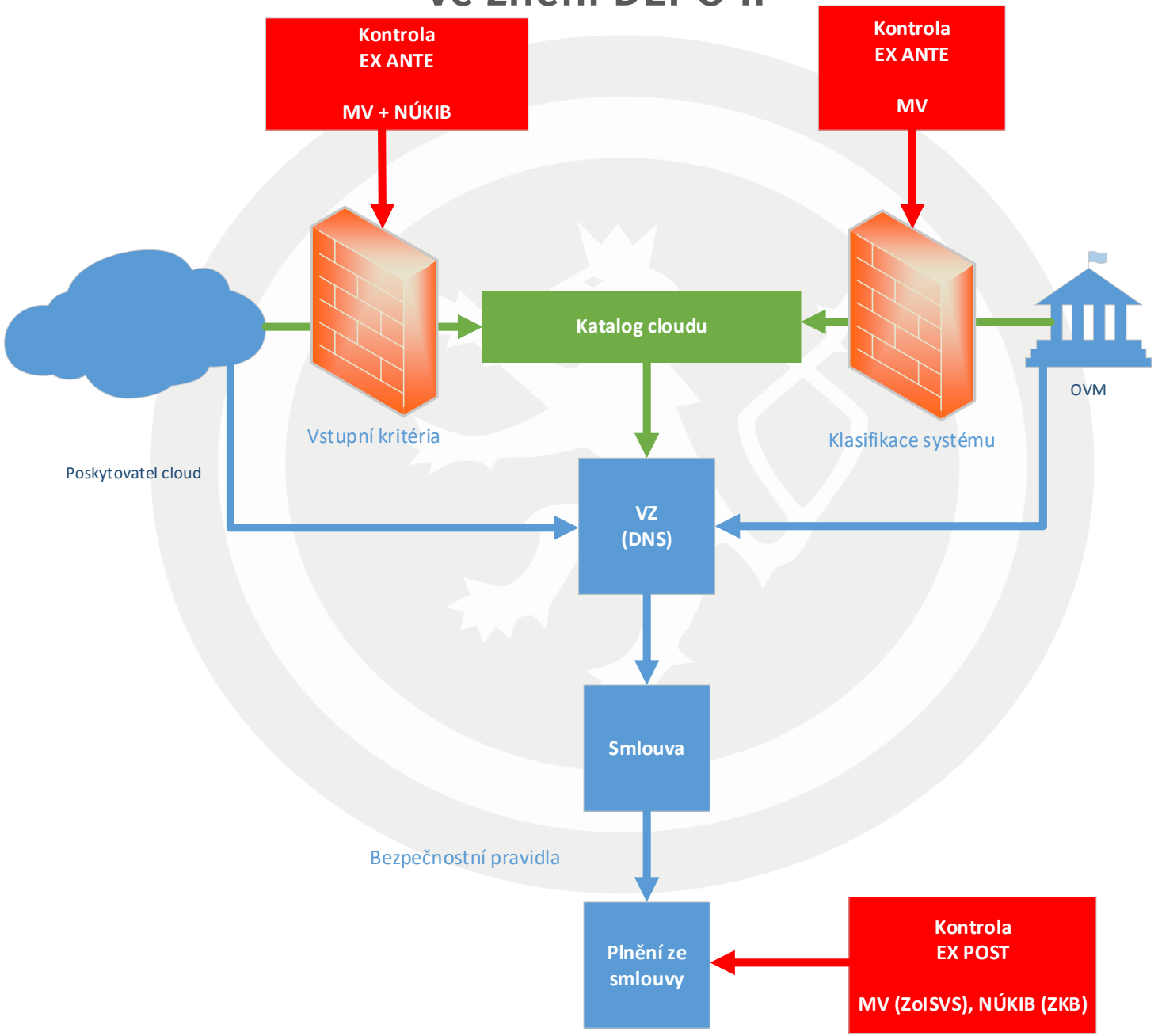
Regulace využívání cloudových služeb – cloudová vyhláška

CyberCon Brno 2020

Adam Kučínský
Národní úřad pro kybernetickou a informační bezpečnost
Odbor regulace

17. září 2020

Schéma schvalování poskytovatelů a nabídek cloud computingu ve znění DEPO II



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.

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

Cloudová vyhláška

Vstupní kritéria

- kritéria, která musí poskytovatel cloudových služeb splnit, **aby mohl vstoupit do tzv. katalogu nabídek** a nabídnout tak své služby orgánům veřejné moci
- kritéria budou rozdílné podle bezpečnostních úrovní služby.

- Obsah podstatně vychází:
  - ze **Souhrnné analytické zprávy** k projektu Příprava vybudování eGovernment cloudu schválené vládou ČR dne 14. 11. 2018 a
  - z **poznatků a diskusí expertní skupiny** vedené NÚKIB v období leden až červenec 2020.

Cloudová vyhláška

Bezpečnostní pravidla

- Záměrem není vytvořit duplicitu k VKB a stanovovat pravidla upravující informační bezpečnost uvnitř organizace zákazníka (např. vytváření systému informační bezpečnosti, klasifikace aktiv a hodnocení rizik, konkrétní technická opatření).

- Lze předpokládat, že zákazník podstatnou část z těchto pravidel zahrne do smluvních ujednání mezi ním a poskytovatelem ve fázi výběru konkrétního poskytovatele cloudových služeb.

- Obsah této části podstatně vychází z obsahu standardů zabývajících se bezpečností cloudových služeb, zejména z:
  - Cloud Computing Compliance Criteria Catalogue (C5:2020) od BSI
  - Úřední sdělení České národní banky ze dne 19. srpna 2016 k výkonu činnosti na finančním trhu – cloud computing
  - Obecné pokyny k outsourcingu u poskytovatelů cloudových služeb, vydané Evropskou pojišťovací asociací
  - ISO/IEC 27017:2015 Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002

Cloudová vyhláška

Stanovení bezpečnostních úrovní informačních systémů

- Informační systémy orgánů veřejné moci, které by měly být provozovány v cloudu, budou podle dopadů narušení bezpečnosti informací zařazeny do některé ze čtyř bezpečnostních úrovní (1 - nízká, 2 – střední, 3 – vysoká, 4 - kritická).

- Příslušně zařazený systém bude moci využít pouze ty nabídky služeb, které jsou zařazeny do stejné nebo vyšší bezpečností úrovně.

- Hodnocení důležitosti informačních systémů veřejné správy se hodnotí pomocí určení kritických dopadů narušení dostupnosti, důvěrnosti a integrity dat nebo ICT služby, na kterých je funkčnost hodnoceného IS závislá.

- Obsah zcela vychází ze Souhrnné analytické zprávy k projektu Příprava vybudování eGovernment cloudu.

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

DĚKUJI ZA POZORNOST

regulace@nukib.cz