# K právní ochraně osobních údajů při jejich předávání v rámci cloudových služeb

## Úvod

Při provozování cloudových služeb bude téměř vždy docházet zároveň ke zpracování osobních údajů. Za zpracování osobních údajů je zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen „zákon o ochraně osobních údajů“) považována jakákoliv operace nebo soustava operací, kterou správce nebo zpracovatel systematicky provádí s osobními údaji, např. jejich shromažďování, zpřístupňování, zveřejňování či třídění, ale také ukládání na nosiče informací, uchovávání a předávání. Především tyto poslední operace budou předmětem tohoto materiálu. Zákazníci cloudových služeb se mohou dříve či později v rámci nabídky těchto služeb setkat s požadavkem jejich poskytovatele na přenos osobních údajů uložených v cloudu do jiných států, velmi často do tzv. třetích zemí[1] mimo EU/EHP. Je odpovědností zákazníka cloudových služeb, jako správce osobních údajů, aby si vybral takového poskytovatele, který je schopen zaručit soulad jim nabízených a realizovaných služeb se zákonem o ochraně osobních údajů. Materiál představuje některé právní instrumenty, jako jsou standardní smluvní doložky, institut „Safe Harbor“ nebo závazná podniková pravidla, tedy tradiční a obecně přijímané právní nástroje, které stanovují právní rámec pro předávání osobních údajů do třetích zemí nezajišťujících přiměřenou úroveň ochrany osobních údajů a upozorňuje na případná rizika vyplývající z jejich aplikace při využívání cloudových služeb. Ostatními aspekty a riziky týkajícími se zpracování údajů v cloudu se věnuje pouze okrajově a většinou pouze v souvislosti s předáváním údajů do jiných států.

Podstatnou vlastností cloud computingu je skutečnost, že nemusí existovat pevné umístění dat zákazníka v rámci sítě datových úložišť poskytovatele cloudových služeb a data mohou migrovat z jednoho datového úložiště do druhého, přičemž každé z nich se může nacházet v jiné zemi, včetně tzv. třetích zemí. Cloud computing v dnešní podobě představuje z pohledu ochrany osobních údajů poměrně velké riziko především pro samotného zákazníka/správce osobních údajů, který je primárně za zpracování osobních údajů odpovědný. Je tedy důležité, aby zákazník všechna rizika vždy pečlivě a předem analyzoval. Cílem tohoto materiálu není vyjmenovat všechna rizika související s poskytováním cloudových služeb,[2] ale zaměřuje se pouze na rizika spojená s využitím datových úložišť, resp. s předáváním osobních údajů do třetích zemí mimo EU/EHP, kde jsou datová úložiště umístěna.

## Definice pojmu cloud computing

V současné době není obsah pojmu cloud computing ze strany odborné veřejnosti zcela přesně vymezen, resp. existuje několik obecných definic. Podobně bychom pro něj stěží

[1] Za třetí zemi se považuje každá země, která není součástí Evropského hospodářského prostoru. Součástí EHP jsou kromě členských zemí EU rovněž Island, Lichtenštejnsko a Norsko. Každá ze zemí EHP, jako smluvní strana Smlouvy o EHP, je součástí vnitřního trhu EU.

[2] Podrobněji se všem aspektům cloud computingu věnuje Stanovisko Pracovní skupiny pro ochranu údajů zřízené podle čl. 29 směrnice 95/46/ES č. 5/2012 ke cloud computingu (dokument WP 196) přijaté dne 1. července 2012 a dostupné na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_cs.pdf#h2-2, kde jsou podrobněji uvedena všechna rizika s touto službou spojená, viz s. 5 tohoto stanoviska.

hledali i vhodný český překlad[3]. Je tedy vhodnější vysvětlit samotnou podstatu cloud computingu, než uvádět jednotlivé definice, případně hledat tu nejvýstižnější. V případě poskytování služeb cloud computingu se v zásadě jedná o to, že některé zdroje, služby nebo aplikace, které uživatel využívá pro zajištění své činnosti, jsou umístěny mimo jeho počítač a práce s nimi probíhá na vzdálených zařízeních jejich poskytovatele, ke kterým uživatel přistupuje přes internet (často pomocí webového prohlížeče) a uživateli je umožněno zdroje, služby nebo aplikace pružně upravovat, měnit a používat dle svých potřeb. Jinými slovy, uživatel nemá svá data uložena ve svém lokálním počítači, ale kdesi „v cloudu“, a přistupuje k nim pomocí aplikací, které si opět neinstaluje do svého počítače, ale které běží „kdesi“. Uživatel pak pouze přistupuje k jejich uživatelskému rozhraní.

Řešení cloud computingu lze rozdělit do tří základních modelů podle druhu poskytovaných služeb:

IaaS (Infrastruktura jako služba) - poskytovatel pronajímá technologickou infrastrukturu, tj. většinou virtuální servery (včetně příslušných služeb). Uživatel může jednoduše, efektivně a ekonomicky nahradit stávající IT systémy nebo je používat v kombinaci s pronajímanou infrastrukturou. Poskytovatelé bývají specializované subjekty, které vytvářejí často komplexní řešení geograficky rozložené ve více oblastech.

SaaS (Software jako služba) - poskytovatel nabízí koncovým uživatelům prostřednictvím webu různé aplikační služby a stará se, aby byly pro uživatele dostupné. Tyto služby mohou nahradit běžné aplikace, které uživatelé instalují v rámci svých lokálních IT systémů. Tak je tomu například u kancelářských aplikací (textový editor, tvorba tabulek a databází, sdílené kalendáře atd.), ale i e-mailových aplikací založených na webových technologiích (Gmail pro firmy).

PaaS (Platforma jako služba) - poskytovatel nabízí řešení pro vývoj a hostování aplikací. Tyto služby jsou obvykle určeny pro subjekty na trhu, které je používají k rozvoji a umístění koncových aplikací určených pro vlastní potřebu nebo jako službu pro potřeby třetích stran.

Z hlediska vlastnictví lze jednotlivé modely rozdělit na:

Veřejný cloud (public cloud) – služby jsou nabízeny a zároveň sdíleny mezi navzájem nesouvisejícími uživateli.

Soukromý (privátní) – služby jsou poskytovány v rámci jedné organizace nebo pro přesně vymezenou množinu subjektů.

Hybridní cloud – je kombinace obou výše uvedených přístupů.

### Zákazník/správce a poskytovatel/zpracovatel

Z pohledu zákona o ochraně osobních údajů je důležité vymezit role hlavních aktérů, zejména role správce[4] a zpracovatele[5] osobních údajů, aby byla jasně stanovena

[3] Spojením dvou anglických slov cloud (mrak) a computing (práce s počítačem) bychom mohli do českého jazyka přeložit jako práce s počítačem na dálku nebo prostě jako kancelář v oblacích.

[4] Ustanovení § 4 písm. j) zákona o ochraně osobních údajů definuje správce takto: „správcem každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatele, pokud zvláštní zákon nestanoví jinak.“

odpovědnost za dodržování pravidel pro ochranu osobních údajů. Dnes je zcela běžné, že správce deleguje některé úkoly související se zpracováním osobních údajů na smluvního partnera, který se tak ocitne v roli zpracovatele. Tento stav obecně souvisí s rozšířením outsourcovaných služeb. V běžných situacích je to správce, který rozhoduje, co by měl smluvní partner dělat a jak, nastavit podmínky, úroveň bezpečnosti dat a další důležité aspekty obchodního vztahu. V praxi to ovšem bude v mnoha případech právě poskytovatel cloudových služeb (zejména v případě větších společností), který bude mít předem nastaveny podmínky poskytované služby, které předloží zákazníkovi, a ten je buď akceptuje jako celek, či nikoliv. Nicméně i přesto je nutné vyjít z toho, že je to zákazník, který určuje účel zpracování, je za ně odpovědný a bez jeho vůle by žádný cloud nemohl existovat, což je také hlavní důvod, proč je zákazník obvykle považován za správce a jeho smluvní partner, tedy poskytovatel cloudových služeb, za zpracovatele.

Stanovisko (WP 196) č. 5/2012 ke cloud computingu k tomu uvádí:

*„Zákazník cloudových služeb určuje konečný účel zpracování a rozhoduje o zadání tohoto zpracování nebo jeho části externí organizaci. Zákazník cloudových služeb tudíž vystupuje jako správce. Podle směrnice se správcem rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který sám nebo společně s jinými určuje účel a prostředky zpracování osobních údajů“. Zákazník cloudových služeb musí jako správce přijmout odpovědnost za dodržování právních předpisů na ochranu údajů a vztahují se na něj veškeré právní závazky stanovené ve směrnici 95/46/ES. Zákazník cloudových služeb může poskytovatele cloudových služeb pověřit výběrem postupů a technických či organizačních opatření, jež mají sloužit k naplnění účelu správce. Poskytovatel cloudových služeb je subjekt, který poskytuje výše popsané různé formy služeb cloud computingu. Pokud poskytovatel cloudových služeb zajišťuje prostředky a platformu a jedná jménem zákazníka cloudových služeb, pak se považuje za zpracovatele údajů, jímž se podle směrnice 95/46/ES rozumí „fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jakýkoli jiný subjekt, který zpracovává osobní údaje pro správce.“*

Zároveň ovšem uvedené stanovisko přiznává i možnost, kdy se i poskytovatel cloudových služeb může ocitnout za určitých okolností v roli správce, když dodává:

„…*Mohou nastat situace, ve kterých může být poskytovatel cloudových služeb v závislosti na konkrétních okolnostech považován buď za společného správce, nebo správce v rámci vlastních pravomocí. Například k tomu může dojít v případě, kdy poskytovatel zpracovává údaje pro vlastní účely.“*

Pro úplnost je nutné dodat, že z uvedeného vztahu správce/zpracovatel vyplývá povinnost pro zákazníka/správce osobních údajů uzavřít zpracovatelskou smlouvu s poskytovatelem cloudových služeb/zpracovatelem osobních údajů podle § 6 zákona o ochraně osobních údajů, která musí obsahovat mj. i záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.[6] Správce bude tudíž vždy odpovědný za osobní údaje, ať jsou uloženy a zpracovávány kdekoliv.

[5] Ustanovení § 4 písm. k) zákona o ochraně osobních údajů definuje zpracovatele takto: zpracovatelem každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona.“

[6] Podrobný obsah smluvních záruk je popsán ve Stanovisku (WP 196) č. 5/2012 ke cloud computingu přijatém dne 1. července 2012 na s. 12.

## Zákonná regulace předávání osobních údajů do jiných zemí

Zákazník cloudových služeb se může v praxi setkat s několika situacemi, kdy bude poskytovatel usazen v jiném státě a zároveň bude docházet ze strany poskytovatele cloudových služeb k předávání a následnému ukládání svěřených osobních údajů do datových úložišť umístěných v různých státech světa. Ve spojitosti s tím je vždy nutné, aby poskytovatel cloudových služeb zákazníka předem informoval o tom, kde mohou být data umístěna, tj. ve kterých zemích a případně i komu konkrétně mohou být data dále předávána a v jaké zemi se příjemce údajů nachází. Jak již bylo uvedeno výše, jedním z hlavních rizik cloud computingu pro ochranu osobních údajů je riziko spojené s předáváním těchto údajů do třetích zemí mimo EU/EHP, které neposkytují osobním údajům dostatečnou úroveň ochrany. Podmínky, za kterých je možné takové předávání realizovat, upravuje zákon o ochraně osobních údajů, konkrétně ustanovení § 27. Účelem a smyslem tohoto ustanovení je zajištění ochrany osobních údajů subjektů údajů, které mají být předány a následně zpracovávány ve třetích zemích. V zásadě mohou být osobní údaje předávány do země mimo EU pouze, pokud tato země zaručuje odpovídající úroveň jejich ochrany. Předávat osobní údaje do třetích zemí nezajišťujících odpovídající úroveň ochrany lze rovněž na základě výjimek uvedených v § 27 odst. 3 písm. a) až g) zákona o ochraně osobních údajů.[7] Naplnění některého právem uznaného důvodu k předávání údajů do třetích zemí musí správce (vývozce) prokázat Úřadu pro ochranu osobních údajů (dále jen „Úřad“) v rámci povolovacího řízení vedeného na základě § 27 odst. 4 zákona o ochraně osobních údajů.

## Odpovídající/přiměřená úroveň ochrany[8]

V souvislosti s přeshraničním tokem osobních údajů je velmi často zmiňován pojem přiměřená nebo odpovídající úroveň ochrany dat. Zajištění odpovídající úrovně ochrany

[7] „Není-li podmínka podle odstavců 1 a 2 splněna, může být předání osobních údajů uskutečněno, jestliže správce prokáže, že

a) předání údajů se děje se souhlasem nebo na základě pokynu subjektu údajů,

b) jsou v třetí zemi, kde mají být osobní údaje zpracovány, vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, například prostřednictvím jiných právních nebo profesních předpisů a bezpečnostních opatření. Takové záruky mohou být upřesněny zejména smlouvou uzavřenou mezi správcem a příjemcem, pokud tato smlouva zajišťuje uplatnění těchto požadavků nebo pokud smlouva obsahuje smluvní doložky pro předání osobních údajů do třetích zemí zveřejněné ve Věstníku Úřadu,

c) jde o osobní údaje, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem; v takovém případě lze osobní údaje zpřístupnit jen v rozsahu a za podmínek stanovených zvláštním zákonem,

d) je předání nutné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána,

e) je předání nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů,

f) je předání nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro uplatnění jiných právních nároků, nebo

g) je předání nezbytné pro ochranu práv nebo životně důležitých zájmů subjektu údajů, zejména pro záchranu života nebo pro poskytnutí zdravotních služeb.“

[8] Odpovídající úroveň ochrany je hlavní zásadou, která se aplikuje při přeshraničních přenosech osobních údajů, a jejímž smyslem je zabránit předávání osobních údajů do třetích zemí, pokud nezaručí přiměřenou úroveň ochrany těmto údajům. Tato zásada vyplývá konkrétně z článku 25 směrnice 95/46/ES a § 27 odst. 1 a 2 zákona o ochraně osobních údajů.

při realizaci mezinárodních datových přenosů s využitím dostupných nástrojů je v současné době poměrně obtížné, což je způsobeno především rostoucím množstvím a složitostí mezinárodního předávání údajů. V zásadě existují dvě možnosti, jak dosáhnout toho, že třetí země bude označena za zemi s přiměřenou úrovní ochrany. První možností je, že odpovídající úroveň ochrany ve třetí zemi bude zajištěna prostřednictvím obecných právních předpisů dotyčné třetí země. Druhou možností je, že tuto ochranu bude garantovat sám správce (vývozce údajů), pokud přijme odpovídající ochranná opatření, která zajistí, že úroveň ochrany předávaných osobních údajů bude v zemi příjemce srovnatelná se standardy ochrany obsaženými v zákoně o ochraně osobních údajů. Taková opatření, resp. záruky mohou vyplývat např. ze smlouvy mezi vývozcem a příjemcem dat, jejíž nedílnou součástí budou standardní smluvní doložky podle příslušného rozhodnutí Komise, případně mohou být naplněna přijetím závazných podnikových pravidel. Pravomoc rozhodnout o tom, zda třetí země zajišťuje odpovídající úroveň ochrany na základě svých národních předpisů nebo svých mezinárodních závazků, má Evropská komise.[9] Úřad touto pravomocí nadán není. Nicméně ze zákona o ochraně osobních údajů vyplývá, že za země poskytující přiměřenou úroveň ochrany jsou považovány i ty, které ratifikovaly Úmluvu Rady Evropy 108, o ochraně osob se zřetelem na automatizované zpracování osobních údajů z roku 1981 (dále jen „Úmluva 108“).[10]

**Modelové příklady předávání do jiných států**

V praxi se mohou zákazníci cloudových služeb v postavení správců osobních údajů setkat s případy, kdy budou osobní údaje v rámci poskytování cloudových služeb předávány do jiných zemí. Přitom přicházejí v úvahu následující možnosti:

1. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nacházejí v zemích EU a údaje budou předávány a uchovávány pouze v jejich rámci

V tomto případě není nutné, aby správce/zákazník přijal dodatečné zvláštní záruky pro přenos údajů,[11] jelikož pro předávání v rámci členských států EU platí zásada volného pohybu osobních údajů, a proto předávání osobních údajů v rámci EU je možné bez povolení Úřadu. Jedná se o předávání v režimu § 27 odst. 1 zákona o ochraně osobních údajů. Správce a zpracovatel jsou povinni mezi sebou uzavřít smlouvu o zpracování osobních údajů ve smyslu § 6 zákona o ochraně osobních údajů[12], přičemž tato smlouva musí obsahovat všechny podstatné náležitosti podle tohoto ustanovení zákona.

2. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nacházejí ve třetích zemích, které ratifikovaly Úmluvu 108 nebo ve třetích zemích, o kterých Komise rozhodla, že poskytují přiměřenou úroveň ochrany, a údaje budou předávány a uchovávány pouze v rámci těchto zemí

[9] Komise v minulosti analyzovala národní předpisy týkající se ochrany osobních údajů v několika zemích a doposud rozhodla o přiměřené úrovni ochrany Andorrského knížectví, Argentiny, Faerských ostrovů, Guernsey, Izraele, Jersey, Kanady, ostrova Man, Nového Zélandu, Švýcarska a Uruguayské východní republiky. Dále Komise rozhodla, že úroveň ochrany je přiměřená za určitých podmínek v USA – případy „Safe Harbor“.

[10] Vedle členských států Evropské unie ratifikovaly Úmluvu 108 tyto státy: Andorra, Arménie, Albánie, Azerbajdžán, Bosna a Hercegovina, Černá Hora, Gruzie, Chorvatsko, Island, Lichtenštejnsko, Makedonie, Moldavsko, Monako, Norsko, Srbsko, Švýcarsko a Ukrajina.

[11] Je důležité nezaměňovat se zárukami, které musí zpracovatel poskytnout v rámci zpracovatelské smlouvy podle § 6 zákona o ochraně osobních údajů. Zde se hovoří pouze o zárukách ve smyslu § 27 tohoto zákona.

[12] „Pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů.“

V těchto případech platí, že všechny tyto země poskytují odpovídající úroveň ochrany. Předávání probíhá v režimu § 27 odst. 2 zákona o ochraně osobních údajů. Dále platí obdobně to, co je uvedeno v bodě prvním.

3. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nacházejí ve zbývajících zemích světa, které nelze podřadit pod bod 1 ani bod 2, tzn. zemích neposkytujících přiměřenou úroveň ochrany, a údaje budou předávány a uchovávány v rámci těchto zemí

V tomto případě musí sám správce (zákazník cloudových služeb) zajistit, aby předávaným osobním údajům byla poskytnuta odpovídající ochrana srovnatelná s ochranou, kterou osobním údajům poskytuje zákon o ochraně osobních údajů. Nejvhodnějšími nástroji jsou standardní smluvní doložky a závazná podniková pravidla (BCR).

### a) Standardní smluvní doložky

Jedním z nejčastěji využívaných nástrojů pro předávání osobních údajů do třetích zemí jsou standardní smluvní doložky.[13] V případě cloud computingu je v zásadě relevantní použití standardních (nebo také vzorových) smluvních doložek, které jsou přílohou rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES. Jak ze samotného názvu vyplývá, jedná se o doložky, které jsou určené pro předávání údajů mezi správcem/zákazníkem na jedné a zpracovatelem/poskytovatelem na druhé straně. Výhodou předávání realizovaných na základě aplikace standardních smluvních doložek je skutečnost, že pokud se stanou součástí smlouvy o poskytování (cloudových) služeb, není nutné žádat Úřad o povolení k předávání do třetích zemí, přičemž je zároveň splněn požadavek zákona o ochraně osobních údajů a předávaným osobním údajům je tímto (z hlediska právní úpravy) zajištěna dostatečná ochrana. Podle tohoto rozhodnutí Komise může zpracovatel osobních údajů (poskytovatel cloudových služeb) v rámci konkrétního zpracování využít rovněž služeb dílčích zpracovatelů.

Doložka č. 11 rozhodnutí Komise 2010/87/EU zavádí nový pojem „dílčí zpracovatel“, kterým se rozumí „*zpracovatel najatý dovozcem údajů nebo jiným dílčím zpracovatelem dovozce údajů, který se zavazuje přijímat od dovozce údajů nebo od jiného dílčího zpracovatele dovozce údajů osobní údaje určené výhradně pro činnosti spojené se zpracováním jménem vývozce údajů po předání v souladu s pokyny vývozce údajů, standardními smluvními doložkami stanovenými v příloze a podmínkami písemné smlouvy o dílčím zpracování.*“

Základním východiskem při využití institutu dílčích zpracovatelů zůstává, že správce je odpovědný za vše, co se stane s osobními údaji, jinými slovy osobní údaje mohou být zpracovány dílčím zpracovatelem pouze s výslovným souhlasem správce. Pokud by ve smlouvě o zpracování dat bylo výslovně stanoveno, že zpracovatel může delegovat celé nebo část zpracování na další subjekt, aniž by se zbavoval své odpovědnosti za dodržování smlouvy se správcem, může zpracovatel outsourcovat části zpracování na jednoho nebo více dílčích zpracovatelů. Pokud tak učiní, musí zpracovatel podniknout kroky k zajištění smluvních záruk, že dílčí zpracovatel se bude také řídit a dodržovat pokyny správce, a přijme nezbytná ochranná opatření k zajištění bezpečnosti zpracovávaných dat.

[13] Čl. 26 odst. 2 směrnice Evropského parlamentu a Rady 95/46/ES stanoví, že členské státy mohou předání nebo předávání osobních údajů do třetích zemí, které nezajišťují odpovídající úroveň ochrany, povolit za předpokladu, že existují určitá ochranná opatření. Tato ochranná opatření mohou zejména vyplývat z příslušných smluvních doložek.

Pokud zpracovatelé externě zadávají služby dílčím zpracovatelům, jsou rovněž povinni informovat o tom zákazníka, konkrétně popsat typ delegované služby, charakterizovat stávající a potenciální subdodavatele, seznámit zákazníka se zárukami, jež tyto subjekty nabízejí poskytovateli služeb cloud computingu.[14]

**b) Závazná podniková pravidla (Binding Corporate rules, dále jen „BCR“)**

BCR jsou interním aktem nadnárodní korporace, přičemž někteří z členů mohou mít sídlo mimo EU, ve třetích zemích, které nezajišťují osobním údajům odpovídající úroveň ochrany. Interní akt obsahuje komplexní politiku v oblasti ochrany osobních údajů s ohledem na jejich mezinárodní předávání pouze v rámci této korporace. V zásadě rozeznáváme BCR pro správce a BCR pro zpracovatele. Zatímco první z nich byla upravena řadou pracovních dokumentů Pracovní skupiny podle čl. 29 směrnice 95/46/ES a v praxi se již osvědčila, druhá na uvedení do praxe teprve čekají.[15] BCR pro správce stanovují společná a závazná pravidla pro předávání osobních údajů, která jsou původně zpracovaná korporací vystupující v roli správce (např. údajů vztahujících se k zákazníkům nebo zaměstnancům). Naproti tomu BCR pro zpracovatele jsou určena k témuž s tím rozdílem, že osobní údaje jsou původně zpracovávány korporací vystupující v roli zpracovatele. Jedná se o nový právní nástroj, který přináší nové možnosti v oblasti externího zpracování dat. Měl by být efektivní především tam, kde dochází k masivnímu předávání údajů zpracovatelem dílčím zpracovatelům v rámci téže korporace a na základě pokynů správce, aniž by bylo zapotřebí uzavřít s každým novým dílčím zpracovatelem zvlášť smlouvu o zpracování. Tím se zásadně liší od standardních smluvních doložek. Cílem nového právního nástroje není přesunout povinnosti správce na zpracovatele. Povinnosti správce a zpracovatele v kontextu mezinárodního předávání zůstávají nezměněny (analogicky jako u standardních smluvních doložek 2010/87/EU), nicméně některé nástroje jsou přizpůsobené zvláštnostem předávání v rámci jedné nadnárodní korporace (např. jeden globální závazek namísto několika smluv, určení odpovědnosti, audit, vzdělávací programy, role inspektora ochrany údajů apod.). Podobně jako v případě BCR pro správce i zde platí, že zpracovatel musí BCR předložit ke schválení vedoucímu dozorovému úřadu v EU, který řídí celý schvalovací proces a následně garantuje, že BCR mohou být považována za nástroj poskytující odpovídající ochranu. Následně ještě musí daný správce osobních údajů, který hodlá nechat zpracovat osobní údaje zpracovatelem se schválenými BCR pro zpracovatele, požádat o povolení k předávání příslušný národní dozorový orgán, pokud je to legislativou vyžadováno. Podle zákona o ochraně osobních údajů je tak nutné učinit podle § 27 na základě splnění požadavku podle odst. 3 písm. b) tohoto ustanovení zákona. Určitou nevýhodou oproti standardním smluvním doložkám zůstává délka schvalovacího procesu na úrovni EU, která se v praxi pohybuje okolo 8 měsíců, i skutečnost, že předávání údajů na základě BCR musí projít povolovacím řízením ještě na národní úrovni. Nicméně pro velké nadnárodní korporace poskytující cloudové služby a nacházející se v roli zpracovatelů může být zavedení BCR pro zpracovatele přínosem, neboť řeší tuto problematiku v globálním měřítku.

4. Zařízení, na nichž jsou uchovávány nebo jinak zpracovávány osobní údaje, se nachází v USA (případy „Safe Harbor“ neboli „bezpečný přístav“)

Speciální postavení v rámci tzv. třetích zemí mají Spojené státy americké.[16] Pro bezpečné předání byl smlouvou mezi USA a EU zaveden tzv. program „Safe Harbor“ („bezpečný

[14] Stanovisko (WP 196) č. 5/2012 ke cloud computingu přijaté dne 1. července 2012, s. 9.

[15] Pracovní skupina podle čl. 29 směrnice 95/46/ES přijala 6. června 2012 pracovní dokument (WP 195) týkající se zásad, které jsou obsahem BCR pro zpracovatele a formulář žádosti o předložení závazných korporátních pravidel pro zpracovatele dostupné na http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

[16] Z hlediska ochrany osobních údajů jsou USA považovány za třetí zemi nezajišťující přiměřenou úroveň ochrany.

přístav“). Předmětem smlouvy je závazek EU umožnit volné předávání osobních údajů ze zemí EU do USA,[17] pokud se na straně příjemce jedná o společnosti, které jsou zařazeny na tzv. „Safe Harbor List.“[18] Z pohledu zákona o ochraně osobních údajů se jedná o předávání v režimu § 27 odst. 2 tohoto zákona, podle kterého mohou být do třetích zemí předány osobní údaje, pokud je tato třetí země označena na základě rozhodnutí orgánu EU za zemi, která poskytuje odpovídající úroveň ochrany. I přes právní zakotvení institutu „bezpečného přístavu“ v rozhodnutí Komise, je na místě otázka, zda certifikace „Safe Harbor“ je skutečně dostatečnou zárukou pro bezpečnost osobních údajů předávaných do USA, resp. zda společnosti na seznamu „Safe Harbor“ nabízejí dostatečné záruky pro předávání osobních údajů do USA. Odpověď na tuto otázku můžeme nalézt ve stanovisku WP29 ke cloud computingu:

*„Pracovní skupina se domnívá, že společnosti vyvážející údaje by se neměly opírat pouze o prohlášení dovozce údajů o tom, že má osvědčení „bezpečného přístavu“. Společnost vyvážející údaje by naopak měla získat důkazy o tom, že existují vlastní osvědčení o přijetí zásad „bezpečného přístavu“, a požadovat důkazy o dodržování těchto zásad, což je důležité zejména s ohledem na informace poskytované subjektům údajů, jichž se zpracování údajů týká.“*[19]

Správce/zákazník odpovědný za předávání údajů by se tedy neměl spokojit s konstatováním poskytovatele cloudu, že má certifikaci „Safe Harbor“, ale ověřit, zda tato certifikace skutečně existuje a je platná a dále požadovat důkazy, že zásady „bezpečného přístavu“ jsou také v praxi dodržovány.

V souvislosti s ochranou zpracovávaných osobních údajů uvádí stanovisko WP29 ke cloud computingu následující:

*„V neposlední řadě zastává pracovní skupina názor, že zásady „bezpečného přístavu“ samy o sobě nemusejí vývozci údajů zaručovat prostředky nezbytné k zajištění toho, že poskytovatel cloudových služeb v USA přijal vhodná bezpečnostní opatření tak, jak mohou vyžadovat vnitrostátní právní předpisy na základě směrnice 95/46/ES. Pokud jde o bezpečnost údajů, jsou s cloud computingem spojena specifická rizika (např. ztráta kontroly, nezabezpečený nebo neúplný výmaz údajů, nedostatečné auditní stopy a selhání izolovanosti), která nejsou dostatečně ošetřena stávajícími zásadami „bezpečného přístavu“ k bezpečnosti údajů. Proto je možné zavést dodatečná ochranná opatření. Například lze využít odbornosti a zdrojů třetích stran, jež jsou schopny posoudit odpovídající úroveň poskytovatelů cloudových služeb na základě různých auditních, standardizačních a certifikačních systémů. Z těchto důvodů může být žádoucí doplnit závazek dovozce údajů k dodržování zásad „bezpečného přístavu“ o dodatečná ochranná opatření, jež by přihlížela ke zvláštní povaze cloud computingu.“*[20]

Přihlášení se k dodržování zásad „bezpečného přístavu“ tedy především legalizuje samotný přenos těchto údajů do USA příslušné certifikované společnosti, nicméně ještě automaticky nezaručuje, že osobní údaje zpracovávané v cloudu jsou dostatečným způsobem chráněny. Stejně tak neexistuje žádná záruka, že zpracování v USA splňuje všechny požadavky podle platného českého práva regulující oblast ochrany osobních údajů. Podobně jako v případě zpracování, prováděném zpracovatelem na základě pokynu správce, tak

[17] Rozhodnutí Komise č. 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států.

[18] Jedná se o seznam společností, které oznámily Ministerstvu obchodu Spojených států, že budou dodržovat zásady „bezpečného přístavu“. Seznam je k dispozici na www.export.gov/safeharbor.

[19] Stanovisko (WP 196) č. 5/2012 ke cloud computingu přijaté dne 1. července 2012, s. 17.

[20] Stanovisko (WP 196) č. 5/2012 ke cloud computingu přijaté dne 1. července 2012, s. 18.

i v případě zpracování v cloudu, zůstává správce primárně odpovědný za dodržování zákona. Proto bude nutné v tomto ohledu smluvně zavázat zpracovatele ve smyslu garance vhodných bezpečnostních záruk. Jestliže bude docházet k předávání osobních údajů mezi správcem/zákazníkem usazeným v ČR a zpracovatelem/poskytovatelem v USA, je nutné uzavřít smlouvu ve smyslu § 6 zákona o ochraně osobních údajů bez ohledu na účast zpracovatele na zásadách „bezpečného přístavu".

*„Cílem smlouvy je ochrana zájmů správce údajů, tedy fyzické či právnické osoby, která určuje účel a prostředky zpracování a která nese plnou odpovědnost za údaje vůči dotčené fyzické osobě (osobám). Smlouva tedy blíže určuje zpracování, které má být prováděno, a veškerá opatření nezbytná k zajištění bezpečnosti údajů."*[21]

## Závěr

Závěrem tohoto materiálu je doporučení správcům/zákazníkům cloudových služeb, aby provedli komplexní a důkladnou analýzu rizik v souvislosti s využíváním cloudových služeb včetně přeshraničního předávání osobních údajů, a to zejména do třetích zemí nezajišťujících přiměřenou úroveň ochrany. Všichni poskytovatelé cloudových služeb by měli svým zákazníkům podávat veškeré informace týkající se přenosu a umístění datových úložišť, aby zákazník mohl správně posoudit všechny výhody a nevýhody poskytované služby. Zákazník by měl zhodnotit i rizika, která mohou vzniknout v případě, že právní předpisy třetí země nebo mezinárodní smlouva obsahují požadavky na příjemce údajů (poskytovatele cloudových služeb), aby zpřístupnil za určitých okolností osobní údaje orgánům veřejné moci (policii, soudu apod.).

Poznámka:
Materiál byl v červenci 2013 publikován ve Věstníku Úřadu pro ochranu osobních údajů, částka 65.

[21] Rozhodnutí Komise č. 2000/520/ES, (FAQ 10).