\ 27.03.2024
\ Praha

Výzvy AI

Nadcházející AI výzvy v kyberbezpečnosti

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.
\ Team leader
vlachova@portos.cz

Mgr. Martin Vlasta
\ CIO
vlasta@portos.cz

AFCEA

PORTOS
Strategic Legal Advisory

\ 00

PORTOS

JIŽ 30 LET
působení v Česku

SPOJENÍ EXPERTŮ
z průmyslu a práva

KOMPLEXNÍ SLUŽBY
podpora správných manažerských postupů

SPRÁVNÁ KOMUNIKACE
tvoříme optimální mediální obraz klienta

Strategic Legal Advisory

Bezchybné právní řešení je samozřejmostí.

Skutečně komplexní službu však tvoří podpora správných manažerských a rozhodovacích postupů, zhodnocení ekonomických, politických či společenských souvislostí a dopadů, stejně tak i správná komunikace a vytváření optimálního mediálního obrazu klienta.

Díky tomuto přístupu jsme si za více než 30 let působení na českém právním trhu vydobyli reputaci stabilní a nezávislé advokátní kanceláře, která patří k důležitým hráčům české advokacie, byznysu i společenského dění.

\ 01a

Aktuálně

NIS2
EU směrnice

Zákon o kyberbezpečnosti
NÚKIB a navazující vyhlášky

Mechanismus NÚKIB
Dodavatelský řetězec

AI ACT
EU nařízení

Národní a unijní implementace AI pravidel
Správní praxe

PORTOS
Strategic Legal Advisory

EK | EP | ER | \

\ 01b

Legislativní proces

Strategic Legal Advisory

Co je nové?

Co je finální?

Co se pro nás reálně mění?

892 stran

8. 12. 2023 politická shoda

\ kompromisní znění

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS
2021/0106(COD)
DRAFT [Final draft as updated on 21/01]
21-01-2024 at 17h11

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
Formula				
1	2021/0106 (COD)	2021/0106 (COD)	2021/0106 (COD)	2021/0106 (COD) Text Origin: Commission Proposal
Proposal Title				
2	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS Text Origin: Commission Proposal
Formula				
3	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT	THE EUROPEAN PARLIAMENT

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS 2021/0106(COD) 21-01-2024 at 17h11 1/892

	Commission Proposal	EP Mandate	Council Mandate	Draft Agreement
	AND THE COUNCIL OF THE EUROPEAN UNION,	AND THE COUNCIL OF THE EUROPEAN UNION,	AND THE COUNCIL OF THE EUROPEAN UNION,	AND THE COUNCIL OF THE EUROPEAN UNION, Text Origin: Commission Proposal
Citation 1				
4	Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof,	Having regard to the Treaty on the Functioning of the European Union, and in particular Articles 16 and 114 thereof, Text Origin: Commission Proposal

PORTOS
Strategic Legal Advisory

EK EP ER \

\ 01b

Legislativní proces

8. 12. 2023 politická shoda

\ kompromisní znění

Strategic Legal Advisory

Co je nové?

Co je finální?

Co se pro nás reálně mění?

Definice AI	~~expertní systémy, neuronové sítě, veškerá statistika~~ autonomie, adaptivita, z dat generuje predikce, obsah, doporučení, rozhodnutí
Povinnost vzdělávat	Poskytovatelé a implementátoři musí školit, zajistit bdělost, prevenci
Zakázané praktiky	Manipulace, ovlivňování nevědomí, zneužívání zranitelností, social scoring
Kategorie rizikovosti high-risk AI system	Annex II (+rozšířený), Annex III (+nový) Výjimky (-zúžení), Nižší režim Obecné AI
Veřejnoprávní pravomoci	EK, DG CNECT, AI Office (100), AI Board Národní regulátor
Povinnosti	Ex-ante notifikace, Ex-post monitoring Dokumentace, Risk management
Sankce	Zakáz. praktiky \ ~~30~~ 35 mil. EUR, ~~6~~ 7% obr. High risk AI \ ~~10~~ 7,5 mil. EUR, 2% obratu

PORTOS
Strategic Legal Advisory

\ 01b

Legislativní proces

Annex II – AI ACT

- Zdravotnické přístroje
- Vozidla
- Nábor, HR a řízení pracovníků
- Vzdělávání a odborný výcvik
- Ovlivňování voleb a voličů
- Přístup ke službám (pojištění, bankovnictví, úvěry, dávky)
- Správa kritické infrastruktury (voda, plyn, elektřina)
- Systémy rozpoznávání emocí
- Biometrická identifikace
- Vymáhání práva, pohraniční kontrola, migrace a azyl
- Správa spravedlnosti
- Specifické produkty a/nebo bezpečnostní komponenty specifických produktů

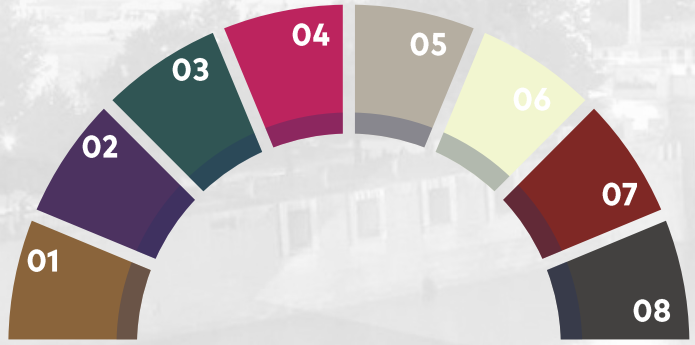
Annex – NIS2

ESSENTIAL Subjekty zásadního významu

- zdravotnictví,doprava
- banky, finance, veřejná správa, vesmír
- voda, infrastruktura, energetika

IMPORTANT Důležité subjekty

- pošta, sociální sítě, e-commerce
- potraviny, odpady
- chemie, elektronika, průmyslové stroje



8. 12. 2023 politická shoda

\ kompromisní znění

PORTOS
Strategic Legal Advisory

\ 01b

Legislativní proces

8. 12. 2023 politická shoda

\ kompromisní znění

Přehled povinností

\ **Hodnocení dopadu**
na základní práva a hodnocení souladu

\ **Registrace**
ve veřejné databázi EU pro systémy AI s vysokým rizikem

\ Implementace **řízení rizik** a systému řízení kvality

\ **Správa dat**
zmírňování zkreslení, reprezentativní tréninková data

\ **Transparentnost**
instrukce pro použití, technická dokumentace

\ **Lidský dohled**
vysvětlitelnost, auditovatelné záznamy, člověk v smyčce

\ Přesnost, robustnost a **kybernetická bezpečnost**

PORTOS
Strategic Legal Advisory

\ 01b

Legislativní proces

8. 12. 2023
politická shoda
\ kompromisní znění

13. 03. 2024
Hlasování v EP
\ schváleno 523 \ 46 \ 49

04-05 2024
Hlasování v ER
\ schválení rady

Implementace
\ účinnost nových povinností

cca 06 2024

▪ zakázané praktiky	▪ kodexy praxe	▪ obecná pravidla	▪ vysoce rizikové systémy
+ 6 m	+ 9 m	+ 12 m	+ 36 m

\ 02

Nové výzvy

NEXT STEPS

A. TECHNICKÉ

B. LIDSKÉ

C. REGULATIVNÍ

PRÁVNÍ REGULACE

PÉČE ŘÁDNÉHO HOSPODÁŘE

ZÁJMY ZÁKAZNÍKŮ A VEŘEJNOSTI

ZÁJMY ENTERPRISE

\ 02

Nové výzvy

NEXT STEPS

A. TECHNICKÉ | B. LIDSKÉ | C. REGULATIVNÍ

\ Low lvl attack

generativní AI nástroje umožňují:

- snažší cílení a personalizaci phishingového útoku (text, obraz, zvuk/hlas)
- automatizované získávání dat a strukturování poznatků pro zjištění sociální sítě oběti (metody sociálního inženýrství)

\ Řešení

vzdělání, osvěta, robustní komunikace

\ High-lvl attack

generativní AI nástroje znemožňuji:

- funkcionalitu antivirů
  klasické statické metody virus fingerprinting (checksum/hash signatures, díky obfuskačním technikám (polymorphic malware) jsou neefektivní

\ Řešení

behavioral, heuristic analysis, multi-layer/core architecture

\ 02

Nové výzvy

NEXT STEPS

A. TECHNICKÉ | B. LIDSKÉ | C. REGULATIVNÍ

\ Low lvl attack

generativní AI nástroje umožňují:

- snažší sociální inženýrství

\ Řešení

vzdělání, osvěta, robustní komunikace

\ Extra HR burden

příchod /odchod pracovníků
soukromý / pracovní život

\ High-lvl attack

generativní AI nástroje znemožňuji:

- funkcionalitu antivirů

\ Řešení

behavioral, heuristic analysis, multi-layer/core architecture

\ Cloud, redundancy a DDOS

Pokročilé AI štíty vyžadují vlastní datacentra nebo cloud (častější řešení) > zásadnější zranitelnost vůči DDOS útokům.

\ 02

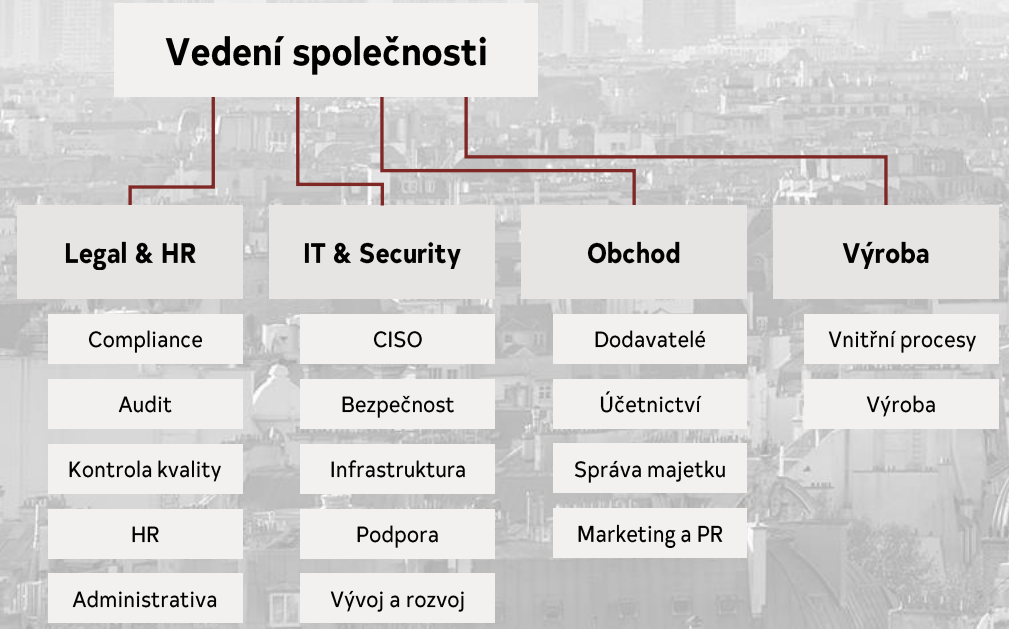
Nové výzvy

NEXT STEPS

A. TECHNICKÉ

B. LIDSKÉ

C. REGULATIVNÍ



KYBERBEZPEČNOST

Tohle teď není finanční priorita.

Je to moc drahé. Kamarád z Číny to umí levněji.

Nemám na to teď čas.

Samozřejmě vím, phishing, virus, macro, je špatný.

Takže můžeme dál, že?

AI

Tady máš X mil. EUR investici a dotaci

Dejte do AI všechny data a zvítězíme!

Chceme všechny cloudy!

Potřebuju vědět všechny informace a nejnovější trendy. AI úplně nová věc!

Mám 30 AI aplikací v telefonů a každý den jedu.

Strategic Legal Advisory PORTOS

\ 02

Nové výzvy

NEXT STEPS

Jaký máte compliance program?

A. TECHNICKÉ — Jsou moje zákaznická data v bezpečí?

B. LIDSKÉ

C. REGULATIVNÍ — Máte alternativní způsoby řešení?

Jak máte řešenou kyberbezpečnost?

Máte plán, jak postupovat v případě útoku?

Jste bezpeční?

Vedení společnosti

Legal & HR	IT & Security	Obchod	Výroba
Compliance	CISO	Dodavatelé	Vnitřní procesy
Audit	Bezpečnost	Účetnictví	Výroba
Kontrola kvality	Infrastruktura	Správa majetku	
HR	Podpora	Marketing a PR	
Administrativa	Vývoj a rozvoj		

Regulátoři

Národní úřad pro kybernetickou a informační bezpečnost

Úřad pro ochranu osobních údajů

Český telekomunikační úřad · ÚOHS · ČNB Česká národní banka

Zákazníci a klienti

Veřejnost a média

Dodavatelé

\ 02

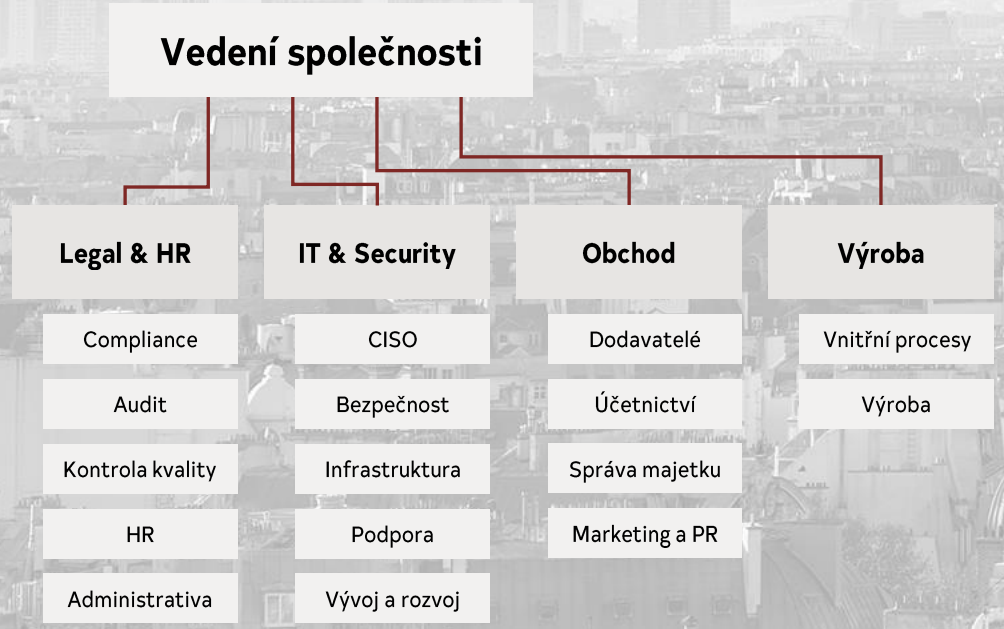
Nové výzvy

NEXT STEPS

A. TECHNICKÉ

B. LIDSKÉ

C. REGULATIVNÍ



Vy AI už používáte?

Ano.

Takže vlastně vyhazujete lidi?

Mám tedy očekávat vyšší cenu, méně usilí, horší výstup?

Takže vy mě pořád sledujete a schromažďujete data a všechny moje data posíláte MSFT / GPT?

A co až vám „ta AI“ přestane fungovat?

Nebudujete náhodou Skynet?

Ne.

Proč ne?

Jste tedy zpátečnická společnost bez inovací?

Do práce stále jezdíte na koni? A server máte Win XP?

Vy se o to „IT“ vůbec nestaráte, proč vás vůbec platím?

\ 02

Nové výzvy

NEXT STEPS

A. TECHNICKÉ

B. LIDSKÉ

REÁLNĚ UŽITEČNÉ A NEZBYTNÉ VĚCI

C. REGULATIVNÍ

CO ZAJÍMÁ KYBERBEZPEČÁKA

REAL BUSINESS SAFETY ZONE

HUMAN RIGHTS POLITICS ZONE

CO ZAJÍMÁ EU ÚŘEDNÍKA

\ 02

Právní výzvy

C.

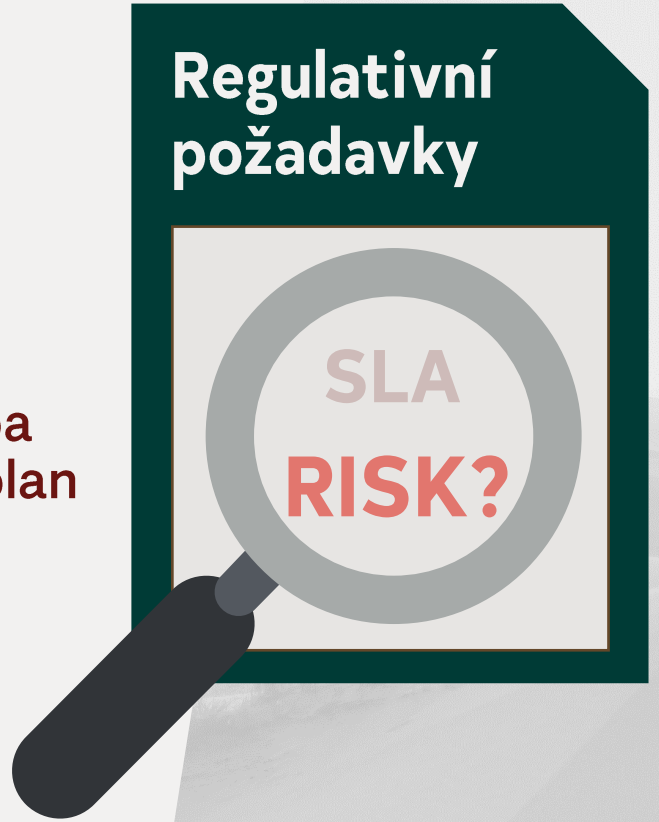
REGULATIVNÍ

\ **Revize a kolize**
pravidel v compliance programu

\ **Příprava dokumentace a ex-ante notifikace**
demonstrace splnění požadavků

\ **Zhodnocení analýzy rizik**
nestranné posouzení metodiky, mapa odpovědností, business continuity plan

\ **Obhajoba při kontrole**
Argumentace závěrů, obrana před správními zásahy, komunikace s veřejností



PORTOS

Strategic
Legal Advisory

Kontakt

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.
\ Team leader
vlachova@portos.cz

Mgr. Martin Vlasta
\ CIO
vlasta@portos.cz

T \ 00 420 224 827 884
W \ portos.cz

Hvězdova 1716/2b
140 00 Prague 4
Czech Republic