24. 8. 2022

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

Cloudy a právo - 3 díl: Povinnosti finančních institucí

V předchozích článcích[*],[**] bylo diskutováno, jaká jsou cloudová řešení, proč mohou mít zákazníci zájem o jejich užívání a jaké základní právní aspekty zahrnuje využití cloudových služeb pro všechny zákazníky bez rozdílu.

V tomto a následujícím pokračování naší série budou popsána základní specifika užití cloudových řešení ve finančním sektoru. Primárně se tyto články budou zabývat regulací užití cloudových služeb u finančních institucí včetně bank, pojišťoven a sektoru platebního styku. Oboje pak bude činěno pohledem účinné právní úpravy.

O chystaném balíčku evropské regulace cloudových služeb a IT bezpečnosti v celém finančním sektoru, kterou má přinést nový evropský akt o digitální provozní odolnosti (DORA) a který má sjednotit pravidla využívání cloudových služeb napříč regulátory a regulovat i samotné poskytovatele cloudových služeb, si povíme v některém z dalších článků.

V tomto článku se konkrétně dozvíte, jaké právní předpisy upravují využívání v outsourcingu ve formě cloudových služeb pro finanční instituce, co si instituce musí před uzavřením smlouvy o poskytování cloudových služeb připravit a jaké další kroky podniknout. V navazujícím článku si pak shrneme, co si musí před uzavřením smlouvy připravit poskytovatel cloudových služeb a co je nutno do této smlouvy promítnout.

Článek přitom nemá za ambici tyto požadavky popsat v jejich úplnosti. Regulace finančního sektoru, včetně otázky outsourcingu a využívání cloudových služeb, je vskutku komplexní. Jen samotný výčet povinností instituce, která hodlá využívat cloud, by přesahoval rozsah tohoto článku. Proto se zaměříme na základní a nejdůležitější kroky, které jsou nutné pro všechny instituce uvažující nebo připravující se na využití cloudových služeb.

Základní právní předpisy a regulace outsourcingu ve finančním sektoru

Jedním z klíčových, a zcela jistě nejkomplexnějších, předpisů jsou pokyny Evropského orgánu pro bankovnictví (EBA) k outsourcingu.[1] Byť tyto pokyny nejsou pro finanční instituce formálně přímo závazné, tak ČNB oznámila v souladu s čl. 16 odst. 3 evropského nařízení o zřízení EBA, že bude postupovat při výkonu dohledu v souladu s pokyny. Výjimkou jsou pojišťovny, které mají uvedené vlastní požadavky v rámci vodítek EIOPA.[2] Obsahově jsou však tyto vodítka s pokyny EBA v podstatě zaměnitelná.

Tyto pokyny EBA primárně upravují, co je outsourcingem, resp. také co je tzv. kritickým outsourcingem, na který se uplatní přísnější požadavky. Dále definují, jak mají být ze strany finanční instituce nastaveny systémy správy a řízení outsourcingu, včetně shrnutí, jaké činnosti a pravomoci by si instituce měly ponechat. Stanoví také požadavky na zásady pro outsourcing a plány kontinuity činností, které by si měla finanční instituce připravit před využíváním outsourcingu. Popisují také, jak dokumentovat užívání outsourcingu, co musí instituce provedením outsourcingu posoudit, co má být obsahem smlouvy o outsourcingu, jak má instituce dohlížet na poskytování outsourcingu a jak nastavit možné ukončení outsourcingového vztahu.

ČNB dále vydala vyhlášku č. 163/2014 Sb., která definuje základní požadavky na outsourcing činností banky obecně, nejen při využití cloudu, zavádí informační povinnost o outsourcingu vůči ČNB a v příloze č. 7 poměrně podrobně vymezuje požadavky na řízení rizik v outsourcingu. Toto zahrnuje jak obecné zásady pro řízení těchto rizik, pravidla o zachování odpovědnosti za výkon činnosti banky, povinnosti provedení analýzy rizik, požadavky na poskytovatele outsourcingu, uzavíranou smlouvu a pohotovostní plány vztahující se k outsourcingu.

Posledním zásadním předpisem je Úřední sdělení ČNB ze dne 19. srpna 2016 k výkonu činnosti na finančním trhu – cloud computing, která zavádí povinnost promítnout využívání cloud computingu do řídicího a kontrolního systému banky, zohlednit vliv outsourcingu na výkon činností banky, provést analýzu rizik užití cloud computingu, vytvořit bezpečnostní zásady pro cloud computing apod.[3]

Co všechno je outsourcingem ve finančním sektoru?

A co je vlastně outsourcingem podle finanční regulace? Podle výše uvedených pokynů EBA, které jej definují nejpodrobněji, se jedná o externí zajištění služeb nebo činností, které je vykonáváno opakovaně nebo průběžně a normálně by spadalo do působnosti banky a bylo jí vykonáváno. Do definice outsourcingu tak bude spadat široké spektrum činností, od scoringu zájemců o úvěrový produkt, přes výkon vnitřní kontroly (externí zajištění funkce compliance), přes archivaci a skartaci smluvní dokumentace až po online nástroje pro interní komunikaci, nebo kontrolu a testování kódu vyvíjených aplikací.

Pokyny EBA rozlišují standardní outsourcing a významný outsourcing, resp. outsourcing kritických funkcí. O něj se jedná tehdy, pokud finanční instituce prostřednictvím třetí osoby zajišťuje činnosti, resp. funkce, které jí jsou svěřeny právními předpisy či k nimž mají povolení (poskytování bankovních a platebních služeb), funkce ovlivňujících její finanční výkonnost nebo kontinuitu služeb, popř. funkcí schopných ovlivnit kontinuitu činnosti finanční instituce jako celku.

V případě, že takový outsourcing využívá služeb cloud computingu, tak na něj plně dopadají výše uvedené požadavky EBA a ČNB.

Využití cloudu ve finančním sektoru krok za krokem

Aby finanční instituce mohla využívat cloud computingu, musí na své straně splnit celou stranu požadavků.

První kroky budou vždy neprávní: Pro správné vyhodnocení, zda a jaký typ cloudu využít a jaké požadavky na poskytovatele cloudu bude finanční instituce mít, je nezbytné zmapovat byznysové požadavky, které mají být využitím cloudových služeb řešeny, a zamýšlený rozsah outsourcovaných funkcí. Finanční instituce rovněž připraví analýzu finančních úspor – pokud úspor nebude dosaženo, cloudový outsourcing ztrácí smysl, resp. je nehospodárný. Návazně si instituce musí posoudit, jak jednotlivé komerčně poskytované služby zapadají do strategií a stávající IT architektury instituce a které z dostupných technických řešení jí z tohoto pohledu vyhovuje nejvíce.

Po obchodním a technickém zmapování stavu a potvrzení záměru cloudovou službu využít by se měl spustit interní proces pro řízení outsourcingu.

Finanční instituce musí nejprve určit, zda je outsourcing dané činnosti outsourcingem ve smyslu uvedeném výše. A pokud ano, zda se jedná o tzv. outsourcing kritických funkcí.

Dále by instituce měla mít připraveny obecné zásady pro outsourcing a řízení rizik pro outsourcing podle přílohy č. 7 vyhlášky ČNB č. 163/2014 Sb. zejména v souvislosti s využíváním outsourcingu podle těchto zásad. Je nutno zajistit, že využíváním outsourcingu nedojde ke snížení ochrany jejích

dat, instituce nepřestane plnit regulatorní požadavky, bude možno nadále vykonávat kontrolu a dohled nad využíváním outsourcingu, nebude nijak dotčena kvalita řídicího a kontrolního systému instituce (na úrovni, jako by činnost vykonávala instituce sama), bude zachována působnost a odpovědnost orgánů instituce, a že instituce zavede zásady a postupy pro řízení rizik při outsourcingu a během celého jeho životního cyklu. Obdobné platí i pro další poskytovatele platebního styku a pojišťovny podle výše uvedených regulací.

Do těchto obecných zásad by měla být dále promítnuta specifika cloud computingu podle sdělení ČNB ze dne 19. srpna 2016. Zejména je tak ze strany poskytovatelů finančních služeb (z definice jde o banky, spořitelní a úvěrní družstva, tuzemské pojišťovny a zajišťovny, ale sdělení je využitelné i pro další instituce pod dohledem ČNB, které využívají cloud computing) potřeba:

- modifikovat plnění regulatorních požadavků na outsourcing obecně na konkrétní scénář cloud computingu. Pokud např. poskytovatel zajišťuje pouze technické prostředí pro chod aplikací instituce (IaaS), tak toto bude mít naprosto minimální vliv na výkon povinností instituce nebo její vnitřní procesy; instituce v zásadě ani nemusí poznat, že něco běží v datovém centru poskytovatele a ne v jejím suterénu; naopak zcela odlišný případ je outsourcing ve formě poskytování software jako služby (SaaS), například služby scoringu (SaaS), kdy kontrola instituce nad způsobem výkonu jí svěřených činností může být omezena pro nedostatek informací o vnitřním fungování služby;
- stanovit přístup ke cloud computingu a hlavní zásady jeho využívání, tj. v jakém rozsahu budete využívat cloud computing a v jaké formě. Instituce si může například rozhodnout, že IaaS cloudy bude využívat pro zálohování dat a jako záložní prostřední pro chod aplikací, a že SaaS službu bude využívat v rámci scoringu zájemců o spotřebitelský úvěr nebo pojištění;
- zohlednit v obecných zásadách outsourcingu a navazujících postupech specifika cloud computingu, zejména zohlednit vliv cloud computingu na plnění povinností finanční instituce, na schopnost jejich plnění prokázat ČNB a na dodržování obezřetnostních požadavků. I zde bude zcela odlišný vliv outsourcingu ve formě IaaS a ve formě SaaS;
- zajistit, že i když bude řešení provozováno v cloudu, bude mít finanční instituce stále stejný přehled nad činnostmi poskytovatele, jako by vše bylo provozováno v prostředí instituce, a aby mohla provést kontrolu nad výkonem svěřených funkcí a jejich souladem s právními předpisy; opět platí, že u IaaS bude tato podmínka ve většině případů splněna, naopak u SaaS nemusí v extrémním případě vědět, proč aplikace dala konkrétní výsledek procesu (zejména v případě užití tzv. umělé inteligence, artificial intelligence);
- zohlednit další specifika cloud computingu při posuzování rizik, tedy zejména posoudit, jaká dodatečná rizika vznikají v případě cloudového řešení oproti provozu aplikací na infrastruktuře instituce; typické je riziko výpadku internetového připojení mezi cloudovou infrastrukturou a institucí.

Další povinné kroky před přechodem do cloudu

Finanční instituce musí dále provést analýzu rizik, která bude zaměřena zejména na rizika spojená s poskytováním finančních služeb, plněním právních povinností, důvěrnosti a zabezpečení dat, fungování vnitřního řídícího a kontrolního systému atd. I v tomto případě se do výsledku analýzy rizik zásadním způsobem projeví, v jaké formě bude outsourcing využíván (s IaaS na jedné a SaaS na druhé straně).

Instituce dále musí připravit pohotovostní plány, které definují její postupy pro případy, kdy cloudové služby nebudou dostupné, kdy poskytovatel cloudových služeb nebude schopen vykonávat mu svěřené činnosti, popř. kdy bude nutno provést ukončení konkrétního cloudového outsourcingu a převod činností zpět na instituci či na nového poskytovatele. Pohotovostní plány by měly pokrýt

alespoň nejvíce rizikové situace, jako jsou nedostupnost poskytované služby, nedostupnost dat, nutnost rychlého odchodu od poskytovatele outsourcingu z vnějších důvodů (závazný pokyn České národní banky, změněná politická či právní situace v zemi poskytování služeb, resp. v zemí sídla poskytovatele outsourcingu atd.).

Dalším krokem je oslovení potenciálních poskytovatelů cloudových služeb a výběr vhodného poskytovatele dle kritérií zvolených institucí. Instituce provede due diligence poskytovatele cloudových služeb, kdy finanční instituce posoudí, zda je poskytovatel dostatečně kvalifikovaný a má dostatečné kapacity pro výkon požadovaných činností, a dále zda poskytovatel není vůči instituci ve střetu zájmů. Provedení hloubkové kontroly je v tomto případě přímo požadavkem pokynů EBA. Zároveň hloubková kontrola a s tím spojený výběr vhodného poskytovatele cloudových služeb z oslovených může velmi napomoci s plněním požadavků dle GDPR i zákona o kybernetické bezpečnosti.

Instituce je povinna dále ověřit, zda postupy poskytovatele v oblasti bezpečnostní informací jsou v souladu s požadavky ČNB a instituce samotné. Toto instituce typicky ověřuje vyžádáním bližších informací o bezpečnostních politikách a praxi poskytovatele. Pokud poskytovatel cloudových služeb disponuje certifikací potvrzující soulad jeho činnosti s dobrou praxí v oblasti ochrany informací, zejména certifikace řady ISO 27xxx, neměl by tento krok být ani pro jednu stranu příliš problematický. Stejně tak instituce ověří pohotovostní plány poskytovatele pro mimořádné situace, a to typicky prostřednictvím doloženém certifikace ISO 22091, obdobného potvrzení nebo doložení interní praxe poskytovatele.

Finanční instituce konečně musí ČNB v předstihu ohlásit, že zamýšlí outsourcovat některé své kritické funkce či činnosti, a to s uvedením poskytovatele cloud computingu a osoby provádějící audit u takového poskytovatele.

Pokud finanční instituce projde všemi výše uvedenými kroky, měla by mít připravenou veškerou klíčovou dokumentaci, která je pro outsourcing potřeba, a současně splní notifikační povinnost vůči ČNB. Nejde ale o výsledek jediný: Velmi podstatné pro instituci je i fakt, že výše zmíněné kroky povedou k identifikaci rizik a seznamu opatření, které instituce buď přímo musí, nebo by alespoň měla řešit ve smlouvě s poskytovatelem cloudových služeb. Například významné riziko nedostupnosti dat na základě nedostupnosti/omezeného fungování platebních karet by tak mělo vést ke smluvnímu zajištění jejich velmi vysoké dostupnosti a povinnosti poskytovatele outsourcingu podílet se na rychlém řešení případných výpadků či zavedení dočasných náhradních řešení (workaround).

Právě smlouva mezi poskytovatelem cloudové outsourcingu a finanční institucí a její obsah spolu s požadavky kladenými na poskytovatele cloudových služeb budou obsahem posledního článku v rámci tohoto seriálu.

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] Evropský orgán pro bankovnictví. Obecné pokyny k outsourcingu ze dne 25. února 2019. EBA/GL/2019/02. [cit. 2022-06-30]. dostupné na www, k dispozici >>> zde.
[2] Evropský orgán pro pojišťovnictví a zaměstnanecké penzijní pojištění. Obecné pokyny k outsourcingu u poskytovatelů cloudových služeb. EIOPA-BoS-20-002 [cit. 2022-06-30]. Dostupné na www, k dispozici >>> zde.
[3] Jde o přehled nejzásadnější, nikoliv přehled úplný: pro ten bude třeba uvažovat i Úřední sdělení ČNB ze dne 27. května 2011 k výkonu činnosti na finančním trhu – operační riziko v oblasti informačního systému, které upravuje zejména požadavky ČNB na výkon on-site auditu ze strany ČNB a poskytování služeb v souladu s pokyny bank, Úřední sdělení ČNB ze dne 10. prosince 2010 k výkonu činnosti na finančním trhu: Kvalitativní požadavky související s výkonem činnosti – základní informace, které obsahuje dílčí požadavky na řídicí a kontrolní systém banky, které se vztahují též k řízení využívání outsourcingu, a vyhlášku ČNB č. 7/2018 Sb. k zákonu o platebním styku, kde zejména bod 86 přílohy upravuje opatření pro kontinuitu činnosti ke zmírnění selhání externích poskytovatelů.

[*] **Cloudy a právo - 1 díl: Proč o nich uvažovat a na co se připravit,** dostupné na www, k dispozici >>> zde.
[**] **Cloudy a právo - 2 díl: Tisíc a jeden právní požadavek**, dostupné na www, k dispozici >>> zde.

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