Jak na nákup **cloudových služeb ve veřejné správě od 1. 1. 2024?**

Mgr. Dominik Vítek, Ph.D.
Mgr. Kryštof Lédl
Advokátní kancelář
PIERSTONE

Prvního ledna vstoupí finálně v účinnost pravidla podle tzv. cloudových vyhlášek, jež musí každá cloudová služba splnit. Jaký bude proces výběru dodavatele cloud computingu? Jak do něj zapadají jednotlivé cloudové vyhlášky? A jaký dopad budou mít pravidla pro využívání služeb cloud computingu ze strany orgánů veřejné správy do oblasti veřejného zadávání?

Pravidla pro využívání služeb cloud computingu ve veřejné správě vyplývají ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů (ZISVS) a z jeho prováděcích vyhlášek – cloudových vyhlášek. Daná pravidla se tak ve smyslu § 1 odst. 1 ZISVS uplatní pouze na orgány veřejné správy (OVS), tj. státní orgány, orgány územních samosprávných celků nebo státní právnické osoby. Ačkoliv tato pravidla nabyla účinnosti již v srpnu 2020, s následnou významnou novelizací v září 2021, fakticky se v praxi uplatní až od 1. 1. 2024. Bude tak možné využívat pouze cloudové služby, které jsou zapsané na 1url.cz/@cloud1, zatímco nabídky zapsané podle předcházejících předpisů, dostupné na 1url.cz/@cloud1a, již zcela přestanou platit.

S letošním rokem končí poslední z přechodných období stanovených ZISVS, kdy mohly OVS využívat služby cloud computingu zapsané v jeho katalogu před zářím 2021, tj. před účinností aktuálního znění zmíněného zákona. Pokud tedy některá cloudová služba nebude k 1. 1. 2024 zapsaná pod výše uvedeným odkazem, nebudou ji OVS moci nadále využívat.

Většinu bezpečnostních požadavků mohou poskytovatelé doložit pomocí ISO certifikátů

Katalog cloud computingu

Podle ZISVS platí, že OVS mohou využívat pouze služby cloud computingu zapsané v katalogu cloud computingu (katalog CC), spravovaném Digitální a informační agenturou (DIA). Požadavky na zápis neplatí jen pro samotné služby, ale rovněž pro jejich poskytovatele, kteří musejí projít clearance procesem a prokázat tak, že nejsou bezpečnostní hrozbou pro Českou republiku. Rámcové požadavky na zápis služeb cloud computingu a jejich poskytovatelů do katalogu CC upravuje primárně ZISVS, přičemž je specifikuje cloudová vyhláška – č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (vyhláška o vstupních kritériích). Ta obsahuje požadavky na zápis poskytovatele cloud computingu do katalogu CC a rovněž podrobné požadavky na zápis cloudových služeb (příloha č. 2, resp. přílohy č. 2–5).

Celá úprava vychází z kategorizace cloudových služeb do čtyř bezpečnostních úrovní (BÚ) – nízká, střední, vysoká a kritická. Orgány veřejné správy tak musejí využívat výhradně cloudové služby registrované v katalogu CC na stejné či vyšší bezpečnostní úrovni, než má infor-

mační systém OVS, pro nějž daný orgán veřejné správy hodlá službu cloud computingu využívat. Bezpečnostní úrovně stanovuje vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (vyhláška o bezpečnostních úrovních). OVS mají zároveň povinnost kategorizovat své informační systémy do popsaných bezpečnostních úrovní – BÚ cloudové služby tak musí být stejná nebo vyšší než BÚ příslušného informačního systému.

Zápis poskytovatele a cloudových služeb do katalogu CC

První fázi registrace do katalogu CC představuje zápis poskytovatele. Každý poskytovatel cloud computingu musí prokázat splnění požadavků dle ZISVS a přílohy č. 1 vyhlášky o vstupních kritériích. Splnění jejích požadavků je třeba prokázat v rámci podané žádosti o zápis poskytovatele. Vyhodnocení splnění daných požadavků je pak v kompetenci DIA a nepřímo rovněž Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), který k registraci vydává závazná stanoviska. Všichni registrovaní poskytovatelé jsou uveřejněni na 1url.cz/@cloud1b.

Každý registrovaný poskytovatel musí rovněž registrovat své cloudové služby. Pouze tak mohou být následně nakupovány a využívány ze strany OVS. Zápis služeb probíhá podle jednotlivých bezpečnostních úrovní, kde BÚ 1 je v zásadě jen formálním procesem, zatímco registrace do BÚ 3 a 4 znamená komplexní proces, kde každá zapisovaná služba musí splnit souhrnný set požadavků. Týkají se například místa a zpracování dat v rámci služeb cloud computingu, certifikace služeb cloud computingu (ISO certifikace, SOC 2 Type II auditní zprávy apod.), šifrování dat atd. Bezpečnostních požadavků týkajících se služeb cloud computingu existuje přibližně 50 a liší se podle bezpečnostní úrovně služby. Nejpřísnější platí pro BÚ 4 – kritická; nicméně v BÚ 4 nemůže být služba poskytována komerčními poskytovateli, nýbrž pouze tzv. státním poskytovatelem cloud computingu, jenž ke dni naší uzávěrky stále nebyl určen.

Většinu bezpečnostních požadavků mohou poskytovatelé doložit prostřednictvím ISO certifikátů, zejména řady 27xxx, tedy ISO 27001, 27017 a 27018.

Veškeré zapsané služby jsou uveřejněny na 1url.cz/@cloud1. Zároveň platí, že takto registrované cloudové služby – které legislativa a katalog CC poměrně nešťastně označují jako „nabídky cloud computingu" – musejí párovat na tzv. poptávky cloud computingu. V praxi to nicméně znamená, že DIA vypíše vzorové kategorie služeb, pro které poskytovatelé registrují své služby („nabídky cloud computingu"). Pokud by OVS zamýšlel nakoupit nějakou cloudovou službu, pro kterou zatím

neexistuje poptávka, může požádat DIA o její zápis.

Povinnosti OVS/OVM při zabezpečení cloudových služeb

Vedle požadavků cloud computingu existuje rovněž set bezpečnostních požadavků, jež dopadají přímo na orgány veřejné správy. Nejedná se tudíž o povinnosti poskytovatelů, nýbrž samotných OVS, které chtějí cloudové služby využívat. Daná bezpečnostní pravidla stanovuje poslední ze tří cloudových vyhlášek, č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu (vyhláška o bezpečnostních pravidlech). Jejich kontrola neprobíhá preventivně neboli ex ante, ale pouze v případě náhodných kontrol čili ex post.

Zmíněná vyhláška stanovuje minimální požadavky pro využívání cloud computingu, jež se vztahují ke kompletnímu životnímu cyklu služby. Některé se již překrývají s požadavky vyhlášky o vstupních kritériích – například na místo uložení a zpracování dat, šifrování a certifikaci. OVS tak mají jistotu, že jim poskytovatelé zapsaní v katalogu CC umožní splnit většinu požadavků podle vyhlášky o bezpečnostních pravidlech. Daný překryv ovšem není stoprocentní a zbytek požadavků musí orgán splnit sám. Jsou zde například požadavky na fyzickou bezpečnost, exit strategii či na právo OVS odstoupit od smlouvy s poskytovatelem cloud computingu.

Ačkoliv v článku zmiňujeme povinnost zajistit plnění pravidel podle vyhlášky o bezpečnostních pravidlech pouze ve vztahu k OVS v působnosti ZISVS, z aktuálního znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (ZKB) vyplývá, že jejich dodržování musejí zajistit všechny orgány veřejné moci. NÚKIB však v dané souvislosti vydal podpůrný materiál Regulace využívání cloud computingu orgány veřejné moci v zákoně o kybernetické bezpečnosti (dostupný na 1url.cz/@cloud1c), podle něhož hodlá povinnosti plynoucí z dané vyhlášky vztahovat jen na OVS dle ZISVS a do budoucna sjednotit regulaci využívání služeb cloud computingu pouze pod uvedený zákon.

Dopady cloudových vyhlášek do zadávání VZ

Jak se tedy cloudové vyhlášky promítnou přímo do oblasti veřejného zadávání? Ačkoliv z výše uvedeného vyplývá, že se vyhlášky o vstupních kritériích a o bezpečnostních úrovních týkají primárně první fáze při výběru dodavatele cloud computingu, mají také určitý dopad na zadávací řízení. DIA ve svém dokumentu Minimální smluvní podmínky smlouvy na dodávku služby cloud computingu (viz 1url.cz/@cloud1d) uvádí, že by měly OVS minimálně zajistit: že (i) zadávací podmínky budou obsahovat podmínku zapsání poskytovatele (dodavatele) a jeho služeb v katalogu cloud computingu; a že (ii) bude smlouva obsahovat povinnost poskytovatele splňovat v průběhu její platnosti veškerá bezpečnostní opatření stanovená vyhláškou o vstupních kritériích pro danou bezpečnostní úroveň. Nad rámec doporučení DIA lze doplnit, že by měly zadávací podmínky stanovit, aby byla dodávaná služba cloud computingu stejné či vyšší bezpečnostní úrovně než informační systém OVS.

Orgány veřejné správy však budou muset do zadávacích podmínek obzvlášť promítnout požadavky podle vyhlášky o bezpečnostních pravidlech. Ani ona, ani jiné právní předpisy přímo nestanoví, jakým konkrétním způsobem se mají dané

požadavky do zadávací dokumentace zanést. Citovaný dokument DIA vyhlášku o bezpečnostních pravidlech ani nezmiňuje. Forma reflektování jejích požadavků tak bude primárně záviset na zvoleném druhu zadávacího řízení, s nejvyšší pravděpodobností však budou většinově vymezeny v rámci technických požadavků, jejichž nesplnění může vést k vyloučení dodavatele ze zadávacího řízení. Některé požadavky vyhlášky o bezpečnostních pravidlech bude nutné rovněž promítnout přímo do (vzorové) smlouvy s dodavatelem, která by měla tvořit součást zadávacích podmínek – typicky půjde o pravidla ohledně práva OVS odstoupit od smlouvy, pravidla ohledně poskytování zákaznických dat apod.

Vyhláška o bezpečnostních pravidlech nicméně nedopadá pouze na nová zadávací řízení: Její pravidla se musejí po 1. 1. 2024 implementovat také do již uzavřených smluv o dodávce služeb cloud computingu, které má OVS uzavřeny. Orgány veřejné správy by si tak měly se svými poskytovateli cloud computingu s předstihem dohodnout úpravu stávajících smluvních podmínek v souladu s úpravou dané vyhlášky.

Podle § 4 vyhlášky o bezpečnostních pravidlech platí: „Orgán veřejné moci, který využívá službu cloud computingu na základě smlouvy s poskytovatelem uzavřené přede dnem nabytí účinnosti této vyhlášky nebo smlouvy, která byla uzavřena na základě smlouvy uzavřené přede dnem nabytí účinnosti této vyhlášky, zajistí dodržování bezpečnostních pravidel pro poskytování služby cloud computingu stanovených touto vyhláškou od 1. ledna 2024.“

Požadavky ZKB a implementace NIS2 do českého právního řádu

Není vyloučeno, aby se na OVS spadající pod působnost ZISVS vztahovaly rovněž požadavky zákona o kybernetické bezpečnosti a prováděcích předpisů, zejména vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (VKB). V takovém případě bude muset orgán veřejné správy při výběru poskytovatele cloud computingu zohlednit rovněž požadavky ZKB a VKB, pokud se má poptávaný cloud computing využívat pro službu regulovanou danými předpisy. Nicméně i zadavatelům, kteří nespadají mezi OVS, a nejsou tak povinni dodržovat pravidla pro využívání služeb cloud computingu podle ZISVS a cloudových vyhlášek, lze doporučit využívat primárně služby cloud computingu zapsané v katalogu CC. U nich totiž mají větší jistotu, že poskytují dostatečnou úroveň kybernetické bezpečnosti a že mohou pravděpodobně naplnit i požadavky podle ZKB a VKB.

Aktuálně se připravuje nový zákon o kybernetické bezpečnosti, jenž má do českého právního řádu implementovat tzv. NIS2 směrnici (směrnice EP a Rady č. 2022/2555, o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii). Ke dni naší uzávěrky se uvedený materiál nacházel ve stavu, kdy byly vypořádávány připomínky podané v meziresortním připomínkovém řízení. NIS2 přitom výrazně rozšiřuje rozsah subjektů, které budou povinny se požadavky na kybernetickou bezpečnost řídit: Z dosavadních asi 360 regulovaných subjektů se předpokládá nárůst zhruba na 6 000 a veřejná správa by pod požadavky tohoto zákona o kybernetické bezpečnosti měla spadnout v zásadě kompletně.

Společně s návrhem nového zákona o kybernetické bezpečnosti se navíc projednává návrh doprovodného zákona, který předpokládá vydání nové vyhlášky o bezpečnostních úrovních a vyhlášky o bezpečnostních pravidlech – nově však na základě zmocnění dle ZISVS, nikoliv podle zákona o kybernetické bezpečnosti. Záměrem vydání nových vyhlášek je ovšem primárně pouze sjednocení úpravy využívání služeb cloud computingu pod ZISVS a jejich znění by se nemělo výrazně lišit od vyhlášek aktuálně účinných.

SHRNUTÍ

- **Od 1. 1. 2024 se v plné míře uplatní pravidla pro využívání služeb cloud computingu vyplývající ze ZISVS a jednotlivých cloudových vyhlášek. Veškeré dosud zapsané a využívané služby tak bude možné využívat, pouze pokud budou registrovány i podle nových pravidel, a tedy propsány na 1url.cz/@cloud1.**
- **Každý OVS musí navíc zajistit splnění podmínek podle vyhlášky č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.**
- **OVS v pozici zadavatelů musejí v zadávacích podmínkách zohlednit bezpečnostní požadavky vyplývající z cloudových vyhlášek.**