10. 8. 2022

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

Cloudy a právo - 1 díl: Proč o nich uvažovat a na co se připravit

Cloudová řešením jsou dnes běžná, dostupná a levná. V praxi je využívá velká část z nás, aniž by si to třeba nutně uvědomovala, např. při zálohování dat z chytrého telefonu nebo přenosu kontaktů z jednoho zařízení do druhého. Cloudy ve stále větší míře využívají i soukromoprávní a veřejnoprávní organizace, ať už k „pouhému“ uchování či získání dodatečné výpočetní kapacity, nebo i jako součást komplexnější služby, např. ve formě aplikace či nástroje pro marketing, spisovou službu, evidenci dokumentace atd.

Využívání cloudových řešení má řadu právních souvislostí a důsledků. Tyto důsledky jsou pochopitelně odlišné pro koncového uživatele, třeba vlastníka telefonu, a jiné pro banku nebo úřad, který využívá komplexní službu od dodavatele.

Cloudy a spotřebitel

Podíváme-li se na cloudy z právního pohledu, pak v případě využití cloudového řešení jednotlivým uživatelem je situace poměrně přehledná: Poskytovatel cloudu nebo služby, která cloud využívá, musí uživatele o této skutečnosti vyrozumět, nastavit pravidla služby ve smlouvě, resp. nejčastěji v obchodních podmínkách, a dodržet další podmínky související se zpracováním osobních údajů. V kontextu cloudových řešení je důležitá především otázka předávání osobních údajů mimo Evropskou unii. Jak si dále ukážeme, předávání osobních údajů mimo Evropskou unii, zejména do USA, kde řada poskytovatelů široce používaných služeb sídlí, je z pohledu GDPR[1] poněkud problematické a vyžaduje přijetí dalších kroků. Nicméně je to spíše starostí poskytovatele služby a její uživatel, spotřebitel, žádné specifické kroky činit nemusí.

Právnická osoba má o mnoho více povinností

Pokud však cloudovou službu využívá podnikatel nebo veřejnoprávní subjekt, je situace o poznání komplikovanější. Do hry totiž vstupuje řada dalších právních aspektů. Některé právní povinnosti, resp. okruhy, které je nutno uplatnit, jsou v zásadě stejné pro všechny organizace, další se však zásadně liší podle toho, o jaký subjekt se jedná.

Jiné povinnosti totiž dopadají na výrobní podnik, který v cloudu provozuje jen mailové servery, jiné povinnosti na zdravotnická zařízení, jiné na banku a z velké části odlišné či dodatečné povinnosti se uplatní i na subjekty veřejné správy. Nejen právní povinnosti při přechodu části dat či infrastruktury do cloudu pak ovlivňuje i otázka, zda je daná organizace povinnou osobou ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti.

Jak se na cloud připravit z právního i faktického hlediska?

Orientace v právních povinnostech souvisejících jak s poskytováním, tak i využitím cloudových služeb není jednoduchá. Proto jsme připravili sérii několika článků, ve kterých nejdůležitější oblasti právních povinností a souvisejících faktických důsledků projdeme. Začneme od společných oblastí práva a pravidel, která se uplatní prakticky pro každou organizaci využívající cloudové řešení. Následně se budeme zabývat oblastmi, kde je regulace pro využití cloudů detailní a specifická, nebo,

z jiného úhlu pohledu, pro zúčastněné subjekty ještě komplikovanější.

Články jsme strukturovali následujícím způsobem:

- V tomto úvodním příspěvku po stručné definici samotného pojmu cloud vytýčíme hlavní právní oblasti, jež je nutno při nabízení i využívání cloudových služeb zohlednit.
- Ve druhém článku projdeme hlavní právní povinnosti z pohledu klienta i poskytovatele cloudu. Identifikujeme klíčové aspekty jednotlivých právních oblastí a z pohledu obou zúčastněných subjektů zdůrazníme, na co se zaměřit především.
- Pokračovat budeme článkem, kde přiblížíme specifická a detailní pravidla pro využití a nabízení cloudových služeb ve finančním sektoru. Tato regulace dopadá především na banky, platební instituce, pojišťovny a další subjekty. Protože je tato regulace detailní a rozsáhlá, nejprve probereme praktické a procesní kroky při přípravě na využití poskytovatele cloudu ze strany finanční instituce i poskytovatele.
- V dalším článku se potom zaměříme na právní požadavky související s využitím cloudu ve finančním sektoru, opět jak z pohledu finanční instituce, tak poskytovatele.
- A naši sérii zakončíme článkem řešícím specifickou otázky kybernetické bezpečnosti a využití cloudu ve veřejném sektoru. Zohledníme i připravovanou novelizaci evropské kyberbezpečnostní směrnice[2], která rozšíří záběr českého zákona o kybernetické bezpečnosti na další sektory a další povinné osoby. Zabývat se budeme i některými specificky využití cloudu ve veřejném sektoru.

České právo a cloud

Nejprve si stručně shrneme, co rozumíme cloudovou službou z pohledu práva. Je vhodné si rovněž ujasnit, jaké jsou nejčastější varianty či typu cloudu. V dalších článcích si ukážeme, že typ zvolené cloudové služby má v praxi dopad na rozsah právních povinností toho, kdo danou službu hodlá využívat.

Stručnou a výstižnou definici cloud computingu nalezneme v § 2 písm. x) zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, podle kterého se cloud computingem „rozumí způsob zajištění provozu informačního systému nebo jeho části prostřednictvím dálkového přístupu k sdílenému technickému nebo programovému prostředku, který je zpřístupněný poskytovatelem cloud computingu a nastavitelný správcem informačního systému“.

Detailnější definici přináší Úřední sdělení České národní banky č. 8/2016 Sb., k výkonu činnosti na finančním trhu – cloud computing. Podle úředního sdělení se pojmem cloud computing „rozumí model uplatňovaný v oblasti informačních a komunikačních systémů a technologií, který umožní získat síťový přístup ke konfigurovatelným výpočetním prostředkům (např. sítě, servery, datová úložiště, aplikace a služby), které jsou sdíleny větším množstvím uživatelů a jejichž kapacita je poskytována a opět uvolňována s minimálními nároky na jejich správu anebo na intervenci poskytovatele cloud computingu.“

A konečně § 2 písm. l) bod 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, popisuje digitální službu spočívající v provozování cloud computingu tak, že daná služba umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet.

Ač každý z uvedených předpisů upravuje pravidla pro využití cloudových řešení v jiné oblasti, definice cloudové služby je v nich fakticky obsahově totožná. Můžeme ji shrnout tak, že se jedná o technicky snadno dostupné, využitelné a konfigurovatelné využití sdílených technických nástrojů a výpočetních prostředků.

Není cloud jako cloud

Cloudové nástroje můžeme rozdělit podle toho, jaké technické a výpočetní prostředky jsou vlastně sdíleny, resp. jaká služba je poskytována. Z tohoto úhlu pohledu lze cloudy dělit na:

- Poskytování infrastruktury (Infrastructure as a Service, IaaS). V tomto modelu zákazník využívá základní technickou infrastrukturu, jako je datové úložiště nebo výpočetní výkon. Rozsah služeb je spíše omezený a poskytovatel cloudu při poskytování této služby obvykle nemá přístup ke zpracovávaným informacím, resp. při běžném provozu by přístup mít neměl. Na druhou stranu, na správném fungování infrastrukturního cloudu závisí, jestli k vlastním datům bude mít přístup zákazník.
- Poskytování platformy (Platforme as a Service, PaaS). Tyto služby obvykle zahrnují jak základní infrastrukturu (sítě, úložiště, výkon), tak i některé služby související s vývojem a přípravou vlastních produkt a aplikace klienta. Klient tak využívá rovněž některé nástroje např. licence pro vývoj aplikace, její testování či údržbu. Role poskytovatele cloudového řešení je tak důležitá i z pohledu odpovědnosti za provozované služby (jejich správná a dohodnutá funkčnost, dostupnost), byť se nejčastěji jedná o službu poskytovanou jednomu komerčnímu zákazníkovi, ne koncovým uživatelům.
- Poskytování služby (Software as a Service, SaaS). Nejkomplexnější forma cloudových služeb spočívá v tom, že poskytovatel cloudu sám provozuje celou aplikaci nebo jiný nástroj, často včetně datového úložiště a další infrastruktury, a zákazník jej „pouze“ využívá pro poskytování svých služeb. Spolu s nejvyšší mírou zapojení poskytovatele se pojí i jeho právní odpovědnost za celkové fungování služby, jejích jednotlivých komponent, ochrany zpracovávaných informací atd.

Z jiného úhlu pohledu, spíše technického nebo na ochranu informací zaměřeného, můžeme cloudové služby dělit podle způsobu nabízení a využívání cloudové služby:

- Veřejný cloud. V praxi nejčastější model, kdy poskytovatel cloudu nabízí své služby a prakticky kdokoliv je může vzdáleně využít, obvykle bez nutnosti dalších právních kroků. Smlouva je uzavírána akceptací podmínek poskytovatele cloudu. Služby jsou všem zákazníkům poskytovány s využitím stejných nástrojů a úložišť, klient nemá garantované fyzické oddělení dat a standardně ani dedikovaný výpočetní výkon pro řešení pouze jeho požadavků, např. při incidentu, výpadku služby, nasazování nové verze aplikace atd.
- Privátní cloud. V tomto modelu má klient dojednány a určeny dedikované prostředky a kapacity pro využití dané služby a nesdílí je s dalšími klienty. Nastavení spolupráce v tomto režimu vyžaduje detailnější úpravu, z pohledu poskytovatele bývá náročnější na kapacity i provoz a obvykle také dražší. Na druhou stranu, z pohledu klienta tento režim snižuje riziko nedostupnosti služby a narušení bezpečnosti zpracovávaných či uchovávaných dat.
- Smíšený cloud. V praxi existují i hybridní modely, které pro část služby využívají veřejný cloud a pro uchování či zpracování citlivějších informací nebo zajištění kritických funkcí cloud privátní, s vyšší jistotou dostupnosti a funkčnosti.

Jaké právní otázky řešit především?

Jaké jsou hlavní právní otázky, které je nutné při využívání cloudových služeb řešit? Bližší rozbor z pohledu klienta i poskytovatele cloudu přineseme v následujících článcích. Nyní jen shrňme to nejdůležitější:

- Péče řádného hospodáře

Cloudové služby jsou obvykle využívány, resp. jejich využití je zdůvodňováno, ekonomickou výhodností. I pro využití tohoto druhu služby platí, že osoby odpovědné za hospodaření s prostředky dané organizace musí zvážit, zda je v jejích podmínkách tato služba skutečně výhodná a efektivní. A její finanční výhodnost by měla být i pravidelně posuzována, revidována, protože se může v čase měnit.

- Odpovědnost za vlastní činnost, produkty a služby

  I při využití některého druhu cloudové služby je organizace odpovědný za svoji činnost a za svoje závazky vůči dalším osobám, třeba koncovým uživatelům. Jinak řečeno, využití datového úložiště od poskytovatele cloudu organizaci nezbavuje soukromoprávní odpovědnosti vůči klientům, se kterými smluvně sjednala dostupnost a funkce její služby, která je na fungování cloudu více či méně závislá. Stejně tak využití cloudu nezbavuje subjekt veřejnoprávní odpovědnosti, typicky v oblasti kybernetické bezpečnosti.

- Autorské právo

  Důležitou oblastí je otázka ochrany autorského práva. Klienti často využívají cloudové nástroje pro vývoj, uchování či provoz svých autorských děl, aplikací či webových rozhraní. Autorským právem však může disponovat i poskytovatel některého cloudového produktu, zejména při nabízení platformy nebo software jako služby. Správné nastavení autorských práv může předejít řadě budoucích sporů.

- Ochrana informací

  Cloudových nástrojů a služeb je využíváno i k uchování či aktivnímu zpracování citlivých informací. Často řešíme osobní údaje, mimo jiné v souvislosti se stále aktuálním tématem jejich předávání mimo Evropskou unii, zejména USA. Ale při využívání cloudových služeb je vhodné myslet i na další důvěrné informace, ke kterým může mít poskytovatel cloudu přístup, ať už se jedná o informace podléhající obchodnímu tajemství (příprava a vývoj nových produktů), povinné mlčenlivosti podle dalších předpisů (např. v oblasti zdravotnictví, advokacie atd.) nebo jde „jen“ o z jiného důvodu obchodně citlivá data.

- Sektorová regulace

  Jak jsme již uvedli, v některých oblastech, kde pro to existuje silný veřejný zájem, jsou pro využití cloudu stanoveny detailnější podmínky. Jedná se typicky o využití cloudu ve finančním sektoru či využití cloudu subjekty v režimu zákona o kybernetické bezpečnosti. Specifiky těchto dvou oblastí se budeme detailně zabývat v dalších článcích.

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] 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).
[2] Návrh Směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148

Další články:

- DEAL MONITOR
- Tři dekády v advokacii a otevřený pohled na to, co profesi i justici nejvíc škodí
- DEAL MONITOR
- 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