OFFICE 365 V. GOOGLE APPS: SROVNÁNÍ Z HLEDISKA OCHRANY OSOBNÍCH ÚDAJŮ[*]

JAN TOMÍŠEK[**]

ABSTRAKT

Tento článek analyzuje poskytování softwaru jako služby z hlediska ochrany osobních údajů. Autor rozebírá možné role zákazníka a poskytovatele softwaru jako služby z pohledu ochrany osobních údajů, shrnuje požadavky na obsah smlouvy mezi zákazníkem jako správcem a poskytovatelem jako zpracovatelem osobních údajů a srovnává smlouvy na Google Apps for Work a Microsoft Office 365 ve světle těchto požadavků. Závěrem jsou čtenáři předloženy úvahy de lege ferenda a kritické zhodnocení připravované novely evropské regulace ochrany osobních údajů v kontextu cloud computingu.

KLÍČOVÁ SLOVA

software-as-a-service, SaaS, cloud, osobní údaje, smlouva, Google Apps, Office 365

ABSTRACT

This article analyses the provision of software as a service in terms of data protection. The author discusses possible roles of a client and a provider of software as a service in terms of protection of personal data, summarizes the requirements on contents of the contract between the client as a controller and the provider as a processor of personal data and compares the contracts for Google Apps for Work and Microsoft Office 365 in the light of these

[*] Tento článek byl ve zkrácené podobě a anglickém znění publikován v Masaryk University Journal of Law and Technology, 2015, roč. 9, č. 1.

[**] Mgr. Bc. Jan Tomíšek je absolvent Právnické fakulty a Fakulty informatiky Masarykovy univerzity a junior associate advokátní kanceláře ROWAN LEGAL. Věnuje se problematice software, ochraně osobních údajů, cloud computingu a kybernetické bezpečnosti. Kontaktní e-mail: jantomisek@gmail.com

requirements. As a conclusion are provided considerations de lege ferenda and critical evaluation of the prepared amendment to the European data protection regulation in the context of cloud computing.

KEYWORDS

software-as-a-service, SaaS, cloud, data protection, contract, Google Apps, Office 365

1. ÚVOD

Cloudové služby nejsou v technologickém světě žádnou novinkou, není je tedy třeba čtenáři dlouze představovat.[1] V případě, že zákazník využívající cloudové služby působí v Evropské unii (dále jen „EU“) a data zpracovávaná pomocí cloudové služby mohu sloužit k identifikaci jakékoli fyzické osoby, může poskytování cloudové služby spadat pod režim směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Směrnice 95/46/ES stanoví řadu požadavků na vztah mezi zákazníkem využívajícím cloudové služby a jejich poskytovatelem.

Od cloudových řešení se očekává podstatné zvýšení efektivity, zejména pro malé a střední podniky (dále jen „SME“), které si obvykle nemohou dovolit, ani plně využít rozsáhlá IT řešení vyhrazená pouze pro jejich potřebu.[2] SME v EU z cloudových služeb nejčastěji využívají e-mail a úložiště dat v cloudu.[3] Tyto služby jsou často integrované v on-line kancelářských balíčcích, jako jsou Microsoft Office 365 nebo Google Apps for Work. Pro SME však může být obtížné posoudit nabídky poskytovatelů těchto cloudových služeb z hlediska ochrany osobních údajů, neboť právní úprava stejně jako smluvní rámce poskytovatelů jsou velmi složité.

---

[1] Pro podrobnější úvod do problematiky cloudových služeb a software jako služby viz TOMÍŠEK, Jan. Licence při poskytování software jako služby. *Revue pro právo a technologie*, Masarykova univerzita, 2014, roč. 2014, č. 10, s. 47-69. ISSN 1804-5383.

[2] Viz Unleashing the Potential of Cloud Computing in Europe. *Evropská komise* [online]. 27 9. 2012 [cit. 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF, s. 4.

[3] Viz Use of cloud computing services. *Eurostat* [online]. Publikováno 16. 1. 2015 [cit. 15. 2. 2015]. Dostupné z: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cicce_use&lang=en

Cílem tohoto článku je proto v prvé řadě sumarizovat požadavky na obsah smlouvy mezi poskytovatelem a zákazníkem cloudových služeb plynoucí ze směrnice 95/46/ES s přihlédnutím k ustanovením některých národních implementací. Následně budou na základě těchto požadavků z hlediska ochrany údajů vyhodnoceny a porovnány smlouvy na poskytování služby Google Apps for Work a Microsoft Office 365 nabízené SME. Na závěr budou diskutovány nedostatky stávajícího právního rámce pro ochranu údajů ve vztahu ke cloud computingu a analyzována potenciální zlepšení, která může přinést připravované obecné nařízení o ochraně údajů.

2. OCHRANA OSOBNÍCH ÚDAJŮ V CLOUDU

Povinnosti zákazníků a poskytovatelů cloudových služeb ve vztahu k ochraně osobních údajů silně závisí na rolích, které jsou jim v konkrétním vztahu přiřazeny směrnicí 95/46/ES. Tyto role jsou dány mnoha faktory, z nichž prvním je charakter dat zpracovávaných v cloudu. V případě, že data nejsou osobními údaji, se směrnice 95/46/ES nemusí vůbec aplikovat. Směrnice 95/46/ES definuje osobní údaje jako „veškeré informace o identifikované nebo identifikovatelné osobě (subjekt údajů)[,]“ kde „identifikovatelnou osobou se rozumí osoba, kterou lze přímo či nepřímo identifikovat, zejména s odkazem na identifikační číslo nebo na jeden či více zvláštních prvků její fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální identity[.]“[4] Široký záběr této definice je dále podporován preambulí směrnice 95/46/ES, která uvádí, že „pro určení, zda je osoba identifikovatelná, je třeba přihlédnout ke všem prostředkům, které mohou být rozumně použity jak správcem, tak jakoukoli jinou osobou pro identifikaci dané osoby[.]“[5]

Rozumná šance, že konkrétní prostředek bude použit a umožní identifikaci, je dána především kontextem každého jednotlivého zpracování.[6] Existují určitá technická opatření, která mohou být v rámci

[4] Viz článek 2 písm. a) směrnice 95/46/ES.

[5] Viz recitál 26 směrnice 95/46/ES.

[6] Lord Hope v odst. 26 rozhodnutí Sněmovny lordů Spojeného království ze dne 9. 7. 2008, Common Services Agency v Scottish Information Commissioner (Scotland), věc [2008] UKHL 47 uvádí: „Kdyby pro příjemce […] dat bylo nemožné identifikovat tyto jednotlivce, informace by v jeho rukách nebyly ‘osobními údaji.‘“

cloudových služeb uplatněna, aby se zabránilo příjemci dat identifikovat dotčené jednotlivce, jako je například anonymizace nebo šifrování dat. Tato opatření mohou zbavit data jejich charakteru osobních údajů ve smyslu směrnice 95/46/ES ve vztahu ke konkrétnímu příjemci,[7] možnost jejich praktického uplatnění je však limitovaná. Například, pokud by adresář v rámci služby cloudového e-mailu byl zašifrovaný tak, že by poskytovatel služby neměl přístup k uloženým adresám, uživatel by nemohl mít k dispozici funkce prohledávání těchto adres, třídění přijatých e-mailů ve své schránce, prevence označení e-mailů z těchto adres za SPAM apod. Pokud by všechny dokumenty, které by měly být uloženy v cloudovém úložišti dokumentů, musely být nejprve prohledány a zbaveny všech odkazů na identifikovatelné jednotlivce, nahrané dokumenty by se v mnoha případech staly zcela nepoužitelnými. Proto musíme předpokládat, že v případě nejčastěji využívaných cloudových služeb, jako je e-mail nebo úložiště dokumentů, uložená a zpracovaná data představují osobní údaje ve smyslu směrnice 95/46/ES.

Je rovněž otázkou, zda jsou osobní údaje v cloudu skutečně zpracovány ve smyslu směrnice 95/46/ES. Vzhledem k tomu, že definice zpracování ve směrnici 95/46/ES[8] je velmi široká obdobně jako definice osobního údaje a že všechny běžné cloudové služby zahrnují ukládání dat, což je operace, která je považována za zpracování, odpověď bude v naprosté většině případů kladná.

Pokud mohou být data nebo jejich části považovány za osobní údaje ve smyslu směrnice 95/46/ES a jsou v cloudu zpracovávána ve smyslu směrnice 95/46/ES, pak alespoň jedna z osob podílejících se na této činnosti musí být správcem těchto osobních údajů. Správcem osobních údajů je podle směrnice 95/46/ES subjekt, který „určuje účel a prostředky zpracování[.]“[9] V případě těch cloudových služeb, které jsou nabízeny

---

[7] Viz HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. The problem of ‘personal data’ in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law* [online]. 2011, vol. 1, no. 4, p. 211-228 [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/1/4/211.full.pdf+html, s. 214.

[8] Zpracováním se dle článku 2 písm. b) směrnice 95/46/ES rozumí „jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace[.]“

[9] Viz článek 2 písm. d) směrnice 95/46/ES.

široké veřejnosti (tj. nejsou vytvořeny na míru individuálním požadavkům zákazníka), je to vždy poskytovatel, kdo určuje vlastnosti služby, jako je formát a rozsah dat, způsob, jakým jsou uložena a prostředky jejich ochrany, přičemž prostor pro jednání o jednotlivých parametrech, může být velmi omezený.[10] Může se proto zdát, že tato rozhodnutí posouvají poskytovatele do role správce osobních údajů.[11] Ve skutečnosti je to však rozhodnutí zákazníka přijmout nabídku konkrétního poskytovatele, které určuje způsob zpracování.[12] Bez tohoto rozhodnutí poskytovatel nebude data vůbec zpracovávat. V případě, že rozhodnutí využít určitou cloudovou službu je na zákazníkovi, pak by on měl být považován za správce osobních údajů, které jsou pomocí této služby zpracovávány.

To však nevylučuje možnost, aby byl poskytovatel správcem také. V případě, že se poskytovatel rozhodne použít data pro jiné účely než ty zvolené zákazníkem, může se také stát správcem údajů,[13] stejně jako když poskytovatel otevřeně využívá data pro marketingové a reklamní účely (jako je poskytování cílené reklamy pro uživatele služeb).

Ve většině situací však bude poskytovatel zpracovatelem osobních údajů - subjektem, který zpracovává osobní údaje pro správce.[14] Toto rozdělení rolí předpokládá i Article 29 Data Protection Working Party (Pracovní skupina pro ochranu dat podle článku 29 směrnice 95/46/ES, dále jen jako „WP29“) stejně jako mnoho národních úřadů pro ochranu údajů ve svých

---

[10] Individuální úpravy služby by většinou výrazně zvýšily náklady pro poskytovatele, a tím narušily jeho obchodní model. Podle zkušeností autora je prostor pro jednání s významnými poskytovateli cloudových služeb velmi omezený i v případě velkých zákazníků, proto jsou jakékoli změny služby nebo jejích podmínek pro SME nedosažitelné.

[11] Tuto možnost diskutují Hon a kol. Viz HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2 *International Data Privacy Law* [online]. 2012, vol. 2, no. 1, pp. 3-18 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/1/3.full.pdf+html, s. 6.

[12] Viz Opinion 05/2012 on Cloud Computing. *Evropská komise* [online]. Article 29 Data Protection Working Party, 2012 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf (dále jen „WP196“), s. 8.

[13] Tento scénář nastal např. v případě Společnosti pro celosvětové mezibankovní finanční telekomunikace (SWIFT), která provedla některé operace jako předání dat dalším příjemcům (konkrétně Ministerstvu financí USA) bez vědomí orgánů, které ji pověřily jako zpracovatele. Následně WP29 vydala stanovisko, že SWIFT by měla být považován za správce zpracovávaných osobních údajů. Viz Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). *Evropská komise* [online]. Article 29 Data Protection Working Party, 2006 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf, p. 26.

[14] Viz článek 2 psím. e) směrnice 95/46/ES.

stanoviscích a doporučeních ve vztahu ke zpracování osobních údajů v cloudu.[15] Přesto se mohou vyskytovat případy, kdy situace nebude tak jasná.

Když poskytovatel cloudu poskytuje zákazníkovi pouze úložnou kapacitou pro nestrukturovaná data (tedy ne například chytré úložiště dokumentů s možností vyhledávání atd.) nebo výpočetní výkon, nemusí mu být (a obvykle není) známa povaha dat, která se zákazník rozhodne zpracovávat prostřednictvím poskytovaných zdrojů. Přesto definice zpracování ve směrnice 95/46/ES nerozlišuje, zda si je zpracovatel vědom osobní povahy údajů, nebo ne. V takovém případě by se pozice poskytovatele měnila v závislosti na typu dat, která se zákazník rozhodne zpracovávat, a to aniž by o tom poskytovatel věděl. Takové rozdělení rolí může mít za následek nevyvážené rozložení povinností a zatěžování jak zákazníka, tak poskytovatele v míře, která není přiměřená v poměru k možnému riziku, které přináší zapojení poskytovatele do činnosti zákazníka.[16]

V tomto směru nám může poskytnout vodítko směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu. Tato směrnice vytváří systém bezpečných přístavů omezujících určité aspekty odpovědnosti některých poskytovatelů služeb informační společnosti. Mezi poskytovateli, jejichž odpovědnost je omezena, jsou také poskytovatelé hostingových služeb,[17] kteří neodpovídají za informace uložené uživatelem služby, pokud „nebyl[i] účinně seznámen[i] s protiprávní činností nebo informací[.]“[18]

---

[15] Viz *Stanovisko č. 65/2013/4* [online]. Úřad pro ochranu osobních údajů, publikováno 1. července 2013 [cit. 11. 2. 2015]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002, s. 3.

Guidance on the use of cloud computing [online]. Srov. též Information Commissioner's Office, 2012, [cit. 11. 2. 2015]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf, p. 8. *Guía para clientes que contraten servicios de Cloud Computing* [online]. Srov. také Agencia Española de Protección de Datos, 2013 [cit. 11. 2. 2015]. Dostupné z: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf, p. 13.

[16] Viz HON, MILLARD, WALDEN, 2012, op. cit., s 11.

[17] Za hosting se dle článku 14 odst. 1 směrnice o elektronickém obchodu považují „služby informační společnosti spočívající v ukládání informací poskytovaných příjemcem služby[.]“

[18] Viz článek 14 odst. 1 písm. a) směrnice o elektronickém obchodu.

Směrnici o elektronickém obchodu můžeme vnímat jako zdroj obecných pravidel týkajících se odpovědnosti poskytovatelů služeb informační společnosti a směrnici 95/46/ES jako zdroj zvláštních pravidel týkajících se odpovědnosti v případech, kdy poskytovatelé služeb informační společnosti zpracovávají osobní údaje. Pak by nebylo možné povinnosti takových poskytovatelů na základě směrnice o elektronickém obchodu ve vztahu k ochraně osobních údajů omezit. Nicméně směrnici 95/46/ES můžeme též vnímat jako obecné pravidlo pro všechny zpracovatele osobních údajů a směrnici o elektronickém obchodu jako zvláštní předpis upravující otázky odpovědnosti, který je aplikovatelný také na nakládání s osobními údaji ze strany poskytovatelů hostingu podle směrnice o elektronickém obchodu. Takovým výkladem v podstatě říkáme, že osobní působnost směrnice o elektronickém obchodu je užší než směrnice 95/46/ES). Na základě této interpretace pak mohou být poskytovatelé hostingu vyňati z postavení zpracovatele osobních údajů.[19]

Může být diskutabilní, zda všechny povinnosti zpracovatele osobních údajů a všechny odpovídající povinnosti správce osobních údajů ve vztahu ke zpracovateli mohou spadat pod pojem „odpovědnost". Navíc, zatímco vynětí poskytovatelů hostingu z pozice zpracovatele osobních údajů může být vyváženým řešením ve vztahu ke cloud computingu, nemusí fungovat v jiných případech a je třeba vzít v úvahu potenciální vedlejší dopady takového závěru.

Nicméně i když uzavřeme, že na poskytovatele hostingu se vztahuje výjimka z povinností zpracovatele osobních údajů dle směrnice 95/46/ES, tato výjimka se bude vztahovat pouze na poskytovatele obsahově neutrálních zdrojů, jakými jsou úložný prostor a výpočetní výkon.[20] V případě Google Apps for Work a Microsoft Office 365 je situace zcela jiná. Obě služby poskytují svým uživatelům e-mailovou schránku, adresář, úložiště dokumentů apod. Je tedy zřejmé, že údaje zpracovávané za použití těchto služeb budou způsobilé k identifikaci jednotlivých uživatelů a dokonce i dalších osob, je tedy třeba považovat je za osobní údaje ve

[19] Tato stanovisko zastává též Sartor. Viz SARTOR, Giovanni. Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? *International Data Privacy Law* [online]. 2013, vol. 3, no. 1, pp. 3-12 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/3/1/3.full.pdf+html

[20] Většina takových služeb spadá do kategorie Infrastructure-as-a-service (IaaS).

smyslu směrnice 95/46/ES. Navíc lze veškerý obsah těchto služeb prohledávat pomocí fulltextových indexů sestavených poskytovateli. Pro vytvoření těchto indexů je nezbytné aktivní zpracování ukládaných dat. Proto budeme dále vycházet ze skutečnosti, že využívání těchto služeb představuje zpracování osobních údajů ve smyslu směrnice 95/46/ES, kdy zákazník je správcem osobních údajů a poskytovatel služeb je jejich zpracovatelem.

3. POŽADAVKY NA SMLOUVU O ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Z výše popsaného rozdělení rolí vyplývá řada požadavků na právní vztah mezi poskytovatelem a zákazníkem. Prvním a nejdůležitějším požadavkem je existence právního aktu upravujícího vztahy mezi zákazníkem jako správcem a poskytovatelem jako zpracovatelem osobních údajů.[21] Zatímco samotná směrnice 95/46/ES neurčuje formu tohoto právního aktu, vnitrostátní právní úpravy jednotlivých členských států často vyžadují, aby měl formu smlouvy.[22] Poskytovatel cloudových služeb, který cílí na zákazníky z celého trhu EU, by měl proto předpokládat, že je z hlediska ochrany osobních údajů nutné se zákazníkem uzavřít smlouvu (obvykle nazývanou smlouva o zpracování osobních údajů, data processing agreement, DPA), která musí být v písemné nebo v jiné ekvivalentní formě.[23]

Směrnice 95/46/ES vyžaduje, aby smlouva stanovila, že „zpracovatel jedná pouze podle pokynů správce[.]“[24] Tento požadavek odráží zásadu omezenosti účelem zpracování, která je zakotvena v článku 6 odst. 1 písm. b) směrnice 95/46/ES, neboť je to zákazník cloudové služby jako správce osobních údajů, kdo určuje účel zpracování. V případě, že by poskytovatel překročil pokyny zákazníka, stal by se sám správcem údajů, jak je popsáno výše.

---

[21] Viz článek 17 odst. 3 směrnice 95/46/ES.

[22] Viz oddíl 1, část II, odst. 12 Data Protection Act 1998 (britský zákon o ochraně osobních údajů). Viz též § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých předpisů, ve znění pozdějších předpisů. Srov. též článek 12 odst. 2 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (španělský zákon o ochraně osobních údajů).

[23] Viz článek 17 odst. 4 směrnice 95/46/ES.

[24] Viz článek 17 odst. 3 směrnice 95/46/ES.

Vzhledem k tomu, že dodržování zásady omezenosti účelem je klíčovou povinností poskytovatele, účel zpracování by měl být uveden ve smlouvě.[25] Jeho vymezení nemusí být totožné s vymezením účelu, pro který byly údaje shromážděny, ale tyto dva účely musí být ve vzájemném souladu (článek 6 odst. 1 písm. b) směrnice 95/46/ES zakazuje zpracování pro účely, které jsou neslučitelné s účelem původním). Aby bylo zajištěno, že jsou pomocí dané cloudové služby zpracovávána pouze data pro daný účel legálně získaná, měla by smlouva uvádět výčet typů osobních údajů, které budou zpracovávány (tj. jméno, emailová adresa, polohové údaje, atd.), stejně jako celkový rozsah a způsob zpracování.[26]

Stanovisko WP29 ke cloud computingu dále doporučuje, aby ve smlouvě byly obsaženy „podrobnosti o rozsahu a způsobu dávání instrukcí zákazníka, které může dávat poskytovateli zejména s ohledem na aplikované SLA (které by mělo být objektivní a měřitelné) a příslušné sankce (finanční nebo jiné včetně možnosti žalovat poskytovatele v případě neplnění).“[27] Ačkoli požadavek na obsažení těchto podrobností ve smlouvě nemá přímou oporu ve směrnici 95/46/ES, jejich absence může způsobit nevymahatelnost smlouvy o zpracování osobních údajů a tím porušení článku 6 odst. 3 směrnice 95/46/ES. Z tohoto důvodu lze jejich zapracování důrazně doporučit nejen z obchodního hlediska, ale také z hlediska ochrany osobních údajů.

Druhou klíčovou povinností poskytovatele cloudových služeb jako zpracovatele osobních údajů, která musí být zahrnuta ve smlouvě, je povinnost dodržovat dohodnutá technická a organizačních opatření zavedená na ochranu osobních údajů proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému sdělování nebo přístupu a všem dalším formám nedovoleného zpracování.[28]

Směrnice 95/46/ES nespecifikuje konkrétní bezpečnostní opatření, která k ochraně osobních údajů musí být zavedena. Jediným požadavkem

[25] Nedostatečné vymezení účelu zpracování bylo švédským úřadem pro ochranu osobních údajů Datainspektionen v případě Salem shledáno jako porušení práva na ochranu osobních údajů. Viz SVANTESSON, Dan Jerker B. Data protection in cloud computing – The Swedish perspective. *Computer Law & Security Review* [online]. 2012, vol. 28, issue 4, s. 476-480 [cit. 15. 2. 2015]. Dostupné ze ScienceDirect: http://linkinghub.elsevier.com/retrieve/pii/S0267364912001021, s. 479.

[26] Viz WP196, s. 13.

[27] Viz WP196, s. 12. Viz také SVANTESSON, 2012, op. cit., s. 479.

[28] Viz článek 6 odst. 1 a 3 směrnice 95/46/ES.

směrnice je, aby zajišťovala „s ohledem na stav techniky a na náklady na jejich provedení, přiměřenou úroveň bezpečnosti odpovídající rizikům vyplývajícím ze zpracování údajů a z povahy údajů, které mají být chráněny.“[29] Některé národní úpravy se drží úrovně podrobnosti směrnice 95/46/ES (například zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých předpisů, ve znění pozdějších předpisů), ale jiné stanoví specifické požadavky nebo opatření zaměřená na různé rizikové profily (například ve Španělsku nebo v Polsku[30]). Poskytovatel cloudových služeb by proto měl zvážit výsledky své analýzy rizik jako základ pro rozhodnutí, zda dále studovat vnitrostátní právní předpisy členských států. Toto bližší nastudování může být u rizikovějších služeb nezbytné, aby bylo zajištěno, že služba bude v souladu s právní úpravou, a tudíž zákaznicky atraktivní na trzích všech jednotlivých členských států EU.

Bezpečnostním opatřením by měl zákazník věnovat pozornost již v okamžiku, kdy vybírá poskytovatele cloudových služeb. Zajištění dodržování těchto opatření zpracovatelem je povinností zákazníka, která musí být plněna průběžně po celou dobu zpracování.[31] Smlouva o zpracování osobních údajů by proto měla dávat zákazníkovi patřičné nástroje, jež mu umožní dohlížet nad dodržováním těchto opatření ze strany poskytovatele, stejně jako prostředky nápravy pro situaci, kdy povinnost dodržovat opatření byla porušena.[32]

Není nezbytné, aby zákazník měl právo provádět audit poskytování služeb osobně přímo u poskytovatele – takový požadavek by byl nepřijatelný pro většinu velkých poskytovatelů.[33] Nicméně poskytovatel

[29] Viz článek 17 odst. 1 směrnice 95/46/ES.

[30] Prováděcí předpis k španělskému zákonu o ochraně osobních údajů stanovuje opatření pro nízkou, střední a vysokou úroveň ochrany a zároveň stanoví, kde se tyto úrovně aplikují. Viz článek 80 Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Obdobný přístup je aplikován v prováděcím předpise k polskému zákonu o ochraně osobních údajů. Viz článek 6 odst. 2 Rozporządzenie Ministra spraw wewnętrznych i administracji Dz. U. z 2004 r. Nr 100, poz. 1024, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[31] Viz článek 17 odst. 2 směrnice 95/46/ES.

[32] Viz WP196, s. 13.

[33] Jejich pozice je v tomto směru pochopitelná. Pokud by každý z velkého počtu jejich zákazníků měl právo provést audit u poskytovatele osobně, strávil by poskytovatel více času řešením auditů než poskytování služeb, což by se neudržitelným způsobem promítlo do jeho nákladů a tedy i ceny služeb, navíc by zvýšený pohyb osob v prostorách poskytovatele mohl ve výsledku spíše ohrozit bezpečnost jeho služeb.

cloudových služeb by měl být povinen poskytnout zákazníkovi dostatečný důkaz plnění bezpečnostních opatření z jeho strany, jakým je bezpečnostní certifikace nebo auditní zpráva, například certifikace dle ISO 27001 nebo nedávno schváleného standardu týkajícího se zpracování osobně identifikovatelných informací v cloudu ISO 27018. Tato povinnost by měla být dále doprovázena právem zákazníka požadovat doplňující informace, pokud shledá předložené důkazy o plnění bezpečnostních opatření jako nedostatečné.

Pokud jde o prostředky nápravy, zákazník zůstává primárně odpovědný za veškeré bezpečnostní incidenty vzniklé v průběhu zpracování,[34] měl by proto mít možnost smluvně převést příslušnou část odpovědnosti na poskytovatele cloudových služeb. Odpovědnost poskytovatele by tedy neměla být limitovaná v takovém rozsahu, aby byla téměř veškerá odpovědnost ponechána na zákazníkovi.[35] Kromě toho by měl zákazník mít možnost vypovědět smlouvu o zpracování osobních údajů, pokud zjistí podstatné porušení dohodnutých opatření, které nebude poskytovatelem v přiměřeném čase napraveno.

Jelikož některé národní právní řády vyžadují, aby vztah mezi poskytovatelem a zákazníkem byl upraven smlouvou, všechny jeho podmínky by měly být výsledkem konsensu obou smluvních stran a neměly by být měněny jednostranně (jinak by takové právní jednání nebylo možné považovat za smlouvu). Přinejmenším ne ty, které se týkají základních podmínek upravujících pokyny zákazníka a bezpečnostní opatření.[36]

Všechny tyto podmínky stanovené ve smlouvě o zpracování osobních údajů musí být zároveň zachovány i v případě, kdy cloudová služba není zajišťována pouze poskytovatelem samotným, ale jeho subdodavateli.

---

[34] To zdůrazňuje Svantesson. Viz SVANTESSON, 2012, op. cit., s. 479.

[35] Na tento problém upozorňuje též MCGILLIVRAY, Kevin. Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology & Intellectual Property*. 2014, roč. 17, č. Fall 2014, pp. 217–253. s. 248.

[36] Švédský úřad pro ochranu osobních údajů dospěl k závěru, že smlouva umožňující jednostranné změny ze strany poskytovatele je v rozporu se švédským zákonem o ochraně osobních údajů. SVANTESSON, 2012, op. cit., s. 477. Podobně Dánský úřad pro ochranu údajů Datatilsynet zakázal magistrátu města Odense používat Google Apps, protože (mezi jinými důvody) smlouva na jejich poskytování mohla být ze strany Google jednostranně měněna. Viz DEBUSSCHE, Julien; VAN ASBROECK, Benoit; CHLOUPEK, Vojtěch a kol. Cloud computing and privacy series: the data protection legal framework (part 2 of 6). *Bird&Bird* [online]. 24 11. 2014 [cit. 15. 2. 2015]. Dostupné z http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-and-privacy-series-the-data-protection-legal-framework

Vzhledem k tomu, že zákazník jako správce osobních údajů musí zajistit, aby byla dodržována vhodná technická a organizační opatření, musí být plnění této povinnosti zajištěno i pokud jde o subdodavatele poskytovatele. Podmínky subdodavatelské smlouvy by proto ve vztahu k ochraně osobních údajů měly kopírovat podmínky smlouvy uzavřené mezi zákazníkem a poskytovatelem. Zákazník by měl být informován o všech subdodavatelích podílejících se na zpracovávání osobních údajů a jeho souhlas by měl být vyžadován k zapojení jakéhokoli nového subdodavatele, který by se na této činnost měl podílet. Předchozí souhlas zákazníka však nemusí být v mnoha případech udržitelným řešením.[37] Smlouva by proto měla poskytovatele zavazovat alespoň k tomu, aby zákazníka o zapojení nového poskytovatele upozornil s dostatečným předstihem, a dávat zákazníkovi právo smlouvu ukončit v případě, že s volbou nového subdodavatele nebude souhlasit.[38]

Pokud je účel zpracování naplněn nebo odpadne titul pro zpracování, typicky tehdy, když subjekt údajů odvolá svůj souhlas se zpracováním nebo je ukončena smlouva o zpracování mezi zákazníkem a poskytovatelem, pak osobní údaje nesmí být dále zpracovávány.[39] Tato možnost by měla být ve smlouvě ošetřena zejména stanovením postupu a časového rámce pro vymazání dat po ukončení smlouvy.[40]

Zákazník musí plnit své povinnosti jako správce osobních údajů, které má vůči subjektům údajů, i v případě, že jsou osobní údaje zpracovávány v cloudu.[41] V některých případech toho však nemusí být schopen bez asistence poskytovatele. Proto by smlouva měla stanovovat povinnost poskytovatele cloudových služeb poskytnout zákazníkovi součinnost v plnění požadavků subjektů osobních údajů zpracovávaných pomocí

---

[37] Např. tam kde má poskytovatel velký počet zákazníků.

[38] „Transparentnost v cloudu znamená, že je nutné, aby zákazník cloudové služby byl informován o všech subdodavatelů podílejících se na poskytování příslušné cloudové služby[.]“ WP196, s. 11. Podobné požadavky byly vzneseny švédským úřadem pro ochranu osobních údajů v případě Salem. Viz SVANTESSON, 2012, op. cit., s. 477. Tento požadavek byl také potvrzen španělským Nejvyšším soudem. DEBUSSCHE, VAN ASBROECK, CHLOUPEK, 2014, op. cit.

[39] Viz článek 6 odst. 1 písm. a) směrnice 95/46/ES.

[40] Viz WP196, s. 13. Tento požadavek je opodstatněný, avšak z technického hlediska velmi problematický např. ve vztahu k dlouhodobým zálohám dat. Jednotlivé zálohy mohou být uloženy v jednom souboru na médiu se sekvenčním přístupem, jako je magnetická páska. V takovém případě je výmaz dat jednotlivého zákazníka prakticky nerealizovatelný.

[41] Práva subjektů údajů jsou stanovena v článcích 12, 14 a 15 směrnice 95/46/ES.

příslušné cloudové služby.[42] Kromě toho by zákazník měl být informován o všech bezpečnostních incidentech týkajících se osobních údajů, jinak by nebyl schopen plnit svoji informační povinnost vůči subjektům zpracovávaných údajů.[43]

Poslední klíčový požadavek na smlouvu o zpracování osobních údajů se vztahuje k umístění zpracovávaných dat. Poskytovatel cloudových služeb nemusí být schopen informovat zákazníka o umístění konkrétní části dat, ale může mu poskytnout seznamem lokalit, kde data mohou být zpracovávána. Zejména jde o datová centra používaná pro poskytování služby zákazníkovi, ale též pracoviště technické podpory a další místa, odkud pracovníci nebo subdodavatelé poskytovatele mohou k datům přistupovat. Tento seznam nemusí nutně specifikovat jednotlivá místa, ale měl by uvádět aspoň země nebo regiony, ve kterých mohou být osobní údaje uloženy nebo odkud k nim může být přistupováno. Bez této informace si nemůže zákazník být jist, že smlouva splňuje veškeré požadavky na předávání osobních údajů do jiných států.

Osobní údaje mohou být předány mimo EU pouze do zemí s odpovídající úrovní ochrany, které jsou určeny rozhodnutími Evropské komise.[44] Do USA mohou být osobní údaje volně předávány, pokud je poskytovatel cloudových služeb jako příjemce těchto údajů certifikován v programu Safe Harbor organizovaném Ministerstvem obchodu USA a zůstává takto certifikovaný po celou dobu zpracování. Do tzv. třetích zemí, které nezajišťují odpovídající úroveň ochrany, mohou být osobní údaje volně předávány ke zpracování za podmínky, že se zákazník a poskytovatel cloudových služeb zaváží dodržovat závazná podniková pravidla (binding corporate rules, BCR) proces schvalování takových pravidel je však složitý a nákladný, zvláště pro SME.[45]

Druhou možnou cestou k předávání osobních údajů do zahraniční bez potřeby zvláštního souhlasu dozorového orgánu je začlenění standardních

[42] Viz WP196, s. 13. Viz také SVANTESSON, 2012, op. cit., s. 478.

[43] Viz WP196, s. 13.

[44] Viz článek 25 směrnice 95/46/ES. Za takové země jsou považovány např. Švýcarsko, Kanada nebo Izrel. Blíže viz. Evropská komise. *Commission decisions on the adequacy of the protection of personal data in third countries* [online]. 18. 12. 2014 [cit. 14. 3. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[45] MCGILLIVRAY, 2014, op. cit., s. 246.

smluvních doložek podle rozhodnutí Komise 2010/87/EU do smlouvy o zpracování údajů.[46] Cílem těchto doložek je smluvní cestou překonat nedostatek náležité ochrany osobních údajů v cílové zemi.

Tyto standardní smluvní doložky nemusí být jedinými podmínkami smlouvy o zpracování osobních údajů. Rozhodnutí Komise 2010/87/EU výslovně uvádí, že „[v]ývozce údajů a dovozce údajů […] mohou do smluv libovolně začlenit jakékoli další doložky, které se vztahují k předmětu obchodu a které jsou podle jejich názoru vhodné pro účely dané smlouvy, nejsou-li v rozporu se standardními smluvními doložkami.“[47]

Existuje samozřejmě mnoho dalších otázek, které by měly být ošetřeny ve smlouvách na poskytování cloudových služeb a které přispívají k nejvyšším standardům v oblasti ochrany osobních údajů, jako je například notifikace o přístupu orgánů činných v trestním řízení k zpracovávaným datům nebo otázka interoperability,[48] ale žádná z nich není z hlediska směrnice 95/46/ES vyžadována.

4. ANALÝZA SMLOUVY O POSKYTOVÁNÍ GOOGLE APPS FOR WORK

Poskytování služby Google Apps pro práci jejím uživatelům se řídí smlouvou Google Apps Enterprise (Online) Agreement[49] (Smlouva GA), která je uzavírána při registraci k službám. Tato smlouva může být dále změněna, pokud zákazník vyjádří souhlas s dodatkem Data Processing Amendment to a Google Apps Agreement[50] (Dodatek DP) nebo Model contract clauses for Google Apps[51] (MCC). Nicméně přijetí těchto dalších smluvních dokumentů je dobrovolné a vyžaduje zvláštní kroky, které musí

[46] Viz články 27 a 26 odst. 4 směrnice 95/46/ES.

[47] Viz recitál 4 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.

[48] Viz WP196, s. 13.

[49] Viz *Google Apps Enterprise (Online) Agreement* [online]. Google, únor 2014 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html

[50] Viz *Data Processing Amendment to Google Apps Agreement* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/dpa_terms.html

[51] Viz *Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/mcc_terms.html.

zákazník provést v administrátorské konzoli.[52] U zákazníků se sídlem v EU je smlouva uzavírána s Google Commerce Limited, společností založenou podle irského práva se sídlem v Dublinu (dále jen „Google“).

Smlouva GA sama o sobě nesplňuje základní požadavky na smlouvu o zpracování osobních údajů. Ačkoli stanoví, že zákazník je správcem osobních údajů a Google jejich zpracovatelem, stejně jako že Google bude vázán pokyny zákazníka,[53] bezpečnostní opatření k ochraně osobních údajů nejsou ošetřena dostatečně.

Odst. 2.2 Smlouvy GA uvádí, že Google může zpracovávat data zákazníka „k následujícím účelům: (a) naplnění Instrukcí; (b) poskytování služeb (jak byly zvoleny zákazníkem prostřednictvím administrátorské konzole); (c) poskytování funkcí produktů s cílem usnadnit Zákazníkovi používání služby, jakož i nástrojů pro Zákazníka k vytváření obsahu; (d) provozu, údržbě a podpoře infrastruktury sloužící k poskytování služeb a (e) reagování na žádosti o zákaznickou podporu“ (překlad JT). Kromě toho Google tamtéž zaručuje, že „bude Data zákazníka zpracovávat pouze v souladu s touto dohodou a nebude zpracovávat Data zákazníka k žádnému jinému účelu“ (překlad JT). Instrukce zákazníka Googlu jsou řešeny v definici pojmu „Instrukce“, kterým se rozumí: „pokyny dané Zákazníkem prostřednictvím administrátorské konzole, pokyny iniciované Zákazníkem a Koncovými uživateli v rámci jejich užívání Služeb, písemné pokyny Zákazníka jak jsou uvedené v této Smlouvě (ve znění pozdějších dodatků a změn) a všechny následné písemné pokyny Zákazníka Googlu a uznané Googlem“ (překlad JT)[54] Nicméně smlouva neuvádí, jaké typy údajů budou na jejím základě zpracovávány. Ostatní podrobnosti ve vztahu k pokynům klienta, jako je například dohoda o úrovni služeb (Service Level Agreement, SLA), jsou ve smlouvě ošetřeny s přijatelnou mírou detailu.

Nedostatečně jsou ve Smlouvě GA upravena bezpečnostní opatření. Smlouva pouze uvádí, že „Google přijme a uplatní vhodná technická a organizační opatření na ochranu Dat zákazníka proti náhodnému nebo nedovolenému zničení, náhodné ztrátě, úpravám, neoprávněnému

[52] Viz Model contract clauses for Google Apps. *Google Apps Help Center* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://support.google.com/a/answer/2888485?hl=en

[53] Viz odst. 2.3 Smlouvy GA.

[54] Viz článek 15 Smlouvy GA.

sdělování nebo přístupu“ (překlad JT),[55] a to bez dalších podrobností. Takovýto obecný popis nesplňuje požadavky směrnice 95/46/ES, protože podle této směrnice opatření musí být přezkoumána a schválena zákazníkem ve vztahu k jeho vlastnímu posouzení rizik.

Google řeší tento nedostatek Smlouvy GA tím, že nabízí svým zákazníkům sídlícím v EU možnost uzavřít Dodatek DP, ale využití této možnosti není zákazníkům automaticky doporučováno.[56] Přitom ti zákazníci, kteří si aktivně nevyhledají tuto možnost a nevyužijí ji, porušují používáním služeb Google Apps své povinnosti plynoucí z legislativy na ochranu osobních údajů.

Dodatek DP překonává některé z nedostatků Smlouvy GA. Dále omezuje účely zpracování tak, že společnost Google může zpracovávat data zákazníka k „(i) poskytování Služeb (což zahrnuje detekci, prevenci a řešení bezpečnostních a technických problémů) a (ii) reagování na žádosti zákazníků o podporu“ (překlad JT).[57] Ve své příloze č. 1 uvádí typy zpracovávaných osobních údajů. Nejdůležitějším zlepšením, které Dodatek DP přináší, je však popis implementovaných bezpečnostních opatření v jeho příloze č. 2. Tento popis je podrobný a umožňuje zákazníkovi, aby zhodnotil, zda jsou tato opatření dostatečná pro jeho rizikový profil.

Pokud jde o důkaz skutečné implementace deklarovaných opatření, Google se zavazuje, že bude pro služby udržovat certifikaci ISO/IEC 27001:2005 nebo srovnatelnou certifikaci, a to po celou dobu trvání Smlouvy GA,[58] a dále auditní zprávu SSAE č. 16 typ II / SAE č. 3402 nebo srovnatelnou zprávu o logických bezpečnostních opatřeních, fyzických bezpečnostních opatřeních a dostupnosti systémů používaných pro poskytování těchto služeb.[59] Tyto smluvní povinnosti by měly být dostatečné k ověření souladu společnosti Google s bezpečnostními opatřeními. Kromě toho Google v současné době uveřejňuje svoji pečeť

[55] Viz odst. 2.5 Smlouvy GA.

[56] Například by mohla být zdůrazněna v rámci průvodce "Začínáme," který se zobrazí při prvním přihlášení k službám.

[57] Viz odst. 5.2 Dodatku DP.

[58] Viz odst. 2.8 Smlouvy GA a odst. 6.4 Dodatku DP.

[59] Viz odst. 2.9 Smlouvy GA a odst. 6.5 Dodatku DP.

věrohodnosti SOC 3 a odpovídající auditní zprávu, které pokrývají další otázky.[60]

Pokud jde o prostředky nápravy pro případ nedodržení bezpečnostních opatření, smlouva umožňuje zákazníkovi, aby ji vypověděl pro porušení, pokud jde o porušení podstatné a nenapravitelné, opakované nebo není napraveno do třiceti dnů po obdržení upozornění na porušení.[61] Kromě toho může zákazník po Googlu požadovat náhradu škody, ale odpovědnost Googlu je v rámci Smlouvy GA značně omezena. Google není odpovědný za ztrátu skutečných nebo předpokládaných zisků, ztráty očekávaných úspor, ztráty obchodních příležitostí, ztrátu reputace nebo poškození dobrého jména, zvláštní, ani nepřímé nebo následné škody a jeho celková odpovědnost nesmí překročit 125% z celkové částky, kterou zákazník zaplatil a měl zaplatit dle Smlouvy GA v daném smluvním roce nebo 50.000 liber.[62] Toto omezení se nevztahuje na odpovědnost za „zneužití důvěrných informací" („misuse of confidential information", překlad JT).[63] Není jasné, jak interpretovat tuto výjimku. Skutečnost, že nebyly použity žádné jednoznačné výrazy jako „porušení povinnosti mlčenlivosti" spíše naznačuje, že by se tato výjimka měla vztahovat pouze na úmyslné, nikoliv nedbalostní jednání. Pokud by tato interpretace měla mít přednost, což je varianta, kterou je nutno na straně zákazníka předpokládat, pak jakákoli odpovědnost společnosti Google za porušení povinností týkajících se ochrany osobních údajů v rámci GA Ageement je značně omezena. Zákazník tedy může nést nepřiměřenou část odpovědnosti za porušení právních povinností, kterému není schopen zabránit.

Stabilita smlouvy může být ovlivněna jednostrannými změnami. Google je oprávněn jednostranně měnit služby[64] a zákazník nemá žádné nástroje nápravy pro případ, že taková změna negativně ovlivní jeho soulad s právními předpisy o ochraně osobních údajů. Tento scénář je přitom možný, neboť způsob fungování služeb určuje způsob zpracování osobních

[60] Viz *SOC 3 Seal of Assurance* [online]. WebTrust, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/soc3_google.html *Service Orgnaization Control (SOC) 3 Report* [online]. Ernst & Young, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/pdfs/soc3_google_2014.pdf

[61] Viz odst. 11.1 Smlouvy GA.

[62] Viz odst. 13.1 a 13.2 Smlouvy GA.

[63] Viz odst. 13.1 Smlouvy GA.

[64] Viz odst. 1.2 Smlouvy GA.

údajů. Kromě toho, Google může jednostranně změnit svou politiku přijatelného použití služeb (Acceptable Use Policy), dohodu o úrovni služeb (Service Level Agreement) a pravidla technické podpory, nicméně u takových změn musí být zákazník informován s 30denním předstihem a může změnu odmítnout. V případě takového odmítnutí se změna na zákazníka nebude vztahovat až do konce aktuálního platebního období.[65] Kromě toho může Google měnit bezpečnostní opatření k ochraně osobních údajů zaručená přílohou č. 2 k Dodatku DP. Ačkoli „žádná taková změna nesmí způsobit podstatnou degradaci bezpečnosti Služeb[,]“[66] nemá zákazník žádnou záruku, že opatření budou po změně odpovídat jeho rizikovému profilu.

Pokud jde o subdodávky, Smlouva GA opravňuje Google používat subdodavatele za podmínky, že smlouvy na subdodávky budou respektovat podmínky Smlouvy GA, pokud jde o přístup a využívání dat zákazníka. Zákazník je oprávněn požadovat informace týkající se subdodavatelů a jejich působiště.[67] Podle Dodatku DP má Google navíc povinnost zajistit soulad subdodávek s MCC a musí provést audit postupů subdodavatele v oblasti bezpečnosti a ochrany osobních údajů.[68] Zákazník však nemá právo být předem informován o zapojení nového subdodavatele, ani právo takové zapojení předem schválit, ani smlouvu z důvodu zapojení nového subdodavatele ukončit.

Je-li poskytování služeb ukončeno, má Google povinnost vymazat data zákazníka v maximální lhůtě 180 dnů.[69] Tato povinnost by měla být dostatečná k naplnění požadavků legislativy na ochranu osobních údajů. Stejně tak přístup k údajům, jejich oprava a výmaz jsou řešeny v Dodatku DP dostatečně na to, aby byl zákazník schopen naplnit požadavky subjektů údajů.[70]

Geografická lokalizace zpracování se může různit, protože Google může předávat data zákazníka „do Spojených států nebo jiné země, ve kterých

[65] Viz odst. 1.3 a 15 Smlouvy GA.
[66] Viz Přílohu č. 2 k Dodatku DP.
[67] Viz odst. 2.15 Smlouvy GA.
[68] Viz článek 11 Dodatku DP a článek 5 přílohy č. 2 k Dodatku DP.
[69] Viz odst. 7.2 Dodatku DP.
[70] Viz odst. 7.1 a 8 Dodatku DP.

mají Google a jeho subdodavatelé svá zařízení“ (překlad JT),[71] což potenciálně mohou být jakékoliv země. Proto je třeba počítat s tím, že data budou předávána i do zemí, které nezaručují odpovídající úroveň ochrany osobních údajů. Pro tento případ Google nabízí zákazníkovi možnost přijmout MCC obsahující standardní smluvní doložky vydané Evropskou komisí, ale nevyužití této možnosti zřejmě nemá vliv na fungování služeb. Zákazníci, kteří se nerozhodnou přijmout MCC, proto nejspíše umožňují nelegální předávání osobních údajů do jiného státu.

Znění MCC, které Google používá, se liší od znění vydaného Evropskou komisí o odstavec doplněný ke klauzuli 6. Tento čtvrtý odstavec stanoví, že celková odpovědnost každé strany v rámci nebo v souvislosti s MCC je omezena na částku zaplacenou společnosti Google za služby v předchozích 12 měsících. Z formulace „aniž jsou dotčeny odstavce 1, 2 a 3 klauzule 6,“ (překlad JT) není jasné, zda odstavec 4 nemá mít žádný dopad na odpovědnost podle odstavců 1, 2 a 3, nebo prostě jen nevylučuje jejich existenci, ale omezuje výši odpovědnosti, která z nich vyplývá. Druhý zmíněný význam se zdá být zamýšlený Googlem, jelikož kopíruje omezení odpovědnosti stanovené ve Smlouvě GA.[72] Je zřejmé, že omezení odpovědnosti je ujednání obchodní povahy, tedy přípustného typu, avšak je možné, že orgány pro ochranu údajů shledají, že takové omezení je v rozporu s předchozími odstavci doložky o odpovědnosti za škodu. Smyslem doložky 6 je zajistit plnou náhradu škody, kterou subjekt údajů utrpěl v průběhu zpracování dat, které se řídí MCC. V případě, že subjekt údajů není schopen čerpat plné odškodnění v důsledku zavedení odstavce 4, je takové ujednání v rozporu se standardními smluvními doložkami, jak byly vydány Evropskou komisí.

Další problém, který může představovat rozpor s MCC, spočívá v auditních právech. Dodatek DP uvádí, že povinnosti v oblasti certifikace bezpečnosti a auditu v rámci Dodatku DP naplňují právo zákazníka na audit a právo na audit jeho orgánu pro ochranu údajů, poskytnuté na základě ustanovení doložky 5 písm. f) a doložky 12 odst. 2 MCC.[73] Skutečnost, že audit není prováděn klientem, není v rozporu s MCC, pokud

[71] Viz odst. 10.1 Dodatku DP.
[72] Viz odst. 13 Smlouvy GA.
[73] Viz odst. 6.7 Dodatku DP.

Google vybere pro audit „kontrolní orgán složený z nezávislých členů s požadovanou odbornou kvalifikací“ (překlad JT).[74] Problémem je výběr auditora, který je zcela ponechán na Googlu, zatímco MCC požadují, aby auditor byl vybrán „vývozcem údajů, popřípadě po dohodě s příslušným orgánem dohledu“ (překlad JT).[75]

5. ANALÝZA SMLOUVY O POSKYTOVÁNÍ MICROSOFT OFFICE 365

Základní podmínky upravující poskytování Office 365 jsou dány Microsoft Online Subscription Agreement[76] (dále jen “Smlouva MOS”) a Privacy Notice,[77] se kterými zákazník vyjadřuje souhlas při objednávání placené verze služeb. Nejdůležitějším dokumentem, na který odkazuje Smlouva MOS, jsou Online Services Terms[78] (dále jen „Podmínky OS“), které konkretizují podmínky pro poskytování on-line služeb, včetně služeb Office 365. Smlouva MOS je uzavírána s Microsoft Ireland Operations Limited, společností založenou podle irského práva se sídlem v Dublinu (dále jen „Microsoft“).

Základní prvky smlouvy o zpracování osobních údajů jsou obsaženy v oddílu Additional European Terms Podmínek OS, která se vztahuje pouze na klienty z Evropského hospodářského prostoru a Švýcarska, a stanoví, že Microsoft je zpracovatel osobních údajů jednající jménem svých zákazníků a že bude jednat pouze na základě pokynů zákazníka. Jako účel zpracování Podmínky OS uvádějí, že „Data zákazníka budou použita pouze k poskytnutí Online služeb zákazníkovi, včetně účelů slučitelných s poskytováním těchto služeb“ a „Microsoft nebude používat data zákazníka nebo z nich odvozovat informace pro jakoukoli reklamu nebo podobné komerční účely.“ (překlad JT) [79] Kategorie zpracovávaných údajů jsou specifikovány jako „e-maily, dokumenty a další data v elektronické

[74] Viz doložku 5 písm. f) MCC.

[75] Viz doložku 5 písm. f) MCC.

[76] Viz *Microsoft Online Subscription Agreement* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Po registraci dostupné z: portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK (aktuální veřejně dostupné znění nebylo nalezeno).

[77] Viz *Privacy Notice* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoft.com/online/legal/v2/?docid=18&langid=en-UK

[78] Viz *Online Services Terms January 1, 2015* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248.

[79] Viz Část General Privacy and Security Terms, odst. Use of Customer Data Podmínek OS.

podobě v rámci Online služeb.“ (překlad JT) [80] Rozsah pokynů zákazníka je omezen pouze na pokyny uvedené ve Smlouvě MOS a Podmínkách OS.[81]

Podmínky OS popisují bezpečnostní opatření, která Microsoft uplatňuje. Popis je spíše obecný, ale pokrývá velké množství oblastí.[82] Pokud jde o důkaz skutečného uplatňování opatření, Microsoft dává zákazníkovi k dispozici svou bezpečnostní politiku, která je v souladu s normami ISO 27001 a 27002 a zároveň zajistí prověření této bezpečnostní politiky nezávislým odborníkem. Shrnutí auditní zprávy Microsoft zákazníkovi na jeho žádost zpřístupní.[83] Microsoft je také nově certifikovaný podle standardu ISO 27018, který cílí právě na ochranu osobních údajů v cloudu.[84]

V případě porušení smlouvy má zákazník zvláštní právo pouze na náhrady, které jsou uvedeny v dohodě o úrovni služeb (Service Level Agreement).[85] Smlouva MOS neopravňuje klienta ukončit smlouvu speciálně pro porušení povinnosti společnosti Microsoft, nicméně i při dlouhodobém předplatném služby může zákazník smlouvu ukončit bez udání důvodu s výpovědní dobou jeden měsíc a právem na vrácení za zbývající části předplatného.[86] Kromě toho má zákazník právo ukončit smlouvu při porušení jeho instrukcí nebo standardních smluvních doložek vydaných Evropskou komisí podle klauzule 5(b) těchto doložek v příloze č. 3 k Podmínkám OS.

Odpovědnost Microsoftu za škody způsobené porušením povinnosti vyplývající z dohody o MOS je omezena na částky zaplacené za služby v průběhu současného smluvního období, které může trvat pouhých 30 dnů[87] a odpovědnost za ušlý zisk, nepřímé škody, narušení podnikání

[80] Příloha č. 1 k Standardním smluvním doložkám v příloze č. 3 k Podmínkám OS.

[81] Viz Část Data Processing Terms, oddíl Additional European Terms, odst. Intent of the Parties Podmínek OS.

[82] Viz Část Data Processing Terms, oddíl Security Podmínek OS.

[83] Viz Část Data Processing Terms, oddíl Certifications and Audits Podmínek OS.

[84] Viz Microsoft adopts first international cloud privacy standard. *Microsoft on the Issues* [online]. Microsoft, publikováno 16. 12. 2015 [cit. 16. 3. 2015]. Dostupné z: http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/

[85] Viz článek 4 odst. a(i) Smlouvy MOS. Srov. též *Service Level Agreement for Microsoft Online Services* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8222

[86] Viz článek 3 odst. b(ii) Smlouvy MOS.

[87] Viz článek 6 odst. a Smlouvy MOS.

a ztrátu obchodních informací je vyloučena, a to i v případě, že byly tyto škody pro příslušnou smluvní stranu rozumně předvídatelné.[88] Toto omezení ponechává významnou část břemene odpovědnosti vůči subjektu údajů na zákazníkovi.

Ani Smlouva MOS ani Podmínky OS neumožňují jednostranné změny. Smlouvu lze měnit pouze po uplynutí smluvního období prostřednictvím postupu pro její prodloužení.[89]

Vyjádřením souhlasu se Smlouvou MOS zákazník rovněž souhlasí s tím, aby Microsoft využíval při poskytování služeb subdodavatele.[90] Každá subdodavatelská smlouva musí obsahovat ujednání, která budou zákazníka chránit alespoň tak, jak jej chrání část Data Processing Terms Podmínek OS. Microsoft je zároveň povinen zákazníka informovat o každém novém subdodavateli, který se má účastnit na poskytování služeb, a to s předstihem nejméně 14 dnů. Pokud zákazník subdodavatele neschválí, může v této lhůtě ukončit smlouvu ve vztahu k dotčené službě.[91]

Microsoft se zavazuje, že vymaže data zákazníka nejpozději do 90 dnů od ukončení poskytování služeb.[92] Microsoft je rovněž povinen poskytnout zákazníkovi možnost opravit, mazat, nebo blokovat zpracovávaná data, nebo učinit takové opravy, odstranění nebo blokování jeho jménem,[93] aby zákazník mohl plnit požadavky subjektů zpracovávaných údajů.

Z hlediska geografické lokalizace zpracování dat Microsoft zaručuje, že bude ukládat nejcitlivější část dat zákazníků z EU v této oblasti.[94] Co se týče ostatních dat, Microsoft je a zavazuje se zůstat certifikovaný v programu Safe Harbor a Podmínky OS ve své příloze č. 3 obsahují standardní smluvní doložky vydané Evropskou komisí. Text těchto doložek není nijak pozměněn. Pokud jde o možné rozpory doložek se Smlouvou MOS a Podmínkami OS, problematickým aspektem je audit poskytování služeb. Podmínky OS uvádějí, že zákazník souhlasí s tím, aby vykonával své právo

[88] Viz článek 6 odst. b Smlouvy MOS.
[89] Viz článek 2 odst. d Smlouvy MOS.
[90] Viz část General Privacy and Security Terms, oddíl Use of Subcontractors Podmínek OS.
[91] Viz část Data Processing Terms, oddíl Privacy, odst. Subcontractor Transfer Podmínek OS.
[92] Viz část Data Retention Podmínek OS.
[93] Viz část Data Processing Terms, oddíl Additional European Terms, odst. Customer Data Access Podmínek OS.
[94] Viz část Data Processing Terms, oddíl Location of Customer Data at Rest, odst. Office 365 Services Podmínek OS.

auditu dle standardních smluvních doložek tím, že dává Microsoftu pokyn nechat audit provést nezávislým profesionálem v oblasti bezpečnosti, jak bylo popsáno výše. Nicméně zákazník má právo tento pokyn změnit. I když to není výslovně uvedeno, toto právo zákazníka může být vykonáváno například tak, že zákazník změní svůj pokyn, pokud neschválí auditora vybraného Microsoftem, a tudíž může ovlivnit výběr auditora, jak požadují standardních smluvní doložky. Podmínky OS navíc výslovně uvádějí, že nic v příslušné části jejich textu nemá měnit nebo upravovat Standardní smluvní doložky ani omezovat práva jakéhokoli dozorčího orgánu či subjektu údajů na základě standardních smluvních doložek.[95] Zbývající část textu Podmínek OS by proto měla být vykládána v duchu tohoto záměru.

6. SROVNÁNÍ SMLUV A DISKUZE

Smluvní rámec Googlu pro poskytování služby Google Apps for Work celkově trpí několika nedostatky, které mohou způsobit jeho rozpor se směrnicí 95/46/ES a jejími vnitrostátními implementacemi. Nejviditelnějším nedostatkem je skutečnost, že smlouva s náležitostmi smlouvy o zpracování osobních údajů není se zákazníky z EU uzavírána automaticky. Místo toho je k jejímu uzavření zapotřebí specifický úkon ze strany zákazníka, přičemž provedení tohoto úkonu není ze strany Google aktivně doporučováno. Za těchto okolností se může snadno stát, že zákazník z EU bude využívat Google Apps for Work, aniž by vyjádřil souhlas s Dodatkem DP a MCC, a tím bude porušovat povinnosti plynoucí z legislativy na ochranu osobních údajů. Google se v takovém případě stane správcem osobních údajů, které mu budou zákazníkem předány, přičemž bude také jednat v rozporu s právními předpisy o ochraně osobních údajů, neboť nelze očekávat, že by Google plnil odpovídající povinnosti, jakými je získání titulu pro zpracování nebo informování subjektů údajů. Není přitom známo, kolik procent uživatelů Google Apps for Work z EU nevyjádřilo souhlas s Dodatkem DP a MCC, ale lze přepokládat, že toto procento nebude zanedbatelné.

Formulace ustanovení Smlouvy GA, která ošetřují omezení odpovědnosti, jsou nejednoznačná a zákazník musí vzít v úvahu možnost, že odpovědnost společnosti Google na základě této smlouvy bude striktně

[95] Viz část Data Processing Terms, oddíl Certifications and Audits Podmínek OS.

omezena. Podobně nejasné formulace jsou vloženy do MCC a mohou být potenciálně v rozporu s rozhodnutím Komise 2010/87/EU. Google je oprávněn jednostranně měnit bezpečnostní opatření stanovená na ochranu osobních údajů, která jsou esenciální náležitostí smlouvy o zpracování osobních údajů. Zákazník nemá právo vznést námitky proti výběru subdodavatelů Googlu podílejících se na zpracování osobních údajů. Právo zákazníka na audit zakotvené v MCC je omezeno v Dodatku DP do té míry, že to může být shledáno v rozporu rozhodnutím Komise 2010/87/EU.

Smluvní rámec pro poskytování Microsoft Office 365 také trpí určitými nedostatky. Nejdůležitější z nich je striktní omezení odpovědnosti, které se vztahuje i na škody způsobené porušením práva na ochranu údajů. Lhůta, ve které musí Microsoft oznámit nového subdodavatele, dává zákazníkovi pouze velmi krátký předstih pro migraci na jinou službu, než se nový subdodavatel začne podílet na poskytování služby a tedy získá potenciální přístup k jeho datům. Také úprava práva auditu v Podmínkách OS může být potenciálně v rozporu se standardními smluvními doložkami.

Porovnáme-li smlouvy na obě služby z hlediska ochrany osobních údajů, vychází z tohoto srovnání podstatně lépe Microsoft Office 365. Nejvýznamnější nedostatek smlouvy na tuto službu, omezení odpovědnosti, není v přímém rozporu s právními předpisy o ochraně osobních údajů, pouze vytváří nerovnováhu smluvního rámce. Další nedostatky jsou diskutabilní a Smlouva MOS spolu s Podmínkami OS jsou obecně v souladu s požadavky směrnice 95/46/ES. Naopak v případě Google Apps for Work jsou nedostatky smlouvy podstatné. Částečně je možné je napravit uzavřením Dodatku DP a MCC, ale některé z nich zůstávají nevyřešeny. Klienti se sídlem v EU používající Google Apps for Work proto čelí riziku porušení zákona o ochraně osobních údajů a následné sankci od svých vnitrostátních orgánů pro ochranu údajů, a to zejména v případě, že neodsouhlasili Dodatek DP a MCC.

Obecně, Smlouva MOS a zejména Podmínky OS ukazují, že Microsoft věnuje otázkám soukromí a ochrany osobních údajů značnou pozornost a požadovaná opatření a obecně doporučované postupy jsou realizovány v rámci výchozího nastavení. To potvrzuje i pokračující a úspěšná spolupráce Microsoftu s WP29. Výsledkem této spolupráce jsou změny provedené v smluvní dokumentaci Microsoftu, které by měly zajistit shodu

s evropskými právními předpisy o ochraně osobních údajů.[96] Smlouva GA nevykazuje takovou úroveň pozornosti věnované otázkám ochrany osobních údajů. Google by mohl pro zákazníky se sídlem v EU zahrnout podmínky Dodatku DP a MCC do smluvního rámce již ve výchozím nastavení.[97] Spolupráce Google s WP29 se také nezdá být tak plodná jako spolupráce Microsoftu.[98]

Důvody těchto rozdílů mohou být různé, přičemž jedním z nich může být nedostatek zkušeností Googlu s evropským trhem. Microsoft vstoupil na evropský trh dlouho před založením Googlu. Zároveň Microsoft jako výrobce softwaru musel čelit vládám jako odběratelům i regulátorům téměř od počátku své existence. Tyto zkušenosti mohou Microsoftu pomáhat, aby se přizpůsobil požadavkům evropských regulačních orgánů rychleji a efektivněji než Google, což vyúsťuje v současné rozdíly v jejich přístupu k ochraně osobních údajů v souvislosti s jejich cloudovými službami.

Společným znakem obou smluv je pak výrazný přenos obchodního rizika na stranu zákazníka (zejména skrze ujednání o omezení odpovědnosti), a to do té míry, která nemusí být vždy akceptovatelná.[99] Vzhledem k nerovnováze sil mezi smluvními stranami se postavení SME vůči poskytovatelům blíží postavení spotřebitele. Tomu odpovídá i podobnost některých ujednání ve smlouvách pro podnikatele a smlouvách nabízených

---

[96] Viz *Letter from the Article 29 Working Party to Microsoft on a new version of the Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 2. 4. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf nebo *Letter for the Article 29 Working Party to Microsoft on the Microsoft Service Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 22. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf

[97] Těmto zákazníkům je předkládána smlouva, která se uzavírá s Google Commerce Limited se sídlem v Irsku, jistý stupeň geografické diferenciace uživatelů tedy straně Google nutně musí probíhat.

[98] Viz *Letter from the Article 29 Working Party to Google on Google Privacy Policy* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 23. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf

[99] Dosud nejsou známy žádné medializované případy, kdy by zákazníkovi cloudové služby vznikla jejím užíváním zásadní škoda, kterou by poskytovatel odmítl zaplatit na základě takových ujednání. I malý počet takovýchto medializovaných případů by však mohl náhled zákaznické veřejnosti na toto obchodní riziko změnit.

spotřebitelům.[100] Ve vztahu ke spotřebitelům přitom může nastoupit přísnější režim ochrany, v jeho světle se taková ujednání mohou ukázat jako zakázaná.[101] Pokud by poskytovatelé byli stíháni např. ze strany správních orgánů[102] za použití takovýchto zakázaných ujednání ve vztahu ke spotřebitelům a následně své podmínky z tohoto důvodu modifikovali, je otázkou, zda by se změny nepromítly i od smluv pro SME.

Samotné služby jsou z technického hlediska v jádru jednotné jak pro podnikatele, tak pro spotřebitele, proto je nepravděpodobné, že by se změny vyvolané prosazováním spotřebitelských práv dotkly právě tohoto jádra. Podstata problémů ve vztahu ke spotřebiteli (stejně jako k podnikateli), totiž netkví v technických otázkách, ale v nastavení smluvních podmínek, které jsou pro spotřebitele a podnikatele samostatné a nezávislé. Jelikož oba diskutovaní poskytovatelé, Google i Microsoft, i přes určité podobnosti, nabízí odlišné podmínky pro podnikatele a spotřebitele, ačkoli nabízené služby jsou ve své podstatě identické,[103] nelze předpokládat, že by od této praxe v budoucnu upustily. Za těchto okolností poskytovatelé nemají důvod promítat případné změny ve prospěch spotřebitelů také do podmínek pro podnikatele. Jedinou nadějí pro podnikatele (vedle budoucího působní tržních sil) je proto použití obecných ustanovení o ochraně slabší smluvní strany,[104] avšak posouzení, zda rozhodné právo, tj. právo anglické,[105] resp. irské,[106] obsahuje relevantní ustanovení, která by byla v tomto směru aplikovatelná, překračuje rozsah tohoto článku. Podrobná komparace mezi podnikatelskými

[100] Viz body Naše záruky a odmítnutí odpovědnosti a Odpovědnost za naše služby Smluvní podmínky společnosti Google. *Ochrana soukromí a smluvní podmínky* [online]. Google, aktualizováno 14. 4. 2014 [cit. 22. 3. 2014]. Dostupné z: http://www.google.com/intl/cs/policies/terms/ Též srov. čl. 11 Smlouva o poskytování služeb společnosti Microsoft. *Windows* [online]. Microsoft, aktualizováno 11. 6. 2014 [cit. 22. 3. 2014]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/microsoft-services-agreement

[101] Srov. např. § 1811 odst. 1 a § 1813 an. občanského zákoníku.

[102] Ať už pro porušení s norem spotřebitelského práva či práva na ochranu osobních údajů.

[103] Nelze vyloučit, že z hlediska technického zabezpečení jsou služby pro podnikatele provozovány na odlišné infrastruktuře, která může být např. lépe zajištěná proti výpadkům, atd.

[104] Srov. § 433 občanského zákoníku. Ve vztahu k podnikatelským smlouvám se však občanský zákoník zpravidla neuplatní díky volbě jiného než českého práva, kdežto spotřebitelé se o kogentní normy českého práva mohou opřít díky čl. 6 nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I)

[105] Odst. 14.11 Smlouvy GA.

[106] Článek 8 odst. h. Smlouvy MOS.

a spotřebitelskými smlouvami a možností prosazení ochrany slabší smluvní strany tak zůstávají možným tématem dalšího výzkumu.

7. DISKUZE SOUČASNÉ A BUDOUCÍ PRÁVNÍ ÚPRAVY

Zákazníci a poskytovatelé musí při působení na trhu cloudových služeb čelit řadě právních překážek. Pro dodržení požadavků směrnice 95/46/ES a její národní implementace na používání služby musí zákazník zajistit, aby byly splněny mnohé požadavky. Tento článek popisuje pouze základní požadavky, které vycházejí ze směrnice 95/46/ES, ale zákazník může být vystaven dalším požadavkům vycházejícím z vnitrostátních právních předpisů na ochranu osobních údajů. Rozdíly mezi národními implementacemi směrnice 95/46/ES komplikují situaci i pro poskytovatele. Ti mohou čelit obtížím při snaze nabízet jednotné služby s podmínkami, které by byly v souladu s právními předpisy o ochraně údajů ve všech členských státech EU.

Ne všechny požadavky jsou přitom výslovně stanoveny právními předpisy a zákazník tedy musí studovat pokyny vydané různými orgány, aby zajistil jejich plné splnění. Např. povinnosti ve vztahu k subdodavatelům vůbec nelze vyčíst ze směrnice 95/46/ES. Úprava předávání osobních údajů do jiných států mimo EU je natolik složitá, že jen malé množství zákazníků bude schopno odvodit odpovídající povinnosti přímo ze směrnice 95/46/ES. Zákazník tak může tápat při určování svých vlastních povinností a následně tím pádem i při posuzování nabídky poskytovatele.

V mnoha případech budou data zpracovávaná pomocí cloudové služby obsahovat pouze omezené množství osobních údajů a tyto údaje nebudou vnímány jako citlivé ze strany příslušných subjektů údajů. V těchto případech mohou být povinnosti stanovené poskytovateli jako zpracovateli osobních údajů nepřiměřené. Na druhé straně v případech, kdy je pomocí cloudové služby zpracováváno velké množství subjektivně citlivých dat, může rámec ochrany údajů postrádat dostatečnou podrobnost, aby vztah mezi poskytovatelem a zákazníkem účinně reguloval.[107]

[107] Například nemusí dostatečně specifikovat bezpečnostní opatření, která by měla být v takovém případě uplatňována.

Nejpodstatnějším nedostatkem současné úpravy je však nevhodné rozložení odpovědnosti mezi správcem a zpracovatelem. Zákazník jako správce osobních údajů je ze zákonného hlediska téměř výlučně odpovědný za prováděné zpracování, což poskytovatelům dovoluje aby svou odpovědnost smluvně omezili na minimum.[108]

Stávající právní rámec tedy trpí nedostatky v oblasti unifikace, srozumitelnosti, škálovatelnosti a vyváženého rozložení odpovědnosti. Budoucí regulace by měla sjednotit právní režim alespoň v rámci celé EU, aby se zjednodušila situace jak pro zákazníky, tak pro poskytovatele. Dále by měla jasně a výslovně stanovit povinnosti na straně zákazníka a poskytovatele cloudových služeb a podobných řešení a přizpůsobovat rozsah povinností podle rizika, které zpracováním vzniká (včetně úrovně rizika, se kterým nebudou spojeny žádné povinnosti dle této regulace, tj. de minimis pravidla).

Obecné nařízení o ochraně údajů, navrhované Evropskou komisí,[109] ve znění pozměňovacích návrhů Evropského parlamentu.[110] si klade za cíl reagovat na výše popsané výzvy. Jednou z hlavních ambicí nařízení je sjednotit právní rámec pro ochranu údajů v EU.[111] Místo další harmonizace vnitrostátních právních předpisů prostřednictvím novely současné směrnice bylo jako právní nástroj zvoleno nařízení, které zajistí maximální unifikaci díky své přímé použitelnosti. Kromě toho obecné nařízení obsahuje ustanovení, která upravují spolupráci a koordinaci mezi nezávislými vnitrostátními orgány pro ochranu údajů.[112] Na druhou stranu přetrvávají pochybnosti, do jaké míry nařízení ponechává členským státům možnost

[108] Ke stejnému závěru dospívá MCGILLIVRAY, 2014, op. cit., s. 250.

[109] Viz *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final* [online]. Evropská komise, 2012 [cit. 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN

[110] Viz *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [online]. Evropský parlament, publikováno 12. 3. 2014 [cit. 15. 2. 2015]. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

[111] Tento pozitivní efekt ve vztahu ke cloudovým službám je předpokládán Evropskou komisí. Viz Unleashing the Potential of Cloud Computing in Europe, 2012, op. cit.

[112] Kapitola VII obecného nařízení.

přijmout zvláštní právní úpravu zpracování osobních údajů v některých odvětvích, jako je např. zdravotnictví, nebo bankovnictví.[113]

Ačkoli je text obecného nařízení podstatně delší a podrobnější než text směrnice 95/46/ES, ne všechny povinnosti správce osobních údajů v souvislosti se zpracováním osobních údajů v cloudu jsou uvedeny jasněji.[114] Například znění obecného nařízení navržené Evropskou komisí stanovovalo výslovně povinnost správce zajistit ověření účinnosti bezpečnostních opatření,[115] tj. jejich audit, ale tato povinnost byla odstraněna a nahrazena obecnou povinností být schopen prokázat přiměřenost a účinnost těchto opatření.[116] Takovou úpravou však vzniká nejistota, jaký standard prokazování bude od správců ve vztahu ke cloud computingu požadován, a může dokonce vznikat nejednotnost v aplikační praxi nezávislých vnitrostátních orgánů napříč EU. Kromě toho obecné nařízení dává Evropské komisi pravomoc vydat četné prováděcí předpisy a orgány pro ochranu údajů mohou schvalovat různé kodexy chování a další prováděcí dokumenty, což může vytvářet potenciálně nejasné hranice mezi závaznými a nezávaznými pravidly. Zda tedy obecné nařízení pomůže objasnit a zvýšit srozumitelnost povinností zákazníků a poskytovatelů cloudových služeb je přinejmenším diskutabilní.

Jako pozitivní aspekt lze vnímat, že obecné nařízení výslovně řeší svůj vztah ke směrnici o elektronickém obchodu, a to ve prospěch této směrnice.[117] Z toho lze dovodit, že v režimu obecného nařízení by na poskytovatele cloudových služeb měly vztahovat výluky z povinností zpracovatele osobních údajů na základě jejich kvalifikace jako poskytovatele hostingu dle směrnice o elektronickém obchodu. Dále návrh nařízení výslovně rozšiřuje povinnosti zpracovatele v oblasti dokumentace, spolupráce s orgány dohledu, bezpečnostních opatření, hodnocení dopadů

[113] K pochybnostem srov. BLUME, Peter. The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp: 269-273 [cit. 24. 4 2015]. Dostupné z Oxford Journals: idpl.oxfordjournals.org/content/4/4/269.full.pdf+html. s. 271. KOTCHY, Waltraut. The proposal for a new General Data Protection Regulation—problems solved? *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp. 274-281 [cit. 24. 4 2015] Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/4/4/274.full.pdf+html. s. 275.

[114] Rozsáhlost textu kritizuje BLUME, 2014, op. cit., s. 270.

[115] Viz článek 22 odst. 3 obecného nařízení ve znění návrhu Evropské komise.

[116] Viz článek 22 odst. 3 obecného nařízení ve znění návrhu Evropského parlamentu.

[117] Viz článek 3 odst. 3 obecného nařízení. Srov. SARTOR, 2013, op. cit., s. 4.

a hodnocení shody s legislativou i na zpracovatele.[118] Dále koncept sektorů zpracování (processing sectors, v českém překladu návrhu Komise nešťastně označených jako odvětví zpracování), které mohou být prohlášeny za oblasti s náležitou úrovní ochrany, může usnadnit předávání osobních údajů do zahraničí.[119] Nařízení také řeší problematiku subdodavatelů, ale v současnosti navrhované znění je velmi obecné.[120]

I přes tato zlepšení flexibility a rozložení odpovědnosti, prostor pro zlepšení zůstává výrazný. Místo sloučení role správce a zpracovatele v jeden odpovědný subjekt s odstupňovanými povinnostmi a odpovědností, návrh nařízení kopíruje původní dichotomii zavedenou směrnicí 95/46/ES. Kromě toho návrh nařízení neobsahuje skutečné pravidlo de minimis, které by osvobodilo zpracování malého rozsahu s nízkým rizikem z jeho působnosti. Velikost zpracování tak ovlivňuje pouze povinnosti s okrajovým vlivem na správce, jako je jmenování inspektora ochrany údajů.[121] Místo toho nařízení přidává správcům další povinnosti[122] a nebere v úvahu rozsah a rizikový profil zpracování. Pokud jde o rozložení odpovědnosti, zpracovatel stále nesdílí se správcem v plném rozsahu primární odpovědnost za bezpečnost a legálnost zpracování.[123]

Specifickou změnou, kterou obecné nařízení přináší, je právo subjektu údajů domáhat se svých práv přímo vůči správci a zpracovateli u soudu.[124] Toto právo je navíc podpořeno tím, že nárok může v zastoupení spotřebitele vymáhat i organizace jednající ve veřejném zájmu.[125] Je otázkou, jaké nároky by mohli dotčení jednotlivci a jejich zástupci

[118] Srov. čl. 28, 29, 30, 33 and 33a obecného nařízení ve znění návrhu Evropského parlamentu. Srov. též. BLUME, Peter. It Is Time for Tomorrow: EU Data Protection Reform and the Internet. *Journal Of Internet Law*. 2015, vol. 18, no. 8, pp. 3-13 [cit. 24. 4 2015]. s. 7.

[119] Srov. čl. 41 obecného nařízení ve znění návrhu Evropského parlamentu. Srov. též. BLUME, 2015, op. cit., s. 9.

[120] Srov. čl. 26 odst. 2 obecného nařízení ve znění návrhu Evropského parlamentu. Původní znění navržené Komisí bylo striktnější a jednoznačnější. Srov. též MCGILLIVRAY, 2014, op. cit., s. 248.

[121] Viz článek 35 odst. 1 písm. b) obecného nařízení.

[122] Viz READING, Viviane. The European data protection framework for the twenty-first century. *International Data Privacy Law* [online]. 2012, vol. 2, no. 3, pp. 119-129. [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/3/119.full.pdf, s. 126.

[123] Zpracovatel není zahrnut v článku 22 odst. 1 navrhovaného nařízení. Srov. též. BLUME, 2015, op. cit., s. 7. MCGILLIVRAY však namítá, že veškerá odpovědnost by neměla být přenášena na zpracovatele, srov. MCGILLIVRAY, 2014, op. cit., s. 248.

[124] Viz. článek 75 obecného nařízení ve znění návrhu Evropské komise. Též srov. READING, 2012, op. cit., s. 126.

uplatňovat v případě cloud computingu obecně a diskutovaných služeb konkrétně. Cloud computing jako takový svou podstatou neodporuje principům ochrany osobních údajů a žádné z výše diskutovaných porušení není natolik flagrantní, aby přímo ohrožovalo subjekty zpracovávaných údajů. Těžko lze tedy z jejich strany očekávat preventivní kroky. Nároky proto mohou být vznášeny spíše v případě bezpečnostních incidentů, které by měly dopad na jednotlivce. Rovněž je možné, že při zásadní změně bezpečnostních opatření by mohli jednotlivci a jejich zástupci napadat možnost těchto změn a případný nedostatek auditních práv. Ve vztahu k současnému stavu tak mohou přímé nároky přinést zlepšení pouze jako hrozba pro poskytovatele, která je může přivést k přísnějšímu uplatňování bezpečnostních opatření. Nelze však předpokládat, že by vedly k úpravě smluvních podmínek.

Celkově se upravený návrh obecného nařízení ve vztahu ke cloud computingu zdá být dosti problematický. S výjimkou alespoň částečné unifikace by v současnosti navrhované znění nejspíše nepřineslo v oblasti cloud computingu výrazná zlepšení. Budoucí revize by se proto měly zaměřit na jeho zjednodušení, zlepšení srozumitelnosti a vyšší škálovatelnost povinností.

Bez ohledu na to, zda by obecné nařízení bylo prospěšné pro zákazníky a poskytovatele cloudových služeb nebo ne, jeho účinnost nelze vzhledem k složitosti unijního legislativního procesu a množství angažovaných organizovaných zájmů očekávat v blízké budoucnosti, stejně jako jakoukoli jinou změnu směrnice 95/46/ES. Proto je třeba pro zákazníky hledat řešení, jak efektivně hodnotit nabídky poskytovatelů cloudových služeb a zajistit soulad zpracování osobních údajů pomocí těchto služeb se směrnicí 95/46/ES.

V reakci na tuto výzvu zřídila Evropská komise oborovou pracovní skupinu pro cloud computing (Cloud Select Industry Group) a v rámci ní podskupinu zaměřenou na standardizaci smluv na poskytování cloudových služeb (Service Level Agreement v širším smyslu). Tato podskupina vydala doporučení pro standardizaci těchto smluv (Cloud Service Level Agreement

[125] Viz. články 73 odst. 2 a 76 obecného nařízení ve znění návrhu Evropského parlamentu. Též srov. REDING, 2012, op. cit., s. 126.

Standardisation Guidelines), které pokrývá i otázky ochrany osobních údajů.[126]

Doporučení je vystavěné na konceptu cílových úrovní služeb (Service Level Objectives), které pokrývají také otázku ochrany osobních údajů. Doporučení je v tomto ohledu relativně podrobné a reflektuje doporučení WP29. Odpovídající cílové úrovně služeb se týkají certifikace, vymezení účelu, minimalizace zpracovávaných údajů, omezení uchovávání a vydání údajů, prokazatelnost záznamů, lokalizaci dat a řešení požadavků subjektů údajů. Kromě toho doporučení zmiňuje také cílové úrovně služeb pro bezpečnost, jako jsou autentizace a řízení přístupu, šifrování, řešení bezpečnostních incidentů, logování a monitorování, audity a ověření bezpečnosti. Doporučení se také věnuje výkonnosti a řízení dat. Pro každou cílovou úroveň služeb doporučení uvádí, jak by měla být ve smlouvě ošetřena.

Podle zkušeností autora jsou tato doporučení v praxi velmi dobře použitelná jak při posuzování, tak při sepisování smluv o zpracování osobních údajů pro cloudové služby. Bylo by proto z praktického hlediska vítaným přínosem, kdyby byla tato doporučení v budoucnu rozpracována např. do standardního smluvního nástroje. Není přitom nezbytné, aby tento nástroj musel být používán povinně jako např. standardní smluvní podmínky pro předávání osobních údajů do třetích zemí bez odpovídající úrovně ochrany. Postačí, pokud tyto standardní podmínky budou kvalitně formulované a vytvořené na základě konsenzu zástupců poskytovatelů, zákazníků i regulátorů. Z pohledu SME by toto řešení bylo podstatným zjednodušením situace, protože v případě nabídky, která by stavěla na standardním smluvním nástroji, by pro ně bylo její posouzení podstatně snadnější. Zároveň by jim tento postup dával dostatečnou míru jistoty o souladu jejich postupu s ochranou osobních údajů.

8. ZÁVĚR

Poskytování cloudových služeb zákazníkům se sídlem v Evropské unii může často spadat do působnosti evropského práva na ochranu údajů, které je

[126] Viz Cloud Service Level Agreement Standardisation Guidelines. *Evropská komise* [online]. Cloud Select Industry Group, Subgroup on Service Level Agreement, publikováno 24. 06. 2014 [cit. 30. 10. 2014]. Dostupné z: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138.

reprezentováno směrnicí 95/46/ES. Zákazníkům a poskytovatelům cloudových služeb mohou být v rámci směrnice 95/46/ES v závislosti na povaze zpracování přiřazeny různé role a z toho vyplývající práva a povinnosti. Zákazník je ve většině případů správcem osobních údajů. Poskytovatel může být správcem osobních údajů, pokud zpracovává osobní údaje pro své vlastní účely, jako je například reklama. Zpracovatelem osobních údajů může být, pokud údaje zpracovává pro zákazníka podle jeho pokynů. Může být také zcela vyňat z působnosti směrnice 95/46/ES, pokud se kvalifikuje jako poskytovatel hostingu podle směrnice o elektronickém obchodu tím, že mu není známa povaha dat zpracovávaných pomocí jeho služby.

V případech, kdy je poskytovatel cloudových služeb zpracovatelem osobních údajů (jako například když je zřejmé z povahy příslušné služby, že jejím prostřednictvím budou zpracovávány osobní údaje) vztah mezi poskytovatelem a zákazníkem cloudových služeb musí být upraven smlouvou o zpracování osobních údajů. Tato smlouva musí stanovit, že poskytovatel je vázán pokyny zákazníka, musí určovat rozsah pokynů zákazníka, účel zpracování a typy zpracovávaných údajů. Dále smlouva musí popisovat bezpečnostní opatření, způsob prokazování uplatňování těchto opatření ze strany poskytovatele a nápravné prostředky pro případ jejich nedodržení. Smlouva nesmí umožňovat jednostranné změny podstatných ujednání a musí upravovat využívání subdodavatelů ze strany poskytovatele. Poskytovatel musí garantovat, jak dlouho po ukončení využívání služeb ze strany zákazníka budou vymazány příslušné osobní údaje, a musí být povinen poskytnout zákazníkovi součinnost při plnění žádosti subjektů údajů. Mají-li být osobní údaje pomocí dané služby zpracovávány mimo EU a země s odpovídající úrovní ochrany, musí být poskytovatel certifikován v programu Safe Harbor pro zpracování v USA a smlouva musí obsahovat standardní smluvní doložky vydané Evropskou komisí pro zpracování v ostatních zemích.

Smluvní rámec pro poskytování Microsoft Office 365 se zdá být v souladu s výše uvedenými požadavky s výjimkou drobných nedostatků a nerovnováhy v otázce odpovědnosti. Smluvní struktura pro poskytování služby Google Apps for Work trpí více závažnými nedostatky, které mohou vést k porušování legislativy na ochranu osobních údajů. Aby byla zajištěna

alespoň minimální úroveň plnění požadavků směrnice 95/46/ES, je třeba ze strany zákazníka provést dodatečné úkony. Google také silně omezuje právo zákazníka na audit a svou odpovědnost vůči zákazníkovi. Smlouva Googlu rovněž umožňuje jednostranně měnit její podstatná ujednání. Přístup společnosti Microsoft vykazuje vyšší stupeň pozornosti věnovaný ochraně osobních údajů. Tento rozdíl může být dán větší zkušeností Microsoftu s evropským trhem a regulací obecně.

Stávající právní rámec pro ochranu údajů při poskytování cloudových služeb trpí nedostatkem unifikace, srozumitelnosti, škálovatelnosti a vyváženého rozložení odpovědnosti. S výjimkou unifikace nelze předpokládat, že připravované obecné nařízení o ochraně osobních údajů přinese podstatné zlepšení, bude-li přijato v aktuálním znění. V dalších revizích by mělo být nařízení zjednodušeno, zapracována klauzule de minimis a rozsah povinností přizpůsoben velikosti a rizikovému profilu zpracování.

Pro potřeby práce se současnou evropskou úpravou ochrany osobních údajů reprezentovanou směrnicí 95/46/ES mohou zákazníci a poskytovatelé cloudových služeb používat Cloud Service Level Agreement Standardisation Guidelines vydané pracovní skupinou Evropské komise. Do budoucna by bylo pro praxi významným přínosem, kdyby tato doporučení byla rozpracována do standardního smluvního nástroje.

Ve vztahu ke cloud computingu by byla z hlediska ochrany osobních údajů vhodná bližší analýza připravovaného obecného nařízení, rozbor podmínek poskytovatelů cloudových služeb cílených na spotřebitele a jejich srovnání s podmínkami pro podnikatele, popřípadě možnost vymáhání změn podmínek pro podnikatele na základě ochrany slabší smluvní strany či zneužití dominantního postavení. Zajímavá by rovněž byla analýza případného právního nástupnictví v kontextu kombinovaných smluvních závazků na poskytování cloudových služeb.

9. POUŽITÉ PRAMENY

9.1 PRÁVNÍ PŘEDPISY A JUDIKATURA

[1] Nařízení Evropského parlamentu a Rady (ES) č. 593/2008 ze dne 17. června 2008 o právu rozhodném pro smluvní závazkové vztahy (Řím I).

[2] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu.

[3] Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

[4] Ústavní zákon č. 23/1991 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.

[5] Zákon č. 89/2012 Sb., občanský zákoník.

[6] Zákon Španělska Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

[7] Zákon Spojeného království Data Protection Act 1998.

[8] Zákon Německé spolkové republiky č. RGBl. 1896 S. 195, Bürgerliche Gesetzbuch, ve znění pozdějších předpisů.

[9] Title 17 of the United States Code, Copyright Act, ve znění pozdějších předpisů.

[10] 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

[11] Nařízení Španělska Real Decreto 1720/2007, Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[12] Nařízení Polské republiky Rozporządzenie Ministra spraw wewnętrznych i administracji Dz. U. z 2004 r. Nr 100, poz. 1024, w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

[13] Rozhodnutí Sněmovny lordů Spojeného království ze dne 9. 7. 2008. Common Services Agency v Scottish Information Commissioner (Scotland). Věc [2008] UKHL 47.

9.2 MONOGRAFIE A ČASOPISECKÉ ČLÁNKY

[14] BLUME, Peter. It Is Time for Tomorrow: EU Data Protection Reform and the Internet. *Journal Of Internet Law*. 2015, vol. 18, no. 8, pp. 3-13 [cit. 24. 4 2015].

[15] BLUME, Peter. The myths pertaining to the proposed General Data Protection Regulation. *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp: 269-273 [cit. 24. 4 2015]. s. 270. Dostupné z Oxford Journals: idpl.oxfordjournals.org/content/4/4/269.full.pdf + html

[16] HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. Who is responsible for 'personal data' in cloud computing?—The cloud of unknowing, Part 2 *International Data Privacy Law* [online]. 2012, vol. 2, no. 1, pp. 3-18. ISSN 2044-4001 [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/1/3.full.pdf + html

[17] HON, Kuan W.; MILLARD, Christopher; WALDEN, Ian. The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law* [online]. 2011, vol. 1, no. 4, pp. 211-228 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/1/4/211.full.pdf + html

[18] KOTCHY, Waltraut. The proposal for a new General Data Protection Regulation—problems solved? *International Data Privacy Law* [online]. 2014, vol. 4, no. 4, pp. 274-281 [cit. 24. 4 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/4/4/274.full.pdf+html

[19] MCGILLIVRAY, Kevin. Conflicts in the Cloud: Contracts and Compliance with Data Protection Law in the EU. *Tulane Journal of Technology & Intellectual Property*. 2014, roč. 17, č. Fall 2014, pp. 217–253.

[20] REDING, Viviane. The European data protection framework for the twenty-first century. *International Data Privacy Law* [online]. 2012, vol. 2, no. 3, pp. 119-129. [cit. 15. 2. 2015]. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/2/3/119.full.pdf

[21] SARTOR, Giovanni. Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? *International Data Privacy Law* [online]. 2013, vol. 3, no. 1, pp. 3-12 [cit. 15. 2. 2015]. ISSN 2044-4001. Dostupné z Oxford Journals: http://idpl.oxfordjournals.org/content/3/1/3.full.pdf+html

[22] SVANTESSON, Dan Jerker B. Data protection in cloud computing – The Swedish perspective. *Computer Law & Security Review* [online]. 2012, vol. 28, issue 4, pp. 476-480 [cit. 15. 2. 2015]. Dostupné ze ScienceDirect: http://linkinghub.elsevier.com/retrieve/pii/S0267364912001021.

[23] TOMÍŠEK, Jan. Licence při poskytování software jako služby. *Revue pro právo a technologie*, Masarykova univerzita, 2014, roč. 2014, č. 10, s. 47-69. ISSN 1804-5383.

9.3 OSTATNÍ LITERATURA

[24] DEBUSSCHE, Julien; VAN ASBROECK, Benoit; CHLOUPEK, Vojtěch a kol. Cloud computing and privacy series: the data protection legal framework (part 2 of 6). *Bird&Bird* [online]. 24 listopadu 2014 [cit. 15. 2. 2015]. Dostupné z http://www.twobirds.com/en/news/articles/2014/global/cloud-computing-and-privacy-series-the-data-protection-legal-framework

[25] Cloud Service Level Agreement Standardisation Guidelines. *Evropská komise* [online]. Cloud Select Industry Group, Subgroup on Service Level Agreement, publikováno 24. 06. 2014 [cit. 30. 10. 2014]. Dostupné z: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?action=display&doc_id=6138.

[26] *Data Processing Amendment to Google Apps Agreement* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/dpa_terms.html

[27] *Google Apps Enterprise (Online) Agreement* [online]. Google, únor 2014 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html

[28] *Guía para clientes que contraten servicios de Cloud Computing* [online]. Agencia Española de Protección de Datos, 2013 [cit. 11. 2. 2015]. Dostupné z: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_Cloud.pdf

[29] *Guidance on the use of cloud computing* [online]. Information Commissioner's Office, 2012, [cit. 11. 2. 2015]. Dostupné z: https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf

[30] *Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [online]. Evropský parlament, publikováno 12. 3. 2014 [cit. 15. 2. 2015]. Dostupné z: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

[31] *Letter from the Article 29 Working Party to Google on Google Privacy Policy* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 23. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf

[32] *Letter from the Article 29 Working Party to Microsoft on a new version of the Enterprise Enrollment Addendum Microsoft Online Services Data Processing Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 2. 4. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140402_microsoft.pdf

[33] *Letter for the Article 29 Working Party to Microsoft on the Microsoft Service Agreement and its Annex I* [online]. *Evropská komise* [online]. Article 29 Data Protection Working Party, publikováno 22. 9. 2014 [cit. 15. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf

[34] Microsoft adopts first international cloud privacy standard. *Microsoft on the Issues* [online]. Microsoft, publikováno 16. 2. 2015 [cit. 16. 3. 2015]. Dostupné z: http://blogs.microsoft.com/on-the-issues/2015/02/16/microsoft-adopts-first-international-cloud-privacy-standard/

[35] *Microsoft Online Subscription Agreement* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Po registraci dostupné z: portal.office.com/Commerce/Mosa.aspx?cl=en&cc=en-UK

[36] Model contract clauses for Google Apps. *Google Apps Help Center* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://support.google.com/a/answer/2888485?hl=en

[37] *Online Services Terms January 1, 2015* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8248

[38] Opinion 05/2012 on Cloud Computing. *Evropská komise* [online]. Article 29 Data Protection Working Party, 2012 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[39] Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT). *Evropská komise* [online]. Article 29 Data Protection Working Party, 2006 [cit. 11. 2. 2015]. Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf, p. 26.

[40] *Privacy Notice* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoft.com/online/legal/v2/?docid=18&langid=en-UK

[41] *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM/2012/011 final* [online]. Evropská komise, 2012 [cit. 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012PC0011&from=EN

[42] *Service Level Agreement for Microsoft Online Services* [online]. Microsoft, 2015 [cit. 13. 2. 2015]. Dostupné z: http://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=8222

[43] *Service Orgnaization Control (SOC) 3 Report* [online]. Ernst & Young, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/pdfs/soc3_google_2014.pdf

[44] Smlouva o poskytování služeb společnosti Microsoft. *Windows* [online]. Microsoft, aktualizováno 11. 7. 2014 [cit. 22. 3. 2014]. Dostupné z: http://windows.microsoft.com/cs-cz/windows/microsoft-services-agreement

[45] Smluvní podmínky společnosti Google. *Ochrana soukromí a smluvní podmínky* [online]. Google, aktualizováno 14. 4. 2014 [cit. 22. 3. 2014]. Dostupné z: http://www.google.com/intl/cs/policies/terms/

[46] *SOC 3 Seal of Assurance* [online]. WebTrust, 2014 [cit. 11. 2. 2015]. Dostupné z: https://cert.webtrust.org/soc3_google.html

[47] *Standard Contractual Clauses (processors) for the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection* [online]. Google, 2015 [cit. 15. 2. 2015]. Dostupné z: https://www.google.com/intx/en/work/apps/terms/mcc_terms.html

[48] *Stanovisko č. 65/2013/4* [online]. Úřad pro ochranu osobních údajů, publikováno 1. 7. 2013 [cit. 11. 2. 2015]. Dostupné z: https://www.uoou.cz/VismoOnline_ActionScripts/File.ashx?id_org=200144&id_dokumenty=3002.

[49] Unleashing the Potential of Cloud Computing in Europe. *Evropská komise* [online]. 27 9. 2012 [cit 15. 2. 2015]. Dostupné z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

[50] Use of cloud computing services. *Eurostat* [online]. Publikováno 16. 1. 2015 [cit. 15. 2. 2015]. Dostupné z: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_cicce_use&lang=en