17. 8. 2022

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

Cloudy a právo - 2 díl: Tisíc a jeden právní požadavek

Jaké právní otázky musí zákazník řešit při využívání cloudových služeb? Co je naopak důležité pro poskytovatele cloudu?

V předchozí části článku[*] jsme vymezili pojem cloudové služby, jejich jednotlivé druhy a typy, a zdůraznili několik okruhů práva, které je nutné při nabízení či využívání cloudových služeb uplatnit. V tomto článku dotčené oblasti probereme do většího detailu. Zdůrazníme klíčové aspekty, které by jak poskytovatel cloudu, tak jeho zákazník měli zvážit, aby se vyhnuli pozdějším problémům. A ty mohou být skutečně různé, od ztráty kontroly nad svými citlivými informacemi, úniku klientských dat, nefungování služby, až po pokuty od různých dozorových úřadů.

Čím začít?

V minulém článku jsme vymezili pět zásadních oblastí práva, které je nutné při poskytování nebo využívání cloudových služeb řešit. Neříkáme tím, že neexistují i další právní souvislosti, resp. předpisy a pravidla, jejichž aplikace by v některých případech přicházela v úvahu. V některých situacích mohou být relevantní rovněž předpisy daňové (odlišný daňový režim pro nákup vlastní vybavení a cloudové služby), jindy pracovněprávní (sledování práce zaměstnance v cloudovém prostředí). V některých specifických případech může být cloud i prostředkem pro spáchání trestného činu. V následujícím textu se však budeme zabývat jen těmi oblastmi, které jsou průřezové a které mají či mohou mít dopad na velkou většinu situací a subjektů využívajících cloudové řešení.

Jedná se o tyto oblasti:

- Péče řádného hospodáře
- Odpovědnost za poskytování produktů a služeb
- Autorské právo
- Ochrana informací
- Sektorová regulace; v některých sektorech existují detailní pravidla upřesňující možnosti využití cloudu. Nejvýznamnějšími případy je veřejná správa a samospráva a finanční sektor. Těmito dvěma oblasti se proto budeme zabývat v samostatných článcích.

Péče řádného hospodáře a cloud

Jedním z nejčastějších argumentů pro využívání cloudových služeb je jejich snadná dostupnost a ekonomická výhodnost.[1] Pro řadu organizací platí, že je jistě jednodušší, rychlejší a levnější využít infrastrukturu, platformu či software provozovaný někým jiným, než jej kupovat, vyvíjet a spravovat vlastními silami.

Ani tento obecný, či spíše obecně přijímaný závěr, však nezbavuje osoby odpovědné za hospodaření s majetkem dané organizace jejich odpovědnosti.

Povinnost péče řádného hospodáře, tzn. povinnost postupovat při správě majetku soukromoprávní organizace či organizační složky státu s odbornou péči, odpovědně a informovaně, nalezneme

především ve dvou předpisech: občanském zákoníku a zákonu o majetku České republiky a jejím vystupování v právních vztazích.

Občanský zákoník v § 159 odst. 1 ukládá každému, kdo přijme funkci ve voleném orgánu právnické osoby (zejména statutární orgány nebo dozorčí rada), aby jednal s péčí řádného hospodáře, loajálně a pečlivě. Pokud tak neučiní, ručí za způsobenou škodu celým svým majetkem.

V případně organizačních složek státu a obchodních společností, které stát ovládá, je úprava velmi obdobná. Podle § 47 odst. 1 zákona o majetku České republiky a jejím vystupování v právních vztazích platí, že fyzická osoba, která, stručně řečeno, rozhoduje či se podílí na rozhodování o majetku České republiky, je povinna postupovat s odbornou péčí. V opačném případě § 47 odst. 2 téhož předpisu uvádí, že dané osobě hrozí občanskoprávní, pracovněprávní a trestněprávní důsledky.

Jinak řečeno, fyzická osoba, která rozhoduje nebo se podílí na rozhodování o tom, že daná organizace využije (nakoupí) cloudové řešení, je, stejně jako při ostatních důležitých rozhodnutích, odpovědná za to, že toto rozhodnutí učinila po pečlivé úvaze a v zájmu dané organizace. I v případě výběru cloudového řešení tak lze silně doporučit zhodnocení ekonomické výhodnosti a zdokumentování jeho výsledku. Podle výše plnění a významu cloudového řešení pro zajištění dalších činností organizace je pak rovněž vhodné nastavit pravidelný přezkum, např. jednou ročně, zda je tento produkt pro organizaci stále výhodný nebo zda se situace změnila a je v zájmu organizace způsob využití cloudu změnit nebo opustit.

Z pohledu poskytovatele cloudového řešení z toho plynou dva základní požadavky.

Prvním je schopnost doložit garantované parametry poskytovaného řešení, ať už se týká jeho funkčnosti, dostupnosti, ochrany dat atd., aby se zákazník o ekonomické výhodnosti daného řešení mohl kvalifikovaně přesvědčit. To platí jak pro jednání před vznikem smlouvy, tak i pro průběžné ověřování činnosti poskytovatele cloudu. Řada právních úprav, od GDPR[2] až po kybernetickou bezpečnost, formuluje právní povinnost, dle které zákazník musí mít možnost ověřit, auditovat, způsob plnění cloudových služeb, a to včetně kontroly na místě. Poskytovatel cloudu by proto měl mít nastaven alespoň základní proces, jakým způsobem bude s kontrolou či auditem ze strany zákazníka spolupracovat.

A druhým je připravenost tyto záruky vtělit do smlouvy. Zákazník, který bude správu svého majetku důsledně řešit, by měl požadovat mj. záruky za řádné fungování služby, nastavená pravidla pro řešení chyb a incidentů, náhradu škody způsobené výpadkem, případně smluvní pokutu. Poskytovatel cloudu proto musí zvážit, jaké záruky může poskytnout, ve které části své služby například závisí na dodávkách od dalších subdodavatelů, a proto může poskytnout jen nějakou garanci.

Využití cloudu nezbavuje odpovědnosti za vlastní činnost

Tuto část můžeme rozdělit do dvou dílčích oblastí: Veřejnoprávní odpovědnost za činnost organizace, která dopadá na subjekty soukromého i veřejného sektoru, a **soukromoprávní odpovědnost** vůči koncovým klientům, která se uplatní především u obchodních korporací.

K **veřejnoprávní odpovědnosti** lze uvést, že ani využití cloudového nástroje nezbavuje organizaci odpovědnosti za její činnost a soulad s regulací.

Cloudové řešení může být součástí řady agend a činností, které podléhají specifické regulaci. Může se jednat například o způsob komunikace se spotřebitelem[3] nebo o zpřístupnění předsmluvních informací[4] v aplikaci, která využívá právě cloudu. Cloudové řešení může být používáno pro evidenci odpracované doby[5], vedení zdravotnické dokumentace[6] nebo archivaci dokumentů,

které je organizace povinna uchovávat po zákonem stanovenou dobu[7].

Za dodržování obecně závazných právních předpisů je odpovědná každá organizace, na kterou se tyto předpisy vztahují, bez ohledu na to, jaké technické prostředky využívá. Jinak řečeno, neschopnost doložit dokumenty či informace, které je organizace povinna po určitou dobu uchovávat, je problémem, ať už byly uloženy na hardware ve sklepě budovy, nebo do cloudu na druhém konci světa.

Praktické důsledky jsou obdobné těm v předchozím bodě: Organizace by si měla zmapovat, jaké její činnosti budou na cloudovém řešení závislé a jaké jsou s nimi spojené veřejnoprávní povinnosti. A podle míry jejich detailu, závažnosti či komplexnosti se pak pokusit ve smlouvě vyjednat co nejdetailnější garanci úrovně a dostupnosti služeb. Z pohledu poskytovatele opět platí, že musí zvážit, k čemu se může ve smlouvě reálně zavázat a co garantovat. Pokud by se zavázal například k vysoké dostupnosti informací, která by však v praxi byla výrazně nižší, a jeho zákazník by kvůli tomu dostal pokutu, mohl by chtít tuto pokutu následně po poskytovateli uhradit.

Soukromoprávní odpovědnost je relevantní pro soukromoprávní organizace, které jsou odpovědné svým koncovým klientům za to, že jim budou poskytovat služby či produkty v domluveném rozsahu a způsobem. Ať už jako cloud využívají infrastrukturu, na které provozují své interní systémy, platformu pro rozvoj e-shopu nebo celou aplikaci, jejímž prostřednictvím uzavírají smlouvy a poskytují plnění koncovým uživatelům, vždy to jsou ony, kdo vstupují do smluvního vztahu se zákazníky a jsou odpovědné za poskytnutí služeb v domluvené kvalitě.

Skutečnost, že pro poskytnutí služby je organizace závislá na funkčnosti a dostupnosti využívaného cloudu, jí této odpovědnosti nezbavuje. Organizace se ani své odpovědnosti nemůže zprostit, například ve smlouvě či obchodních podmínkách.

Z tohoto důvodu je z pohledu zákazníka nezbytné nejen co nejpřesněji upravit požadavky na poskytovanou cloudovou službu (dostupnost, funkčnost atd.), ale upravit i odpovědnost poskytovatele cloudu za škodu způsobenou zákazníkovi tím, že cloudová služba nebude dohodnuté podmínky splňovat.

Z pohledu poskytovatele cloudu a posílení jeho právní jistoty při poskytování služeb i v případném sporu pak z podstaty věci platí opačný přístup: Poskytované služby, související postupy (např. odstraňování chyb a výpadků) a záruky poskytovatele ve smluvní dokumentaci popsat spíše obecněji. Podoba výsledné smlouvy pak bývá výsledkem odlišné vyjednávací pozice a síly obou zúčastněných, když typicky u velkých poskytovatelů cloudových služeb se o předem připravené smluvní dokumentaci vyjednává jen obtížně.

Autorské právo a cloud

Pokud si zákazník nechá určitý software provozovat v cloudu, zejména v případě cloudu typu IaaS nebo PaaS, si měl by si ověřit, zda je k takovému užití software oprávněn. Licence může totiž tento způsob užití software zcela zakazovat, případně může pro takové užití aplikace stanovit odlišné poplatky, než pro užití na vlastním technickém vybavení zákazníka (tzv. on-premise). Typicky se bude jednat o situace, kdy jsou poplatky za využití software stanovené podle používaných serverů či virtuálních serverů nebo procesorů či virtuálních procesorů.

Další zásadní oblastí, na kterou by se měl zákazník zaměřit, je získání dostatečných oprávnění ke kreativním dílům vytvořeným při migraci do cloudu. Hlavním cílem tohoto kroku je, aby při ukončení používání cloudových služeb byl schopen provoz software sám převzít, případně jím pověřit jiného poskytovatele. Totéž platí o získání práv ke know-how cloudového poskytovatele v této oblasti.

Podrobněji se tomuto tématu budeme věnovat v následujícím článku.

V cloudu je klíčová ochrana informací

Poskytovatel cloudu z podstaty věci vždy má nebo technicky může mít přístup k informacím, které jeho prostřednictvím zákazník uchovává nebo zpracovává. I v případě, kdy jsou data zašifrována a poskytovatel cloudu nemá k dispozici šifrovací klíč, může svojí činností či naopak nečinností způsobit, že zákazník se ke svým datům nedostane, nebo že se k nim dostane ten, kdo by neměl. Ochrana informací je tak jednou z klíčových otázek.

Z pohledu zákazníka je vhodné si ujasnit, k jakým datům může mít přístup poskytovatel cloudu, byť jen teoreticky nebo v omezených případech, typicky při opravě incidentů, jak jsou tato data citlivá a zda je jejich ochrana předmětem samostatné právní úpravy.

Z těch nejčastějších kategorií důvěrných informací můžeme zmínit tyto:

- Obchodní tajemství

  Obchodním tajemstvím české právo rozumí konkrétní, veřejně nedostupné a ocenitelné informace související s podnikáním, resp. závodem, u nichž jejich vlastník zajišťuje jejich utajení[8]. Může se jednat jak o informace o ekonomické situaci a výkonnosti dané organizace, ale i o jejích dodavatelích, přípravě nových produktů, úpravě designu webových stránek či mobilní aplikace, úmyslu zahraniční expanze atd. Stejná ochrana je typicky smlouvou svěřována také dalším chráněným informacím, které sice definici obchodního tajemství nesplňují, ale u nichž má zákazník i tak zájem na jejich ochraně. Obě tyto kategorie informací jsou v praxi často zahrnuty pod jednu širokou definici důvěrných informací, aby nebylo nutno pracně zjišťovat, zda je daná informace chráněná jako obchodní tajemství nebo nikoli.

  Ochranu důvěrných informací, ke kterým může mít poskytovatel cloudové služby přístup, je kromě technických opatření vhodné řešit také ve smlouvě. V ní je z pohledu zákazníka nutné definovat, jaké důvěrné informace budou chráněny, zda a za jakých podmínek k nim poskytovatel cloudu může přistupovat, zda a proč je může sdílet s dalšími subjekty, například členy svojí podnikatelské skupiny, a že je nemůže využívat pro vlastní účely.

- Osobní údaje

  Osobní údaje jsou definovány[9] velmi široce, jaké jakékoliv informace, které se týkají přímo či nepřímo určené nebo určitelné fyzické osoby.[10] Při využívání cloudových služeb tak bude docházet k předávání osobních údajů, minimálně informací o některých zaměstnancích zákazníka (zejména zaměstnanců interně odpovědných za využití cloudového řešení), cloud však je také často využíván ke zpracování klientských či zaměstnaneckých dat ve větším rozsahu.

  Při hodnocení cloudu z pohledu pravidel pro zpracování osobních údajů je nutné posoudit především tyto otázky:

  - Jaká bude role poskytovatele cloudu?

    Ve velké většině případů, kdy poskytuje infrastrukturu, platformu nebo službu pro zpracování osobních údajů, resp. pro zajištění činnosti, jejíž

součástí je zpracování osobních údajů, bude poskytovatel cloud v postavení zpracovatele. Zpracovatelem osobních údajů je subjekt, který pro správce, zákazníka, uchovává nebo jinak zpracovává osobní údaje. Povinností správce je ověřit bezpečnostní a technické záruky zpracovatele za ochranu zpracovávaných dat a uzavřít s ním smlouvu, jejíž náležitosti poměrně detailně stanoví obecné nařízení v čl. 28 odst. 3. V případě infrastrukturního cloudu lze podle okolností případu uvažovat o tom, že by poskytovatel cloudu zpracovatel nebyl, neboť součástí jím poskytované služby není či nemusí být zpracování osobních údajů.

- Kde budou osobní údaje uchovávány?

  Obecné nařízení zajišťuje volný tok osobních údajů v rámci Evropské unie, resp. Evropského hospodářského prostoru, ovšem pro jejich předání mimo hranice EU/EHP stanoví poměrně přísná pravidla. Pokud nedochází k předání údajů do bezpečné třetí země (např. Argentina, Kanada, Izrael, Japonsko, Švýcarsko), ale jsou užity tzv. standardní smluvní doložky, je kontextu judikatury SDEU[11] a výkladových stanovisek EDPB[12] před předáním dat do třetí země nutné vyhodnotit rizika, jaká z toho dotčeným osobám mohou plynout, a zvolit vhodné právní[13] i technické či organizační opatření, aby daná rizika byla minimalizována.

- Jaké další povinnosti je třeba plnit?

  Zde se v prvé řadě jedná o informační povinnost podle čl. 13 či 14 GDPR, případně o vyřízení žádosti dotčené osoby, subjektu údajů, o uplatnění jejich práv podle čl. 15-20 GDPR.

  Z dalších povinností jmenujme zejména o doplnění záznamů o činnostech zpracování[14], nastavení procesu pro řízení porušení zabezpečení osobních údajů, ke kterému může dojít u zpracovatele[15], či obecně nastavení odpovídajících bezpečnostních opatřeních[16].

  Pro poskytovatele cloudu, který bude či může být v postavení zpracovatele osobních údajů, z toho plyne nutnost být připraven na jednání o uzavření zpracovatelské smlouvy či využití nástrojů pro bezpečné zpracování dat mimo EU/EHP, zejména standardních smluvních doložek.

- Informace podléhající mlčenlivosti

  Organizace, která využívá cloudové řešení, může zpracovávat informace podléhající i dalším úpravám mlčenlivosti. Typicky půjde o bankovní tajemství (tomu bude věnován následující článek), informace o zdravotním stavu nebo například údaje chráněné advokátní mlčenlivostí[17]. Je odpovědností zákazníka, aby posoudil, zda informace, pro jejichž uchování či zpracování hodlá využít cloudové řešení, podléhají specifické regulaci, povinnosti mlčenlivosti, a co to pro něj v konkrétním případě znamená.

Mgr. Bohuslav Lichnovský, LL.M.,
působící v Bohuslav Lichnovský GALI LEGAL, advokátní kancelář
e-mail: lichnovsky@galilegal.com

Mgr. František Nonnemann,
konzultant v oblasti ochrany osobních údajů a compliance, člen Výboru Spolku pro ochranu osobních údajů
e-mail: nonnemann@volny.cz

_____

[1] Srov. obecný přehled na - dostupné na www, k dispozici >>> zde nebo naopak analýzu ekonomické výhodnosti cloudového řešení v poměrně úzce vymezeném segmentu, vedení elektronické zdravotnické dokumentace: dostupné na www, k dispozici >>> zde.
[2] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
[3] Např. § 4-§ 5a zákona č. 634/1992 Sb., o ochraně spotřebitele,
[4] Např. předsmluvní informace v oblasti pojišťovnictví podle § 83 a násl. zákona č. 170/2018 Sb., o distribuci pojištění a zajištění.
[5] Viz § 96 zákona č. 262/2006 Sb., zákoník práce.
[6] Viz § 53 a násl. zákona č. 372/2011 Sb., o poskytování zdravotních služeb.
[7] Kupříkladu dokumentaci související s poskytováním platebních služeb, resp. plněním souvisejících povinností, je platební instituce podle § 31 odst. 1 zákona č. 370/2017 Sb. povinna uchovávat po dobu alespoň 5 let.
[8] Srov. § 504 zákona č. 89/2012 Sb., občanský zákoník.
[9] Srov. čl. 4 bod 1) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
[10] Bližší výklad viz Nulíček, M. Donát, J. Nonnemann, F. Lichnovský, B. Tomíšek, J. Kovaříková, K. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR.
[11] Zejména rozsudek Soudního dvora EU ze dne 16. července 2020 ve věci C-311/18, tzv. kauza Schrems II, kterou byl zrušen nástroj pro bezpečné předávání údajů do USA, Privacy Shield.
[12] Především Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad s úrovní ochrany osobních údajů v EU, dostupné na www, k dispozici >>> zde.
[13] Nejčastěji, ne však výlučně, se jedná o standardní smluvní doložky ve smyslu čl. 46 odst. 2 bodu

c) nebo d) obecného nařízení o ochraně osobních údajů, jejichž vzory jsou uvedeny v prováděcím rozhodnutí Komise 2021/914 ze dne 4. června 2021 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení Evropského parlamentu a Rady (EU) 2016/679.
[14] Čl. 30 obecného nařízení o ochraně osobních údajů.
[15] Čl. 33-34 obecného nařízení o ochraně osobních údajů; k odpovědnosti správce za řízení porušení zabezpečení osobních údajů, ke kterému došlo u zpracovatele, srov. také Nonnemann, F. Špatné řízení „data breaches" na pozadí kauzy Twitter, dostupné na www, k dispozici >>> zde, a Nonnemann, F. Jak posílit řízení „data breaches" při zapojení zpracovatele?, dostupné na www, k dispozici >>> zde.
[16] Čl. 32 obecného nařízení o ochraně osobních údajů.
[17] Vítek, D. Suchánková, L. Advokátní tajemství v cloudu. Dostupné na www, k dispozici >>> zde.

[*] **Cloudy a právo - 1 díl: Proč o nich uvažovat a na co se připravit**, dostupné na www, k dispozici >>> zde.

Další články:

- Vybrané otázky poskytování zdravotních služeb na dálku
- DEAL MONITOR
- „Za každou kauzou je živý příběh"
- Ombudsman na Maltě – základní parametry a role. A v čem bychom se mohli poučit i my v Česku?
- DEAL MONITOR
- DEAL MONITOR
- Rozhovor s JUDr. Veronikou Janoušek Rudolfovou, samostatnou advokátkou specializující se na sportovní právo
- DEAL MONITOR
- DEAL MONITOR
- DEAL MONITOR
- Fotbaloví agenti vs. FIFA ve světle stanoviska generálního advokáta Soudního dvora Evropské unie