12. 2. 2024

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Jak se mění regulace cloudu v roce 2024?

Používáte nebo poskytujete služby v oblasti cloudových technologií? Měli byste zbystřit, jelikož rok 2024 přináší řadu legislativních změn. Evropská certifikace je za dveřmi, orgány veřejné správy čeká ukončení spolupráce s neověřenými provozovateli cloudových služeb a také soukromí poskytovatelé narazí na novinky nejen ve smluvní dokumentaci. Pojďme si nové povinnosti představit detailněji.

Používání cloudových služeb kontinuálně roste. Objevuje se čím dál více SaaS[1] startupů a na cloud přechází již i veřejný sektor. Růst popularity cloudových technologií ještě zrychlila nedávná pandemie a v příštích letech se stále očekává růst o desítky procent ročně. Cloudové technologie jsou levné a efektivní, ale nesou s sebou bezpečnostní riziko, jelikož jakákoliv cloudová služba je druhem outsourcingu. Z toho důvodu existují jak na české, tak i na evropské úrovni typické snahy o regulaci. Od nového roku jsou v České republice legislativní změny v regulaci cloudu hned dvě.

Evropská certifikace

V rámci Evropské unie se připravuje pod právním rámcem Cybersecurity Actu (Reg. 2019/881) jednotná evropská kyberbezpečnostní certifikace pro produkty, služby a procesy, která bude platit pro celý jednotný trh. Právní úprava je již účinná a aktuálně se dokončují schémata, která budou stanovovat konkrétní pravidla pro certifikaci jednotlivých sektorů. Prvním schématem, které přijala Evropská komise 31. ledna 2024 je schéma certifikace pro ICT produkty (EUCC) a lze očekávat, že brzy bude následovat i schéma pro cloudové služby (EUCS) a schéma pro 5G sítě (EU5G).

Ačkoliv certifikace zatím nebude povinná, počítá se s tím, že zájem o ni bude napříč jednotným trhem velký. Lze totiž předpokládat, že tyto standardy budou používat technologické společnosti, které chtějí demonstrovat svoji bezpečnost, veřejní zadavatelé se budou na tyto standardy odkazovat v zadávacích řízeních, a i poptávka spotřebitelů bude oceňovat ověřené a bezpečné produkty a služby. Je proto dobré nezaspat a být v této oblasti aktivní již dnes.

Česká regulace cloudu

V Česku je regulace cloudu rozdělena do dvou zákonů, které na sebe svojí právní úpravou navazují. Prvním je zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS) a zákon č. 181/2016 Sb., o kybernetické bezpečnosti (ZKB), který navíc čekají zásadní změny v reakci na směrnici NIS 2.

Na rozdíl od evropské regulace je česká právní úprava již několik let účinná a po novelizaci DEPO (zákonem č. 261/2021 Sb.) je od 1. 9. 2021 zbavena i původních legislativních neduhů.[2] Dopadá na orgány veřejné správy, kterým nařizuje využívat pouze ty cloudové služby, jenž jsou zapsány v katalogu cloud computingu, což je veřejný seznam, kam se zapisují jak nabídky či poptávky služeb cloud computingu, tak i cloudové služby které orgány veřejné správy již aktuálně využívají. Využívá-li orgán veřejné správy cloudové služby, které nejsou zapsány v katalogu, musí jejich využívání ze zákona ukončit nejpozději do 12 měsíců od momentu kdy se o tom dozví.

To nepřímo tlačí soukromé společnosti zapisovat se do katalogu cloud computingu. K tomu ale potřebují nejprve zapsat sebe jako poskytovatele a následně pak i své služby, a to do některé ze čtyř definovaných bezpečnostních úrovní. Podmínkou pro zápis je ale splnění požadavků, které Digitální

informační agentura (DIA) spolu s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) prověřují.

Ptáte se, proč není povědomí o této povinnosti vyšší? Domníváme se, že za to může přechodná lhůta, která umožňovala, aby orgány veřejné správy využívaly služby nezapsané do katalogu, pokud orgán veřejné správy začal využívat danou službu cloud computingu před 1. zářím 2021. V takovém případě bylo možné cloudovou službu dosud používat. Platnost této výjimky ale skončila na konci roku 2023 a v roce 2024 již nebude možné nejen začít využívat nezapsané služby, ale ani pokračovat v používání dříve vysoutěžených cloudových služeb.

Povinná ustanovení ve smlouvách o poskytování cloudu

Druhá část regulace dopadá na orgány veřejné moci, které jsou současně orgány veřejné správy dle ZoISVS.[3] Těm vyhláška o bezpečnostních pravidlech stanoví konkrétní požadavky, které musí ve svých smlouvách o využívaní služeb cloud computingu povinně sjednat. V závislosti na příslušné bezpečnostní úrovni se tak jedná například o požadavky na lokalizaci dat, ISO certifikace, systém řízení bezpečnosti informaci, zálohováni dat, dobu ukládaní provozních údajů nebo šifrovaní. Tímto jsou opět k dodržování těchto pravidel nepřímo nuceni i soukromí poskytovatelé cloud computingu, kteří tyto smlouvy uzavírají.

Každá nově uzavřená smlouva orgánu veřejné moci s poskytovatelem cloud computingu by tak měla obsahovat smluvní ujednání, která zajistí, že bude cloudová služba soukromým poskytovatelem splňovat určitý bezpečnostní standard stanovený novou vyhláškou z července 2023.

Tato povinnost však nedopadá pouze na nově uzavírané smlouvy cloud computingu, ale také na již zavedené cloudové služby. Smlouvy k nim se tak budou muset „dodatkovat“. Ačkoliv se jedná o povinnost, která byla v ZKB již déle, konkrétní bezpečnostní požadavky byly představeny až v červenci 2023, a proto je vhodné svoji cloudovou smluvní dokumentaci v roce 2024 aktualizovat. V opačném případě hrozí až milionová pokuta.

Závěr

Cloudové technologie bývají označovány za budoucnost v poskytování informačních technologií,[4] a proto není divu, že se jejich provoz začíná více regulovat. Pozor by si měly dát tedy orgány veřejné správy, které mají ze zákona povinnost ukončit v roce 2024 spolupráci s dosavadními poskytovateli cloudových služeb, pokud nejsou zapsáni v katalogu cloud computingu a s těmi dosavadními upravit svoji smluvní dokumentaci.

Změna se však týká i soukromých poskytovatelů cloudu, kterým doporučujeme upravit své smluvní vzory a v případě zájmu o poskytování služeb také veřejnému sektoru se zapsat do katalogu cloud computingu.

Specializovaný tým HAVEL & PARTNERS má zkušenosti jak s úpravou nezbytné smluvní dokumentace, tak i se zápisy významných technologických společností do katalogu cloud computingu nebo spory před regulátorem a rád se všemi aspekty cloudu efektivně pomůže.

JUDr. Jakub Klodwig
Koncipient

Mgr. Pavel Amler
Vedoucí advokát

JUDr. Dalibor Kovář
Partner

HAVEL & PARTNERS
ÚSPĚCH SPOJUJE

HAVEL & PARTNERS s.r.o., advokátní kancelář

Florentinum, recepce A
Na Florenci 2116/15
110 00 Praha 1

Tel.: +420 255 000 111
Fax: +420 255 000 110
e-mail: office@havelpartners.cz

[1] SaaS neboli „software as a service“ znamená poskytování softwaru jako služby.

[2] KLODWIG, Jakub. Příručka právní regulace cloudu. Brno: Nugis Finem Publishing, [2022]. ISBN 978-80-7614-008-0.

[3] Viz výkladové stanovisko NÚKIB k § 4 odst. 5 ZKB, dostupné na 2023-07-14_vyklad-ust-par-4-odst-5_v1.1.pdf (gov.cz).

[4] KLODWIG, Jakub. Data jsou nové zlato. Podcasty 21. [12.12.2023]. Dostupné na: Jakub Klodwig: Data jsou nové zlato | Právo21 – Právo srozumitelně a pro všechny (pravo21.cz).

Další články:

- Hodnotící dotazníky jako obchodní sdělení v kontrolním plánu ÚOOÚ pro rok 2026
- Konec „severních ateliérů“? Nový stavební zákon otevírá dveře k rekolaudaci ubytovacích jednotek na plnohodnotné byty
- Byznys a paragrafy, díl 33.: Prevence střetu zájmů (jednatel × společnost)
- Jak se vyhnout zákazu a postihu dohod o určování cen pro další prodej?
- Střet zájmů členů volených orgánů obchodních korporací: pravidla, proces a následky
- Nová „tlačítková” povinnost pro e-shopy
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Zákon Lugového: jak Rusko přepisuje pravidla mezinárodních arbitráží
- Novelizace nařízení EU o odlesňování (EUDR)