Aktuální informace z regulace kybernetické bezpečnosti
a
nové podpůrné materiály NÚKIB

Adam Kučínský

Národní úřad pro kybernetickou a informační bezpečnost
Odbor regulace

8. září 2020

Nové podpůrné materiály

Nový web NÚKIB

V průběhu srpna spojil NÚKIB své dosavadní weby www.nukib.cz a www.govcert.cz do aktuálního a jediného

www.nukib.cz

Podpůrné materiály a další informace od odboru regulace a odboru kontroly naleznete nově na

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola

Podpůrné materiály – VTC standard

- **Cíl:** Stanovit minimální požadavky na bezpečnost a funkcionality VTC aplikací s ohledem na důvěrnost informací (primární adresáti státní správa)
- **Nosné části:** Klasifikace informací, funkční požadavky, bezpečnostní požadavky, pravidla pro uživatele
- **Použití v ZVZ:** Jako inspirace, požadavky je nutno si odůvodnit, může být i přísnější
- **Vztah k ZKB:** Nelze bez dalšího aplikací standardu mít ZKB za splněný
- **Termín vydání:** Vydáno
- **Vymahatelnost**: Dobrovolné
- Vydáno ve spolupráci s:
  - NAKIT
  - a dalšími – VZ, BIS, ÚZSI, AFCEA, AČR, CISCO, MICROSOFT, GESTO, ATS TELCOM

Dokument zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

Podpůrné materiály – Minimální bezpečnostní standard

- **Cíl:** Stanovit minimální bezpečnostní požadavky na systémy mimo ZKB
- **Nosné části:**
  - Manažerská část – organizační opatření,
  - Technická část – technické opatření;
  - ➢ Bez analýz, seznam požadavků.
- **Použití v ZVZ:** Jako inspirace, požadavky je nutno si odůvodnit, může být i přísnější
- **Vztah k ZKB:** Nelze bez dalšího aplikací standardu mít ZKB za splněný
- **Termín vydání:** Vydáno
- **Vymahatelnost**: Dobrovolné
- Vydáno ve spolupráci s MV a NAKIT
- V plánu je ještě zpracovat přílohu k požadavkům na logování

Dokument zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

Podpůrné materiály – Bezpečnostní doporučení v kyberprostoru pro vrcholové vedení

- **Cíl:** vytvořit pro premiéra/vládu/poslance a další vrcholové vedení bezpečnostní doporučení pro pohyb v kyberprostoru
  - Cílí primárně na uživatele, kteří často nejsou úplně v moci interního IT/bezpečnosti
- **Nosné části:** Práce s firemním počítačem a smartphonem, bezpečná komunikace, zabezpečení online účtů
  - Dokument obsahuje téměř 30 základních bezpečnostních opatření, kterými by se mělo vrcholové vedení organizací a jejich čelní představitelé řídit. Opatření jsou rozdělena do témat:
- **Použití v ZVZ:** nerelevantní
- **Vztah k ZKB:** Nelze bez dalšího aplikací doporučení mít ZKB za splněný
- **Termín vydání:** Do konce ZÁŘÍ 2020
- **Vymahatelnost**: Dobrovolné

Podpůrné materiály – (Ne)poskytování informací o bezpečnosti

NÚKIB aktualizoval a přepracoval dokument k (ne)poskytování informací v oblasti kybernetické bezpečnosti a bezpečnosti systémů nakládajících s utajovanými informacemi.

Dokument je rozdělen do tří částí a shrnuje doporučení NÚKIB k poskytování informací na žádost veřejnosti. Omezení poskytování informací rozpracovává z těchto pohledů:

1. **§ 10a zákona o kybernetické bezpečnosti** – informace, jejíž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti
   - vhodné pro použití u bezpečnostní dokumentace (aktiva s vysokým hodnocením)
2. **§ 11 odst. 1 písm. d) zákona o svobodném přístupu k informacím** – informace, jejíž poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření
   - vhodné pro použití u informací o bezpečnostních opatřeních
3. **§ 7 zákona o svobodném přístupu k informacím** – utajované informace

Dokument zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

(Ne)poskytování informací o bezpečnosti

NÚKIB navrhuje změnu zákona č. 106/1999 Sb., o svobodném přístupu k informacím.

Návrh ze strany NÚKIB:

V § 11 se doplňuje odstavec 7, který včetně poznámky pod čarou č. 21 zní:

„(7) Povinný subjekt neposkytne informaci o seznamu prvků kritické infrastruktury[21)] a informace, jejichž poskytování je vyloučeno zákonem o kybernetické bezpečnosti.

_____

[21)] § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.“

Důvod:

Nutno chránit seznam prvků KI/KII

Aktuální fáze legislativního procesu:

26. 8. 2020 ukončeno připomínkové řízení, nyní jsou vypořádávány připomínky

Podpůrné materiály – Provozovatel systému - informování

NÚKIB plánuje aktualizovat podpůrný materiál k provozovateli systému a doplnit do něj vzory informování provozovatele systému a významného dodavatele, který má vliv na bezpečnost.

Vzor informování obsahuje povinné náležitosti podle:

- § 8 odst. 1 písm. b) a c) a odst. 3 vyhlášky o kybernetické bezpečnosti,
- tzn. zohledňuje obsah podpůrného materiálu k provozovateli systému:

„(Informování) *by však mělo být provedeno **prokazatelně**, **adresně** a ve vztahu ke každému jednotlivému provozovateli **samostatně**. Podstatnými náležitostmi prokazatelnosti bude **informace o tom, že se jedná o provozovatele konkrétního systému podle zákona o kybernetické bezpečnosti**, s čímž je neodmyslitelně spjato také **stanovení systému** spadajícího do působnosti zákona o kybernetické bezpečnosti, vymezení technických a programových prostředků, které tvoří určený systém, resp. **vymezení činností dodavatele v rámci určeného systému**, **a to tak, aby došlo k dostatečné identifikaci toho, pro co se dodavatel stává provozovatelem daného systému“.***

Dokument bude zveřejněn zde:

www.nukib.cz – Kybernetická bezpečnost – Regulace a kontrola – Podpůrné materiály

Novela vyhlášky č. 317/2014 Sb., o významných informačních systémech

Novela vyhlášky č. 317/2014 Sb., o významných informačních systémech

Cíl:

- Zjednodušit **a zpřehlednit proces identifikace**
- Zvýšit **efektivnost** vyhlášky
- Zvýšit **právní jistotu** adresátů

Fáze:

- **ZVEŘEJNĚNO VE SBÍRCE ZÁKONŮ = novela je platná**
- Plná citace právního předpisu zní: Vyhláška č. 360/2020 Sb., kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.
- Příslušnou částku Sbírky zákonů lze nalézt zde: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=360/2020&typeLaw=zakon&what=Cislo_zakona_smlouvy

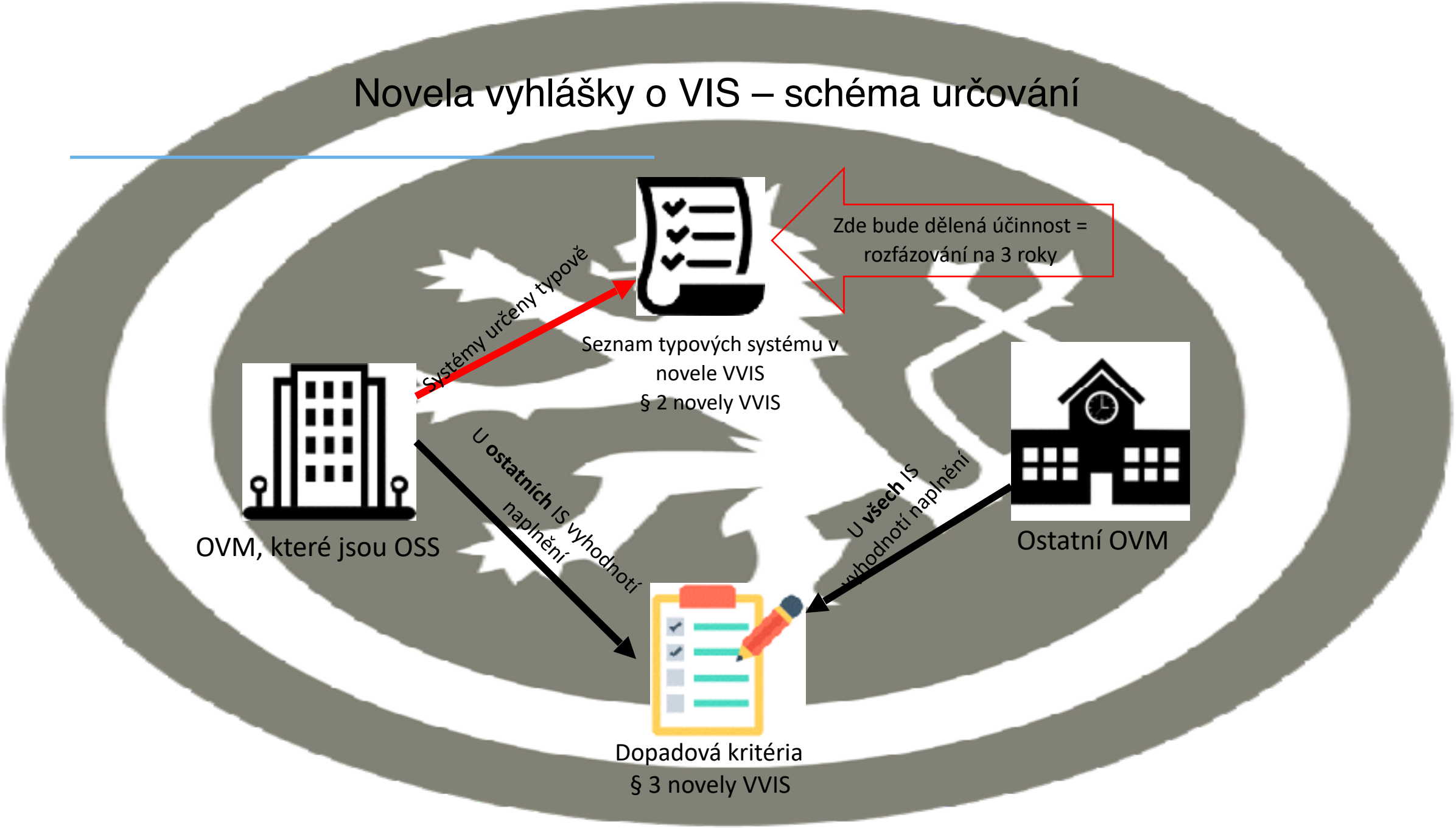
Účinnost:

- 1. 1. 2021

Koncept vyhlášky

- U organizačních složek státu (OSS) a krajů vyjmenuje vyhláška IS, které se určí „defaultně“ = vždy budou VIS
- Ostatní OVM (a OSS a kraje u těch nevyjmenovaných) posoudí kritéria = IS, které naplní budou VIS

Novela vyhlášky o VIS – schéma určování



Pevně „defaultně“ vymezené systémy - § 2

(1) Významný informační systém podle § 2 písm. d) zákona je informační systém spravovaný orgánem veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný při **výkonu působnosti orgánu veřejné moci** k zajištění

a) **elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,**

b) **kontrolní nebo inspekční činnosti anebo státního dozoru,**

1. vlna - 2021

c) **výkonu veřejné moci při přípravě na krizové situace a jejich řešení,**

d) **výkonu spisové služby,**

e) **vedení úřední desky způsobem umožňujícím dálkový přístup,**

2. vlna - 2022

f) **mezinárodní spolupráce, nebo**

g) **zadávání veřejných zakázek.**

3. vlna - 2023

(2) Významným informačním systémem podle § 2 písm. d) zákona je dále také informační systém spravovaný orgánem veřejné moci, který naplňuje určující kritéria stanovená v § 3.

(3) Významným informačním systémem **není informační systém, jehož správcem je obec.**

(4) Platí, že významný informační systém uvedený v odstavci 1 naplňuje určující kritéria.

Naplnění dopadových kritérií - § 3

Bude platit od začátku – nebude dělená účinnost

§ 3

Určující kritéria

(1) Určujícím kritériem je skutečnost, že narušení bezpečnosti informací v informačním systému, který není uveden v § 2 odst. 1, by mohlo způsobit

a) omezení či narušení **poskytování služeb nebo informací** orgánem veřejné moci veřejnosti,

b) **omezení či narušení hospodaření** orgánu veřejné moci,

c) jiné omezení či narušení **fungování orgánu veřejné moci**

d) omezení či narušení fungování, poskytování služeb nebo informací veřejnosti, nebo hospodaření **jiného** orgánu nebo osoby podle § 3 zákona,

e) **zásah do osobního života** nebo do práv fyzických nebo právnických osob postihující **nejméně 50 000 osob**, nebo

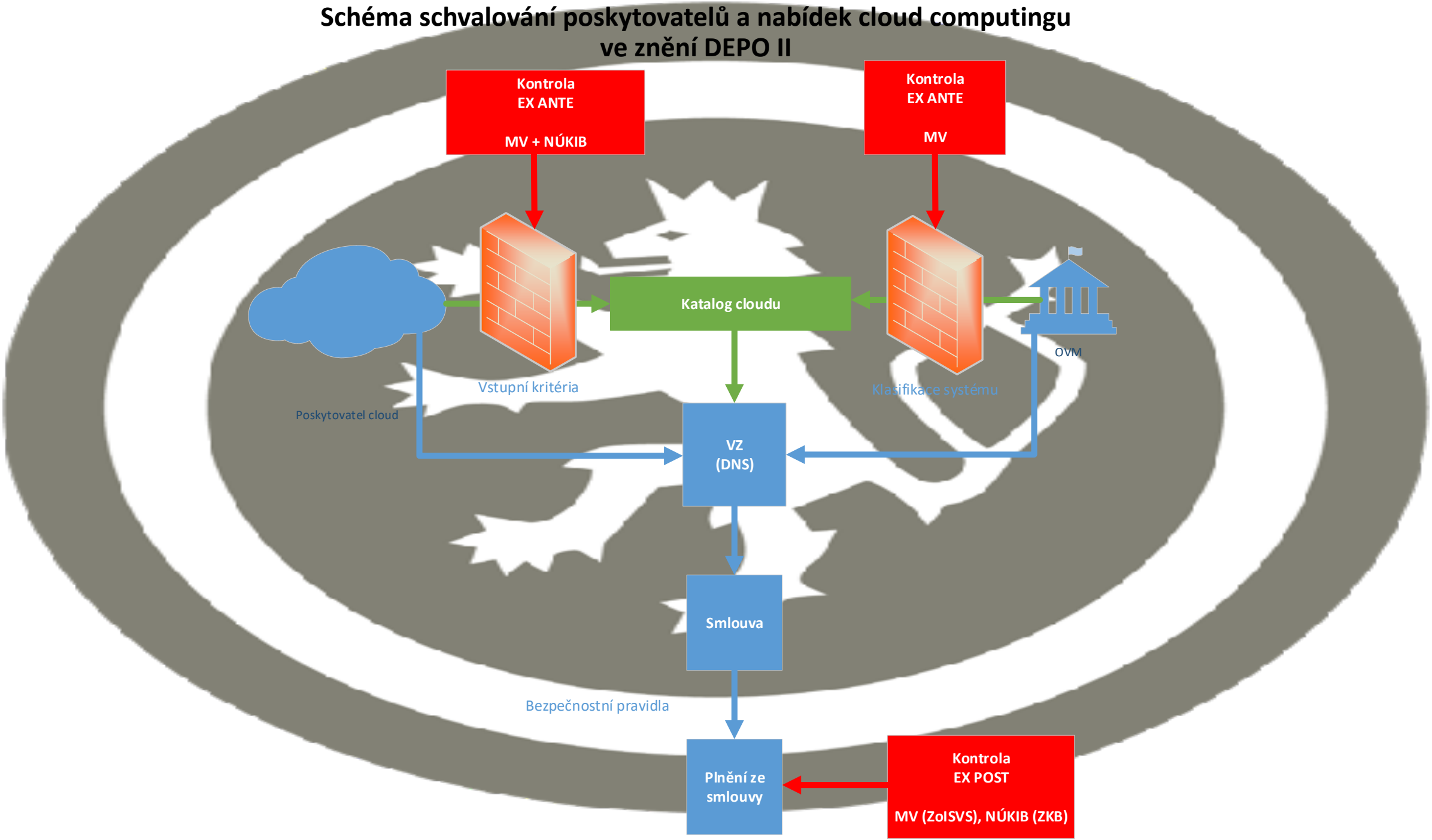
f) ohrožení či narušení **veřejného zájmu**,

a toto omezení, narušení, zásah či ohrožení **nebude možné odvrátit bez vynaložení nepřiměřených nákladů**.

eGovernment CLOUD

Problematika lokace zpracování dat

Schéma schvalování poskytovatelů a nabídek cloud computingu ve znění DEPO II



Schvalování poskytovatelů a nabídek cloud computingu ve znění DEPO II

/zatím neschválený návrh/

Poskytovatelé
§ 6m

Požadavky na poskytovatele cloud computingu poskytujícího cloud computing orgánu veřejné správy

Poskytovatelem cloud computingu poskytujícím cloud computing orgánu veřejné správy může být pouze osoba nebo jiné právní uspořádání, které

a) jsou způsobilé zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,

b) jsou bezúhonné v rozsahu bezúhonnosti požadované po kvalifikovaném správci kvalifikovaného systému elektronické identifikace,

c) jsou způsobilé pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.

Nabídky cloud computingu
§ 6n

Požadavky na cloud computing využívaný orgánem veřejné správy

Orgán veřejné správy může využívat a poskytovatel cloud computingu může orgánu veřejné správy poskytovat pouze cloud computing,

a) který umožňuje splnění požadavků kladených na informační systém veřejné správy informační koncepcí České republiky,

b) který umožňuje dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,

c) který umožňuje orgánu veřejné správy postupovat podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu podle zákona upravujícího kybernetickou bezpečnost,

d) jehož bezpečnostní úroveň je stejná nebo vyšší než bezpečnostní úroveň informačního systému veřejné správy, k jejichž provozu je využíván,

e) který v případě, že je jeho poskytování závislé na jiném cloud computingu, je poskytovaný s využitím cloud computingu splňujícího požadavky podle písmene b) až d) a poskytovaného státním poskytovatelem cloud computingu nebo poskytovatelem cloud computingu zapsaným v katalogu cloud computingu,

f) u něhož v případě, že je jeho poskytování závislé na více poskytovatelích cloud computingu, je každý poskytovatel cloud computingu státním poskytovatelem cloud computingu nebo poskytovatelem cloud computingu zapsaným v katalogu cloud computingu.

Tři části cloudové vyhlášky

VSTUPNÍ KRITÉRIA
(§ 6m nebo § 6n písm. b ZoISVS)

ID/ 1 2 3 4

1. Certifikace ISO 27k
2. Šifr. algoryt. VKB
3. …
4. …
5. …

BEZPEČNOSTNÍ PRAVIDLA PRO OVM
(§ 6n písm. c ZoISVS)

A) Řízení přístupu
B) Náležitosti smluv
C) …
D) …
E) …

BEZPEČNOSTNÍ ÚROVNĚ IS (DOPADY) (§ 4 odst. 5 ZKB)

Úr./dopad: mrtví/peníze/…

1 †	$
2 ††	$$
3 †††	$$$
4 ††††	$$$$

Zpracování dat mimo EU

- **Dle sdělení zástupců průmyslu zpracování dat mimo území EU/EHP**, nebo alespoň možnost takového zpracování**, je nezbytné pro fungování některých služeb** (například translate, pokročilé bezpečnostní funkce – korelace signálů z bezpečnostních senzorů) **a pro zajištění podpory téměř všech služeb** (odesílání logů, crashdump souborů a jejich zaslání pro zpracování do celého světa atd.)

- Pokud dojde k odeslání dat mimo EU za účelem jejich zpracování, je v podstatě nemožné dohlédnout, zda data byla zpracována pouze za účelem, pro který byla vyvezena, nebo byla případně zneužita

Ze smluvních podmínek mnohých vendorů často vyplývá, že data mohou být že data mohou být uložena kdekoli kde daný vendor uzná za vhodné/potřebné..

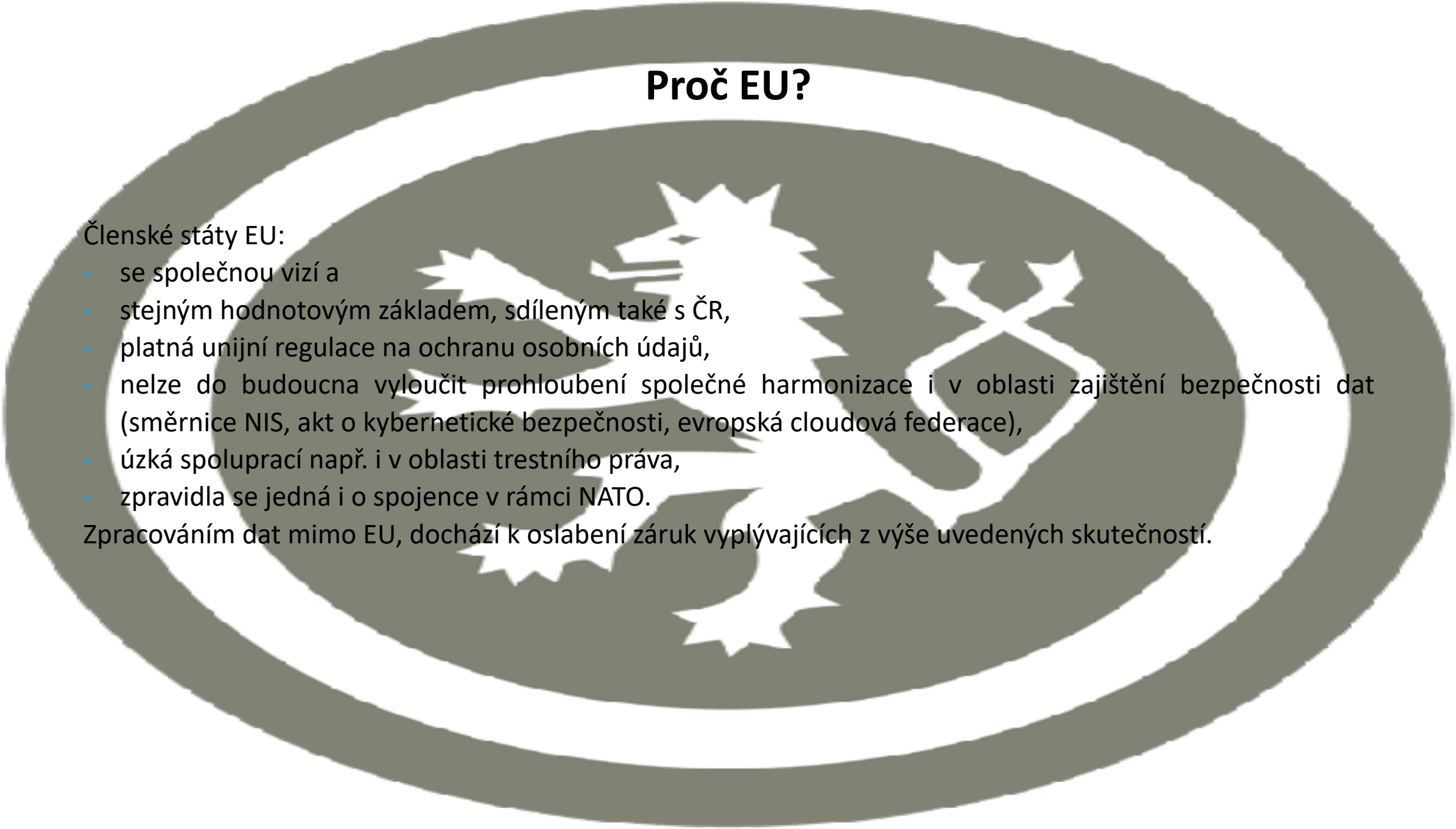
Viz např. odstavec 99, str. 21 zprávy Evropského inspektora ochrany osobních údajů z 2. července 2020. Dostupné online z: https://edps.europa.eu/data-protection/our-work/publications/papers/outcome-own-initiative-investigation-eu-institutions_en

Dále je pro problematiku cloudu také významné zrušení tzv. Privacy-Shield – viz např. sdělení ÚOOÚ dostupné: zde: https://www.uoou.cz/uoou-k-nbsp-dopadum-zruseni-stitu-soukromi-eu-usa-na-spravce/d-43874

Rizika ne/zpracování mimo EU

- **garance trvalého uložení v EU nabízená poskytovateli ≠ veškeré zpracování**
- zpracování dat mimo EU může být i podstatnou výhodou globálních poskytovatelů z hlediska bezpečnosti (např. porovnání vzorků infikovaných maker)
- **Cloud bude vždy závislý na důvěře vlastníka dat (státu) v poskytovatele a na poctivosti poskytovatele**
  - **Zákazník dává svá data mimo své systémy do správy dalšího subjektu**
  - **EX ante kontrola nikdy nezaručí 100 % bezpečnost**
  - **EX ante kontrola se snaží přiměřené posoudit rizika spojená s dodavatelem**
- pokud legislativa nebude stanovovat povolené nakládání s daty, bude pro zákazníka i regulátora výrazně obtížné až nemožné (s ohledem na jeho vyjednávací možnosti při dojednávání smlouvy vůči globálním poskytovatelům) efektivně řídit, dohlížet a kontrolovat objem dat, který je zpracováván mimo EU
- Rizikem může být přístup zahraničních bezpečnostních služeb v případě uložení mimo EU
- Problematický může být přístup k datům pro české bezpečnostní složky, pokud jsou data uložena v zemích bez dostatečné justiční spolupráce s ČR

Proč EU?



Členské státy EU:

- se společnou vizí a
- stejným hodnotovým základem, sdíleným také s ČR,
- platná unijní regulace na ochranu osobních údajů,
- nelze do budoucna vyloučit prohloubení společné harmonizace i v oblasti zajištění bezpečnosti dat (směrnice NIS, akt o kybernetické bezpečnosti, evropská cloudová federace),
- úzká spoluprací např. i v oblasti trestního práva,
- zpravidla se jedná i o spojence v rámci NATO.

Zpracováním dat mimo EU, dochází k oslabení záruk vyplývajících z výše uvedených skutečností.

Návrh NÚKIB

- aby poskytovatelé cloudových služeb museli alespoň poskytnout informace o:
  - **místu**,
  - **rozsahu**,
  - **době** a
  - **účelu** zpracování dat mimo území EU

Na toto bylo ze strany zástupce poskytovatelů sděleno, že:

- tyto informace jsou schopni poskytnout pouze omezeně ve vztahu k místu, účelu a pouze k určitým typům dat a určitým typům zpracování,
- při stanovení požadavku na poskytnutí výše uvedených údajů, může opět dojít k omezení nabídky služeb ze strany globálních poskytovatelů, nebo ke sdělení pouze obecných účelů zpracování, širokých rozsahů dat.

K tomuto tématu probíhají další jednání…

Jak to řeší jinde?

- **USA**
  - Specifická situace – mají vlastní vládní cloud dedikovaný v USA
  - Komerční poskytovatelé vytvořili speciální nabídku jen pro USA
  - V ČR asi neaplikovatelné – jsme malý trh
- **NĚMECKO**
  - Do takového detailu jako my nejdou – přenáší to na úroveň jednotlivých zákazníků – OVM
  - Každý zákazník - OVM si musí oklasifikovat data a rozhodnout se jak bude postupovat
  - V současném konceptu pro nás neaplikovatelné

DĚKUJI ZA POZORNOST

regulace@nukib.cz

NÚKIB