31. 8. 2022

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

Cloudy a právo - 4 díl: Jak se má připravit poskytovatel cloudu?

V tomto seriálu cloud a právo se budeme věnovat zejména samotnému poskytovali cloudových služeb. Shrneme, co musí poskytovatel cloudových služeb před uzavřením smlouvy připravit s finanční institucí (bankou, pojišťovnou, platební institucí atd.) a co je nutno do smlouvy promítnout.

Také tento článek bude řešit specifika užití cloudových řešení ve finančním sektoru, tj. regulací užití cloudových služeb u finančních institucí včetně bank, pojišťoven a sektoru platebního styku.

Nabízet cloud bance není jen tak

S poskytovateli cloudových služeb se v běžném životě setkáváme dnes a denně, když po nich jako běžní uživatelé – spotřebitelé nemusíme chtít víc, než aby byla u nich bezpečně uložena data. V rámci finančního sektoru je ale situace výrazně specifičtější. Špatné fungování či výpadky cloudového řešení totiž mohou v krajním případě způsobit i nedostupnost peněžních prostředků klientů finančních institucí, což může mít významný dopad na řadu dalších oblastí. Proto je i regulace využití cloudu, resp. obecně outsourcingu ve finančním sektoru tak komplexní a detailní.

Pokud instituce již prošla kroky dle předchozích dílů seriálu, má sama připravenou veškerou klíčovou vnitřní dokumentaci, která je pro outsourcing potřeba, identifikovala rizika, která ji může outsourcing určité funkce či činnosti přinést, a vyhotovila seznam opatření, které buď přímo musí, nebo by alespoň měla řešit ve smlouvě s poskytovatelem cloudových služeb. Ty oslovuje obvykle ve větší šíři, aby měla prostor pro výběr toho nejvhodnějšího, u kterého následně provádí hloubkovou kontrolu.

Poskytovatel cloudových služeb, který chce nabízet služby i finančním institucím, musí být na tuto hloubkovou kontrolu připraven. Měl by mít zejména připraven **popis vnitřních postupů a opatření pro omezení rizik**, včetně specifikace životního cyklu dat, požadavků na šifrování dat, procesů zabezpečení sítě a sledování bezpečnosti. Dle standardu ISO 27xxx pak toto zahrnuje zejména definici celkového systému řízení bezpečnosti informací (Information Security Management System, ISMS), politiku informační bezpečnosti, metodiku hodnocení rizik a jejich posouzení, provozní postupy pro správu IT, principy zabezpečeného systémového inženýrství a protokoly aktivit uživatelů, výjimek a bezpečnostních událostí.

Dále si poskytovatel musí připravit **popis způsobu záznamu a evidence odstávek a technologických incidentů na infrastruktuře** poskytovatele, jakož i samotné záznamy o těchto odstávkách.

Poskytovatel rovněž musí mít k dispozici **pohotovostní plány pro mimořádné situace, včetně havarijních** (business continuity plány), ideálně vycházející z ISO 22091 či ISO 22301. Ty by měly zahrnovat zejména definici procesu přípravy, aktualizace a testování pohotovostních plánů, zásady kontinuity provozu a cíle kontinuity provozu a samotné havarijní plány alespoň pro kritické funkce či součástí nabízené cloudové služby.

Pokud poskytovatel roste a chystá se na svůj první projekt v oblasti finančního outsourcingu, může

jen samotná příprava těchto dokumentů zabrat měsíce pilné práce. Pokud ale poskytovatel získal výše uvedené ISO certifikace nebo certifikace dle obdobných standardů, bude mít zpravidla veškeré tyto dokumenty a procesy připravené a celý proces hloubkové kontroly bude značně urychlen.

Umístění dat

Pro finanční instituci je současně nezbytné, aby od poskytovatele získala potvrzení a ujištění, v jaké zemi budou její data uložena a kde má poskytovatel datová centra. Dle místa uložení pak může zohlednit související rizika, která se budou lišit v případě infrastruktury v České republice, Evropské unii, Spojeném království nebo dokonce Spojených státech amerických. Zde se vedle regulace outsourcingu, který stanovuje zejména povinnost dostat se okamžitě k datům v případě krize poskytovatele, dostává ke slovu i GDPR, které bude doplňovat do smluv jak obvyklou zpracovatelskou doložku, tak podrobnější systémy řízení a řešení incidentů s dopadem na osobní údaje.

Případné předávání dat do USA nebo do jiných zemí mimo Evropský hospodářský prostor (EHP) musí být promítnuto do smluvní dokumentace a vnitřní dokumentace finanční instituce. V případě předávání dat mimo EHP musí instituce vybrat vhodný nástroj pro toto předávání dat, což jsou v současnosti nejčastěji tzv. Standardní smluvní doložky pro předávání dat mezi zeměmi EU a třetími zeměmi (také známé jako „SCCs[1]“). Pokud budou na základě těchto doložek předávána data mimo EHP, bude pro zajištění srovnatelné ochrany osobních údajů nutno doplnit k dokumentaci také tzv. transfer impact assessment a často i zavést dodatečná opatření k ochraně dat.[2]

Poskytovatel musí také zaznamenávat bezpečnostní události a incidenty: instituce by si měla ve smlouvě vymínit, že má přístup k záznamům o těch incidentech, které se týkají jí využívaných služeb, resp. jejích dat, a že o nich bude neprodleně informována, aby mohla mitigovat rizika vyplývající z jakéhokoliv neoprávněného přístupu k datům.

Vše výše uvedené lze zajistit vhodně nastavenou outsourcingovou smlouvou: pojďme se na ni podívat.

Outsourcingová smlouva je základ

Nyní přichází na řadu smlouva, kterou poskytovatel cloudových služeb na konci celého kontraktačního procesu s finanční institucí uzavírá. Smlouva musí jasně popisovat, jaké povinnosti jsou na poskytovatele cloudových služeb kladeny a vzájemné rozložení odpovědnosti mezi finanční institucí a poskytovatelem cloudu.

V rámci smlouvy lze využívat i obecné smluvní podmínky, které má poskytovatel cloudových služeb připravené: Mohou zde ovšem nastat problémy s jejich obecným nastavením v rámci běžných B2B vztahů, když by smluvní podmínky byly nastavené ve prospěch poskytovatele cloudových služeb způsobem, který by nebyl v souladu s požadavky finanční regulace a finanční instituce by tak na ně neměly přistoupit. Pro poskytovatele cloudu, který hodlá své služby nabízet i finančním institucím, tak lze doporučit přípravu specifického dodatku ke smlouvě či smluvním podmínkám, který bude reflektovat právě požadavky finanční regulace, popř. specifické dokumentace pro finanční instituce. To je ostatně běžnou praxí u velkých poskytovatelů cloudu. Stejně tak je v případě užití podmínek poskytovatele náročnější docílit porovnatelnosti nabídek jednotlivých poskytovatelů, instituce tak může preferovat užití její smlouvy, popř. respektování alespoň dílčích podmínek připravených institucí (například zaměřených na plnění regulatorních požadavků).

Co do obsahu samotné smlouvy, tato musí v první řadě obsahovat jasný a úplný popis externě zajištěné funkce, kterou bude poskytovatel cloudové služby zajišťovat. Součástí popisu jsou by měly být i jasně definované parametry dostupnosti a fungování outsourcované služby (SLA). Ty mohou být

upraveny (a v praxi často jsou) zmíněnými obecnými podmínkami poskytovatelů cloudových řešení s tím, že v rámci vzájemného vztahu se uplatní nejpřísněji nastavené parametry.

Zde je ale namístě technické ověření, jaké SLA parametry instituce skutečně potřebuje. Pokud je outsourcovaná funkce zásadní pro provádění plateb, je zřejmé, že instituce bude chtít maximálně přísné SLA parametry a výpadky budou zásadním problémem pro její podnikání. Pokud však instituce outsourcuje systém pro vnitřní procesy (např. HR, archivace dokumentů atd.), nemusí být ekonomické připlácet si výraznou přirážku za dostupnost na úrovni 99,999 %, když by instituci bez problému stačila i dostupnost nižší.

Jak zabezpečit informace?

Samostatným a důležitým bodem jsou informace a jejich bezpečnost. Už v rámci předchozích kroků včetně úvodního posouzení vhodnosti poskytovatele a jeho rámcové kontroly, resp. navazující hloubkové kontroly by měla mít finanční instituce jasný přehled o tom, jakým způsobem se budou u poskytovatele zpracovávat neosobní data i osobní údaje, kde budou uloženy nebo kam a jak se budou předávat. Smlouva pak tyto výsledky musí odpovídajícím způsobem zohlednit, aby byly splněny veškeré legislativní požadavky na úpravu ve smlouvě, která je stanovená zejména EBA pokyny. Dále je třeba splnit legislativní požadavky související s transparentností a výkonem práv subjektů osobních údajů, stanovené zejména GDPR.

Řízení dodavatelů a ochrana dat

Zásadním ustanovením bude v tomto případě vždy možnost využívat další subjekty zapojené do dodavatelského řetězce na straně poskytovatele, ať už se budou podílet na zpracování osobních údajů nebo na zajištění dalších činností nutných pro poskytovanou cloudovou službu. V případě outsourcingu kritické/důležité funkce by nový dodavatel měl vždy podléhat předchozímu výslovnému souhlasu finanční instituce: u ostatních funkcí je možné částečně využívat předpokládaného souhlasu pro lepší smluvní flexibilitu na straně poskytovatele, uvedené však nelze vždy doporučit jako best practise. Zde je namístě zohlednit také komerční realitu, kdy česká finanční instituce pravděpodobně nebude v pozici, aby si na globálním poskytovateli služeb vymínila možnost udělit nesouhlas se zapojením dílčího dodavatele, což by vedlo k nutnosti zásadních změn vnitřních procesů na straně takového poskytovatele.

Výpadky a incidenty

Dalším prvkem, který je třeba do smlouvy promítnout, jsou rizika a mitigační opatření, přičemž zde odkazujeme zejména na výše uvedené dokumenty o vnitřních postupech a opatřeních pro omezení rizik. Častým problémovým ustanovením je zde obvykle stanovená povinnost poskytovatele informovat o skutečnostech, které mohou mít dopad na poskytovanou službu (například plánované výpadky, nutné aktualizace, ukončení podpory určitého produktu apod.). Je zde potřeba jednoznačně vymezit, jaké skutečnosti má finanční instituce na mysli, a to ideálně za využití modelových situací ve smlouvě. V takovém případě se pak ve smlouvě daleko lépe popisují důsledky neposkytnutí těchto informací, které mohou mít podobu povinných součinností, aktualizací dokumentace, smluvních pokut a v krajních případech okamžitých výpovědí smlouvy bez náhrady nákladů.

Další oblastí je systém pro řízení bezpečnostních incidentů, jejich zaznamenávání, ohlašování a postupy jejich řešení. Tyto smluvní prvky zohledňují informace o poskytovateli cloudových služeb v rámci kontraktačního procesu získané v rámci hloubkové kontroly, současně je ale třeba dbát a správně adresovat rizika na straně finanční instituce, jak byla zjištěna na základě analýzy rizik. Smluvní prvky budou zde ovlivněny výsledkem této analýzy i s přihlédnutím k formě využívaného outsourcingu (zda jde o IaaS nebo SaaS).

Právo na audit a další povinnosti

Dále je třeba ve smlouvě upravit možnost auditu poskytovatele cloudových služeb, a to jak ze strany finanční instituce, tak ze strany nezávislého externího auditora nebo ČNB. Nezávislý externí auditor musí mít možnost provádět audit v pravidelných časových intervalech: ČNB a finanční instituce by pak měla mít možnost auditovat poskytovatele cloudové služby v jakékoliv odůvodnitelné situaci, a to včetně provádění on-site auditu (auditu na místě poskytování služby či uložení dat). Součástí je samozřejmě povinnost součinnosti poskytovatele v rámci těchto auditů: poskytovatel nesmí finanční instituci omezovat účinné uplatňování práv na přístup a na audit.

Zejména u velkých poskytovatelů cloudových služeb se pak setkáváme s tím, že toto právo (v kontextu velkého množství svých zákazníků) omezují a umožňují vykonat prostřednictvím doložené výsledků nezávislého auditu, tzv. „pool auditu“ spolu s dalšími zákazníky, popř. stanoví požadavek na předchozí oznámení a omezení rozsahu jen na nezbytnou míru. I tyto varianty jsou možné, avšak nesmí dojít k narušení práva finanční instituce na posouzení a ověření, jak je outsourcovaná služba v praxi poskytována a smlouva plněna. Současně tímto nesmí dojít k omezení auditního oprávnění ČNB.

Poskytovatel by dále za předem stanovenou cenu (nezávisí na tom, zda paušální nebo hodinovou) měl být schopen poskytovat finanční instituci podporu s provozem, a to včetně alokace personálu, který bude mít odpovídající kompetence a bude řádně proškolen pro poskytovanou službu. S tím souvisí i vnitřní bezpečnostní politiky poskytovatele ohledně striktních podmínek přístupu jeho pracovníků k datům finanční instituce. Ty by měla finanční instituce již znát v průběhu hloubkové kontroly a následně zohlednit ve smlouvě. V neposlední řadě pak může jít o úpravu postupů pro zamezení střetu zájmů.

Pozor na vendor lock-in

Samostatnou kategorií smlouvy je exitová strategie, jejíž nedostatečná úprava může mít za výsledek v lepším případě porušení pokynů EBA, v horším případě vznik vendor lock-in. Tímto pojmem se myslí závislost na produktech či službách konkrétního dodavatele, například z důvodu, že pro přechod k jinému dodavateli je nutno získat zdrojový kód, práva změny software či popis datové struktury, které však zákazník nemá. V takovém případě zbývají zákazníkovi často jen dvě možnosti, tj. pokračovat ve spolupráci za podmínek diktovaných dodavatelem (často výrazně méně výhodných, než nabízí konkurence), nebo stávající technické řešení opustit (tj. zahodit investované prostředky) a zvolit nákladný a často i rizikový (např. co do možnosti ztráty dat) přechod k novému dodavateli.

Finanční instituce by proto měla mít možnost odchodu od poskytovatele bez narušení její činnosti kdykoliv poptat už proto, že musí mít možnost smlouvu s okamžitou účinností vypovědět, a to jak na základě pokynu ČNB, tak z vlastní vůle. To částečně souvisí i s možností kontinuálně monitorovat kvalitu poskytovaných služeb, kterou by měla mít finanční instituce zahrnout ve smlouvě s poskytovatelem, aby v případě (trvalého) poklesu pod limitní parametry kvality měla banka možnost ukončit externí zajišťování funkce a převést její výkon na sebe nebo na nového poskytovatele.

Vhodné smluvní nastavení spolupráce finanční instituce a poskytovatele cloudu při exitu je tedy prvním povinným aspektem. Upozorňujeme zde i zejména na řádnou úpravu vzájemné spolupráce původního a nového poskytovatele při přenosu dat a úpravu postupu tohoto předávání. Výsledkem by mělo být rozložení jasně popsaných povinností, které povede k řádnému přenosu dat k novému poskytovateli, dokumentované likvidaci dat u poskytovatele původního a možnost provedení auditu, kterým lze obojí řádně ověřit a zdokumentovat. Smluvní ustanovení, zda a v jakém rozsahu náleží poskytovateli původního cloudu za tento přenos dat odměna, pak nesmí způsobit faktickou nemožnost tento přenos provést.

Druhým povinným aspektem je příprava strategie exitu, kterou lze jako smluvní povinností pověřit poskytovatele, popř. pro jejíž vytvoření lze poskytovateli uložit povinnost součinnosti. Tato strategie exitu bude pro finanční instituce obsahovat připravený seznam kroků, které instituce musí postupně učinit, aby byl proveden exit bez negativních dopadů na poskytování služeb, a pro tyto kroky odpovědné osoby. Ani jeden z aspektů není radno podcenit: nedostatečně nebo nevhodně upravený exit téměř vždy přinese vyšší náklady, než které by byly třeba na jeho řádnou implementaci včetně povinností součinnosti, přípravy dokumentace a řádné úpravy předávání dat. Dobře připravená strategie exitu umožní pracovníkům IT oddělení instituce nebo konkurenčního poskytovatele cloudového řešení na jejím základě převzít provoz funkce, aniž by došlo ke krizím v procesu převzetí. Pokud toto neplatí (což ověřte ještě před podpisem smlouvy s poskytovatelem), je třeba exitové povinnosti zpřesnit.

Ačkoliv by instituce měly být připraveny provést exit v zásadě kdykoliv, ne vždy je možné přesunout celou funkci způsobem, který umožní plynulý přechod mezi řešeními. Instituce by tak měly do svých smluvních i finančních plánů zahrnout přechodná období, kdy bude využívat dva poskytovatele cloudových služeb. I tak ale obvykle budou tato přechodná období výhodnější než problémy vzniklé při migraci funkce nebo úplná nemožnost od poskytovatele odstoupit.

Peníze až na posledním místě?

Finanční závazky obou stran jsou samozřejmým prvkem smlouvy: Poskytovatel cloudové služby na sebe v tomto přísně regulovaném odvětví bere značnou zodpovědnost a musí splnit celou řadu regulatorních povinností, proto může být odměna za externí zajištění funkce banky nebo pojišťovny vyšší než za poskytování srovnatelných cloudových služeb mimo finanční sektor. Již výše byly zmíněny náhrady za alokaci personálu, za poskytování podpory nebo za přenos dat v rámci exitu, značné náklady jsou spojeny také s přípravou nutné dokumentace popsané výše.

Ve smlouvě je rovněž potřeba jednoznačně vyjasnit nároky stran, která vzniknou v případě nedostupnosti služby, bezpečnostních incidentů a vzniku škody na straně finanční instituce nebo osob, kterým škoda v důsledku nedostupnosti či nefunkčnosti outsourcované služby vznikla. Tato ustanovení do velké míry navazují nebo reflektují předchozí části smlouvy, zejména vymezení poskytovaných služeb, jejich dostupnosti a záruk za zabezpečení dat.

Cloud ve finančním sektoru: ano či ne?

Zavedení outsourcingu ve finančních institucích vyžaduje úsilí, čas a vynaložené prostředky jak na straně institucí, tak poskytovatelů outsourcovaných služeb. V případě cloudových služeb a řešení to platí ještě více. Z pohledu finančních institucí však lze podle autorů konstatovat, že díky outsourcingu a zaměření se na klíčové funkce a obsluhu klientů mohou finanční instituce dosahovat lepších výsledků, ať už v případě faktického poskytování bankovních, platebních či dalších služeb, tak i zajištění ochrany a dostupnosti dat.

Požadavky na řízení outsourcingu a přípravu souvisejících právních dokumentů jsou rozsáhlé. Související regulatorní pravidla, která jsme v našem seriálu představili, jsou však poměrně návodná, byť někdy mohou omezovat možnosti výběru poskytovatelů. Právní požadavky jsou jasně definovány a záleží na finančních institucích a poskytovatelích cloudových řešení, zda je budou v praxi plnit, kolik kapacit na ně vyčlení a zda se spokojí s formálním souladem s regulací, nebo zda regulace využijí k důslednému zmapování a správnému nastavení spolupráce.

Za autory článků lze určitě doporučit, aby se instituce zaměřily na materiální splnění legislativních požadavků, a to při zohlednění specifik konkrétního projektu. Splnění všech právních požadavků na využití cloudového outsourcingu je náročné, ale v konečném důsledku pomůže instituci zajistit

poskytování svých služeb a plnění všech právních a regulatorních povinností i v případě budoucích problémů či výpadku na straně poskytovatele cloudu.

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] Evropská komise. Standardní smluvní doložky pro předávání údajů mezi státy EU a státy mimo EU. [cit. 2022-07-21]. dostupné na www, k dispozici >>> zde.
[2] Evropský sbor pro ochranu osobních údajů. Doporučení č. 01/2020 o opatřeních, která doplňují nástroje pro předávání s cílem zajistit soulad úrovní ochrany osobních údajů ze dne 18. června 2021. EBA/GL/2019/02. [cit. 2022-07-21]. 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.
[**] **Cloudy a právo - 2 díl: Tisíc a jeden právní požadavek**, dostupné na www, k dispozici >>> zde.
[***] **Cloudy a právo - 3 díl: Povinnosti finančních institucí**, dostupné na www, k dispozici >>> zde.

Další články:

- 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
- DEAL MONITOR