



Vzniká nový druh: virtuálny právnik

IT PRÁVO | Cloudové úložiská dát začínajú byť v advokácii nevyhnutnosťou. Sú bezpečnejšie ako klasické archívy a šetria náklady.

Martin Ducar

martin.ducar@mafrasslovakia.sk

Žiadna kancelária, minimum nákladov a len balíček cloudových služieb a pripojenie na internet. Toto je budúcnosť poskytovania právnych služieb. Virtuálni právnici sú už dnes napríklad v Spojených štátoch plnohodnotnou protiváhou k bežným advokátskym kanceláriám. Tie sa pomaly, ale isto presúvajú z obchodných centier do pohodlia obývačiek. Komunikácia s klientmi prebieha na diaľku a len výnimočne pri osobných stretnutiach. Zatiaľ však drvivá väčšina právnych firiem funguje hybridne online, ale aj v klasických biznis priestoroch. Poskytovanie cloudových služieb v advokácii je momentálne predmetom diskusie, ani právo Európskej únie, ani slovenský právny poriadok na túto tému zatiaľ nereagovali. Keďže zákon o advokácii cloud nezakazuje, technologický pokrok má nateraz zelenú.



Potenciálna hrozba používania cloudu spočíva predovšetkým v obave, že sa servery poskytovateľa nachádzajú v tretích krajinách.

ILUSTRÁČNÁ SNÍMKA: DREAMSTIME

úniku dát neoprávnenej osobe a zároveň v prípade ich vydania by orgánom činným v trestnom konaní v podstatnej miere skomplikovalo ich zneužitie," hovorí pre HN Pázmányová. Paradoxne by sa týmto spôsobom mohla dosiahnuť väčšia ochrana dát klientov ako pri uchovávaní dokumentov v písomnej podobe alebo na vlastnom serveri.

Červené tlačidlo

Ďalšou alternatívou sú podľa advokátky riešenia typu „red button“. Aplikácia funguje na princípe, že osoba ukládajúca dáta v cloude má taktiež možnosť ich okamžite, stlačením červeného tlačidla, zmazať. „Týmto spôsobom možno efektívne zlikvidovať dáta, ak hrozí, že sa k nim dostane nepovoláná osoba, a pritom ich má aj naďalej zálohované k dispozícii,“ odporúča Pázmányová.

Európske a americké advokátske odborné orgány vydali pre advokátov uvažujúcich o využívaní cloudových služieb rozsiahle odporúčania.

„V ich zmysle by mal advokát preveriť napríklad meno poskytovateľa na trhu, jeho skúsenosti a špecializáciu, sídlo a miesto uloženia serverov, potenciálne riziká straty či zneužitia údajov alebo napríklad aj formu šifrovania a zabezpečenia,“ tvrdí Vojčík. Advokát by si mal preveriť taktiež rozsah zodpovednosti poskytovateľa, jeho poistenie, možnosti ukončenia zmluvy a migrácie dát zo serverov poskytovateľa na advokátom určené miesto bez toho, aby si pôvodný poskytovateľ zachoval ich kópiu. Dôležité je tiež zabezpečiť, že poskytnuté dáta do cloudu nebudú v žiadnom prípade poskytnuté tretím osobám.

Pozor na tretie krajiny

Advokát je povinný zachovávať mlčanlivosť o všetkých veciach, o ktorých sa dozvedel pri výkone svojej práce. Preto nie je napríklad v prípade súdneho konania povinný vydať listinu alebo iné veci, ktoré sú zo zákona diskretne. Môže však advokát dáta uložené na serveroch považovať za miesto, ktoré vôbec mlčanlivosti podlieha? Podľa českého najvyššieho súdu áno. U susedov dokonca ochranu písomných a elektronických dát zrovnoprávnili. „Súd vyslovil názor, že dáta uložené na cloudových úložiskách patria pod priestory, v ktorých advokát vykonáva advokáciu,“ hovorí pre HN manažujúci part-

ner advokátskej kancelárie Vojčík & Partners Leo Vojčík.

Na druhej strane poskytovateľ cloudu, ktorý má takéto údaje k dispozícii na svojich serveroch, viazaný zákonnou mlčanlivosťou byť nemusí. Kritika cloudu, ktoré majú servery uložené napríklad na území Spojených štátov, poukazuje aj na nedostatočnú ochranu osobných údajov americkou legislatívou. Fyzické umiestnenie má teda význam aj z hľadiska ochrany osobných údajov. Pri používaní cloudu dôjde takmer vždy k ich prenosu, a to napríklad osobných údajov zamestnancov alebo klientov. Potenciálna hroz-



Šifrovanie v cloude zabráni úniku dát a zároveň v prípade ich vydania orgánom činným v trestnom konaní skomplikuje ich zneužitie.

Veronika Pázmányová, vedúca advokátka v kancelárii Glatzová & Co

ba používania cloudu tak môže spočívať predovšetkým v obave, že sa servery poskytovateľa nachádzajú v tretích krajinách, kde právny poriadok umožňuje ich kontrolu štátnymi orgánmi. „Advokát by sa mohol dozvedieť o prípadnej kontrole servera poskytovateľa až po jej vykonaní, čo je z pohľadu advokáta a jeho klienta nežiaduce,“ upozorňuje Vojčík.

To, či je e-uloženie dát bezpečnejšie ako napríklad ich fyzické archivovanie v archívoch advokáta alebo u tretích osôb, je otáznosť. Všeobecne však žiadna forma dodržiavania povinnosti mlčanlivosti nie je absolút-

nou zárukou, že sa k chráneným dokumentom nikto nikdy nedostane. „Riziko tu existuje rovnako ako pri uchovávaní písomností v písomnej podobe alebo ich uchovávaní elektronicky na vlastných serveroch, keďže písomnosti možno ukradnúť a servery hacknúť,“ myslí si vedúca advokátka kancelárie Glatzová & Co. Veronika Pázmányová.

Dáta pod zámkom

Riešením môže byť kvalitné šifrovanie ukladaných dát v cloude, pričom heslo k nim by mal len advokát a jeho zamestnanci, a teda osoby viazané zákonnou mlčanlivosťou. „Zabránilo by sa

NÁZOR Z PRAXE

Za stratu uožených dát cloudoví poskytovatelia často vôbec neručia

Zmluvy o poskytovaní cloudovej služby neraz obsahujú právne nevýhodné podmienky.

Cloud computing je v súčasnosti využívaný mnohými malými a strednými firmami. Umožňuje im totiž významne šetriť náklady, napríklad za nákup a správu vlastnej IT infraštruktúry či softvérových licencií. S využívaním tejto technológie sú spojené viaceré riziká, ktorých by si firmy mali byť vedomé.

Čo je cloud computing?

Cloud computing je spôsob poskytovania IT služieb na diaľku, najmä prostredníctvom internetu. Spočíva v tom, že zákazník od poskytovateľa získa ako službu IT infraštruktúru, napríklad server, ktorý sa využije ako úložisko pre vlastné dáta, platformu pre vývoj a hosting svojich aplikácií alebo najčastejšie o určitý softvér. Takouto softvérovou službou môže byť e-mail, účtovný softvér či úložisko. Ten však nie je nainštalovaný vo firme – u zákazníka, ale na cudzom vzdialenom serveri, ktorý môže a nemusí patriť

poskytovateľovi služby alebo jeho subdodávateľom. Zákazník si teda navonok prenajíma cudzie IT zdroje a na diaľku nimi spracúva vlastné dáta alebo e-dokumenty.

Nevýhodné zmluvné podmienky

Malé a stredné firmy majú zvyčajne len malú možnosť ovplyvniť obsah zmluvy o poskytovaní cloudovej služby. Tie pritom často umožňujú jednostranne prerušiť alebo ukončiť poskytovanie služby a vylučujú zodpovednosť poskytovateľa za škody spôsobené zákazníkom, vrátane prípadov, keď dôjde k strate alebo kompromitácii uložených dát.

Ochrana osobných údajov

Firmy využívajúce cloudové služby by mali taktiež brať do úvahy zákon o ochrane osobných údajov. Podľa neho sú práve ony zodpovedné za spracovanie osobných údajov prostredníctvom cloudu a jeho súlad so zákonom.

Spoločnosti si musia byť vedomé, že ak si zvolia cloudového poskytovateľa, ktorý údaje ukladá na serveroch mimo Európskej únie, musia navyše splniť podmienky na cezhraničný prenos osobných údajov poskytovateľovi, ktoré sú značne komplikované. Je bežné, že zákazník nevie, kde všade sa prenášajú, ukladajú či zálohujú jeho dáta, teda kde sú servery poskytovateľa alebo jeho subdodávateľov a kto k jeho dátam môže mať prístup. Zákazník teda často nemá dostatočné informácie o tom, ako sú spracúvané údaje, za ktoré podľa zákona zodpovedá a za ktoré mu môžu byť uložené pokuty.

Firmy by nemali podceňovať výber cloudového poskytovateľa, čítanie jeho všeobecných podmienok či politiky súkromia a zväziť prípadne aj drahšieho poskytovateľa, ktorého zmluvné podmienky budú pre ich podnikanie v konečnom dôsledku menším rizikom.

Výhody cloudu v advokácii

Zníženie nákladov na vlastníctvo a údržbu IT štruktúry

Podpora mobility dát v rámci výkonu povolania bez obmedzenia miesta a času

Vyššia bezpečnosť uchovávaní dát v elektronickej podobe, a to v prípade dôveryhodných poskytovateľov

Sofistikované zálohovanie kópií listinnej dokumentácie (výhoda napríklad v prípade živelných pohrôm v mieste sídla kancelárie)



Petra Zabudková, IT právnička Disig, a. s.