Aktuální stav kybernetické bezpečnosti v České republice

AFCEA

Adam Kučínský
Národní úřad pro kybernetickou a informační bezpečnost
Odbor regulace

23. září 2020

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
- Novelizovaná vyhláška je již dostupná i zde: https://www.zakonyprolidi.cz/cs/2020-360/zneni-20210101

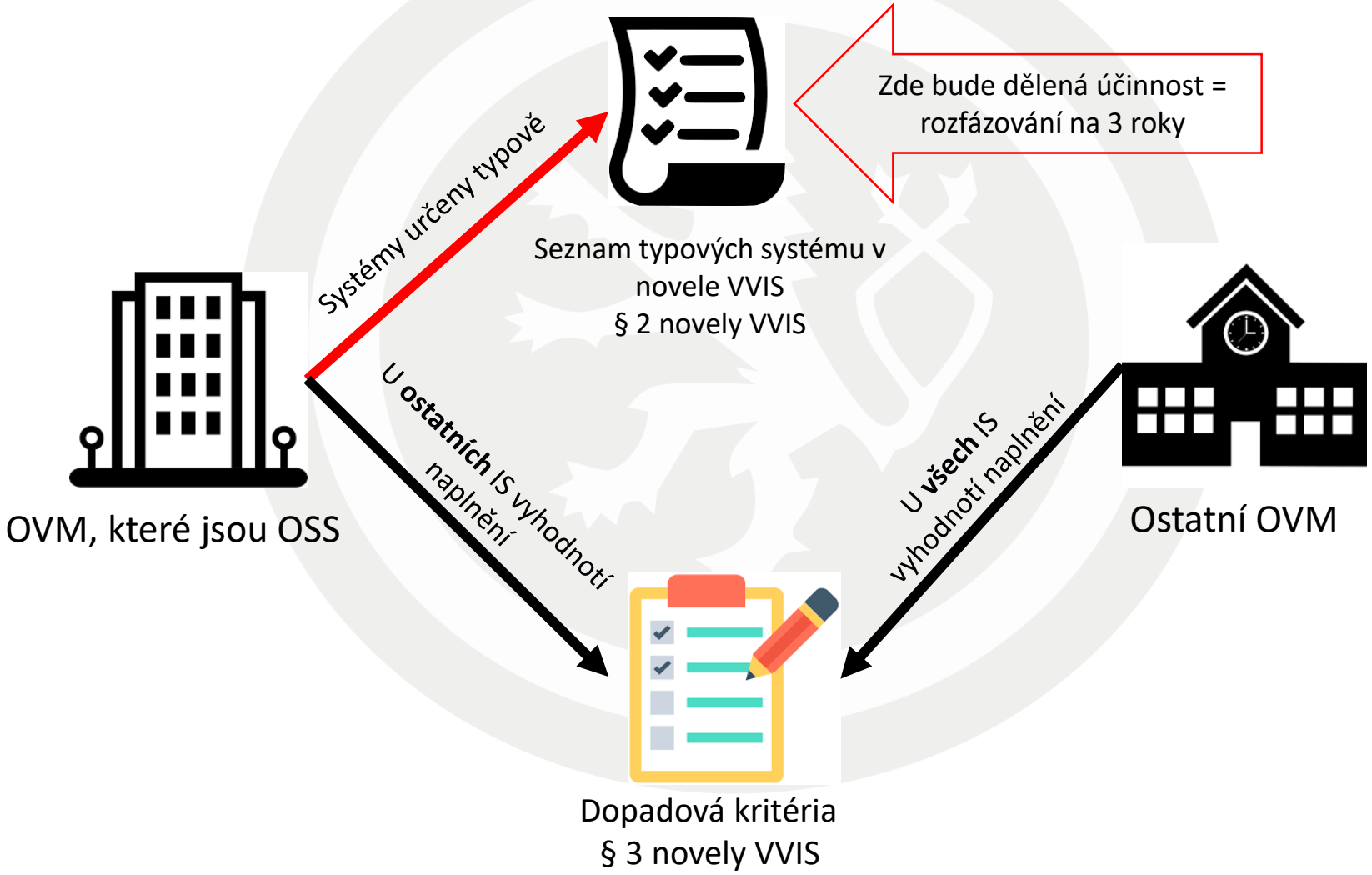
Účinnost:

- 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 je 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, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný 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

Platí od začátku – bez dělené účinnosti

§ 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 nebo hospodaření jiného orgánu nebo osoby podle § 3 zákona, popřípadě omezení či narušení poskytování služeb nebo informací veřejnosti tímto orgánem nebo osobou,

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**.

Evidence systémů

§ 3

(2) Orgán veřejné moci vede seznam všech informačních systémů, kterých je správcem, a u každého informačního systému, který **není uveden v § 2 odst. 1**, posoudí naplnění určujících kritérií podle odstavce 1. O výsledku posouzení vede správce informačního systému písemný záznam, který je součástí seznamu podle věty první.

Prakticky:

- Systémy, které nejsou určeny typově podle seznamu v § 2 a podléhají tak posouzení dle § 3 jsou přidány na tento seznam
- Po posouzení těchto systémů je výsledek (identifikace/neidentifikace VIS a důvody pro toto rozhodnutí) uveden rovněž v seznamu

Cíle:

- Přenositelnost obsahu úvahy o posouzení ne/naplnění kritérií VIS pro budoucí zodpovědné zaměstnance
- Získat auditní stopu, že k posouzení došlo a jakou úvahou bylo vedeno

Novely zákona o kybernetické bezpečnosti

Vývoj:

- Za poslední rok jedna novelizace ZKB od 1. 2. 2020, další novelizace v procesu

Novelizace přestupků a drobné opravy:

- Novelizace opravuje chyby z ZKB v § 5 (bezpečnostní opatření) a § 25 (přestupky)
- Účinná od 1. 2. 2020

Novelizace kontaktních údajů, přestupků v souvislosti s cyber security aktem a předávání informací z evidence kybernetických bezpečnostních incidentů:

- Hlášení rozsahu veřejných IP adres systému, přestupky v oblasti certifikace kybernetické bezpečnosti a neposkytování informací z evidence, které by ohrozily zájem chráněný zákonem o kybernetické bezpečnost
- Účinná v budoucnu

Novelizace v souvislosti s regulací cloudů (+ zákon o ISVS):

- Úprava zmocnění k vydání cloudové vyhlášky a k stanovení místa zpracování údajů v rámci cloudu
- Účinná v budoucnu

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 výše uvedených témat.
- **Použití v ZVZ:** nerelevantní
- **Vztah k ZKB:** Nelze bez dalšího aplikací doporučení mít ZKB za splněný
- **Termín vydání:** Vydáno v 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:

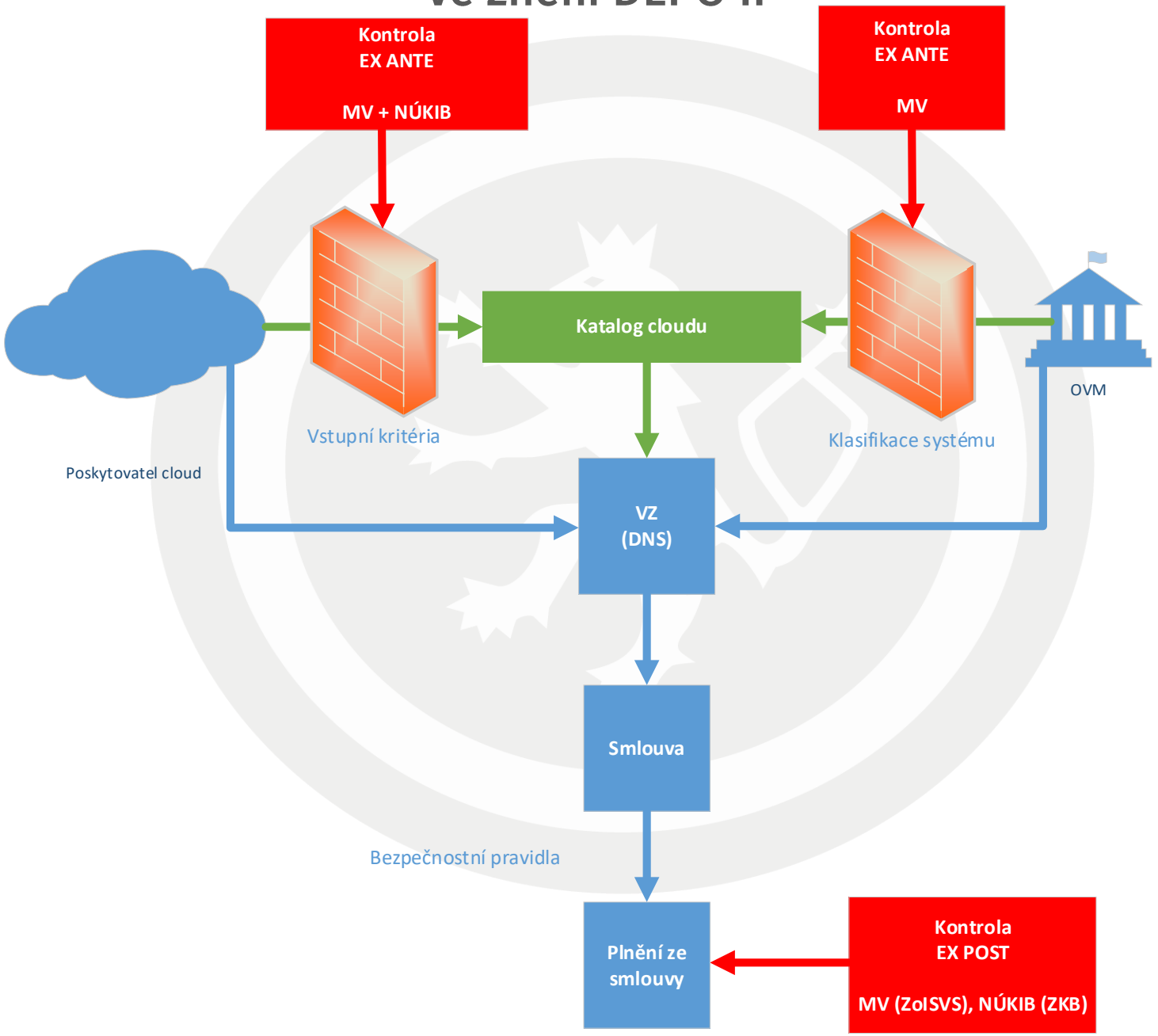
„(Informování) *by však mělo být provedeno **prokazatelně**, **adresně** a ve vztahu ke každému jednotlivému provozovateli **samostatně**. Podstatnými náležitostmi prokazatelnosti bude **informace o tom, že se jedná o provozovatele konkrétního systému podle zákona o kybernetické bezpečnosti**, s čímž 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

Regulace využívání cloudových služeb – cloudová vyhláška

Schéma schvalování poskytovatelů a nabídek cloud computingu ve znění DEPO II



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 †††† $$$$

Kritéria pro tzv. ex ante kontrolu

Schvalování poskytovatelů a nabídek cloud computingu ve znění DEPO II

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.

Zpracování dat mimo EU

- **Dle vyjádření zástupce poskytovatelů cloudových služeb za ICT UNII je zpracování dat mimo území EU/EHP**, nebo alespoň možnost takového zpracování**, 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.)

- Z pohledu NÚKIB, 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.

Například ze smluvních podmínek společnosti Microsoft vyplývá, že data posbíraná Microsoftem mohou být uložena kdekoli bude společnost Microsoft chtít.

Viz odstavec 99, str. 21 zprávy Evropského inspektora ochrany osobních údajů o vyšetřování podmínek využití služeb Microsoftu institucemi Evropské unie.
Dostupné online z: https://edps.europa.eu/data-protection/our-work/publications/papers/outcome-own-initiative-investigation-eu-institutions_en

Zpracování dat mimo EU – zrušení Privacy - Shield

Z vyjádření ÚOOÚ k rozsudku Evropského soudního dvora ve věci C-311/18 na přenos údajů mezi správcem v EU a zpracovatelem ve třetí zemi (USA) – zrušení tzv. Privacy-Shield vyplývá následující pro správce následují:

- V případě předání údajů do třetí země je třeba prověřit**, zda vhodné záruky a ochranná opatření v doložkách skutečně zajišťují srovnatelnou úroveň ochrany zaručené v Unii GDPR a Listinou.**
- **Brát v úvahu i relevantní prvky právního řádu třetí země**.
- Každý správce předávající údaje do USA by měl hledat a navrhovat řešení v podobě dalších bezpečnostních záruk (např. uložení dat včetně metadat pouze na území EU, šifrování bez zadních vrátek apod.).
- Dodržovat **zásadu transparentnosti a informovat subjekt údajů o konkrétních opatřeních a postupech, komu a do jakých zemí jsou údaje předány, za jakých podmínek, jak jsou chráněny, případně rizika s tím související**.

Viz ÚOOÚ k dopadům zrušení Štítu soukromí EU-USA na správce
Dostupné online z: 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 dat 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 důvěryhodnosti poskytovatele**
  - Zákazník dává svá data mimo své systémy do správy dalšího subjektu
  - Ex ante kontrola se snaží přiměřené posoudit rizika spojená s využíváním cloudových služeb
  - Pokud nebude Ex ante kontrola dostatečná nebude možné posoudit rizika související se zpracováním a exportem dat
- Pokud legislativa nebude stanovovat povolené nakládání s daty, bude pro zákazníka i regulátora **téměř nemožné efektivně řídit, dohlížet a kontrolovat objem dat, který je zpracováván mimo EU**
- Je téměř nemožné reálně zjistit přístup cizích entit – např. zahraničních bezpečnostních služeb v případě uložení mimo EU
- Problematický přístup k datům pro české bezpečnostní složky, pokud jsou data uložena v zemích bez dostatečné justiční spolupráce s ČR

Návrh NÚKIB k poskytnutí informací v ex ante kontrole a informování zákazníků (orgánů veřejné moci)

A. Aby poskytovatelé cloudových služeb poskytli v **EX ANTE** kontrole informace o **obvyklém/předpokládaném**:
   - **místu**,
   - **rozsahu**,
   - **době** a
   - **účelu** zpracování dat mimo území EU.

B. Aby poskytovatelé cloudových služeb poskytly zákazníkům (orgánům veřejné moci) v rámci veřejné zakázky a při plnění smlouvy informace o:
   - **místu**,
   - **rozsahu**,
   - **době** a
   - **účelu** zpracování dat.

Tak aby byl zákazník schopen vyhodnotit s ohledem na typ informací vkládaných do cloudu riziko, které dané zpracování představuje.

Návrh NÚKIB k EX ANTE kontrole - věcný záměr cloudové vyhlášky

Vstupní kritéria (ID 7)

Zákaznická data a provozní údaje jsou trvale a nepřetržitě uloženy výlučně na území členských států EU/EHP.

= vždy musí být dostupná na území EU/EHP – tím není vyloučeno zpracování jinde.
= zpracování/uložení mimo EU/EHP musí být dočasné

Vstupní kritéria (ID VK 8)

Zákaznická data a provozní údaje jsou zpracovávány na území členských států EU (EHP). Aniž je dotčeno pravidlo v ID 7, v **odůvodněných** případech, po **nezbytně nutnou dobu**, v **nezbytném** rozsahu **mohou být zákaznická data a provozní údaje zpracovávány i na území jiných států**, které zajišťují odpovídající úroveň ochrany ve smyslu čl. 45 GDPR, nebo jinde pokud materiální dodavatel poskytl vhodné záruky ve smyslu čl. 46, 47 GDPR.

Návrh NÚKIB k pravidlům pro OVM - věcný záměr cloudové vyhlášky

Bezpečnostní pravidla ID 1.2

Zákazník zajistí, že mu materiální dodavatel nebo prodejce poskytne v popisu systému a smluvních ujednáních jasnou a srozumitelnou **informaci o poloze** systémových komponent, včetně těch zajišťovaných systematickými zpracovateli, **ve kterých jsou nebo mohou být zákaznická data a provozní údaje zpracovávány, ukládány a zálohovány**.

Zákazník musí **být schopen určit polohu zpracování a ukládání zákaznických dat a provozních údajů** včetně záloh zákaznických dat a provozních údajů **podle smluvně dostupných možností.**

Zákazník dále zajistí, že u zákaznických dat a provozních údajů zpracovávaných mimo území členského státu EU/EHP poskytne materiální dodavatel popis toho, jak bude chráněn ve smyslu čl. 45, 46 a 47 GDPR.

Bezpečnostní pravidla ID 1.3

Zákazník zajistí, že mu materiální dodavatel nebo prodejce poskytne jasnou, srozumitelnou a průběžně aktualizovanou informaci o **důvodech**, pro něž ~~obvykle~~ dochází nebo může docházet při využívání cloudové služby ke zpracování zákaznického obsahu mimo území členského státu EU/EHP, ~~průměrnou~~ **dobu** po kterou je nebo může být zákaznický obsah ~~obvykle~~ zpracováván mimo území členského státu EU/EHP a ~~obvyklý~~ **rozsah** zákaznického obsahu, který je nebo může být zpracováván mimo území členského státu EU/EHP.

= zde je třeba uvádět co možná nejpřesněji, aby zákazník mohl posoudit rizika pro zpracování informací v jednotlivých zemích.

Obvyklý/předpokládaný údaj není dostatečný.

Bezpečnostní pravidla ID 1.4

Zákazník zajistí, že zákaznická data a provozní údaje jsou trvale a nepřetržitě uloženy výlučně na území členských států EU/EHP.

= míří primárně na dostupnost informací, nebrání zpracování mimo EU

Bezpečnostní pravidla ID 1.5

Zákazník zajistí, že zákaznická data a provozní údaje jsou zpracovávány na území členských států EU (EHP). Aniž je dotčeno pravidlo ID 1.4, v odůvodněných případech, **po nezbytně nutnou dobu, v nezbytném rozsahu mohou být zákaznická data a provozní údaje zpracovávány i na území jiných států**, které zajišťují odpovídající úroveň ochrany ve smyslu čl. 45 GDPR, nebo jinde pokud materiální dodavatel poskytl vhodné záruky ve smyslu čl. 46, 47 GDPR. Výjimky pro specifické situace dle čl. 49 GDPR nejsou dotčeny.

Jak to řeší jinde?

- **USA**
  - **Specifická situace – mají vlastní vládní cloud dedikovaný v USA**
  - **Komerční poskytovatelé vytvořili speciální nabídku jen pro USA**
  - **V ČR pravděpodobně neaplikovatelné**

- **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**
  - **Mají nepovinný standard C5 který definuje co mají zákazníci požadovat - nepovinné**

- **ESTONSKO**
  - **Umožňuje využití cloudu pro informace nízké důvěrnosti.**
  - **Pro informace vyšší důvěrnosti (včetně osobních údajů) vyžaduje šifrování v úložišti i při přenosu a držení šifrovacích klíčů výhradně zákazníkem (což dle informací z Estonska pro zpracování není možné – funkční pouze pro prosté úložiště)**
  - **Všechna data musí být v EU**

Bilance a výzvy pro regulaci v nejbližší době

- Posunout určování povinných osob
- Zlepšit zohledňování bezpečnosti v prostředí veřejných zakázek – bude nový podpůrný materiál
- Dokončit projekt metodiky k analýze rizik – bude nový podpůrný materiál
- Sjednocení hlášení kybernetických incidentů
- Zlepšení pokrytí odvětví zdravotnictví
- Navázání užší spolupráce s dalšími regulátory (zejména u kritické infrastruktury)
- **Dotáhnout problematiku regulace cloudu**
- **Neustále zvyšovat úroveň poskytovaných služeb**

Povinné osoby pod ZKB

Doposud určeno:

- 52 subjektů kritické informační infrastruktury se 120 systémy
  - V případě kritické informační infrastruktury aktuálně probíhá revize dosavadního určení

- 50 provozovatelů základních služeb s 55 systémy
  - V případě provozovatelů základní služby aktuálně probíhá proces určování (určují se vždy celá odvětví najednou)
  - Celkový počet finálně určených subjektů se odhaduje kolem 200 provozovatelů základní služby

Typické problémy určování jsou celková vytíženost odboru regulace (především cloudová vyhláška) a snaha subjektů vyhnout se regulaci za každou cenu.

DĚKUJI ZA POZORNOST

regulace@nukib.cz