PIERSTONE

Právní regulace kybernetické bezpečnosti mimo ZoKB a VKB.

PIERSTONE

9. dubna 2024

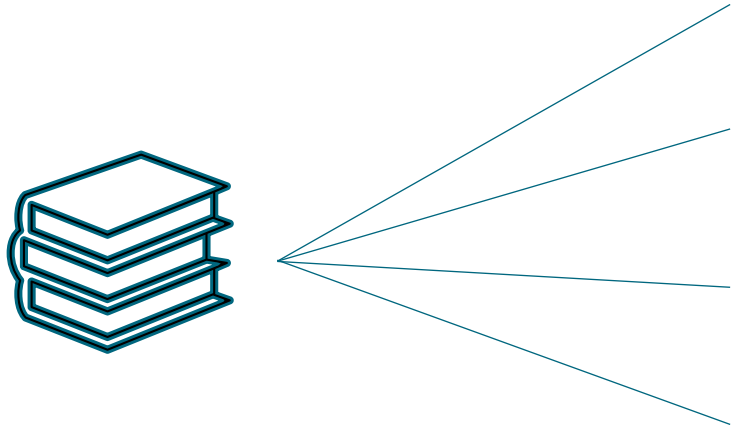
Mgr. Dominik Vítek, Ph.D.
Managing Associate | Advokát

Aplikovatelná právní úprava.

PIERSTONE

Právní rámec

Současný regulatorní rámec.

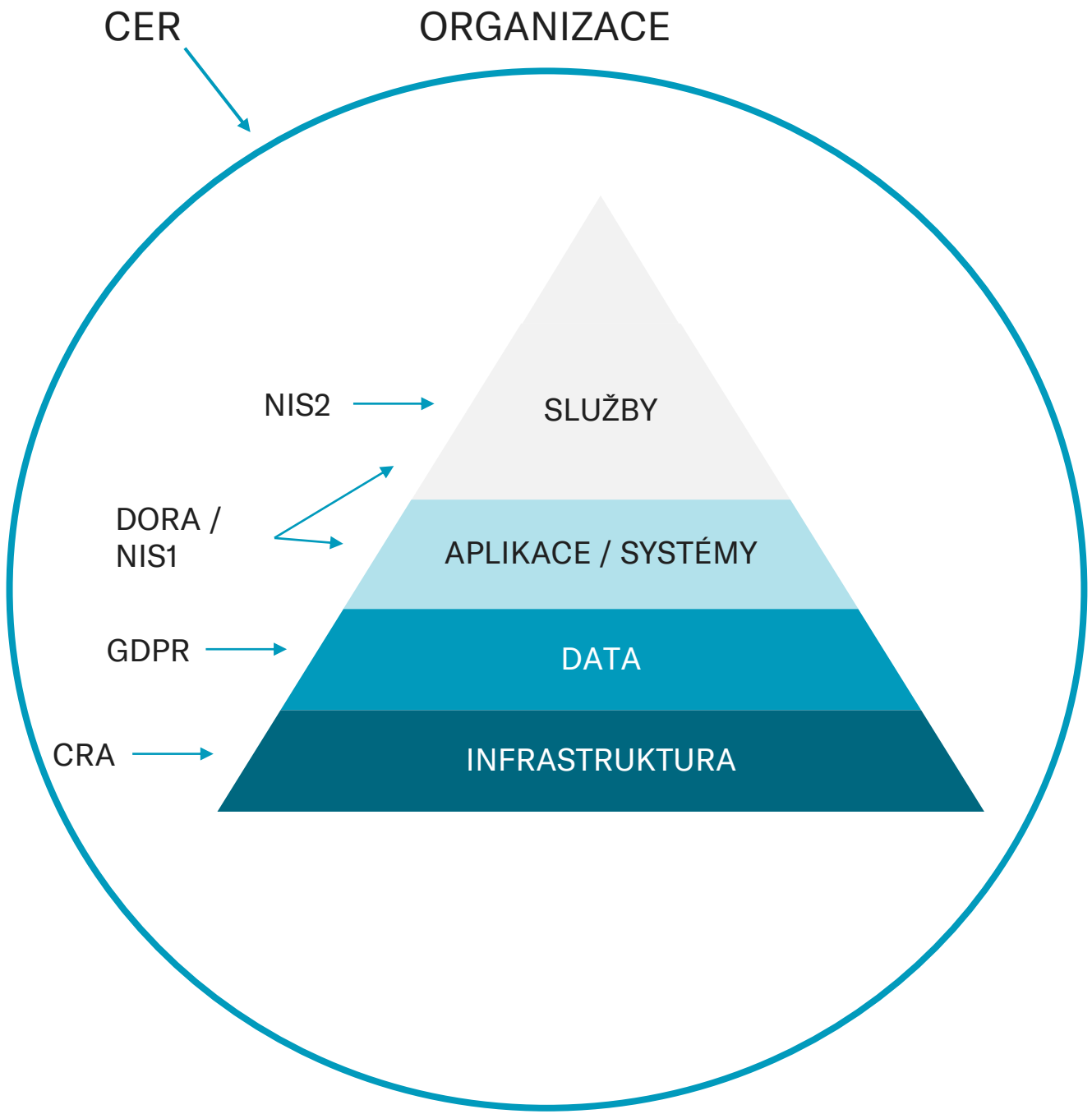


- GDPR (čl. 32, čl. 28) → Zákon č. 110/2019 Sb.
- Cybersecurity Act → Přímo aplikovatelné od 27.6.2019 → EUCS → 5G
- NIS1 → ZKB → Prováděcí předpisy
- NIS2 → Návrh zákona → Návrh vyhlášek
- CER (Critical Entities Resilience Directive) → Věcný záměr zákona
- Zákon o platebním styku → Prováděcí předpisy ČNB
- DORA (Digital Operational Resilience Act) → Přímo aplikovatelné od 17.1.2025 → Adaptační zákon
- CRA (Cyber Resilience Act) → Přímo aplikovatelné 12/24 měsíců po vyhlášení

PIERSTONE

Právní rámec

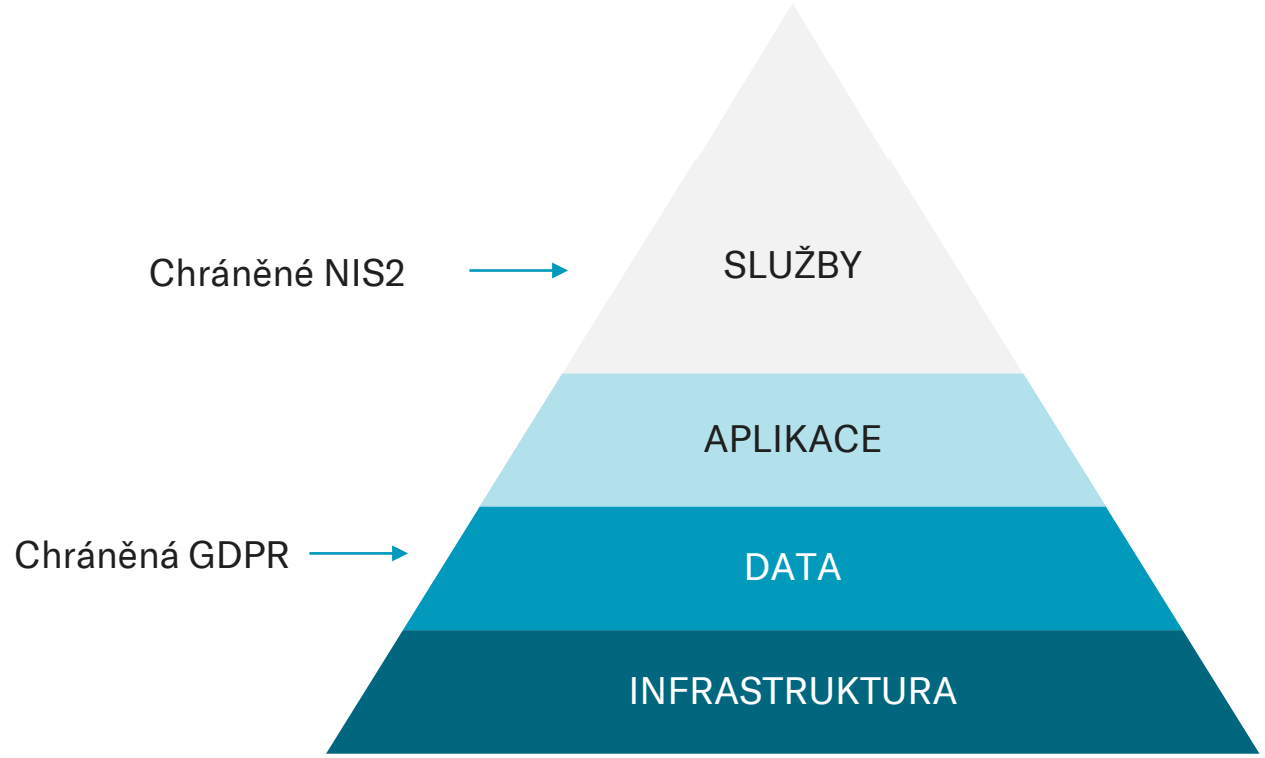
Aplikace regulací kybernetické bezpečnosti.



PIERSTONE

GDPR

Průnik NIS2 s GDPR.



- Vztah NIS2 k GDPR – spolupráce a koordinace, nejsou dotčeny pravomoci dle GDPR
- Významné sankce – pozastavení výkonu řídíce funkce, pozastavení platnosti certifikace, pokuta společnosti
- Spolupráce a koordinace NÚKIB s ÚOOÚ

PIERSTONE

CER

CER a návrh zákona.

Lhůta pro transpozici: **17. října 2024**

1 **Změna přístupu** od určování fyzických prvků kritické infrastruktury k určování subjektů kritické infrastruktury **poskytujících základní služby.**

2 **Požadavky na subjekty kritické infrastruktury:**
- posouzení rizik, zavedení opatření k zajištění odolnosti, plány odolnosti, hlášení incidentů

3 Systém **ověřování spolehlivosti kritických pracovníků** subjektů kritické infrastruktury

4 Vznik nového informačního nástroje v podobě **Portálu kritické infrastruktury**

5 Provázání s **ZKB 2.0** a **DORA**

PIERSTONE

Další povinnosti v oblasti kybernetické bezpečnosti.

PIERSTONE

Občanský zákoník

Odpovědnost (dle civilního práva).

1. Porušení **smluvní povinnosti** (§ 2913).
   - Objektivní odpovědnost.
   - Smluvní omezení.
   - Možnost liberace (§ 2913).
2. Porušení **zákonné povinnosti** (§ 2911).
   - Subjektivní odpovědnost.
   - Zákonný standard pečlivosti (§ 2912).
3. Porušení prevenční povinnosti **v konkrétních oblastech regulace.**
   - GDPR, ZEK, ZKB, zákon o platebním styku, ...
4. **Obecná** prevenční povinnost (§ 2900).
5. Význam **compliance, předcházení** a **minimalizace důsledků.**

PIERSTONE

TREND: CERTIFIKACE

Regulované certifikace

1. BSI:C5
2. Katalog cloud computingu
3. EUCS
4. GDPR Certifikace

Nařízení 2019/881 „Cybersecurity Act“

EUCS – ENISA

Cloud Computing

Mezinárodní standardy zabezpečení.

- **Soc 2 Type I.** (organizace a správa interních systémů)
  Soc 2 Type II. (bezpečnost interních systémů)
- **ISO/IEC 27001** (správa a bezpečnost informací a interních systémů)
  ISO/IEC 27018 (ochrana osobních údajů v cloudu)
- **PCI DSS** (bezpečnost údajů z platebních karet)
- **HIPPA** (ochrana údajů o zdravotním stavu)

Děkuji za Vaši pozornost.

Dominik Vítek
dominik.vitek@pierstone.com

PIERSTONE
Perlová 371/5, Praha
www.pierstone.com | in