PRACOVNÍ SKUPINA PRO OCHRANU ÚDAJŮ ZŘÍZENÁ PODLE ČLÁNKU 29

01037/12/CS
WP 196

Stanovisko č. 05/2012 ke cloud computingu

Přijaté dne 1. července 2012

Tato pracovní skupina byla zřízena podle článku 29 směrnice 95/46/ES. Jedná se o nezávislý evropský poradní orgán ve věci ochrany údajů a soukromí. Její úkoly jsou popsány v článku 30 směrnice 95/46/ES a článku 15 směrnice 2002/58/ES.

Její sekretariát zajišťuje Ředitelství C (Základní práva a občanství Unie) Generálního ředitelství pro spravedlnost Evropské komise, B-1049 Brussels, Belgie, kancelář č. MO-59 02/013.

Internetové stránky: http://ec.europa.eu/justice/data-protection/index_cs.htm

Shrnutí

Skupina zřízená podle článku 29 analyzuje v tomto stanovisku všechny otázky, jež jsou relevantní pro poskytovatele služeb cloud computingu působící v Evropském hospodářském prostoru (dále jen „EHP“) i jejich zákazníky s přihlédnutím k platným zásadám stanoveným ve směrnici EU o ochraně údajů (95/46/ES), případně ve směrnici o soukromí a elektronických komunikacích 2002/58/ES (ve znění směrnice 2009/136/ES).

Přes uznávaný ekonomický i sociální přínos cloud computingu toto stanovisko nastiňuje, jak může široké zavádění cloudových služeb obnášet i rizika pro ochranu údajů: jde především o nedostatek kontroly nad osobními údaji a nedostatečné informace o tom, kde a kým jsou údaje zpracovávány či dále zpracovávány. Veřejné orgány i soukromé podniky by měly tato rizika v případě zájmu o cloudové služby pečlivě zvážit. Toto stanovisko posuzuje otázky spojené se sdílením zdrojů s jinými stranami, nedostatkem transparentnosti řetězce v rámci externího zajišťování služby, neexistencí společného globálního rámce pro přenositelnost údajů a nejistotou ohledně přípustnosti předávání osobních údajů poskytovatelům cloudových služeb usazeným mimo EHP. Podobně je ve stanovisku jako závažný problém zdůrazněna netransparentnost způsobu, jakým správci údajů poskytují subjektům údajů informace o zpracovávání jejich osobních údajů. Subjekty údajů musí[1] být informovány o tom, kdo a za jakým účelem zpracovává jejich údaje, aby byly schopny vykonávat práva, která jsou jim v tomto ohledu přiznána.

Hlavním závěrem tohoto stanoviska je doporučení podnikům a orgánům veřejné zprávy, které chtějí využívat cloud computing, aby jako první krok provedly komplexní a důkladnou analýzu rizik. Všichni poskytovatelé cloudových služeb v EHP by měli svým zákazníkům podávat veškeré informace nezbytné ke správnému posouzení všech výhod a nevýhod spojených s přijetím této služby. Hlavními elementy, o něž se nabídka služeb cloud computingu opírá, by měla být bezpečnost, transparentnost a právní jistota pro zákazníky.

V doporučeních tohoto stanoviska se zdůrazňuje odpovědnost zákazníka cloudových služeb jako správce, jenž by si měl vybrat takového poskytovatele, který zaručuje soulad s právními předpisy EU v oblasti ochrany údajů. Pokud jde o odpovídající smluvní záruky, stanovisko doporučuje, aby byly v každé smlouvě mezi zákazníkem a poskytovatelem cloudových služeb upraveny dostatečné záruky ohledně technických a organizačních opatření. Důležité je rovněž doporučení, aby zákazník ověřil, zda poskytovatel cloudových služeb může vždy zaručit zákonnost mezinárodního předávání údajů.

Rozvoj cloud computingu coby globálního technologického paradigmatu představuje – jako každý evoluční proces – náročný úkol. Nynější stanovisko lze chápat jako důležitý krok při vymezování úkolů, jichž by se měly v nadcházejících letech zhostit orgány pro ochranu údajů.

Obsah

[1] Klíčová slova „MUSÍ“, „NESMÍ“, „JE POVINEN“, „MĚL BY“, „NEMĚL BY“, „DOPORUČUJE SE“, „MŮŽE“ a „VOLITELNÝ“ v tomto dokumentu je nutné vykládat tak, jak je popsáno v žádosti o připomínky č. 2119, jež je k dispozici na adrese: http://www.ietf.org/rfc/rfc2119.txt. Pro lepší čitelnost však tato slova nejsou v tomto stanovisku psána velkými písmeny.

1. Úvod

Pro jedny je cloud computing jednou z největších technologických revolucí poslední doby. Pro druhé jde pouze o přirozený vývoj technologií na cestě ke kýženému poskytování služeb výpočetní techniky po vzoru veřejných služeb (*utility computing*). V každém případě je cloud computing u mnoha zainteresovaných subjektů v centru rozvoje jejich technologických strategií.

Cloud computing sestává z technologií a modelů služeb, jež se zaměřují na internetové používání a poskytování aplikací IT, kapacitu zpracovávání dat, úložiště a paměťový prostor. Díky poměrně jednoduché konfiguraci, rozšíření a přístupnosti zdrojů na vyžádání (*on demand*) na internetu může z cloud computingu plynout výrazný ekonomický přínos. Vedle ekonomických výhod může cloud computing přinášet i výhody v oblasti bezpečnosti. Zejména malé a střední podniky si mohou tímto způsobem pořizovat špičkové technologie, které by si jinak nemohly dovolit.

Škála služeb, jež poskytovatelé cloud computingu nabízejí, je široká: od virtuálních systémů zpracování (které pracují paralelně s tradičními servery pod přímou kontrolou správce nebo je nahrazují) přes služby na podporu vývoje aplikací a pokročilý hosting po internetová softwarová řešení, která mohou nahradit aplikace tradičně nainstalované na osobních počítačích koncových uživatelů. Jedná se například o programy na zpracování textu, záznamníky a kalendáře, evidence dokumentů ukládaných on-line a externí e-mailová řešení. Některé nejběžnější definice těchto různých typů služeb jsou uvedeny v příloze tohoto stanoviska.

Pracovní skupina podle článku 29 v tomto stanovisku analyzuje platné právní předpisy a povinnosti pro správce údajů v EHP a pro poskytovatele cloudových služeb zákazníkům v EHP. Toto stanovisko se zaměřuje na situaci, kde v uvažovaném vztahu mezi správcem a zpracovatelem představuje zákazník správce a poskytovatel cloudových služeb zpracovatele. Pokud poskytovatel cloudových služeb vystupuje rovněž jako správce, musí splňovat další požadavky. Předpokladem pro využívání technologie cloud computingu tudíž je, aby správce provedl náležitou analýzu rizik, do níž zahrne i umístění serverů, na kterých se údaje zpracovávají, a zváží rizika a přínos z hlediska ochrany údajů podle níže uvedených kritérií.

Toto stanovisko uvádí platné zásady jak pro správce, tak pro zpracovatele podle obecné směrnice o ochraně údajů (95/46/ES), např. určení a omezení účelu, výmaz údajů či technická a organizační opatření. Toto stanovisko obsahuje pokyny ohledně bezpečnostních požadavků, jež mají sloužit jako strukturální i procedurální ochranná opatření. Zvláštní důraz se klade na smluvní ujednání, jež v této souvislosti upravují vztah mezi správcem a zpracovatelem. Tradičně patří mezi cíle bezpečnosti údajů jejich dostupnost, integrita a důvěrnost. Ochrana údajů se však neomezuje jen na bezpečnost údajů, a proto se k těmto cílům přidávají i specifické cíle v oblasti ochrany údajů, jako je transparentnost, izolovanost, schopnost intervence a přenositelnost, na kterých se zakládá právo jednotlivce na ochranu údajů zakotvené v článku 8 Listiny základních práv EU.

Pokud jde o předávání osobních údajů mimo EHP, analýze jsou podrobeny jednak příslušné nástroje, jako jsou standardní smluvní doložky přijaté Evropskou komisí, konstatování odpovídající úrovně ochrany údajů a možná budoucí závazná podniková pravidla pro

zpracovatele, jednak rizika pro ochranu údajů plynoucí z mezinárodních žádostí o vymáhání práva.

Závěr tohoto stanoviska tvoří doporučení pro zákazníky cloudových služeb coby správce, pro poskytovatele cloudových služeb coby zpracovatele a pro Evropskou komisi s ohledem na budoucí změny evropského rámce pro ochranu údajů.

Berlínská Mezinárodní pracovní skupina pro ochranu údajů v telekomunikacích přijala v dubnu 2012 *Sopotské memorandum*[2], ve kterém se posuzují otázky ochrany soukromí a údajů v rámci cloud computingu a v němž je zdůrazněno, že cloud computing nesmí vést ke snížení standardů ochrany údajů oproti klasickému zpracovávání údajů.

2. Rizika cloud computingu pro ochranu údajů

Jelikož se toto stanovisko zaměřuje na zpracovávání údajů využívající služeb cloud computingu, přihlíží se pouze ke zvláštním rizikům, jež se týkají tohoto kontextu [3]. Většina těchto rizik spadá do dvou širokých kategorií: i) nedostatek kontroly nad údaji a ii) nedostatečné informace o samotném zpracovávání (netransparentnost). Zvláštní rizika cloud computingu, jež jsou posuzována v tomto stanovisku:

Nedostatek kontroly

Poskytnutím osobních údajů systémům spravovaným poskytovatelem cloudových služeb mohou zákazníci těchto služeb ztratit výlučnou kontrolu nad těmito údaji a nemohou aktivovat technická a organizační opatření nutná k zajištění dostupnosti, integrity, důvěrnosti, transparentnosti, izolovanosti[4], schopnosti intervence a přenositelnosti údajů. Nedostatek kontroly se může projevovat takto:

- Nedostatečná dostupnost kvůli chybějící interoperabilitě (závislost na poskytovatelích, *vendor lock-in*): Pokud poskytovatel cloudových služeb používá proprietární technologii, může být pro zákazníka cloudových služeb obtížné přemísťovat data a dokumenty mezi různými cloudovými systémy (přenositelnost údajů) nebo vyměňovat si informace se subjekty, které využívají cloudových služeb spravovaných jinými poskytovateli (interoperabilita).
- Nedostatečná integrita způsobená sdílením zdrojů: Cloud sestává ze sdílených systémů a infrastruktury. Poskytovatelé cloudových služeb zpracovávají osobní údaje pocházející z různých zdrojů, tj. od různých subjektů údajů či organizací, a může dojít ke střetu zájmů anebo zpracování může sloužit různým cílům.
- Nedostatek důvěrnosti ve smyslu žádostí o vymáhání práva adresovaných přímo poskytovateli cloudových služeb: osobní údaje zpracovávané v cloudu mohou být předmětem žádostí o vymáhání práva podaných donucovacími orgány členských států EU nebo třetích zemí. Existuje riziko, že osobní údaje mohou být sděleny (cizím) donucovacím orgánům bez platného právního základu EU, čímž by došlo k porušení právních předpisů EU pro ochranu údajů.

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf

3 Vedle rizik týkajících se osobních údajů zpracovávaných „v cloudu“, na něž toto stanovisko výslovně upozorňuje, je třeba rovněž brát v úvahu všechna rizika spojená s externím zpracováváním osobních údajů.

4 V Německu byl zaveden širší pojem „nespojitelnost“ (*unlinkability*). Srov. poznámka pod čarou 24.

- Neschopnost intervence kvůli komplikovanosti a dynamice řetěze v rámci externího zajišťování služby: Cloudová služba nabízená jedním poskytovatelem, může sestávat z kombinace služeb od různých poskytovatelů, jež lze dynamicky přidávat či odstraňovat v průběhu platnosti zákaznické smlouvy.
- Neschopnost intervence (práva subjektů údajů): Je možné, že poskytovatel cloudových služeb nezajistí nezbytná opatření a nástroje, jež by správci napomohly při správě údajů, např. pokud jde o přístup k údajům, jejich výmaz či opravu.
- Chybějící izolovanost: Poskytovatel cloudových služeb může využívat fyzickou kontrolu nad údaji od různých zákazníků k propojování osobních údajů. Pokud mají administrátoři dostatečná práva na přednostní přístup (*high-risk roles*), mohli by propojovat informace od různých zákazníků.

Nedostatek informací o zpracování (transparentnost)

Z nedostatečné informovanosti o operacích zpracování údajů v rámci cloudové služby vyplývá riziko jak pro správce, tak pro subjekty údajů, jelikož ti nemusí být obeznámeni s možnými hrozbami a riziky, a tak nemohou přijmout opatření, jež považují za vhodná.

Některé potenciální hrozby mohou vyplynout z neobeznámenosti správce s těmito skutečnostmi:

- Řetězec zpracování zahrnuje více zpracovatelů a subdodavatelů.
- Osobní údaje jsou zpracovávány na různých místech v rámci EHP, což má přímý dopad na právní předpisy použitelné pro veškeré spory ohledně ochrany údajů, k nimž může dojít mezi uživatelem a poskytovatelem.
- Osobní údaje jsou předávány do třetích zemí mimo EHP. Třetí země nemusí zajišťovat odpovídající úroveň ochrany údajů a předávání údajů nemusí být spojeno s vhodnými ochrannými opatřeními (např. standardní smluvní doložky nebo závazná podniková pravidla), a mohlo by být tudíž nezákonné.

Subjekty údajů, jejichž osobní údaje jsou zpracovávány v cloudu, musí být informovány o totožnosti správce údajů a účelu zpracování (stávající povinnost pro všechny správce podle směrnice o ochraně údajů (95/46/ES). Správci by vzhledem k možné komplikovanosti řetězce zpracování v prostředí cloud computingu a pro zajištění řádného zpracování údajů vůči subjektu údajů (článek 10 směrnice 95/46/ES) měli v rámci osvědčených postupů podávat i informace o zpracovatelích či dílčích zpracovatelích poskytujících cloudové služby.

3. Právní rámec

3.1 Rámec pro ochranu údajů

Příslušným právním rámcem je směrnice o ochraně údajů 95/46/ES. Tato směrnice se použije na všechny případy, ve kterých jsou osobní údaje zpracovávány v důsledku využívání služeb cloud computingu. Směrnice o soukromí a elektronických komunikacích 2002/58/ES (ve znění směrnice 2009/136/ES) se použije na zpracovávání osobních údajů ve spojení s veřejně dostupnými službami elektronických komunikací v rámci veřejných komunikačních sítí

(telekomunikační operátoři), a je tudíž relevantní v případech, kdy se při poskytování těchto služeb využívá cloudové řešení[5].

3.2 Použitelné právo

Kritéria pro stanovení použitelnosti právních předpisů jsou uvedena v článku 4 směrnice 95/46/ES, jenž upravuje právo použitelné pro správce[6] usazené v jednom či více státech EHP i právo použitelné pro správce mimo EHP, kteří ale pro zpracování osobních údajů používají prostředky umístěné v EHP. Pracovní skupina podle článku 29 tuto otázku analyzovala ve svém stanovisku 8/2010 k použitelnému právu[7].

Faktorem, který vede k použití práva EU na správce, je v prvním případě místo jeho usazení a provozované činnosti (čl. 4 odst. 1 písm. a)) bez ohledu na model cloudové služby. Použitelné je právo země, ve kterých je správce zadávající služby cloud computingu usazen, a nikoliv místa, v němž se nachází poskytovatelé cloud computingu.

Pokud by byl správce usazen v různých členských státech a zpracování údajů by tvořilo část jeho činností v těchto státech, použitelné je pak právo každého členského státu, ve kterém se toto zpracování uskutečňuje.

V čl. 4 odst. 1 písm. c)[8] je stanoveno použití právních předpisů pro ochranu údajů na správce, kteří nejsou usazeni v EHP, avšak používají automatizované či neautomatizované prostředky umístěné na území některého členského státu s výjimkou případů, kdy jsou tyto prostředky použity pouze pro účely tranzitu. Z toho vyplývá, že pokud je zákazník cloudových služeb usazen mimo EHP, ale využije služeb poskytovatele cloudových služeb umístěného v EHP, pak poskytovatel „exportuje“ předpisy na ochranu údajů i na zákazníka.

3.3. Úkoly a odpovědnost jednotlivých aktérů

Jak již bylo uvedeno, cloud computing zahrnuje řadu různých aktérů. Je třeba posoudit a vyjasnit jejich úlohu, a stanovit tak konkrétní povinnosti ve vztahu ke stávajícím právním předpisům na ochranu údajů.

Je třeba připomenout, že pracovní skupina podle článku 29 již ve svém stanovisku č. 1/2010 k pojmům „správce“ a „zpracovatel“ poukazovala na to, že *„hlavním významem pojmu správce je určit, kdo je odpovědný za dodržování pravidel pro ochranu údajů a jak mohou subjekty údajů uplatňovat svá práva v praxi. Jinými slovy: přidělit odpovědnost.“* Je třeba, aby zúčastněné strany měly tato dvě obecná kritéria odpovědnosti za dodržování příslušných předpisů a přidělení odpovědnosti na paměti po celou dobu příslušné analýzy.

---

5 Směrnice 2002/58/ES o soukromí a elektronických komunikacích (ve znění směrnice 2009/136/ES): Směrnice 2002/58/ES o soukromí v telekomunikacích se použije na poskytovatele služeb elektronických komunikací zpřístupněných veřejnosti, kteří musí zajistit splnění povinností týkajících se důvěrnosti komunikace a ochrany osobních údajů, dále upravuje práva a povinnosti v oblasti sítí a služeb elektronických komunikací. V případech, kdy poskytovatelé *cloud computingu* vystupují jako poskytovatelé veřejně přístupných služeb elektronických komunikací, vztahuje se na ně tato směrnice.

6 Pro definici pojmu správce viz čl. 2 písm. h směrnice, analýzou pojmu se zabývalo i stanovisko pracovní skupiny podle článku 29 č. 1/2010 k pojmům „správce“ a „zpracovatel“.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_cs.pdf

8 Podle čl. 4 odst. 1 písm. c) jsou právní předpisy členského státu použitelné, pokud „správce není usazen na území Společenství a používá za účelem zpracování osobních údajů prostředků, automatizovaných či nikoli, umístěných na území zmíněného členského státu, ledaže jsou tyto prostředky použity pouze pro účely tranzitu přes území Společenství“.

3.3.1 Zákazník cloudových služeb a poskytovatel cloudových služeb

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*[9, 10].

Jak je uvedeno ve stanovisku č. 1/2010, pro hodnocení správy zpracování lze použít několik kritérií[11]. 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.

Je třeba zdůraznit, že i v komplikovaných systémech pro zpracování údajů, v nichž při zpracovávání osobních údajů vystupují různí správci, musí být zajištěno dodržení pravidel pro ochranu údajů a jasně přidělena odpovědnost za možné porušení těchto pravidel. Cílem je vyvarovat se stavu, kdy je ochrana osobních údajů omezena nebo dojde k negativnímu kompetenčnímu konfliktu či se vyskytnou další problémy kvůli tomu, že některé povinnosti a práva vyplývající ze směrnice nejsou zajištěny žádnou ze stran.

V současném nastavení služeb cloud computingu může docházet k tomu, že zákazníci nemají přílišný prostor při vyjednávání smluvních podmínek pro využívání cloudových služeb, jelikož mnohé tyto služby bývají nabízeny standardizovaným způsobem. V konečném důsledku je to však zákazník, kdo za různým účelem rozhoduje o převedení veškerého zpracování údajů nebo jeho části na cloudové služby; zásadní je v tomto případě to, že poskytovatel cloudových služeb bude mít vůči zákazníkovi úlohu smluvního dodavatele. Podle stanoviska Pracovní skupiny podle článku 29 č. 1/2010[12] k pojmům správce a zpracovatel *„by se nerovnováha s ohledem na smluvní sílu malého správce údajů vůči poskytovatelům služeb neměla považovat za důvod, aby správce přijal ustanovení a podmínky smluv, jež nejsou v souladu s právem v oblasti ochrany údajů.“* Z tohoto důvodu si správce musí vybrat poskytovatele cloudových služeb, který zaručuje soulad s právními předpisy na ochranu údajů. Zvláštní důraz je třeba klást na znaky platných smluv, jež musí obsahovat jednak soubor standardizovaných opatření na ochranu údajů včetně opatření, jež pracovní skupina nastiňuje v bodě 3.4.3 (technická a organizační opatření) a v bodě 3.5 (přeshraniční

---

9 Toto stanovisko se zaměřuje pouze na obvyklý vztah správce–zpracovatel.

10 Prostředí cloud computingu mohou využívat i fyzické osoby (uživatelé) k výlučně osobním či domácím aktivitám. V těchto případech je třeba důkladně prozkoumat, zda platí tzv. výjimka pro domácí použití, podle níž uživatelé správce nepředstavují. Tato otázka však přesahuje působnost tohoto stanoviska.

11 Např. úroveň pokynů, sledování ze strany zákazníka cloudových služeb, odborné znalosti stran.

12 Stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“ - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_cs.pdf

toky údajů), jednak jakékoliv další mechanismy vhodné pro usnadnění hloubkových kontrol a odpovědnosti (např. nezávislé audity a certifikace služeb poskytovatele prováděné třetí stranou – viz bod 4.2).

Úkolem poskytovatelů cloudových služeb (jako zpracovatelů) je zajistit důvěrnost. Směrnice 95/46/ES stanoví, že: *„jakákoli osoba, která jedná z pověření správce nebo zpracovatele, jakož i samotný zpracovatel, který má přístup k osobním údajům, je může zpracovávat pouze podle pokynů správce, ledaže právo stanoví jinak.“* Zásadní povinností rovněž je, aby poskytovatel cloudových služeb při přístupu k údajům v průběhu poskytování těchto služeb dodržoval ustanovení článku 17 směrnice (viz oddíl 3.4.2).

Zpracovatelé musí přihlížet k typu příslušného cloudu (veřejný, soukromý, komunitní či hybridní, IaaS, SaaS či PaaS [viz příloha a) Modely nasazení – b) Modely poskytování služby]) a typu služby, jenž si zákazník smluvně sjednal. Zpracovatelé jsou odpovědní za přijetí bezpečnostních opatření v souladu s právními předpisy EU tak, jak jsou uplatňovány v jurisdikcích správce a zpracovatele. Zpracovatelé musí rovněž napomáhat a poskytovat podporu správci při dodržování (vykonávaných) práv subjektů údajů.

3.3.2 Subdodavatelé

Do služeb cloud computingu může být zapojena řada smluvních stran, jež vystupují jako zpracovatelé. Zpracovatelé běžně externě zadávají zpracování údajů dílčím zpracovatelům, kteří pak získávají přístup k osobním údajům. Pokud zpracovatelé externě zadávají služby dílčím zpracovatelům, jsou povinni informovat o tom zákazníka, přičemž popíší typ dále delegované služby, charakterizují stávající a potenciální subdodavatele a seznámí zákazníka se zárukami, jež tyto subjekty nabízejí poskytovateli služeb cloud computingu a jež mají zajistit soulad se směrnicí 95/46/ES.

Veškeré příslušné povinnosti se proto musí vztahovat i na dílčí zpracovatele – prostřednictvím smluv mezi poskytovatelem cloudových služeb a subdodavatelem, jež odrážejí ustanovení smlouvy mezi poskytovatelem cloudových služeb a zákazníkem. Pracovní skupina podle článku 29 ve svém stanovisku č. 1/2010 k pojmům „správce“ a „zpracovatel“ upozorňovala na větší počet zpracovatelů v případech, v nichž mohou mít zpracovatelé přímý vztah se správcem nebo mohou působit jako subdodavatelé, kterým zpracovatelé externě zadali část zpracovávání, jímž byli pověřeni. *„Směrnice nebrání tomu, aby z důvodu organizačních požadavků bylo za zpracovatele údajů nebo dílčí zpracovatele určeno několik subjektů, a to rozdělením příslušných úkolů. Všechny tyto subjekty však musí při provádění zpracování dodržovat pokyny vydané správcem údajů.“*[13]

V těchto situacích musí být povinnosti a úkoly vyplývající z právních předpisů na ochranu údajů jasně stanoveny a nesmí docházet k jejich rozptýlení v průběhu subdodavatelského řetězce nebo v rámci externího zajištění služeb. Cílem je přidělit jasnou odpovědnost za zpracovávání údajů a zajistit jeho účinnou kontrolu.

Možný model záruk, který lze použít k vyjasnění úkolů a povinností zpracovatelů při externě zadávaném zpracovávání údajů, byl poprvé uveden v rozhodnutí Komise ze dne 5. února 2010 o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích[14]. Podle tohoto modelu je dílčí zpracovávání povoleno pouze

[13] Viz WP 169, stanovisko č. 1/2010 k pojmům „správce“ a „zpracovatel“, s. 29 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_cs.pdf)

[14] Viz Často kladené dotazy, FAQ II.5 v dokumentu WP 176.

s písemným souhlasem správce a formou písemné dohody, jež dílčímu zpracovateli ukládá stejné povinnosti jako zpracovateli. Neplní-li dílčí zpracovatel své povinnosti týkající se ochrany údajů na základě této písemné dohody, je zpracovatel vůči správci nadále plně odpovědný za splnění povinností dílčího zpracovatele podle takovéto dohody. Ustanovení tohoto typu by mohlo být součástí veškerých smluvních doložek mezi správcem a poskytovatelem cloudových služeb, který má záměr poskytovat služby prostřednictvím subdodavatelů. Tímto budou zajištěny nezbytné záruky pro dílčí zpracovávání.

Podobné řešení týkající se záruk v průběhu dílčího zpracovávání obsahuje nedávný návrh Komise na obecné nařízení o ochraně údajů[15]. Jednání zpracovatele musí být upraveno smlouvou nebo jiným právním aktem, který zavazuje zpracovatele vůči správci a který kromě dalších povinností stanoví zejména to, že zpracovatel zapojí do zpracování údajů dalšího zpracovatele pouze s předchozím souhlasem správce (čl. 26 odst. 2 návrhu).

Podle názoru pracovní skupiny podle článku 29 může zpracovatel externě zadávat svou činnost pouze se souhlasem správce, který jej obecně může poskytnout na začátku služby[16] s tím, že zpracovatel má jasnou povinnost informovat správce o veškerých zamýšlených změnách týkajících se přidání či náhrady subdodavatele a že správce má po celou dobu možnost vznést proti těmto změnám námitku či smlouvu ukončit. Poskytovatel cloudových služeb by měl mít jasnou povinnost uvádět jména všech pověřených subdodavatelů. Kromě toho by měla být mezi poskytovatelem cloudových služeb a subdodavatelem podepsána smlouva, jež odráží ustanovení smlouvy mezi poskytovatelem cloudových služeb a zákazníkem. Správce by měl mít možnost využít smluvních opravných prostředků v případě porušení dohody ze strany dílčího zpracovatele. To lze zajistit tak, že i) zpracovatel bude přímo odpovědný správci za jakékoliv porušení smlouvy pověřenými dílčími zpracovateli, ii) bude vytvořeno právo třetí strany ve prospěch správce ve smlouvách podepsaných mezi zpracovatelem a dílčími zpracovateli, nebo iii) uvedené smlouvy budou podepsány jménem správce údajů, čímž se stane smluvní stranou.

3.4 Požadavky na ochranu údajů ve vztahu zákazník-poskytovatel

3.4.1 Dodržování základních zásad

Zákonnost zpracování osobních údajů v cloudu se odvíjí od dodržování základních zásad stanovených v právních předpisech EU na ochranu údajů. Konkrétně je třeba zajišťovat transparentnost vůči subjektu údajů, dodržovat zásadu určení a omezení účelu a mazat osobní údaje, jakmile jejich uchovávání již není nutné. Kromě toho musí být přijata vhodná technická a organizační opatření, jež zajistí odpovídající úroveň ochrany a bezpečnosti údajů.

3.4.1.1 Transparentnost

Transparentnost má pro řádné a legitimní zpracování osobních údajů klíčový význam. Podle směrnice 95/46/ES musí zákazník cloudových služeb poskytnout subjektu údajů, od kterého získává údaje, informace o své totožnosti a účelu zpracování. Zákazník cloudových služeb by měl rovněž poskytovat veškeré doplňující informace, například ohledně příjemců či kategorií příjemců údajů, což může zahrnovat i zpracovatele a dílčí zpracovatele, pokud jsou tyto

---

15 Návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů ze dne 25. 1. 2012.

16 Viz Často kladené dotazy FAQ II, 1) dokumentu WP 176 přijatého dne 12. července 2010.

doplňující informace nezbytné pro zajištění řádného zpracování údajů vůči subjektu údajů (viz článek 10 směrnice)[17].

Transparentnost musí být zajištěna ve vztazích mezi zákazníkem cloudových služeb, poskytovatelem cloudových služeb a případně subdodavateli. Zákazník cloudových služeb je schopen posoudit zákonnost zpracování osobních údajů v cloudu pouze tehdy, informuje-li ho poskytovatel o všech relevantních otázkách. Správce uvažující o využití služeb poskytovatele cloud computingu by si měl pozorně prostudovat jeho podmínky a posoudit je z hlediska ochrany údajů.

Transparentnost je v cloudu zajištěna tehdy, je-li si zákazník cloudových služeb informován o všech subdodavatelích, kteří se na poskytování příslušné cloudové služby podílejí, a o umístění všech datových center, ve kterých mohou být osobní údaje zpracovávány[18].

Pokud poskytování služby vyžaduje instalaci softwaru do systémů zákazníka cloudových služeb (např. zásuvné moduly v prohlížeči), měl by poskytovatel v rámci osvědčených postupů o této okolnosti zákazníka informovat, zejména o jejích dopadech z hlediska ochrany a bezpečnosti údajů. Pokud poskytovatel cloudových služeb tuto otázku neřeší dostatečně, měl by ji otevřít zákazník cloudových služeb předtím, než je začne využívat.

3.4.1.2 Určení a omezení účelu

Podle zásady specifikace a omezení účelu musí být osobní údaje shromažďovány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmějí být dále zpracovávány způsobem neslučitelným s těmito účely (srov. čl. 6 odst. 1 písm. b) směrnice 95/46/ES). Zákazník cloudových služeb musí určit účel(y) zpracování předtím, než začne od subjektu údajů shromažďovat osobní údaje, a informovat o nich subjekt údajů. Zákazník cloudových služeb nesmí zpracovávat osobní údaje pro jiné účely, které nejsou slučitelné s původními účely.

Kromě toho je třeba zajistit, aby osobní údaje (nezákonně) pro další účely nezpracovával poskytovatel cloudových služeb nebo některý z jeho subdodavatelů. V typickém případě může cloud computing lehce zahrnovat velký počet subdodavatelů, proto je třeba riziko zpracování osobních údajů pro jiné, neslučitelné účely považovat jako značně vysoké. V zájmu minimalizace tohoto rizika by měla smlouva mezi poskytovatelem cloudových služeb a zákazníkem upravovat technická a organizační opatření a poskytovat záruky pro evidenci a kontrolu příslušného zpracovávání osobních údajů, které provádějí zaměstnanci poskytovatele cloudových služeb nebo subdodavatelů[19]. Za porušení právních předpisů v oblasti ochrany údajů by měly být ve smlouvě stanoveny sankce ukládané poskytovateli nebo subdodavateli.

3.4.1.3 Výmaz údajů

Podle čl. 6 odst. 1 písm. e) směrnice 95/46/ES musí být osobní údaje uchovávány ve formě umožňující identifikaci subjektů údajů po dobu ne delší, než je nezbytné pro uskutečnění cílů, pro které jsou shromažďovány nebo dále zpracovávány. Osobní údaje, jež již nejsou potřeba, musí být vymazány nebo zcela anonymizovány. Pokud nelze tyto údaje vymazat kvůli zákonem dané archivaci (např. daňové předpisy), měl by být přístup k těmto osobním údajům

---

17 Podobně je nutné informovat subjekt údajů tehdy, pokud údaje neposkytuje sám subjekt údajů, nýbrž jsou zaznamenány z různých zdrojů, nebo pokud jsou sdělovány třetí osobě (viz článek 11).

18 Teprve tehdy bude schopen posoudit, zda mohou být osobní údaje předány do tzv. třetí země mimo EHP, která nezajišťuje odpovídající úroveň ochrany ve smyslu směrnice 95/46/ES. Srov. rovněž oddíl 3.4.6 níže.

19 Srov. oddíl 3.4.3 níže.

blokován. Je odpovědností zákazníka cloudových služeb zajistit, aby byly osobní údaje vymazány, jakmile již nejsou ve výše uvedeném smyslu nezbytné[20].

Zásada výmazu údajů platí pro osobní údaje bez ohledu na to, zda jsou uchovávány na pevných discích nebo na jiných nosičích (např. záložních páskách). Jelikož osobní údaje mohou být uchovávány nadbytečně na různých serverech na různých místech, je třeba, aby byly nenávratně vymazány na každém stupni (tzn. předchozí verze, dočasné soubory i fragmenty souborů musí být rovněž vymazány).

Zákazníci cloudových služeb si musí být vědomi toho, že registrační údaje[21] usnadňující kontrolovatelnost uložení, změn či výmazu údajů mohou rovněž představovat osobní údaje týkající se osoby, jež iniciovala příslušné zpracování[22].

Zabezpečený výmaz osobních údajů vyžaduje, aby nosiče dat byly zničeny nebo demagnetizovány nebo aby uložené osobní údaje byly přepsáním skutečně odstraněny. Pro přepsání osobních údajů je třeba použít speciální softwarové nástroje, jež data mnohonásobně přepisují v souladu s uznávanou specifikací.

Zákazník cloudových služeb by se měl ujistit, že poskytovatel cloudových služeb zajišťuje zabezpečený výmaz ve výše uvedeném smyslu a že smlouva mezi poskytovatelem a zákazníkem jasně výmaz osobních údajů upravuje[23]. Totéž platí pro smlouvy mezi poskytovateli cloudových služeb a subdodavateli.

3.4.2 Smluvní záruky vztahu „správce“–„zpracovatel“

Pokud se správci rozhodnou smluvně sjednat služby cloud computingu, musí si zvolit zpracovatele poskytujícího dostatečné záruky s ohledem na technická bezpečnostní opatření a organizační opatření usměrňující zpracování, jež má být provedeno, a musí dbát na dodržování těchto opatření (čl. 17 odst. 2 směrnice 95/46/ES). Kromě toho mají právní povinnost podepsat s poskytovatelem cloudových služeb formální smlouvu, jak stanoví čl. 17 odst. 3 směrnice 95/46/ES. Podle tohoto článku musí být vztah mezi správcem a zpracovatelem upraven smlouvou nebo jiným závazným právním aktem. Pro zachování důkazů jsou části smlouvy nebo právního aktu o ochraně údajů a požadavky související s technickými a organizačními opatřeními potvrzeny písemně nebo jinou rovnocennou formou.

Smlouva musí přinejmenším stanovovat to, že se zpracovatel řídí pokyny správce a že zpracovatel musí přijmout technická a organizační opatření k náležité ochraně osobních údajů.

V zájmu právní jistoty by smlouva měla dále upravovat následující body:

1. Podrobnosti (rozsah a podmínky) pokynů zákazníka určených poskytovateli, zejména pokud jde o platné dohody o úrovni služeb (jež by měly být objektivní a měřitelné) a příslušné sankce (finanční nebo jiný postih včetně možnosti žalovat poskytovatele v případě nedodržení smlouvy).
2. Bezpečnostní opatření, jež musí poskytovatel cloudových služeb dodržovat v závislosti na rizicích, jež vznikají při zpracovávání údajů, a na povaze údajů, jež

---

[20] Výmaz údajů hraje roli jak po dobu trvání smlouvy o cloud computingu, tak po jejím ukončení. Význam má také v případě nahrazení či odchodu subdodavatele.

[21] Poznámky k požadavkům na evidenci jsou uvedeny níže v bodě 4.3.4.2.

[22] To znamená, že je třeba vymezit přiměřené lhůty pro uchovávání registračních souborů a zavést postupy pro zajištění včasného výmazu nebo anonymizace těchto údajů.

[23] Srov. oddíl 3.4.3 níže.

mají být chráněny. Velmi důležité je uvést konkrétní technická a organizační opatření, jako například opatření nastíněná níže v bodě 3.4.3. Tímto není dotčeno použití případných přísnějších opatření, jež mohou být stanovena v zákazníkových vnitrostátních právních předpisech.

3. Předmět a časový rozvrh cloudové služby dodávané příslušným poskytovatelem, rozsah, způsob a účel zpracovávání osobních údajů prováděného poskytovatelem cloudových služeb, jakož i typy zpracovávaných údajů.
4. Podmínky navrácení (osobních) údajů nebo zničení údajů po dokončení služby. Dále je třeba zajistit, aby byly údaje na žádost zákazníka cloudových služeb bezpečně vymazány.
5. Zařazení doložky o mlčenlivosti závazné pro poskytovatele cloudových služeb i všechny jeho zaměstnance, kteří mohou přijít s údaji do styku. Přístup k údajům mohou mít pouze oprávněné osoby.
6. Povinnost poskytovatele podporovat zákazníka při usnadňování výkonu práv subjektů údajů na přístup ke svým údajům, na jejich opravu a výmaz.
7. Smlouva by měla výslovně stanovit, že poskytovatel cloudových služeb nesmí sdělovat údaje třetím stranám, a to ani pro účely uchovávání, ledaže je ve smlouvě ustanovení o subdodavatelích. Smlouva by měla uvádět, že dílčí zpracovatelé mohou být pověřeni zpracováním pouze na základě souhlasu, jenž obecně uděluje správce v souladu s jasnou povinností zpracovatele informovat správce o veškerých zamýšlených změnách v tomto ohledu s tím, že správce má po celou dobu možnost vznést proti těmto změnám námitku nebo smlouvu ukončit. Poskytovatel cloudových služeb by měl mít jasnou povinnost uvádět jména všech pověřených subdodavatelů (např. ve veřejném digitálním rejstříku). Je třeba zajistit, aby smlouvy mezi poskytovatelem cloudových služeb a subdodavatelem odrážely ustanovení smlouvy mezi zákazníkem a poskytovatelem cloudových služeb (tj. aby se na dílčí zpracovatele vztahovaly stejné smluvní povinnosti jako na poskytovatele cloudových služeb). Zejména musí být zaručeno, že poskytovatel cloudových služeb i veškeří subdodavatelé jednají pouze na základě pokynů zákazníka cloudových služeb. Jak je vysvětleno v kapitole o dílčím zpracování, musí být ve smlouvě jasně upraven řetězec odpovědnosti. Zpracovatel by měl mít povinnost rámcově upravovat mezinárodní předávání osobních údajů, například podepsáním smluv s dílčími zpracovateli na základě rozhodnutí 2010/87/EU o standardních smluvních doložkách.
8. Upřesnění oznamovací povinnosti poskytovatele cloudových služeb vůči zákazníkovi v případě jakéhokoliv narušení ochrany údajů, jež může mít dopad na údaje zákazníka.
9. Povinnost poskytovatele cloudových služeb poskytnout seznam míst, ve kterých mohou být údaje zpracovávány.
10. Právo správce na dohled a příslušnou povinnost poskytovatele cloudových služeb spolupracovat.
11. Mělo by být smluvně upraveno, že poskytovatel cloudových služeb musí zákazníka informovat o relevantních změnách týkajících se příslušné cloudové služby, jako je zavedení dalších funkcí.
12. Smlouva by měla upravovat evidenci a kontrolu příslušného zpracovávání osobních údajů, které provádí poskytovatel cloudové služby nebo subdodavatelé.
13. Povinnost oznamovat zákazníkovi cloudových služeb veškeré právně závazné požadavky na zveřejnění osobních údajů ze strany donucovacího orgánu, není-li to

jinak zakázáno, například trestním právem, aby byla zajištěna důvěrnost vyšetřování v rámci výkonu práva.

14. Obecná povinnost poskytovatele zaručit, že jeho vnitřní organizace a systémy zpracovávání údajů (případně organizace a systémy dílčích zpracovatelů) jsou v souladu s použitelnými vnitrostátními a mezinárodními právními požadavky a normami.

V případě porušení smlouvy ze strany správce musí mít osoba, jež utrpí újmu v důsledku nezákonného zpracovávání údajů, právo obdržet od správce náhradu za způsobené škody. Pokud zpracovatelé použijí údaje pro jiné účely nebo je sdělí či použijí v rozporu se smlouvou, měli by být rovněž považováni za správce a zodpovídat se z porušení smlouvy, do něhož byli osobně zapojeni.

Je třeba poznamenat, že v mnoha případech nabízejí poskytovatelé cloud computingu standardizované služby a správci pak mají podepsat smlouvy, v nichž je upravena standardizovaná forma zpracování osobních údajů. Tato nerovnováha ve smluvní pozici mezi malým správcem a velkými poskytovateli služeb by neměla správcům sloužit k ospravedlnění toho, že akceptují doložky a podmínky smlouvy, jež nejsou v souladu s právními předpisy na ochranu údajů.

3.4.3 Technická a organizační opatření v rámci ochrany a bezpečnosti údajů

Podle čl. 17 odst. 2 směrnice 95/46/ES si zákazníci cloudových služeb (jednající jako správci údajů) musí vybrat poskytovatele cloudových služeb, kteří přijmou vhodná technická a organizační opatření na ochranu osobních údajů, za která odpovídají.

Kromě hlavních cílů v oblasti bezpečnosti, tedy dostupnosti, důvěrnosti a integrity, je třeba věnovat pozornost i doplňkovým cílům v oblasti ochrany údajů, jimiž jsou transparentnost (viz výše bod 3.4.1.1), izolovanost[24], schopnost intervence, odpovědnost a přenositelnost. V tomto oddíle jsou zdůrazněny hlavní cíle v oblasti bezpečnosti údajů, aniž by byla dotčena jiná doplňková a na bezpečnost zaměřená analýza rizik[25].

3.4.3.1 Dostupnost

Zajištění dostupnosti znamená zajištění včasného a spolehlivého přístupu k osobním údajům.

Závažnou hrozbou pro dostupnost údajů v cloudu je neočekávaná ztráta síťového propojení mezi zákazníkem a poskytovatelem nebo snížení výkonnosti serverů způsobené zlovolným jednáním, jako jsou útoky typu distribuovaného odepření služby (*Denial of Service*)[26]. Dostupnost dále ohrožují neočekávaná hardwarová selhání síťových systémů i systémů pro zpracování nebo uchovávání údajů v cloudu, dále pak výpadky elektřiny nebo jiné problémy infrastruktury.

Správci údajů by měli kontrolovat, zda poskytovatel cloudových služeb přijal vhodná opatření, jež by na rizika narušení systému reagovala a k nimž patří např. záložní připojení

---

[24] V Německu byl zaveden v právních předpisech širší pojem „nespojitelnost“ (*unlinkability*), který podporuje i konference komisařů pro ochranu údajů.

[25] Srov. např. dokument ENISA na: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[26] Útok typu odepření služby představuje koordinovaný pokus o dočasné nebo časově neomezené znepřístupnění počítače nebo síťových zdrojů oprávněným uživatelům (např. prostřednictvím velkého množství atakujících systémů, jež ochromí svůj cíl obrovským počtem externích komunikačních požadavků).

k internetové síti, uchovávání nadbytečných údajů a mechanismy pro efektivní zálohování dat.

3.4.3.2 Integrita

Integritu lze definovat jako vlastnost, jež spočívá v pravosti údajů, které nebyly během zpracovávání, uchovávání nebo předávání nijak zlovolně či náhodně pozměněny. Pojem integrity lze rozšířit i na systémy IT, které pak musí zpracovávat osobní údaje tak, aby u nich nedošlo k žádné změně.

Odhalování změn osobních údajů lze dosáhnout pomocí šifrovacích a autentizačních mechanismů, jako jsou autentizační kódy nebo podpisy zprávy.

Narušení integrity systémů IT v cloudu je možné zamezit nebo odhalit pomocí příslušných systémů detekce nebo prevence (IPS/IDS). To je obzvlášť důležité v rámci takového otevřeného síťového prostředí, v jakém jsou cloudy obvykle provozovány.

3.4.3.3 Důvěrnost

V prostředí cloudu může k důvěrnosti osobních údajů při správném provádění významně přispět šifrování, i když při něm nedochází k jejich nezvratné anonymizaci[27]. Osobní údaje by měly být šifrovány při každém předávání i v případě disponibility pro neaktivní údaje[28]. V některých případech (např. služba uložení dat v rámci IaaS) se nemusí zákazník cloudových služeb spoléhat na šifrovací systém nabízený poskytovatelem, nýbrž může zašifrovat osobní údaje již před jejich odesláním na cloud. Při šifrování neaktivních údajů je třeba věnovat zvýšenou pozornost správě šifrovacích klíčů, jelikož od důvěrnosti šifrovacích klíčů se v konečném důsledku odvíjí i ochrana údajů.

Komunikace mezi poskytovatelem a zákazníkem cloudových služeb, jakož i mezi datovými centry by měla probíhat v zašifrované podobě. Vzdálená správa cloudové platformy by měla fungovat prostřednictvím zabezpečeného komunikačního kanálu. Pokud zákazník plánuje nejen uložení, ale i další zpracování osobních údajů v cloudu (např. vyhledávací databáze záznamů), musí mít na paměti, že zašifrování údajů není možné zachovat při jejich zpracovávání (vyjma velmi specifických výpočetních operací).

Mezi další technická opatření, jež mají zajistit důvěrnost, patří mechanismy autorizace a přísné ověřování (např. dvoufaktorová identifikace). Ve smluvních doložkách by měly být rovněž stanoveny povinnosti ohledně důvěrnosti údajů pro zaměstnance zákazníků cloudových služeb, poskytovatelů cloudových služeb a subdodavatelů.

3.4.1.4 Transparentnost

Technická a organizační opatření musí fungovat v zájmu transparentnosti tak, aby bylo možné provádět přezkum, srov. bod 3.4.1.1.

3.4.3.5 Izolovanost (omezení účelu)

V infrastrukturách cloudu sdílí zdroje, jako jsou úložiště, paměť a sítě, mnoho nájemců. Tak vzniká nové riziko zpřístupnění údajů a jejich zpracování pro neoprávněné účely. Smyslem

---

[27] Směrnice 95/46/ES, 26. bod odůvodnění: „vzhledem k tomu, (…) že zásady ochrany se nevztahují na údaje, které byly anonymizovány tak, že subjekt údajů již není identifikovatelný; (...)“. Stejně tak nepovedou technické postupy na fragmentaci údajů, jež mohou být v rámci poskytování cloudových služeb použity, k nezvratné anonymizaci, a proto z nich nevyplývá, že povinnosti ochrany údajů neplatí.

[28] To platí zejména pro správce údajů, kteří hodlají předávat citlivé údaje ve smyslu článku 8 směrnice 95/46/ES (např. údaje týkající se zdraví) na cloud nebo kteří jsou ze zákona vázáni povinností zachovávat profesní tajemství.

cíle ochrany údajů spočívající v jejich izolovanosti je tento problém řešit a přispět k zajištění toho, že údaje nebudou použity nad rámec svého původního účelu (čl. 6 odst. 1 písm. b) směrnice 95/46/ES), a k zachování důvěrnosti a integrity[29].

Pro dosažení izolovanosti je v prvé řadě nezbytná řádná správa práv a funkcí ohledně přístupu k osobním údajům, jenž podléhá pravidelnému přezkumu. Je třeba se vyhnout zavádění funkcí s nadměrnými právy (např. žádný uživatel ani administrátor by neměl být oprávněn k přístupu k celému cloudu). Obecněji řečeno, administrátoři a uživatelé musí mít zajištěn pouze přístup k informacím, jež jsou nezbytné pro jejich legitimní účely (podle zásady minimálních práv).

Izolovanost se také odvíjí od technických opatření, jakými jsou posílení hypervizorů a řádná správa sdílených zdrojů, pokud se nástroje virtualizace využívají ke sdílení fyzických zdrojů různými zákazníky cloudových služeb.

3.4.3.5 Schopnost intervence

Podle směrnice 95/46/ES má subjekt údajů právo na přístup k údajům, na jejich opravu, výmaz nebo blokování a právo na námitku (srov. článek 12 a 14). Zákazník cloudových služeb musí ověřit, že poskytovatel cloudových služeb nebrání plnění těchto požadavků technickými a organizačními překážkami, včetně případů, kdy údaje dále zpracovávají subdodavatelé.

Smlouva mezi zákazníkem a poskytovatelem by měla stanovit, že poskytovatel cloudových služeb je povinen podporovat zákazníka při usnadňování výkonu práv subjektů údajů a zajistit, aby totéž platilo i pro jeho vztahy k případným subdodavatelům[30].

3.4.3.6 Přenositelnost

V současné době většina cloudových poskytovatelů nevyužívá standardní datové formáty a rozhraní služeb usnadňující interoperabilitu a přenositelnost mezi různými poskytovateli cloudových služeb. Pokud se zákazník cloudových služeb rozhodne o přechod od jednoho poskytovatele k druhému, může tato chybějící interoperabilita vyústit v situaci, kdy je nemožné nebo přinejmenším obtížné předat zákazníkovy (osobní) údaje novému poskytovateli (tzv. závislost na poskytovatelích, *vendor lock-in*). Totéž platí i pro služby, které zákazník vyvinul na platformě nabízené původním poskytovatelem (PaaS). Zákazník cloudových služeb by měl zkontrolovat, zda a jak poskytovatel zaručuje přenositelnost údajů a služeb dříve, než si cloudovou službu objedná[31].

3.4.4.7 Odpovědnost

Odpovědnost IT lze definovat jako schopnost zjistit, co a jakým způsobem daný subjekt dělal v určitém okamžiku v minulosti. V oblasti ochrany údajů má tento pojem často širší význam a popisuje schopnost zúčastněných stran prokázat, že podnikly náležité kroky, jež zajišťují plnění zásad ochrany údajů.

Odpovědnost IT je obzvlášť důležitá pro vyšetření narušení bezpečnosti osobních údajů, při němž zákazníci, poskytovatelé a subdodavatelé cloudových služeb nesou část operační

---

29 Srov. 3.4.1.2.

30 Srov. výše oddíl 3.4.2 bod 6. Poskytovatel může dokonce dostávat instrukce ke zodpovídání dotazů jménem zákazníka.

31 Poskytovatel by měl pokud možno využívat standardní nebo otevřené datové formáty a rozhraní. V každém případě by měly být sjednány smluvní doložky upravující zajištěné formáty, zachování logických vztahů a případné náklady na přechod k jinému poskytovateli cloudových služeb.

odpovědnosti. Klíčový význam v tomto ohledu má schopnost cloudové platformy zajistit spolehlivé mechanismy monitorování a komplexní evidence.

Poskytovatelé cloudových služeb by mimo to měli poskytovat písemné doklady o vhodných a účinných opatřeních, jejichž výsledkem je plnění zásad ochrany údajů uvedených v předchozích oddílech. Jako příklady těchto opatření lze jmenovat postupy na zajištění identifikace veškerých operací zpracování údajů, na zodpovězení žádostí o přístup, na přidělení zdrojů včetně jmenování inspektorů ochrany údajů, kteří odpovídají za organizaci dodržování předpisů na ochranu údajů, či nezávislé postupy certifikace. Správci údajů by měli být rovněž schopni na příslušnou žádost prokázat příslušnému orgánu dohledu zavedení nezbytných opatření[32].

3.5 Mezinárodní předávání

Podle článků 25 a 26 směrnice 95/46/ES je volný pohyb osobních údajů do zemí mimo EHP možný pouze tehdy, zajišťuje-li dotyčná země nebo příjemce odpovídající úroveň ochrany údajů. V jiných případech musí správci (či společní správci) a jejich zpracovatelé zavést zvláštní ochranná opatření. Podstatou cloud computingu je však nejčastěji to, že vůbec neexistuje pevné umístění údajů v rámci sítě poskytovatele cloudových služeb. Údaje se mohou nacházet v jednom datovém centru ve 14:00 a na druhém konci světa o dvě hodiny později. Zákazník cloudových služeb proto může jen zřídka vědět v reálném čase, kde jsou jeho údaje umístěny či uloženy, či kam jsou předávány. Tradiční právní nástroje, které stanoví rámec upravující předávání údajů do třetích zemí, jež nezajišťují odpovídající ochranu, naráží v tomto kontextu na své limity.

3.5.1 Tzv. bezpečný přístav a vhodné země

Konstatování odpovídající úrovně ochrany, včetně „bezpečného přístavu“, je zeměpisně omezeno a nevztahuje se na veškeré předávání údajů v rámci cloudu.
Organizacím v USA, které dodržují dané zásady, mohou být údaje legálně podle předpisů EU předávány, jelikož se má za to, že tyto přijímací organizace zajišťují odpovídající úroveň ochrany předávaných údajů.

Při absenci účinného prosazování zásad ochrany údajů v prostředí cloudu však nelze podle názoru pracovní skupiny považovat pouhé „vlastní osvědčení“ o přijetí zásad bezpečného přístavu za dostatečné. Podle článku 17 směrnice EU je navíc pro účely zpracování podepsat smlouvu mezi správcem a zpracovatelem, což potvrzují i odpovědi na často kladenou otázku (FAQ) 10 v rámcových dokumentech mezi EU a USA ohledně zásad „bezpečného přístavu“. Tuto smlouvu nemusí předem schvalovat orgány pro ochranu údajů v EU. Tato smlouva blíže určuje zpracování, které má být prováděno, a veškerá opatření nezbytná k zajištění bezpečnosti údajů. Různé vnitrostátní předpisy a orgány pro ochranu údajů mohou stanovit další požadavky.

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

[32] Pracovní skupina poskytla na téma odpovědnost podrobné připomínky ve svém stanovisku č. 3/2010 k zásadě odpovědnosti: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_cs.pdf.

zejména s ohledem na informace poskytované subjektům údajů, jichž se zpracování údajů týká[33,34].

Pracovní skupina má rovněž za to, že zákazník cloudových služeb musí ověřit, zda standardní smlouvy vypracované poskytovateli jsou v souladu s vnitrostátními požadavky ohledně smluvního zpracování údajů. Vnitrostátní právní předpisy mohou vyžadovat vymezení dílčího zpracování ve smlouvě, což zahrnuje umístění a další údaje o dílčích zpracovatelích a dohledatelnost údajů. Poskytovatelé cloudových služeb obvykle zákazníkům tyto informace neposkytují – jejich závazek dodržovat zásady „bezpečného přístavu" nemůže nahradit absenci výše uvedených záruk, pokud je vyžadují vnitrostátní právní předpisy. V takových případech by měl vývozce sáhnout po jiných dostupných právních nástrojích, jako jsou standardní smluvní doložky nebo závazná podniková pravidla.

V neposlední řadě zastává pracovní skupina názor, že zásady „bezpečného přístavu" samy o sobě nemusí 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[35]. 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)[36], která nejsou dostatečně ošetřena stávajícími zásadami „bezpečného přístavu" k bezpečnosti údajů[37]. 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[38]. 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.

3.5.2 Výjimky

Výjimky podle článku 26 směrnice 95/46/ES umožňují vývozcům údajů předávat údaje mimo EU bez poskytnutí dodatečných záruk. Pracovní skupina podle článku 29 však přijala stanovisko, podle něhož se výjimky mají vztahovat pouze na případy, ve kterých nejde o opakované, rozsáhlé ani strukturální předávání údajů[39].

Na základě tohoto výkladu je takřka nemožné se v kontextu cloud computingu odvolávat na uvedené výjimky.

3.5.3 Standardní smluvní doložky

Standardní smluvní položky, které přijala Komise EU za účelem stanovení rámce pro mezinárodní předávání údajů mezi dvěma správci nebo mezi správcem a zpracovatelem, jsou založeny na dvoustranném přístupu. Pokud je poskytovatel cloudových služeb považován za

---

33 Viz německý orgán pro ochranu údajů: http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

34 Pro požadavky týkající se dílčích zpracovatelů vit bod 3.3.2.

35 Viz stanovisko dánského orgánu pro ochranu údajů: http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution.

36 Podrobně popsaná v dokumentu ENISA: Cloud computing – Benefits, Risks and Recommendations for Information Security, k dispozici na: https://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

37 „Organizace musí přijmout přiměřená bezpečnostní opatření na ochranu osobních údajů před jejich ztrátou a zneužitím, neoprávněným přístupem k nim, jejich vyzrazením, změnou nebo zničením."

38 Viz bod 4.2 níže.

39 Pracovní dokument č. 12/1998: Předávání osobních údajů do třetích zemí: Uplatňování článků 25 a 26 směrnice EU o ochraně údajů, přijaté pracovní skupinou dne 24. července 1998, (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

zpracovatele, mohou být mezi ním a správcem sjednány podle rozhodnutí Komise 2010/87/EU vzorové doložky jakožto základ pro prostředí cloud computingu, jež nabízí dostatečná ochranná opatření v kontextu mezinárodního předávání údajů.

Pracovní skupina konstatuje, že kromě těchto standardních smluvních doložek by poskytovatelé cloudových služeb mohli zákazníkům nabízet i ustanovení, jež vycházejí z jejich praktických zkušeností, pokud nejsou v přímém ani nepřímém rozporu se standardními smluvními doložkami přijatými Komisí či pokud nepoškozují základní práva a svobody subjektů údajů[40]. Společnosti však standardní smluvní doložky nemohou měnit. Po změně by již doložky nebyly „standardní“[41].

Pokud je poskytovatel cloudových služeb vystupující jako zpracovatel usazen v EU, může být situace komplikovanější, jelikož se vzorové doložky obecně vztahují pouze na předávání údajů od správce údajů v EU zpracovateli mimo EU (viz 23. bod odůvodnění rozhodnutí Komise o standardních doložkách 2010/87/EU a dokument WP 176).

Pokud jde o smluvní vztah mezi zpracovatelem mimo EU a dílčím zpracovatelem, měla by existovat písemná smlouva, jež dílčím zpracovatelům ukládá stejné povinnosti, jaké jsou pro zpracovatele stanoveny ve vzorových doložkách.

3.5.4 Závazná podniková pravidla: směrem ke globálnímu přístupu

Závazná podniková pravidla představují kodex chování pro společnosti, jež předávají údaje v rámci své skupiny. Takové řešení bude stanoveno i v kontextu cloud computingu v případě, kdy poskytovatel je zpracovatelem údajů. Pracovní skupina podle článku 29 v současné době pracuje na závazných podnikových pravidlech pro zpracovatele, jež umožní předávání údajů v rámci skupiny ku prospěchu správců, aniž by bylo nutné podepisovat smlouvy mezi zpracovatelem a dílčími zpracovateli u každého zákazníka[42].

Díky těmto závazným podnikovým pravidlům pro zpracovatele by měli zákazníci poskytovatele možnost svěřit své osobní údaje zpracovateli a zároveň by byla zajištěna odpovídající úroveň ochrany údajů předávaných v rámci obchodní činnosti poskytovatele.

4. Závěry a doporučení

Podniky a orgány veřejné správy, které chtějí využívat cloud computing by jako první krok měly provést komplexní a důkladnou analýzu rizik. Tato analýza by měla řešit rizika týkající se zpracování údajů v cloudu (nedostatek kontroly a informací – viz výše oddíl 2) s přihlédnutím k typu údajů zpracovávaných v cloudu[43]. Zvláštní pozornost je třeba věnovat i posouzení právních rizik ve vztahu k ochraně údajů, jež se týkají zejména bezpečnostních požadavků a mezinárodního předávání. Další obavy vyvolává zpracovávání citlivých údajů prostřednictvím cloud computingu. Aniž by byly dotčeny vnitrostátní právní předpisy,

---

40 Viz Často kladené dotazy, FAQ IV B1.9 9: Mohou společnosti zahrnout standardní smluvní doložky do rozsáhlejší smlouvy a dodat specifické doložky? - zveřejněné Komisí na: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

41 Viz FAQ IV B1.10: Mohou společnosti měnit standardní smluvní doložky schválené Komisí?

42 Viz pracovní dokument: *Working Document 02/2012 setting up a table with the elements and principles to be found in Processor Binding Corporate Rules*, přijatý dne 6. června 2012: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp195_en.pdf

43 ENISA vypracovala seznam rizik, jež je třeba zohlednit:

vyžaduje takové zpracování dodatečná ochranná opatření[44]. Níže uvedené závěry je třeba chápat jako kontrolní seznam pro respektování ochrany údajů zákazníky a poskytovateli cloudových služeb podle současného právního rámce. U některých doporučení se přihlédlo k budoucímu vývoji regulačního rámce jak na úrovni EU, tak i mimo ni.

4.1 Pokyny pro zákazníky a poskytovatele služeb cloud computingu

- Vztah správce-zpracovatel: toto stanovisko se zaměřuje na vztah zákazník-poskytovatel jakožto na vztah správce-zpracovatel (viz bod 3.3.1). Za konkrétních okolností však může docházet k situacím, kdy poskytovatel cloudových služeb vystupuje rovněž jako správce, např. pokud opětovně zpracovává některé osobní údaje pro vlastní účely. V takovém případě má poskytovatel cloudových služeb plnou (společnou) odpovědnost za zpracování a musí splnit všechny právní povinnosti stanovené ve směrnici 95/46/ES, případně 2002/58/ES.
- Odpovědnost zákazníka cloudových služeb jako správce: zákazník musí jakožto správce přijmout odpovědnost za dodržování právních předpisů na ochranu údajů a vztahují se na něj všechny právní závazky stanovené ve směrnici 95/46/ES, případně směrnici 2002/58/ES, a to zejména vůči subjektům údajů (viz bod 3.3.1). Zákazník by si měl vybrat poskytovatele cloudových služeb, který zaručuje soulad s právními předpisy EU na ochranu údajů, zajištěný formou vhodných smluvních ochranných opatření, jež jsou shrnuta níže.
- Ochranná opatření v případě existence subdodavatelů: každá smlouva mezi poskytovatelem cloudových služeb a zákazníkem by měla obsahovat ustanovení ohledně subdodavatelů. Smlouva by měla uvádět, že dílčí zpracovatelé mohou být pověřeni zpracováním pouze na základě souhlasu, jenž obecně uděluje správce v souladu s jasnou povinností zpracovatele informovat správce o veškerých zamýšlených změnách v tomto ohledu s tím, že správce má po celou dobu možnost vznést proti těmto změnám námitku nebo smlouvu ukončit. Poskytovatel cloudových služeb by měl mít jasnou povinnost uvádět jména všech pověřených subdodavatelů. Poskytovatel cloudových služeb by měl s každým subdodavatelem podepsat smlouvu, v níž se odrážejí ustanovení jeho smlouvy se zákazníkem cloudových služeb. Zákazník by si měl zajistit smluvní opravné prostředky v případě porušení dohody ze strany poskytovatelova subdodavatele (viz bod 3.3.2).
- Soulad se základními zásadami ochrany údajů:
    - Transparentnost (viz bod 3.4.1.1): poskytovatel cloudových služeb by měl během sjednávání smlouvy informovat zákazníka o všech důležitých aspektech, jež v rámci jejich služeb souvisejí s ochranou údajů. Zákazník by měl být zejména informován o všech subdodavatelích, kteří se na poskytování příslušné cloudové služby podílejí, a o všech místech, ve kterých mohou být údaje poskytovatelem cloudových služeb anebo jeho subdodavateli uloženy nebo zpracovávány (zejména tehdy, pokud se některá nebo všechna uvedená místa nacházejí mimo EHP). Zákazník by měl obdržet jasné informace o technických a organizačních opatřeních přijatých poskytovatelem. Zákazník by měl v rámci osvědčených postupů informovat subjekty údajů o poskytovateli cloudové služby a o všech případných subdodavatelích i o místech, ve kterých mohou být údaje poskytovatelem cloudových služeb anebo jeho subdodavateli uloženy či zpracovávány.

[44] Viz Sopotské memorandum, srov. poznámka pod čarou č. 2.

- Určení a omezení účelu (bod 3.4.1.2): zákazník by měl zajistit soulad se zásadami určení a omezení účelu a dbát na to, aby poskytovatel ani jeho případní subdodavatelé nezpracovávali žádné údaje pro jiné účely. Příslušné závazky by měly být upraveny formou vhodných smluvních ujednání (včetně technických a organizačních ochranných opatření).
- Uchovávání údajů (3.4.1.3): zákazník odpovídá za zajištění výmazu osobních údajů (poskytovatelem nebo případnými subdodavateleli) v každém jejich úložišti, jakmile již nejsou potřebné pro dané účely. Smluvně by měly být upraveny zabezpečené mechanismy výmazu údajů (zničení, demagnetizace, přepsání).

- Smluvní záruky (viz body 3.4.2, 3.4.3 a 3.5):
  - Obecně: smlouva s poskytovatelem (a smlouvy, jež mají být uzavřeny mezi poskytovatelem a subdodavateli) by měla obsahovat dostatečné záruky, jež se týkají technických bezpečnostních opatření a organizačních opatření (podle čl. 17 odst. 2 směrnice) a jež jsou potvrzeny písemně nebo jinou rovnocennou formou. Smlouva by měla podrobně upravovat pokyny zákazníka pro poskytovatele včetně předmětu a časového rozvrhu služby, objektivní a měřitelné úrovně služeb a příslušné (finanční nebo jiné) sankce. Smlouva by měla uvádět bezpečnostní opatření, jež je třeba dodržovat i) v závislosti na rizicích zpracování a povaze údajů, ii) v souladu s níže uvedenými požadavky a iii) s výhradou případných přísnějších opatření stanovených v zákazníkových vnitrostátních právních předpisech. Pokud hodlají poskytovatelé cloudových služeb využít standardních smluvních doložek, měli by zajistit jejich soulad s požadavky na ochranu údajů (viz bod 3.4.2). V příslušných doložkách by měla být zejména uvedena technická a organizační opatření přijatá poskytovatelem.
  - Přístup k údajům: přístup k údajům by měly mít pouze oprávněné osoby. Smlouva by měla obsahovat doložku o mlčenlivosti pro poskytovatele a jeho zaměstnance.
  - Sdělování údajů třetím osobám: tato otázka by měla být upravena výhradně smluvně. Podle smlouvy by poskytovatel povinně uváděl jména všech svých subdodavatelů (např. ve veřejném digitálním rejstříku) a zajišťoval zákazníkovi přístup k informacím o případných změnách. Tak bude mít zákazník možnost vznést proti těmto změnám námitku nebo smlouvu ukončit. Smlouva by měla rovněž stanovit povinnost poskytovatele oznamovat veškeré právně závazné požadavky na zveřejnění osobních údajů ze strany donucovacího orgánu, není-li to jinak zakázáno. Zákazník by měl zaručit, že poskytovatel odmítne veškeré právně nezávazné požadavky na zveřejnění údajů.
  - Povinnost spolupracovat: zákazník by měl zajistit povinnost poskytovatele i) spolupracovat, pokud jde o právo zákazníka na dohled nad zpracováním, ii) usnadňovat výkon práv subjektů údajů na přístup ke svým údajům, na jejich opravu a výmaz a iii) případně oznamovat zákazníkovi cloudových služeb jakékoliv narušení ochrany údajů, jež má dopad na údaje zákazníka.
  - Přeshraniční předávání údajů: zákazník by měl ověřit, zda může poskytovatel cloudových služeb zaručit zákonnost přeshraničního předávání údajů a pokud možno omezit předávání údajů na země vybrané zákazníkem. Předávání údajů do třetích zemí, jež nezajišťují odpovídající ochranu údajů, vyžaduje příslušná

zvláštní ochranná opatření – použití ujednání „bezpečného přístavu“, standardních smluvních doložek či závazných podnikových pravidel. Použití standardních smluvních doložek pro zpracovatele (podle rozhodnutí Komise 2010/87/EU) vyžaduje určité úpravy v prostředí cloudu (s cílem předejít smlouvám mezi poskytovatelen a jeho dílčími zpracovateli u každého zákazníka zvlášť), z čehož může vyplývat nutnost předchozího povolení vydané příslušným orgánem pro ochranu údajů. Smlouva by měla obsahovat seznam míst, ve kterých může být služba poskytována.

- Evidence a kontrola zpracování: zákazník by měl vyžadovat, aby zpracovávání údajů prováděné poskytovatelem a jeho subdodavateli bylo evidováno. Zákazník by měl mít pravomoc provádět kontrolu tohoto zpracovávání, avšak lze akceptovat i audity prováděné třetí stranou vybranou poskytovatelem nebo příslušná certifikace, pokud je zaručena plná transparentnost (např. možností obdržet kopii osvědčení o auditu třetí strany nebo kopii auditní zprávy ověřující osvědčení).
- Technická a organizační opatření: jejich účelem by mělo být zmírnění rizik vyplývajících z nedostatku kontroly nad údaji a nedostatku příslušných informací, na něž lze v prostředí cloud computingu narazit nejčastěji. Pomocí technických opatření má být zajištěna dostupnost, integrita, důvěrnost, izolovanost, schopnost intervence a přenositelnost tak, jak je vymezeno v tomto stanovisku; organizační opatření jsou pak zaměřena na transparentnost (podrobně viz bod 3.4.3).

4.2 Osvědčení třetích stran o ochraně údajů

- Nezávislá ověření či osvědčení renomovanou třetí stranou může pro poskytovatele cloudových služeb představovat věrohodný způsob, jak prokázat dodržení závazků uvedených v tomto stanovisku. Toto osvědčení by přinejmenším uvádělo, že kontroly v oblasti ochrany údajů podléhají auditu či přezkumu renomovanou třetí stranou podle uznávaných norem v souladu s požadavky uvedenými v tomto stanovisku [45]. V kontextu cloud computingu by potenciální zákazníci měli zkontrolovat, zda poskytovatelé cloudových služeb mohou poskytnout kopii tohoto osvědčení o auditu třetí strany nebo kopii auditní zprávy ověřující toto osvědčení, a to i s ohledem na požadavky uvedené v tomto stanovisku.
- Jednotlivé audity údajů umístěných na serverech v mnohostranném, virtualizovaném prostředí mohou být technicky nerealizovatelné a za určitých okolností mohou dokonce zvyšovat rizika pro existující kontroly bezpečnosti fyzické a logické sítě. V těchto případech lze příslušný audit třetí strany vybraný správcem považovat za dostačující (navzdory právu jednotlivých správců na kontrolu údajů).
- Přijetí norem a osvědčení v oblasti soukromí je nezbytné pro budování korektních vztahů mezi poskytovateli cloudových služeb, správci a subjekty údajů.
- Tyto normy a osvědčení by měly řešit jednak technické záležitosti (jako je umístění nebo šifrování údajů), jednak postupy uvnitř organizace poskytovatele cloudových služeb, jež zajišťují ochranu údajů (jako je kontrola přístupu nebo zálohování údajů).

[45] K těmto normám by patřily normy, jež vydává Mezinárodní organizace pro normalizaci, Rada pro mezinárodní auditorské a ověřovací standardy a Rada pro auditorské standardy Amerického institutu autorizovaných auditorů, za předpokladu, že splňují požadavky uvedené v tomto stanovisku.

4.3 Doporučení: další vývoj

Pracovní skupina si je plně vědoma toho, že ochranná opatření a řešení nastíněná v tomto stanovisku nemohou spletité otázky cloud computingu vyřešit beze zbytku. Na druhou stranu představují solidní základ pro zabezpečené zpracování osobních údajů, jež zákazníci usazení v EHP svěří poskytovatelům cloudových služeb. Tento oddíl upozorňuje na některá problematická místa, s nimiž je třeba se v krátkodobém až střednědobém horizontu vypořádat. Cílem je rozšířit stávající ochranná opatření, asistovat odvětví cloud computingu při řešení uvedených problémů a zároveň zajišťovat respekt k základním právům na soukromí a ochranu údajů.

- Vyváženější rozdělení odpovědnosti mezi správcem a zpracovatelem: pracovní skupina vítá ustanovení článku 26 návrhu Komise na obecné nařízení o ochraně údajů, jejichž cílem je zajistit větší odpovědnost zpracovatelů vůči správcům tím, že jim napomáhají zajišťovat plnění povinností zejména v oblasti bezpečnosti a souvisejících oblastech. Článek 30 návrhu zavádí zákonnou povinnost zpracovatele přijmout vhodná technická a organizační opatření. V návrhu je objasněno, že zpracovatel, jenž neplní správcovy pokyny, se považuje za správce a vztahují se na něho specifická pravidla o společných správcích. Pracovní skupina podle článku 29 má za to, že návrh jde správným směrem při zmírňování nerovnováhy, s níž se lze často setkat v prostředí cloud computingu, v němž může být pro zákazníka (zejména malý či střední podnik) obtížné vykonávat podle právních předpisů na ochranu údajů plnou kontrolu způsobu, jakým poskytovatel dodává požadované služby. Vzhledem k nerovnoměrnému právnímu postavení subjektů údajů a uživatelů z řad malých podniků vůči velkým poskytovatelům cloud computingu se doporučuje aktivnější přístup spotřebitelských a podnikatelských zájmových organizací s cílem vyjednat vyváženější obchodní podmínky těchto společností.

- Přístup k osobním údajům pro účely bezpečnosti státu a vymáhání práva: je nesmírně důležité přidat do budoucího nařízení ustanovení zakazující správcům působícím v EU sdělovat osobní údaje do třetích zemí, pokud je vyžaduje soudní či správní orgán dané třetí země, ledaže by to bylo výslovně povoleno mezinárodní dohodou, upraveno smlouvami o vzájemné právní pomoci nebo schváleno orgánem dohledu. Vhodným příkladem právního základu pro tyto případy je nařízení Rady (ES) č. 2271/96[46]. Pracovní skupina je tímto nedostatkem v návrhu Komise zneklidněna, jelikož se od něj odvíjí značná ztráta právní jistoty pro subjekty údajů, jejichž osobní údaje jsou uloženy v datových centrech po celém světě. Z tohoto důvodu by pracovní skupina chtěla zdůraznit[47] nutnost začlenit do nařízení povinnost používat – v případě sdělování údajů nedovoleného právem Unie či členských států – dvoustranné dohody o vzájemné právní pomoci.

- Zvláštní opatření přijímaná veřejným sektorem: je třeba přidat zvláštní ustanovení, pokud jde o povinnost veřejného orgánu nejdříve posoudit, zda předávání, zpracování a uložení údajů mimo území státu může vystavit bezpečnost a soukromí občanů a bezpečnost a hospodářství státu nepřijatelným rizikům, zejména týká-li se citlivých databází (např. údaje ze sčítání lidu) nebo služeb (např. zdravotnictví)[48]. Rozhodně by se tato otázka měla

---

46 Nařízení Rady (ES) č. 2271/96 ze dne 22. listopadu 1996 o ochraně proti účinkům právních předpisů přijatých určitou třetí zemí uplatňovaných mimo její území, jakož i proti účinkům opatření na nich založených nebo z nich vyplývajících, Úř. věst. L 309, 29.11.1996, s. 1: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:CS:HTML

47 Srov. dokument WP 191 – stanovisko č. 01/2012 k reformě právních předpisů o ochraně osobních údajů, s. 22.

48 V tomto ohledu vydala ENISA následující doporučení ve svém dokumentu: *Security & Resilience in Governmental Clouds* (Bezpečnost a odolnost vládních cloudů, http://www.enisa.europa.eu/activities/risk-management/emerging-and-future-risk/deliverables/security-

zvažovat při každém zpracování citlivých údajů v rámci cloudu. V tomto ohledu by vlády jednotlivých států a orgány Evropské unie mohly pokročit při zvažování koncepce „evropského vládního cloudu“ jakožto nadnárodního virtuálního prostoru, v němž by platila jednotná a harmonizovaná pravidla.

- Evropské partnerství pro cloud computing: pracovní skupina podporuje strategii evropského partnerství pro cloud computing, kterou představila místopředsedkyně Evropské komise Neelie Kroesová v lednu 2012 v Davosu[49]. Ve snaze o stimulaci evropského trhu v oblasti cloud computingu zahrnuje tato strategie i zadávání veřejných zakázek v oblasti IT. Předávání osobních údajů evropskému poskytovateli cloudových služeb, na nějž se vztahují výhradně evropské právní předpisy na ochranu údajů, by mohlo pro zákazníky znamenat značné výhody. Za tímto účelem by se zejména prosazovalo přijetí společných norem (především v oblasti interoperability a přenositelnosti údajů) a podporovala právní jistota.

and-resilience-in-governmental-clouds/at_download/fullReport): „Pokud jde o architekturu, v případě citlivých aplikací se soukromé a komunitní cloudy jeví jako řešení, jež v současné době nejlépe vyhovuje potřebám veřejné správy, jelikož nabízejí nejvyšší úroveň správy, kontroly a přehlednosti, třebaže je při plánování soukromého nebo komunitního cloudu nutné věnovat zvláštní pozornost velikosti infrastruktury.“

[49] Neelie Kroesová, místopředsedkyně Evropské komise odpovědná za digitální agendu: Zřízení evropského partnerství pro cloud computing, Světové ekonomické fórum Davos, Švýcarsko, 26. ledna 2012: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1 23.

PŘÍLOHA

a) Modely nasazení

Soukromý cloud[50] označuje infrastrukturu IT, jež je vyhrazena pro jednu organizaci. Je umístěna v prostorách organizace nebo je její správa externě zadána třetí straně (obvykle prostřednictvím hostingu serveru), jež je striktně podřízena správci. Soukromý cloud lze srovnat s klasickými datovými centry. Rozdílem jsou technické úpravy, jež mají jednak optimalizovat využívání dostupných zdrojů, jednak časem tyto zdroje postupně rozšiřovat prostřednictvím drobných investic.

Veřejný cloud je naopak infrastruktura vlastněná poskytovatelem, který se specializuje na služby, jež zpřístupňují jeho systémy uživatelům, podnikům či správním orgánům, s nimiž je pak tedy poskytovatel sdílí. Přístup ke službám může být zajištěn prostřednictvím internetu, což s sebou nese zpracovávání předávaných údajů anebo předávání údajů do systémů poskytovatele služeb, který tak přebírá klíčovou úlohu, pokud jde o účinnou ochranu údajů zadaných do jeho systémů. Spolu s údaji musí uživatel převést i značnou část kontroly nad těmito údaji.

Vedle veřejného a soukromého cloudu existují i tzv. zprostředkované nebo hybridní cloudy, ve kterých jsou služby poskytované soukromou infrastrukturou kombinovány se službami zakoupenými na veřejném cloudu. Je třeba se rovněž zmínit o „komunitních cloudech“, ve kterých infrastrukturu sdílí vícero organizací ve prospěch určité uživatelské komunity.

Cloudové systémy se díky pružnosti a jednoduchosti své konfigurace vyznačují jistou elastičností, tj. mohou být upraveny podle konkrétních požadavků zákazníka na základě jeho uživatelských potřeb. Uživatelé nemusí spravovat žádné systémy IT. O ty se na smluvním základě plně stará externí třetí strana, v jejímž cloudu jsou data uložena. Jedná se často o velké poskytovatele s rozsáhlou infrastrukturou, jejichž cloud může zahrnovat vícero umístění, a uživatelé proto nemusí vědět, kde přesně jsou jejich data uložena.

b) Modely poskytování služby

V závislosti na požadavcích uživatele je na trhu k dispozici několik cloudových řešení, která lze rozdělit do tří hlavních skupin, kategorií či modelů. Tyto modely lze obvykle uplatnit jak na soukromé, tak i veřejné cloudy:

---

[50] Národní ústav pro normalizaci a technologie (National Institute of Standards and Technology, USA), který již několik let pracuje na normách pro cloudové technologie a jehož definice jsou uvedeny i v dokumentu ENISA, vymezuje uvedené pojmy takto:
Soukromý cloud
Infrastruktura cloudu je provozována pouze pro jednu organizaci. Spravuje ji sama organizace nebo třetí strana. Může se nacházet v prostorách organizace nebo mimo ně. Je třeba poznamenat, že soukromý cloud se alespoň zčásti opírá o technologie, jež jsou typické i pro veřejný cloud. Patří sem zejména technologie virtualizace, jež podporují reorganizaci (nebo přezkum) architektury zpracovávání údajů, jak bylo popsáno výše.
Veřejný cloud
Infrastruktura cloudu je zpřístupněna široké veřejnosti nebo velké průmyslové skupině. Vlastní ji organizace, jež se zabývá prodejem cloudových služeb.

- **IaaS (*Cloud Infrastructure as a Service*, cloudová infrastruktura jako služba):** poskytovatel pronajímá technologickou infrastrukturu, tj. virtuální vzdálené servery, kterých v souladu s příslušnými mechanismy a ujednáními využívá koncový uživatel. Cílem je zjednodušit, zefektivnit i nahradit firemní systémy IT v prostorách společnosti anebo využívat pronajatou infrastrukturu souběžně s firemními systémy. Poskytovatelé tohoto modelu jsou většinou specializované subjekty na trhu, které se opírají o fyzickou a rozsáhlou infrastrukturu, jež se často nachází v různých zeměpisných oblastech.
- **SaaS (*Cloud Software as a Service*, software v cloudu jako služba):** poskytovatel dodává prostřednictvím internetu služby v podobě různých aplikací a zpřístupňuje je koncovým uživatelům. Tyto služby mají nahrazovat klasické aplikace, které si uživatelé instalují do svých lokálních systémů. Uživatelé tak podle tohoto modelu mají v konečném důsledku externalizovat svá data určitému poskytovateli. Typickým příkladem jsou na internetu založené kancelářské aplikace, jako jsou tabulkové editory, nástroje na zpracování textu, elektronické rejstříky a kalendáře, sdílené kalendáře atd. Dané služby však mohou také zahrnovat cloudové e-mailové aplikace.
- **PaaS (*Cloud Platform as a Service*, cloudová platforma jako služba):** poskytovatel nabízí řešení pro pokročilý vývoj a hosting aplikací. Tyto služby jsou obvykle určeny subjektům na trhu, které je využívají k vývoji a hostingu proprietárních, na aplikacích založených řešení s cílem reagovat na příslušné požadavky v rámci firmy anebo poskytovat služby třetím stranám. Opět platí, že díky službám dodávaným poskytovatelem PaaS již uživatel nemusí být odkázán na určitý anebo dodatečný interní hardware či software.

Zdá se, že kompletní přechod na veskrze veřejný cloudový systém není v krátkodobém horizontu realizovatelný, a to zejména pokud jde o rozsáhlé subjekty, jako jsou významné společnosti nebo organizace, jež musí plnit specifické závazky, např. hlavní banky, státní úřady, velké obce apod. Je tomu tak zejména z těchto dvou důvodů: zaprvé je zde hybný faktor investic nezbytných pro tento přechod a zadruhé je třeba vzít v potaz obzvláště cenné anebo citlivé údaje, jež mají být v konkrétních případech zpracovávány.

Další faktor, jenž hovoří ve prospěch soukromých cloudů (přinejmenším ve výše uvedených případech), souvisí s tím, že poskytovatel veřejného cloudu často nemůže zajistit takovou kvalitu služby (podle dohod o úrovni služeb, *Service Level Agreements*), jež by například odpovídala kritičnosti služby poskytované zpracovatelem – důvodem může být nedostatečná či nepřiměřená šířka pásma nebo spolehlivost sítě v dané oblasti nebo konkrétní spojení mezi poskytovatelem a uživatelem. Naopak lze v některých výše uvedených případech logicky předpokládat pronájem soukromého cloudu (jelikož se může ukázat jako nákladově efektivnější) nebo využití modelu hybridního cloudu (jenž se skládá jak z veřejných, tak soukromých prvků). Ve všech případech by se měly pečlivě zohlednit příslušné důsledky.

Při neexistenci mezinárodně uznávaných norem existuje riziko různých, podle individuálních potřeb upravovaných nebo federovaných cloudových řešení, což by přineslo větší komplikace při přechodu k jinému poskytovateli (souvisí s tím i jev nazvaný *privacy monocultures,* monokultury soukromí)[51], dále by tím byly vytvořeny překážky pro plnou kontrolu nad údaji a nebyla by zajištěna interoperabilita. Jak interoperabilita, tak přenositelnost údajů jsou přitom klíčovými faktory nejen pro rozvoj cloudové technologie, ale i pro plný výkon práv na ochranu údajů, jimž se těší subjekty údajů (např. právo na přístup k údajům či na jejich opravu).

---

[51] Viz studie Evropského parlamentu *„Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy"* zveřejněná v prosinci 2011.

V tomto ohledu současná debata o cloudových technologiích názorně odhaluje napětí, jež existuje mezi ekonomickým a právním přístupem (jak bylo stručně popsáno v oddíle 2 výše). I když lze z hlediska ochrany údajů – s přihlédnutím ke specifickým podmínkám jejich zpracování – využít i doporučit soukromé cloudy, nemusí se pro příslušné organizace jednat o dlouhodobě udržitelné řešení zejména z ekonomického hlediska. Je třeba pečlivě posoudit zájmy jednotlivých subjektů, jelikož v současnosti nelze v této oblasti poukázat na nějaké univerzálně použitelné řešení.