\ 5.2.2025
\ Praha

Kybernetická bezpečnost v aktuální legislativě EU

\ JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.

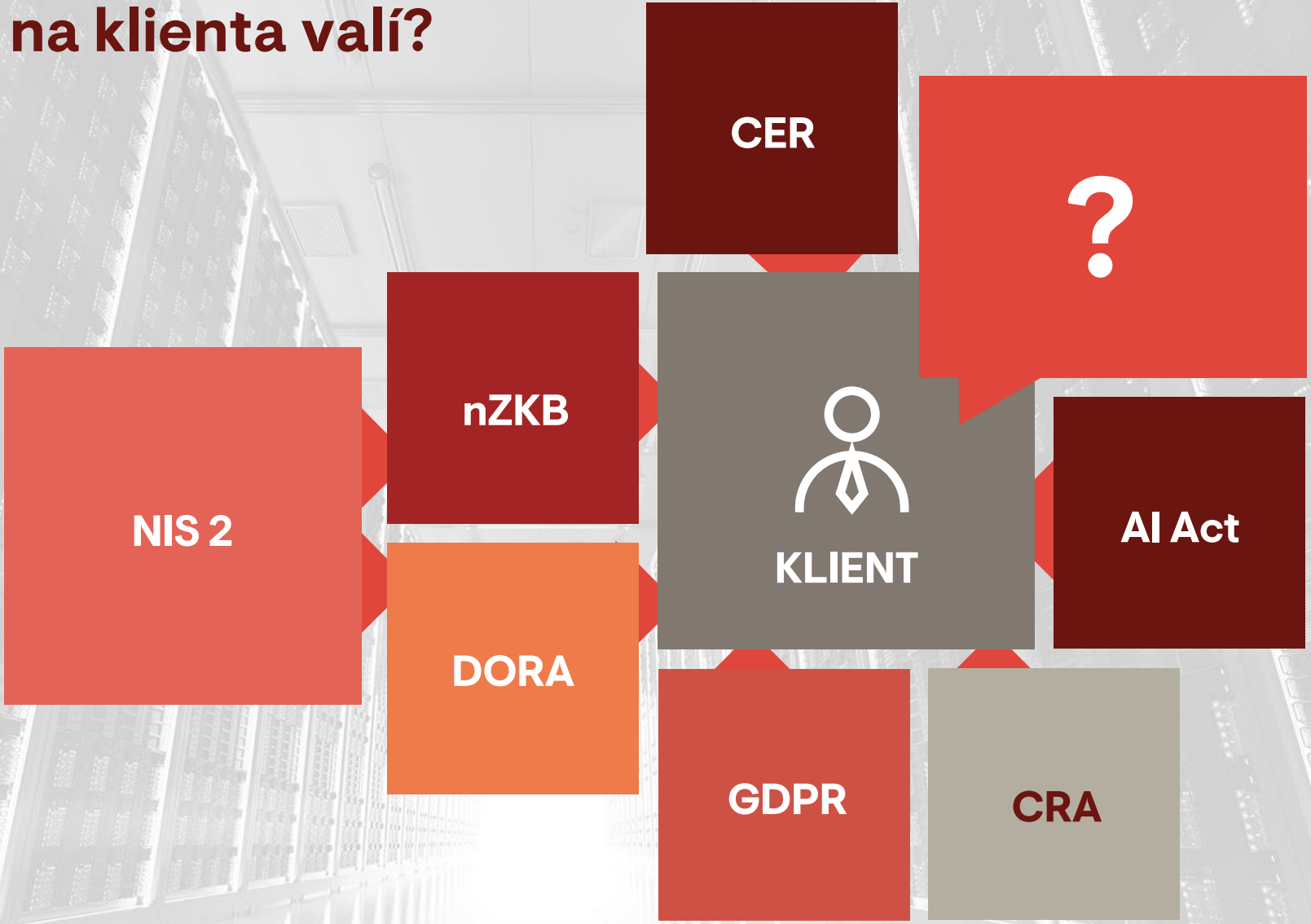
PORTOS
Strategic
Legal Advisory

AFCEA

OBSAH

PORTOS

\ 01 Co vše se na klienta valí?



\ 02 Implementace NIS 2

Listopad 2022

návrh Směrnice NIS 2 schválen Evropským Parlamentem

Prosinec 2022

publikace Směrnice NIS 2 v Úředním věstníku EU

16. října 2024

lhůta pro implementaci Směrnice NIS 2 do českého právního řádu

01 02 03 2022 04 05 2025

Prosince 2022

návrh Směrnice NIS 2 schválen Radou

Leden 2023

počátek běhu transpoziční lhůty Směrnice NIS 2

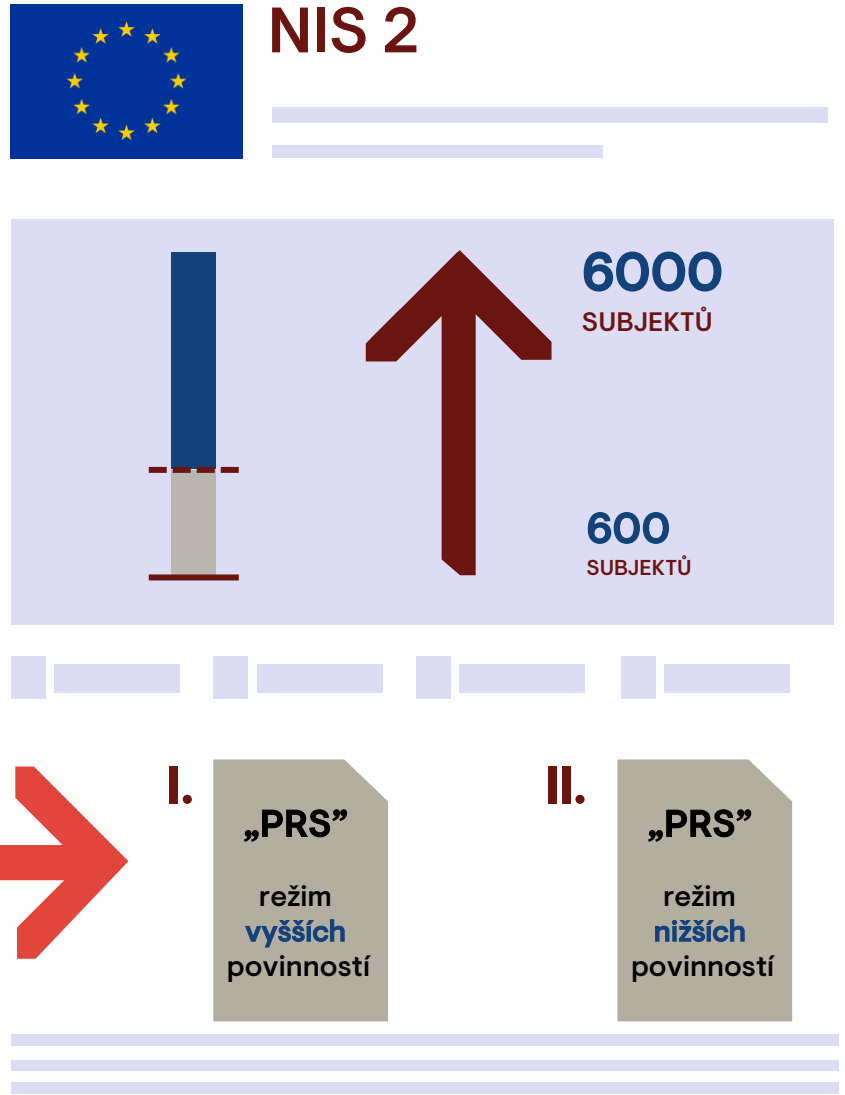
2025

Předpokládaný začátek účinnosti Nového zákonu o kybernetické bezpečnosti

\ 03 Nejdůležitější principy NIS 2

Rozšiřuje oblast působnosti regulace

- **doplňuje nová odvětví** podle jejich významu pro hospodářství a společnost,
- **zavádí jasný limit** pro velikost
- do oblasti působnosti směrnice budou zahrnuty všechny střední a velké organizace **ve vybraných odvětvích**
- zároveň se členským státům ponechává určitá flexibilita, pokud jde o **identifikaci menších subjektů** s vysokým bezpečnostním rizikovým profilem
- návrh zákona pracuje s pojmem **„poskytovatel regulované služby“**, se kterými se pojí



\ 04 Nový zákon o kybernetické bezpečnosti (nZKB)

- Primárním důvodem přijímání nového zákona o kybernetické bezpečnosti je přijetí směrnice NIS 2 a nutnost promítnout její obsah do vnitrostátní úpravy
- Hlavním účelem zákona je chránit „regulované služby“, jejichž narušení by mohlo mít dopad na zabezpečení důležitých společenských nebo ekonomických činností nebo bezpečnost v České republice.
- Regulované organizace jsou v návrhu zákona označovány jako poskytovatelé regulované služby jsou rozděleny do dvou režimů
    I. Nižších povinností
    II. Vyšších povinností
- K návrhu zákona jsou připravovány další doprovodné právní předpisy, kdy důležitým je zejména návrh vyhlášky o regulovaných službách.

\ 05 Nařízení o digitální provozní odolnosti finančního sektoru (Nařízení DORA)

- Platnost Nařízení: od 16. ledna 2023
- Účinnost Nařízení: od 17. ledna 2025
- Prakticky plně speciální ke směrnici NIS 2, navíc má formu nařízení

- **Základní požadavky regulace dle DORA**
  I. Nastavení interního systému řízení rizik vyplývajících z outsourcingu
  II. Promítnutí regulatorních požadavků do smluvních ujednání s externími poskytovateli

\ 05 Nařízení o digitální provozní odolnosti finančního sektoru (Nařízení DORA)

DORA – rozšíření stávajícího rámce

- Zejména pro banky a pojišťovny jsou již nyní stanoveny ve zvláštních právních předpisech povinnosti
  - např. posouzení rizik outsourcingu, požadavky na smluvní ujednání poskytovatele
- Pro instituce, které mají povinnosti již nyní, bude nařízení DORA v části řízení rizik spojených s třetími stranami představovat pouze úpravu stávajícího stavu
- Pro další instituce představuje DORA nový regulatorní rámec
- Evropské orgány dohledu definují a vydají regulační a prováděcí technické normy RTS a ITS a poskytnou subjektům specifikace a návod k implementaci konkrétních požadavků DORA

\ 06 The European Critical Entities Resilience Directive (CER)

Účinnost Směrnice: **od 16. ledna 2023**

Transpoziční lhůta Směrnice: **do 17. října 2024**

Účelem Směrnice je:

I. **Posílit odolnost kritických subjektů, které poskytují základní služby důležité pro veřejnou bezpečnost, zdraví, zabezpečení nebo hospodářskou stabilitu v EU.**

II. **Zaměřit se na snižování rizik, zajištění kontinuity služeb a zlepšení připravenosti na různé druhy narušení.**

\ 07 The European Cyber Resilience Act (CRA)

European Cyber Resilience Act je právní rámec, který popisuje požadavky na kybernetickou bezpečnost hardwarových a softwarových produktů s digitálními prvky uváděných na trh Evropské unie.

Mezi hlavní cíle Nařízení patří řešení dvou problémů:

- Nízké úroveň kybernetické bezpečnosti produktů s digitálními prvky, která se projevuje rozsáhlými zranitelnostmi a nedostatečným a nedůsledným poskytováním bezpečnostních aktualizací k jejich odstranění
- Nedostatečné porozumění a přístup uživatelů k informacím, které jim brání ve výběru produktů s odpovídajícími vlastnostmi kybernetické bezpečnosti nebo v jejich bezpečném používání.

Okruh povinných subjektů:

- Výrobci, distributoři a dovozci digitálních produktů v EU.
- Softwarové a hardwarové společnosti vyvíjející produkty s připojením k internetu.
- Organizace, které používají digitální produkty ve své infrastruktuře.

\ 08 Artificial intelligence act (AI Act)

Účelem Nařízení je:

- Zlepšení fungování vnitřního trhu pomocí jednotného právního rámce vývoje, uvádění na trh, uvádění do provozu a používání systému umělé inteligence
  v Evropské unii.
- Důraz se klade na ochranu zdraví, bezpečí, základních práv deklarovaných Chartou základních práv

Regulace umělé inteligence na základě rizik

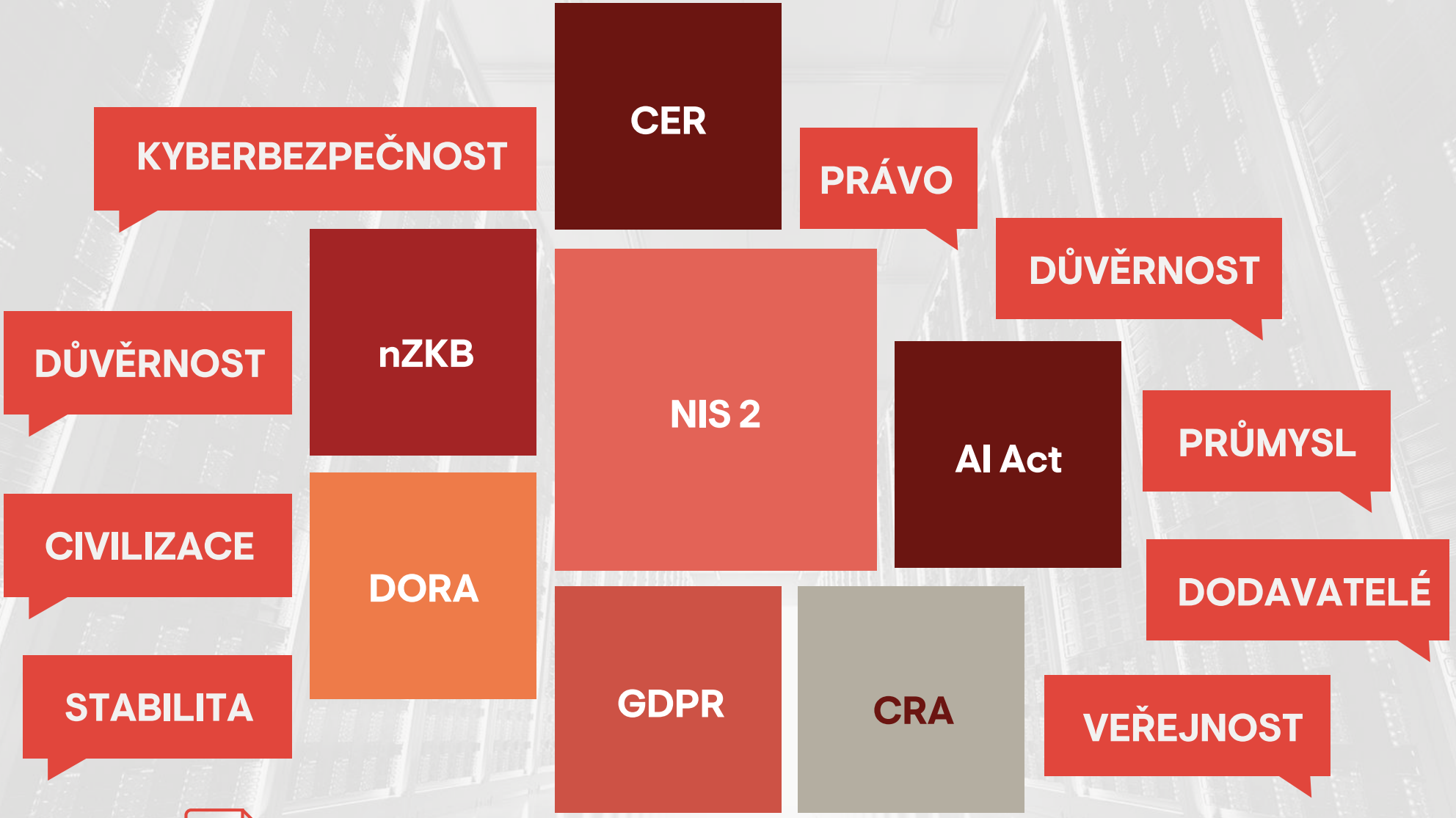
- Nepřijatelné riziko – zakázané
- Vysoké riziko – přísně regulované
- Omezené riziko
- Minimální riziko

\ 08 Artificial intelligence act (AI Act)

Akt o umělé inteligenci dopadá primárně na subjekty zapojené do regulace a vývoje umělé inteligence.

Hlavními kategoriemi jsou:

- Vývojáři – navrhují, vyvíjejí, nebo vytvářejí AI systémy.
- Poskytovatelé – uvádí systémy umělé inteligence na trh EU nebo je zpřístupňují pro použití v tomto prostoru, ať už jsou založeny v EU nebo mimo ni.
- Uživatelé – Mezi uživatele patří organizace a podniky používající systémy umělé inteligence ve svých operacích, produktech, nebo službách. Nařízení zahrnuje jak veřejný, tak soukromý sektor.
- Dovozci – Dováží do Evropské unie systémy umělé inteligence za účelem další distribuci nebo použití.
- Distributoři – Zprostředkovávají poskytování systémů umělé inteligence konečným uživatelům v EU.


KYBERBEZPEČNOST
CER
PRÁVO
DŮVĚRNOST
DŮVĚRNOST
nZKB
NIS 2
AI Act
PRŮMYSL
CIVILIZACE
DORA
DODAVATELÉ
STABILITA
GDPR
CRA
VEŘEJNOST

PORTOS

Strategic
Legal Advisory

Kontakt

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.

vlachova@portos.cz

T \ 420 603 174 997
W \ vlachova@portos.cz

Hvězdova 1716/2b
140 00 Prague 4
Czech Republic