USMERNENIA CCBE

PRE ADVOKÁTOV TÝKAJUCE SA VYUŽÍVANIA CLOUDOVÝCH SLUŽIEB

Conseil des barreaux européens – Council of Bars and Law Societies of Europe
association internationale sans but lucratif
Rue Joseph II,40 – bte 8 – B 1000 Brussels – Belgium – Tel.+32 (0)2 234 65 10 –E-mail ccbe@ccbe.eu – www.ccbe.eu

Usmernenia CCBE pre advokátov týkajúce sa využívania cloudových služieb

OBSAH

I. ÚVOD

1. Rozsah pôsobnosti usmernení

Účelom tohto dokumentu je prispieť k zvýšeniu povedomia o rôznych rizikách spojených s cloudovými službami. Usmernenia v druhej časti dokumentu sú určené členským advokátskym komorám a právnickým spoločnostiam Rady advokátskych komôr Európy (CCBE) a upriamujú pozornosť na určité otázky, ktoré budú advokáti s najväčšou pravdepodobnosťou musieť riešiť pri prijímaní informovaných rozhodnutí v oblasti poradenstva alebo využívania cloudových služieb.

2. Cloud computing

Pojem „cloud computing“ alebo cloudové služby je všeobecný výraz pre infraštruktúru informačných technológií, ktorá slúži na ukladanie a spracovávanie údajov a softvéru na diaľku v dátovom stredisku poskytovateľa cloudových služieb alebo v prepojených strediskách, ktoré sú dostupné vo forme služby prostredníctvom internetu. Podľa Amerického národného inštitútu pre normy a technológie (NIST) cloudové služby umožňujú všadeprítomný, pohodlný a na požiadanie dostupný prístup k zdieľanému fondu konfigurovateľných výpočtových zdrojov, akými sú siete, servery, úložiská, aplikácie a služby, ktoré môžu byť poskytnuté rýchlo a pri vynaložení minimálneho úsilia manažmentu alebo interakcie s poskytovateľom služieb.[1]

3. Cloudové služby v agende Európskej komisie

Európska komisia zdôraznila potrebu prijať celoeurópsku stratégiu pre oblasť cloudových služieb v dokumente Digitálny program pre Európu. Tri hlavné oblasti, ktoré by sa mali riešiť v tomto kontexte s cieľom zabezpečiť Európe maximálny prínos z cloudových služieb, zahŕňajú:

- právny rámec: ide najmä o ochranu údajov a právo na súkromie, vrátane ich medzinárodného rozmeru. Týka sa to aj právnej úpravy s dopadom na zavedenie cloudových služieb vo verejných a súkromných organizáciách,
- technické a obchodné základy: cieľom je rozšíriť podporu pre výskum v EÚ so zameraním na kritické otázky, akými sú bezpečnosť a dostupnosť cloudových služieb,
- trh: podporu získajú pilotné projekty zamerané na spustenie cloudových služieb. S cieľom maximálne využiť potenciál verejného obstarávania bude Komisia prehlbovať vzťahy s partnermi verejného sektora v členských štátoch a na regionálnej úrovni, aby sa zabezpečil spoločný prístup k otázke cloudových služieb.

Ako Komisia uvádza, v niektorých oblastiach sa táto práca už začala, vrátane verejnej konzultácie z roku 2011, na ktorú reagovala svojím stanoviskom CCBE.[2]

4. Cloudové služby pre advokátov: prínos a riziká

Advokátske kancelárie - rovnako ako iné podnikateľské subjekty - využívajú cloudové služby z rôznych dôvodov. Zníženie nákladov predstavuje jeden z nich. Cloudové služby môžu viesť k zníženiu nákladov na kúpu serverov a softvéru alebo na zamestnancov starajúcich sa o údržbu serverov. Navyše, mnohé cloudové aplikácie umožňujú prístup z akéhokoľvek miesta, a preto uľahčujú prácu mimo pracovných priestorov, čím znižujú náklady na nájom a cestovanie, rovnako tiež uľahčujú prepojenie jednotlivých kancelárií, ktoré majú niekoľko pobočiek.

Cloudové služby môžu zjednodušiť výpočtovú prácu mnohým advokátskym kanceláriám. V prípade firiem s existujúcou IT infraštruktúrou softvérové programy na báze cloudu môžu znížiť celkovú zložitosť informačných technológií. Podobne v prípade začínajúcich kancelárií bez zabehnutých softvérových systémov je relatívne jednoduché vytvoriť od základov efektívny systém riadenia využitím cloudových softvérových programov.

---

[1] P. Mell a T. Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology, US Department of Commerce (január 2011).

[2] Odpoveď CCBE na verejnú konzultáciu Európskej komisie o cloudových službách.

Systém cloudových služieb zvyčajne poskytuje väčšiu flexibilitu pre konečného užívateľa vzhľadom na to, že cloudové služby sú prístupné cez internet z akéhokoľvek miesta v akomkoľvek čase. Na rozdiel od softvérových systémov na stolových počítačoch alebo softvérových systémov s využitím serverov platformy založené na cloude možno využiť pri akomkoľvek type počítača alebo zariadenia pripojiteľného na internet s využitím akéhokoľvek operačného systému. Pokiaľ majú užívatelia prístup k internetu, môžu mať zároveň prístup k súborom uloženým v cloude. Cloudové služby ako také majú potenciál umožniť advokátom poskytovanie právnych služieb novým a efektívnejším spôsobom v prospech ich klientov.

Popri mnohých nezanedbateľných výhodách však cloudové služby môžu priniesť so sebou súbor rizík a výziev pre advokátov, v prvom rade vo vzťahu k ochrane údajov, po druhé vo vzťahu k zásade mlčanlivosti a dôvernosti, a po tretie vo vzťahu k ďalším stavovským povinnostiam osôb vykonávajúcich advokáciu. Hoci prvá a druhá oblasť sú úzko prepojené, nie sú nevyhnutne identické. Advokát by si tiež mal byť vedomý komerčných rizík, ktorým sa môže vystaviť, napr. následkom dočasnej nedostupnosti jeho cloudových služieb, ktoré môže spôsobiť narušenie kontinuity poskytovania právnych služieb.

V porovnaní s používaním počítačov a serverov v priestoroch užívateľa alebo plne pod kontrolou užívateľa podstata cloudových služieb spočíva vo využití tretej osoby, vzdialeného poskytovateľa cloudových služieb, vrátane služby uchovávania údajov. Poskytovateľ cloudových služieb v zásade vlastní alebo prenajíma od iných poskytovateľov obrovské dátové strediská, ktoré môžu byť v prípade najväčších poskytovateľov cloudu poprepájané, čím vytvárajú sieť serverov, z ktorých niektoré môžu byť umiestnené v krajinách mimo EHP, kde sa uplatňujú iné a možno aj nižšie štandardy ochrany údajov. V niektorých prípadoch sú tieto strediská umiestnené v krajinách, ktoré nerešpektujú v plnej miere princípy právneho štátu. Navyše, ak existuje sieť cloudových serverov, údaje môžu byť vyčlenené a uložené na rôznych serveroch (dokonca v rozličných krajinách), a prípadne môžu neustále migrovať medzi týmito servermi. Vo väčšine prípadov prevádzkovateľ siete si sám nie je vedomý, kde presne sa v danej sieti konkrétny údaj v danom čase nachádza. Tieto okolnosti zjavne otvárajú pre advokátov špecifické otázky a možné obavy týkajúce sa štandardov ochrany údajov a ochrany pred potenciálnou krádežou, stratou alebo zverejnením dôverných informácií.

Advokátov sa najviac dotýkajú nasledovné otázky vyplývajúce z cloudových služieb[3]:

Sporné otázky spojené s profesijným tajomstvom a ochranou osobných údajov:

- údaje uložené v prostredí dátových úložísk môžu byť vystavené riziku neoprávneného prístupu buď v podobe neoprávneného fyzického vstupu do priestorov, v ktorých sú servery umiestnené, alebo elektronicky, buď zamestnancami poskytovateľa alebo subdodávateľmi alebo tretími osobami, napr. hackermi cez internet,
- využívanie cloudových služieb advokátmi vedie k potrebe objasniť, či treba získať súhlas klienta pred použitím cloudových služieb na uchovanie alebo prenos dôverných informácií,
- využívanie cloudových služieb advokátmi vedie k potrebe objasniť mieru zodpovednosti advokáta v súvislosti so spoľahlivosťou a bezpečnosťou cloudových úložísk, na ktorých sa nachádzajú údaje klienta.

Sporné otázky spojené s extrateritorialitou:

- cloudové služby môžu zahŕňať spracovávanie dát na serveroch v štátoch, ktoré majú slabšiu efektivitu mechanizmov právnej ochrany elektronicky uchovávaných informácií, než predpisuje legislatíva v rámci EÚ/EHP, a ktoré nespadajú do regulačného rámca EÚ. Poskytovatelia cloudových služieb môžu podliehať miestnym vnútroštátnym predpisom, ktoré ich zaväzujú odovzdať údaje európskych advokátov uložené na cloudových serveroch národným autoritám tretích štátov mimo EÚ,
- ďalším rizikovým faktorom je zahraničná legislatíva s predĺženou rukou, v zmysle ktorej existuje povinnosť sprístupniť informácie na žiadosť vnútroštátnych orgánov nielen v prípade domácich spoločností poskytujúcich cloudové služby, ale aj v prípade zahraničných

[3] Väčšina týchto otázok je rozpracovaná v nasledovných štúdiách: The Law Society of Scotland's Cloud Computing - Advice for the profession (Škótska právnická spoločnosť: Cloud computing – odporúčania pre advokátov) (2012) a American Bar Association's Commission on Ethics 20/20 Working Group on the Implications of New Technologies Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology (Výbor pre etiku 20/20 Americkej advokátskej komory, Pracovná skupina pre problematiku dopadu nových technológií: tematický dokument o dôvernosti informácií klienta a používaní technológie advokátmi) (September, 2010).

spoločností, ktoré sú vo výlučnom vlastníctve spoločností domovského štátu. V tomto smere môžu byť cloudové služby predmetom nejasných postupov, ako má poskytovateľ reagovať, alebo aké následky bude mať odmietnutie poskytovateľa sprístupniť informácie na žiadosť vládnych orgánov.

Sporné otázky spojené s (miestnymi) deontologickými/regulačnými požiadavkami:

- problémy môžu nastať aj z dôvodu rozdielnych alebo protichodných miestnych požiadaviek národných advokátskych komôr alebo právnických spoločností, ktoré musia advokáti dodržiavať pri práci s dôvernými údajmi.

Sporné otázky spojené s uzatváraním zmluvy s poskytovateľom cloudových služieb:

- cloudové služby môžu byť predmetom nejasnej úpravy, pokiaľ ide o vlastníctvo uložených údajov,
- poskytovatelia cloudových služieb môžu zlyhať v otázke adekvátneho zálohovania údajov a/alebo poskytnutia nepretržitej dostupnosti ich cloudových služieb,
- cloudové služby môžu byť predmetom nedostatočného zašifrovania,
- cloudové služby môžu byť predmetom nejasnej úpravy, pokiaľ ide o informovanie zákazníkov o narušení bezpečnosti,
- cloudové služby môžu byť predmetom nejasnej úpravy, pokiaľ ide o celkové obdobie uchovávania údajov,
- cloudové služby môžu byť predmetom nejasnej úpravy, pokiaľ ide o zničenie údajov, ak si advokátska kancelária viac neželá, aby dané údaje boli dostupné na cloudovom serveri, alebo ak žiada o presun údajov do inej advokátskej kancelárie,
- cloudové služby môžu spôsobiť problémy v prípade, keď advokátska kancelária rozviaže vzťah s poskytovateľom cloudových služieb, prípadne ak sa zmení osoba poskytovateľa, alebo poskytovateľ skončí na trhu s cloudovými službami. Vtedy môže vzniknúť problém s jednoduchým prístupom k dátam pomocou dostupného softvéru.

5. Usmernenia CCBE o cloudových službách

Ako bolo načrtnuté vyššie, cloudové služby predstavujú pre advokátov konštruktívnu alternatívu k tradičnému systému infraštruktúry informačných technológií. Okrem značných výhod však predstavujú aj súbor rizík a výziev majúcich dopad na schopnosť advokátov dodržiavať zákonné povinnosti ako správcovia údajov v zmysle smernice na ochranu údajov, v zmysle stavovských etických kódexov a predpisov, najmä pokiaľ ide o zásadu mlčanlivosti a v zmysle požiadaviek regulačných systémov, pod ktoré spadajú, napr. povinnosť viesť účtovné záznamy, ktoré môžu podliehať kontrole príslušného regulačného orgánu, alebo povinnosť zabezpečiť kontinuitu podnikania v prípade, ak advokátska kancelária ukončí poskytovanie právnych služieb.

Je nevyhnutné, aby advokáti pri rozhodovaní o otázke využitia cloudových služieb vo svojich kanceláriách prijali kroky smerom k zabezpečeniu ochrany údajov klienta a k zachovaniu dôvernosti vzťahu s klientom a aby venovali adekvátnu pozornosť možným vyššie uvedeným rizikám. V praxi však môže nastať situácia, kedy advokát, podobne ako iný spotrebiteľ, nebude mať dostatok informácií na to, aby s istotou považoval bezpečnostné opatrenia za postačujúce. V tejto súvislosti CCBE pripravila súbor usmernení, ktoré sa týkajú využívania cloudových služieb advokátmi. Ich účelom je zvýšiť povedomie advokátov o rôznych rizikách spojených s cloudovými službami a pomôcť advokátom prijímať informované rozhodnutia týkajúce sa technológie.

II. USMERNENIA CCBE PRE ADVOKÁTOV TÝKAJÚCE SA VYUŽÍVANIA CLOUDOVÝCH SLUŽIEB

Národné advokátske komory a právnické spoločnosti by mali advokátov, ktorí uvažujú o využití cloudových služieb pre svoje kancelárie, upozorniť, aby zvážili nasledovné aspekty:

A. Predpisy na ochranu osobných údajov a princíp mlčanlivosti advokáta

V prvom rade by advokáti pri otázke využitia cloudových služieb mali ako všeobecné pravidlo vziať do úvahy ustanovenia predpisov o ochrane osobných údajov a princíp mlčanlivosti advokáta. Mali by si najmä preveriť, či je v zmysle vnútorných stavovských predpisov dovolené ukladať dáta mimo priestorov advokátskej kancelárie, a ak áno, ubezpečiť sa, že poskytovateľ cloudových služieb nepodlieha jurisdikcii s predĺženou rukou, ktorá ho zaväzuje odovzdať údaje európskych advokátov uložené na cloudovom serveri národným/vnútroštátnym orgánom tretích štátov mimo EÚ. Advokátom odporúčame zvážiť, či vzhľadom na tieto obavy v danom prípade nie je vhodnejšie využiť cloudovú službu od poskytovateľa v rámci EHP a od poskytovateľa, ktorý nepodlieha jurisdikcii s predĺženou rukou (bez ohľadu na jeho sídlo), pokiaľ je to možné zistiť.

B. Predbežný prehľad riešení cloudových služieb

Advokátske kancelárie bez výnimky spracovávajú rozličné druhy údajov, na ktoré sa vzťahujú rôzne požiadavky na zaobchádzanie a ochranu, najmä s prihliadnutím na prvoradú povinnosť profesijného tajomstva/mlčanlivosti. Advokáti zvažujúci využitie cloudových služieb by mali v prvom rade porozmýšľať nad modelom služby, ktorý by vhodne splnil súčasné a budúce potreby ich kancelárií. Pri používaní cloudového softvéru ako služby[4] alebo cloudovej infraštruktúry ako služby[5] advokáti budú musieť zabezpečiť, aby boli v oboch prípadoch splnené podmienky na spracovávanie a uchovávanie údajov, ku ktorým s najväčšou pravdepodobnosťou patria osobné a citlivé údaje, rovnako ako aj informácie, na ktoré sa vzťahuje povinnosť mlčanlivosti. Advokáti, ktorí údaje spracovávajú externe, preto musia byť informovaní a vedomí si týchto aspektov. Pri prenose a uchovávaní údajov treba tiež zvážiť vhodnosť kódovania/šifrovania údajov.

Za daných okolností, ak advokát plánuje využiť cloudové služby, v prvom rade sa musí rozhodnúť, či využije cloudový softvér alebo cloudovú infraštruktúru.

Po druhé, cloudové služby môže poskytovať verejný alebo súkromný poskytovateľ. Verejný poskytovať cloudových služieb ponúka služby, ktoré môže využiť ktokoľvek, zatiaľ čo súkromný poskytovateľ cloudových služieb bude v zásade vo vlastníctve a/alebo pod kontrolou malej skupiny subjektov. Napríklad, v niektorých členských štátoch sa advokáti z vlastnej iniciatívy spojili za účelom vytvorenia súkromného cloudu. Rozdiel medzi verejným a súkromným cloudom zaváži najmä pri rozhodovaní o tom, ktorý poskytovateľ predstavuje nižší rizikový faktor, napr. pokiaľ ide o možnosť uchovávania údajov na serveroch umiestnených mimo územia EHP, alebo pokiaľ ide o jurisdikciu s predĺženou rukou. Použitie verejného cloudu nie je automaticky nevhodné pod podmienkou, že advokát predbežne vyhodnotil riziko v súvislosti s poskytovateľom, bezpečnosťou strediska údajov a ustanoveniami dohody o rozsahu/úrovni poskytovaných služieb. V prípade, že pri tomto hodnotení rizika vzniknú obavy, je možné, že poskytovatelia (najmä menšie a stredne veľké podniky) budú ochotní upraviť svoje služby, a/alebo spoločne rokovať o zmene zmluvných podmienok.

Pred uzavretím zmluvy by si mal advokát ako konečný užívateľ cloudových služieb overiť:

[a] skúsenosti,

---

[4] Cloudový softvér ako služba (SaaS - Cloud Software as a Service): IaaS: Poskytovateľ poskytuje prostredníctvom internetu služby rôznych aplikácií a sprístupňuje tieto aplikácie konečným užívateľom. Tieto služby majú často nahradiť bežné aplikácie, ktoré by si používatelia museli inštalovať na svojich lokálnych systémoch. Používatelia teda potom majú externalizovať svoje údaje konkrétnemu poskytovateľovi služby. Platí to napríklad v prípade typických kancelárskych aplikácií založených na webe, ako sú tabuľkové editory, nástroje na spracovanie textu, komputerizované registre a záznamníky, zdieľané kalendáre, atď. Tieto služby však zahŕňajú aj cloudové e-mailové aplikácie.
Zdroj: Pracovná skupina zriadená podľa článku 29, Stanovisko 05/2012 ku cloud computingu

[5] Cloudová infraštruktúra ako služba (IaaS – Cloud Infrastructure as a Service): Poskytovateľ prenajíma technologicky vzdialené servery, ktoré môžu koneční užívatelia v súlade s mechanizmami a dojednaniami využívať. Cieľom je zjednodušiť, zefektívniť a umožniť nahradenie IT systémov nachádzajúcich sa v priestoroch spoločnosti a/alebo používanie prenajatej infraštruktúry spoločne s používaním systémov spoločnosti. Takíto poskytovatelia sú zvyčajne špecializovanými trhovými aktérmi a využívajú fyzickú a komplexnú infraštruktúru, ktorá často zahŕňa viacero geografických oblastí.
Zdroj: Pracovná skupina zriadená podľa článku 29, Stanovisko 05/2012 ku cloud computingu

[b] povesť,

[c] špecializáciu,

[d] sídlo a prevádzku poskytovateľa cloudových služieb.

Nezávisle od toho by mal advokát overiť nasledovné:

[a] solventnosť, spoľahlivosť, vlastníctvo a kapitálovú primeranosť poskytovateľa,

[b] potenciálny konflikt záujmov,

[c] riziko zneužitia uchovávaných informácií,

[d] presné miesto, kde sa nachádzajú severy,

[e] v rámci svojich možností fyzickú a elektronickú bezpečnosť serverov a dátového strediska, v ktorom sú umiestnené

[f] platnú občianskoprávnu, trestnoprávnu a verejnoprávnu úpravu.

C. Predbežné hodnotenie citlivosti údajov

Všetky advokátske kancelárie spracovávajú rozličné druhy údajov, na ktoré sa vzťahujú rôzne požiadavky na zaobchádzanie a ochranu. Každé rozhodnutie uchovávať informácie na cloudovom serveri musí byť nevyhnutne spojené s vyhodnotením typu informácie (údaje o zamestnancoch, údaje o trestných činoch, všeobecné právnické archívy a pod.) a posúdením úrovne ochranného opatrenia, ktoré by malo byť prijaté.

D. Posúdenie bezpečnostných opatrení

Akékoľvek hodnotenie poskytovateľov cloudových služieb by malo zahŕňať vyhodnotenie prijatých opatrení technickej, fyzickej a organizačnej bezpečnosti v súlade s národnými a medzinárodnými štandardmi riadenia rizika v oblasti informačných technológií, napr. ISO 27001:2005 (systém riadenia informačnej bezpečnosti) a ISO 9001 (systém riadenia kvality). Certifikáty vydané uznávanými audítormi informačných technológií môžu slúžiť ako vhodné kritérium hodnotenia. Tam, kde sa dá, by mal advokát tiež zhodnotiť spoľahlivosť vlastných bezpečnostných štandardov v rámci advokátskej kancelárie, a to prijímaním pravidiel týkajúcich sa informačných a komunikačných technológií a informovaním a vzdelávaním svojich zamestnancov. Vzhľadom na to, že advokátske kancelárie zriedkavo úspešne realizujú v plnom rozsahu účinný systém manažmentu hesiel, odporúčame zvážiť tokenizáciu alebo zavedenie elektronických identifikačných preukazov pri prihlasovaní sa k službe. Advokáti by vo všeobecnosti mali vždy zvážiť odbornú podporu a radu pri výbere a monitorovaní poskytovateľov cloudových služieb.

E. Porovnanie existujúcej infraštruktúry informačných technológií v advokátskej kancelárii s ukladaním údajov do cloudu

Pri hodnotení cloudových služieb by mali advokáti vykonať porovnanie s ich súčasnou infraštruktúrou informačných technológií v advokátskej kancelárii. Toto hodnotenie umožní advokátskej kancelárii rozhodnúť sa, či zmena v prospech cloudovým úložísk prispeje k zníženiu alebo zvýšeniu rizík.

F. Hodnotenie schopnosti obnoviť dáta v prípade zlyhania poskytovateľa cloudovej služby, zlyhania advokátskej kancelárie alebo sporu zo zmluvného vzťahu medzi poskytovateľom a advokátom

Advokát nechce čeliť následkom prerušenia kontinuity výkonu povolania z dôvodu zlyhania poskytovateľa cloudových služieb. Navyše, v rámci mnohých právnych systémov majú advokáti povinnosť zakotvenú v stavovských a zákonných požiadavkách mať údaje klienta a ďalšie dokumenty, ktoré nemusia obsahovať osobné alebo klientove údaje (napr. účtovné záznamy advokátskej kancelárie), dostupné pre účely inšpekcie/kontroly príslušnými stavovskými alebo národnými regulačnými orgánmi. Ak k týmto dokumentom nie je možné získať prístup na žiadosť príslušných orgánov buď z dôvodu zlyhania poskytovateľa cloudových služieb, zlyhania na strane advokáta (vedúceho k porušeniu zmluvnej povinnosti alebo k ukončeniu zmluvy s poskytovateľom cloudových služieb) alebo z dôvodu sporu zo zmluvného vzťahu s poskytovateľom cloudovej služby, následkom ktorého sa uplatní záložné právo alebo právo na zadržanie údajov advokáta poskytovateľom, advokát môže byť uznaný za vinného v disciplinárnom konaní, alebo za vinného zo spáchania správneho deliktu z dôvodu neposkytnutia údajov alebo iných dokumentov. Takýto priestupok alebo disciplinárne previnenie môže byť považované za pretrvávajúce alebo opakované, pokým trvá neschopnosť poskytnúť požadovaný materiál.

Preto by advokát pri hodnotení poskytovateľov cloudových služieb mal zhodnotiť svoju zraniteľnosť, pokiaľ ide o stavovské alebo právne následky spôsobené nedostupnosťou údajov. Mal by zvážiť, či je nevyhnutné snažiť sa o dojednanie vhodných zmluvných podmienok, aby zabezpečil nepretržitú dostupnosť aj v prípade zmluvného sporu alebo zlyhania poskytovateľa či jeho vlastnej advokátskej kancelárie. Rovnako by mal zhodnotiť, či je nevyhnutné hľadať prostriedky na prekonanie nedostupnosti dát. Napríklad, zmluvné právo na obnovenie dát bude mať obmedzený účinok, ak sú tieto dáta v podobe, ktorá nie je ľahko čitateľná. Za žiaduce možno považovať zabezpečenie nepretržitej dostupnosti softvéru, ktorý je nevyhnutný na čítanie dát, napr. uložením licencie k danému softvéru do úschovy v prospech advokáta.

G. Preventívne opatrenia

Je dôležité zvážiť minimálne nasledovné aspekty:

[a] rozsah služby,

[b] dostupnosť systému,

[c] termíny/lehoty na opravu vád a odstránenie porúch,

[d] zmluvné pokuty za neplnenie alebo omeškanie (ak sú vykonateľné v zmysle platného práva),

[e] zmeny požiadaviek na službu,

[f] povinnosť poskytovateľa služby adaptovať systém v súlade s legislatívnymi zmenami,

[g] vylúčenie angažovania subdodávateľov bez predchádzajúceho súhlasu,

[h] licencie, najmä ubezpečenie, že softvér, ktorý poskytovateľ používa, má náležité osvedčenie,

[i] vlastníctvo uložených údajov a výlučné právo na prístup k nim,

[j] dohody na ochranu osobných údajov, najmä s ohľadom na požiadavky platných vnútroštátnych predpisov,[6]

[k] bezpečnostné opatrenia a zodpovednosť,

[l] povinnosť neposkytnúť informácie,

[m] monitoring a vykazovanie,

[n] technická dokumentácia, dokumentácia postupov a dokumentácia užívateľa/správcu systému,

[o] právo na kontrolu a audit, vrátane hodnotenia štandardov,

[6] Napríklad § 11 nemeckého zákona o ochrane osobných údajov.

[p] záložný systém, pohotovostný plán na obnovu,

[q] ustanovenie o Software-ESCROW pre prípad platobnej alebo podnikateľskej neschopnosti poskytovateľa cloudovej služby,

[r] umiestnenie serverov – v rámci štátu, EHP alebo mimo EHP, ak rešpektujú európske štandardy práva na súkromie a dôvernosť informácií/zásady mlčanlivosti,

[s] poistenie, záruky, záväzky, náhrada škody,

[t] ukončenie zmluvy,

[u] ustanovenia o ukončení poskytovania služby a o riadení výstupu, vrátane prenosu a výmazu údajov,

[v] mediácia, zmierenie a/alebo rozhodcovské konanie,

[w] rozhodné právo a súdna právomoc.

H. Rezervný plán

Pozornosť treba venovať skutočnosti, že dostupnosť cloudových služieb závisí od neprerušeného sieťového pripojenia. Advokát by mal zvážiť, či nie je potrebné mať k dispozícii alternatívu alebo záložný/podporný spôsob pripojenia na internet pre prípad zlyhania primárneho pripojenia.

I. Transparentnosť

S cieľom zabezpečiť transparentnosť právnych služieb by mal advokát zvážiť informovanie budúcich klientov o skutočnosti, že jeho advokátska kancelária využíva cloudové služby. Tento cieľ je možné dosiahnuť doplnením informácie do všeobecných podmienok zmluvy o poskytovaní právnych služieb, ktoré sa upravia po vzájomnej dohode s jednotlivými klientmi. Toto ustanovenie by umožnilo poskytnúť podrobnejšiu informáciu o cloudových službách na báze individuálnej žiadosti. Treba poznamenať, že v niektorých právnych poriadkoch sa môže vyžadovať súhlas klienta. Zahrnutie informácie do všeobecných podmienok zmluvy o poskytovaní právnych služieb odporúčame najmä v prípade, ak advokátska kancelária využíva cloudové služby poskytovateľa na serveroch umiestnených v inej jurisdikcii. V týchto prípadoch by bolo vhodné, aby advokát získal informovaný súhlas klienta pred tým, ako uloží jeho dáta na takéto servery. Advokát by mal poskytnúť klientovi informáciu o poskytovateľovi cloudových služieb, ako aj o právnej úprave ochrany osobných údajov, práva na súkromie a zásady mlčanlivosti advokáta v krajine, kde sa nachádzajú servery.

J. Všeobecné hľadisko na záver

Ako bolo uvedené v týchto usmerneniach, cloudové služby prinášajú mnohé riziká a otvárajú mnohé otázky, najmä pokiaľ ide o dôvernosť informácií/mlčanlivosť advokáta a uchovávanie údajov. CCBE vyzýva advokátske komory a právnické spoločnosti k zvyšovaniu povedomia svojich členov s cieľom dosiahnuť, aby advokáti venovali maximálnu pozornosť a prijali adekvátne preventívne opatrenia. Právne a technické záruky by mal poskytovať advokátom poskytovateľ cloudových služieb (napr. záruka dlhodobého zálohovania dát a pod.). V praxi nemusí byť pre advokátov jednoduché realizovať všetky tieto usmernenia. Odporúčame, aby advokátske komory a právnické spoločnosti stanovili mechanizmy, ktoré pomôžu advokátom splniť vyššie uvedené pokyny, napr. vytvorením vlastnej cloudovej infraštruktúry, ktorá je v súlade so spomínanými usmerneniami. Takémuto kroku by malo predchádzať vykonanie posúdenia vplyvu.