 2018/858, \(EU\) 2018/1139 a \(EU\) 2019/2144 a směrnice 2014/90/EU, \(EU\) 2016/797 a \(EU\) 2020/1828 \(akt o umělé inteligenci\)](#)
- Důvěra v AI (omezení black box)
- Rozčlenění povinností dle charakteru AI a úrovně automatizace
- [Evropský přístup k umělé inteligenci](#)
- [EU AI Act Compliance Checker](#)

**MUNI**

**Díky za pozornost**

[loutocky@muni.cz](mailto:loutocky@muni.cz)