Univerzita Karlova v Praze
Právnická fakulta

# Právní aspekty Cloud computingu

## SaaS jako forma „cloudových služeb“

**Diplomová práce**

2016 Markéta Ohnišťová

Univerzita Karlova v Praze
Právnická fakulta

Markéta Ohnišťová

# Právní aspekty Cloud computingu

## SaaS jako forma „cloudových služeb“

**Diplomová práce**

Vedoucí diplomové práce: JUDr. Irena Holcová

Ústav práva autorského, práv průmyslových a práva soutěžního

Datum vypracování práce: 2016

Prohlašuji, že předloženou diplomovou práci jsem vypracovala samostatně a že všechny použité zdroje byly řádně uvedeny. Dále prohlašuji, že tato práce nebyla využita k získání jiného nebo stejného titulu.

Markéta Ohnišťová

Poděkování

Děkuji vedoucí práce, paní JUDr. Ireně Holcové, za ochotu vést mou diplomovou práci, její trpělivý přístup a za cenné rady, které mi při psaní práce poskytla. Velice si vážím její pomoci a pochopení.

# Obsah

# Úvod

Vzhledem k tomu, že se Cloud computing (zkráceně nazývaný jako cloud) stal fenoménem IT služeb v několika posledních letech, rozhodla jsem se tuto oblast online světa zpracovat v diplomové práci optikou právních aspektů s ním souvisejících. Cloud computing představuje řešení, které je dnes už všudypřítomné, neboť se jedná o model se zatím nejúspornější a nejefektivnější formou výpočetního výkonu, který je dostupný jak jednotlivcům tak malým i středním podnikům. Cloudovou infrastrukturu můžeme dnes vidět skoro za každou online službou, ať už se jedná o sociální sítě, emailové schránky, software na sdílení dokumentů či jinak využívaná datová centra. V rámci velice složité výpočetní infrastruktury je nám umožněno sdílet informace v reálném čase s místy kdekoli na světě, a navíc celé s neomezitelnou kapacitou, přičemž je tato služba dostupná téměř všem na základě platebního modelu založeného na skutečné spotřebě služby.

V rámci náročného konceptu cloudové infrastruktury vzniklo několik nejasností ohledně technických aspektů cloudu, smluvních podmínek uzavíraných formulářovou formou smluv mezi poskytovateli služeb a uživateli, anebo otázky zajištění bezpečnosti přenášených informací. Vzhledem k tomu, že mezi danými informacemi jsou zpracovávány i osobní údaje, zasahuje do Cloud computingu značně i právním rámcem stanovená ochrana osobních údajů, neboť ty jsou pro uživatele nejcitlivější složkou. Nakládání s osobními údaji je upraveno na evropské úrovni formou dosavadní směrnice 95/46/ES, která je transponována do vnitrostátních právních předpisů. Směrnice vznikala v 90. letech a je tedy zřejmé, že dostatečně neodráží technologický vývoj a s tím související změněné, mnohdy zvýšené, požadavky na ochranu osobních údajů. Následkem toho bylo přijato obecné nařízení o ochraně osobních údajů 2016/679, které reflektuje progresivní vývoj v technologiích a nové aspekty ochrany osobních údajů. Těm se v posledních letech věnovala bohatě i judikatura Soudního dvora Evropské unie.

Práce si klade za cíl analyzovat smluvní úpravu zpracování osobních údajů ve dvou nejtypičtějších SaaS cloudových službách Google Apps (for Work) a Microsoft

Office 365. Práce je rozdělená do tří základních kapitol, které jsou z podstaty teoretické. Poslední podkapitola je zaměřená na praktickou část a samotnou analýzu a komparaci zmíněných smluvních úprav.

V první kapitole je definován Cloud computing jako takový, jeho historické ukotvení, včetně stručného nákresu jeho jednotlivých modelů služeb, a zároveň snaha o právní rámec této služby vyplývající ze soft law Evropské unie (EU).

Druhá kapitola se věnuje striktně konkrétnímu cloudovému řešení, službě software jako služba (SaaS). Cílem této kapitoly je shrnout požadavky na smluvní úpravu tohoto druhu služby vycházející z dosavadní platné právní úpravy a současně způsoby poskytování služby SaaS formou vhodných licencí.

Třetí kapitola se zabývá problematikou ochrany osobních údajů v Cloud computingu. Nejprve jsou vymezeny požadavky na ochranu osobních údajů, které vyplývají z evropské právní úpravy představené v první části kapitoly. V první podkapitole se práce zaobírá částečnou komparací požadavků na ochranu osobních údajů mezi dosavadní směrnicí a čerstvě přijatým nařízením, aplikovatelným od roku 2018. V další podkapitole se práce snaží zanalyzovat na základě těchto teoretických aspektů smlouvy o zpracování osobních údajů u vybraných SaaS služeb dvou světových IT gigantů.

Problematika osobních údajů je v komplexnějším technologickém prostředí stále více a více aktuálnější problematikou, kterou se zabývají nejen zákonodárci, ale i samotní technologové. Pro praktickou část této práce jsem si zvolila smluvní úpravy služeb, které jsou notoricky známé, lehce dostupné a především snadno porovnatelné, neboť se jedná téměř o analogické produkty, služby, které nabízejí. To vše i za cenu toho, že je velice pravděpodobné, že tyto smlouvy jsou už několikrát zpracovány v rámci komparace jejich smluvních podmínek a není to tedy natolik neprozkoumaná oblast.

# 1 Co je Cloud computing?

Z dnešního pohledu používá Cloud computing (dále jen cloud) skoro každý uživatel internetových služeb a sítí. Optikou běžného uživatele se s cloudem setkáme, byť nevědomě, při každém nahrání fotografie na sociální síť, emailové korespondenci prostřednictvím webového rozhraní, Skype hovoru či komunikaci na sociálních platformách a mnoho dalších dnes už každodenních aktivit na Internetu. Je to technologie relevantní jak pro jednotlivce tak pro obchodní společnosti či dokonce vládní orgány.

Cloud computing svou komplexností nepředstavuje novou technologii, nýbrž nový způsob poskytování přístupu k informačním zdrojům formou služby na vyžádání. Pod daný pojem řadíme procesy jako úschova dat a jejich softwarové zpracování pomocí počítačových programů (kterým se přezdívá pojmem software[1], používaným v praktické oblasti informačních technologií), jako například emailová schránka, které jsou navíc dostupné v reálném čase, poskytované na vyžádání bez závazku.[2]

Myšlenka cloudu sahá až do doby 50./60. let, kdy se prvně začaly vyskytovat tzv. mainframe počítače, což byly centrální počítače, do kterých bylo možné vkládat data prostřednictvím terminálu složeného z kazetových pásek či karet. Proces byl zdlouhavý a hrozilo chybné zpracování při zadávání příkazů. Profesor John MaCarthy, který pracoval na univerzitě Massachusetts Institute of Technology (MIT), celý proces zrevolucionizoval tím, že navrhl myšlenku propojení terminálů s několika kancelářemi najednou a řadění jednotlivých úkolů jednotlivě za sebe a doručování výpočetních zdrojů jako veřejnou službu podobně jako servisní střediska, která se datují do šedesátých let.[3] Jedním z hlavních historických milníků Cloud computingu byl však

[1] Softwarem se obecně myslí programové vybavení počítačů skládajících se z různých prvků jako jsou datové soubory, databáze, manuály apod. Softwarem se dá označit též vše, co není hardwarem, ale je v něm obsaženo. Zdroj: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580,

[2] *Cloud Computing: Benefits, risks and recommendations for information security* [online]. European Network and Information Security Agency (ENISA), 2009 [cit. 2016-08-20]. Dostupné z: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[3] MELL, Peter, Tim GRANCE,. The NIST Definition of Cloud Computing *Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-145 [online]. U.S.

příchod Salesforce.com v roce 1999, který zavedl koncept doručení podnikových aplikací prostřednictvím jednoduché webové stránky. Touto službou firma připravila cestu pro tradiční i specializované firmy, jak dodávat aplikační software[4] (dále také jako aplikace) přes Internet. Aplikacemi se má na mysli aplikační software, který umožňuje uživateli činnosti podle jednotlivých funkcí softwaru. Další vývojové stádium v této oblasti představoval Amazon Web Services v roce 2002, který prvně poskytl sadu služeb vystavěných na základu cloudu, včetně úložiště, výpočetních technologií a i dokonce lidské inteligence skrze Amazon Mechanical Turk. Stejná firma pak následně v roce 2006 zavedla převratně do oběhu cloud Amazon Elastic Compute (EC2) ve formě obchodní webové služby, která umožnila malým firmám a jednotlivcům pronajmout si výpočetní zdroje ke spuštění vlastních počítačových aplikací. Další významný mezník zaznamenala cloudová technologie v roce 2009, kdy byl spuštěn Web 2.0 a Google společně s dalšími provozovateli začali nabízet podnikové aplikace na systému prohlížeče, tedy jako jsou např. Google Apps.[5] Posléze se ke Googlu připojil další technologický gigant Microsoft s nabídkou cloudových onlinových služeb, které fungovaly spolehlivě a snadno se používaly, a to spustilo řetězový účinek v celém technologickém průmyslu.

Při snaze definovat Cloud computing musíme zmínit jeho základní elementy. Jedná se o model služby na vyžádání pro poskytování přístupu k výpočetním zdrojům založených na virtualizaci sdílené výpočetní technologie. Architektura cloudových technologií obsahuje vždy vysoce abstraktní zdroje, je v krátké době lehce škálovatelná a flexibilní, schopná poskytnout okamžitou odpověď, je vystavěná na sdílených zdrojích (jako např. hardware, databáze, paměť), navíc jedná se o službu na vyžádání

---

Department of Commerce: National Institute of Standards and Technology, 2011 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[4] Aplikační software je vedle systémového softwaru druhou kategorií rozdělen podle toho, komu a k čemu je určen. V informačních systémech se rozlišuje např. podnikový informační systém (ERP systém), systém pro řízení dodavatelských vztahů (SCM systém), systém řízení vztahů se zákazníky (CRM systém), systém řízení lidských zdrojů (HRM systém), systém pro správu obsahu (CMS systém), systém pro správu životního cyklu výrobku (PLM systém), manažerský informační systém (BI systém) anebo informační systém exekutivy (EIS systém). Systémovým softwarem je umožněno fungování počítače a tím i aplikačního softwaru. Zdroj: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 32-33.

[5] ARIF, Mohamed. A history of cloud computing. *ComputerWeekly.com* [online]. 2009 [cit. 2016-08-10]. Dostupné z: http://www.computerweekly.com/feature/A-history-of-cloud-computing

s platebním systémem „pay as you go“ a disponuje programátorským managementem (prostřednictvím WS API).[6]

Národní ústav pro normalizaci a technologie USA (NIST), který poskytuje technické vedení ohledně infrastruktury měrného systému a standardizace v oblasti hospodářských a veřejnoprávních záležitostí americké vlády, definoval Cloud computing jako model umožňující všudypřítomný pohodlný a dostupný na vyžádání síťový přístup ke sdíleným konfigurovatelným výpočetním zdrojům (jako např. sítě, servery, úložiště dat, aplikace a služby), které mohou být rychle a nenáročně poskytnuty a opět odebrány, aniž by do systému musel zasahovat poskytovatel služby. Cloudový model se zakládá na pěti základních vlastnostech, třech servisních modelech a čtyřech metodách zapojení.[7]

Základními vlastnostmi cloudu jsou *i)* tzv. *on-demand* samoobslužné služby, prostřednictvím kterých může spotřebitel jednostranně profitovat automaticky z vlastností výpočetních zdrojů, jako např. čas serveru nebo síťové úložiště, podle vlastních potřeb, aniž by musel osobně komunikovat s jednotlivými poskytovateli služeb; *ii) broad network připojení*, který zajišťuje jednoduchý přístup ke cloudovým službám skrze síťové připojení jakéhokoli zařízení s webovým prohlížečem (jako jsou mobily, tablety, přenosné nebo stacionární počítače); *iii) resource pooling* na základě něhož jsou výpočetní zdroje poskytovatele sdíleny a které slouží řadě spotřebitelů prostřednictvím několikastranného nájemního modelu s různými fyzickými a virtuálními prostředky přiřazovanými na dynamickém principu podle potřeb zákazníka; *iv) rapid elasticity* systém pak souvisí se schopnostmi zvýšit a naopak snížit, v některých případech i automaticky, výpočetní výkon výchozích a příchozích požadavků; *v) measured service* značí fakt, že cloudové systémy automaticky kontrolují a optimalizují využití zdrojů za použití měřící funkcionality na jisté úrovni abstrakce

[6] *Cloud Computing: Benefits, risks and recommendations for information security* [online]. European Network and Information Security Agency (ENISA), 2009 [cit. 2016-08-20]. Dostupné z: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

[7] MELL, Peter, Tim GRANCE,. The NIST Definition of Cloud Computing *Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-145 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2011 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

odpovídající danému typu poskytované služby (např. úložiště, procesování, široké pásmo, či počet aktivních uživatelských účtů).[8]

V souhrnu je podle mezinárodní právnické literatury Cloud computing revoluční inovací, stejně jako byla ve své době levná elektřina dostupná na požádání. Z pohledu uživatelů se jedná o změnu nákladů, neboť uživatel si pronajme IT zdroje od třetí strany v rámci cloudu tehdy, kdy je potřebuje, aniž by si je musel kupovat a nákladová položka se mu změní z kapitálových na provozní výdaje. Charakter přelomové technologie má Cloud computing i kvůli faktu, že přináší nový způsob dodání výpočetních zdrojů jakožto služby dodávané prostřednictvím sítě, nejčastěji Internetu, jejichž rozsah může být modifikovaný na základě požadavku uživatele. Jedná se díky tomu tak o systém, který není závislý na konkrétním umístění, výpočetní zdroje jsou flexibilní a dovolují tak jejich rychlou a bezproblémovou alokaci na vyžádání. Uživatelé cloudu mají k dispozici virtualizované zdroje, které jsou poskytované ze společného souboru a které mohou být využívány podle rozsahu potřeby společně s dalšími uživateli. Platba je pak následně stanovena v závislosti na využité zdroje poskytovatele uživatelem (viz již dříve zmíněná platební metoda „pay as you go"). Poskytované cloudové služby většinou závisí na komplexním a několikavrstvém propojení mezi několika poskytovateli.[9]

Mezi výhody Cloud computingu patří *snížené náklady na vlastnictví IT infrastruktury a rozložení investic do delšího období*[10], využitím cloudové infrastruktury totiž odpadají náklady na vlastnictví hardwaru a s tím spojené další výdaje včetně rozšiřování kapacit. Tyto klasické fixní náklady jsou nahrazeny pravidelnými odměnami za služby podle vyžitých služeb a rozloženy do delšího období. Cloud dále podporuje *mobilitu a vnitrofiremní komunikaci*[11] tím, že na něm provozované aplikace jsou permanentně dostupné všem zaměstnancům a i jiným pobočkám objednatele prostřednictvím Internetu. Velcí poskytovatelé cloudových služeb mají velice

[8] MELL, Peter, Tim GRANCE,. The NIST Definition of Cloud Computing *Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-145 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2011 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[9] (ed.). Cloud Technologies and Services. MILLARD, Christopher a W Kuan HON. *Cloud Computing Law*. Oxford University Press, 2013, s. 448. ISBN 978-0-19-967167-0, s. 3-4.

[10] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 311.

[11] Tamtéž, s. 311.

sofistikovanou IT infrastrukturu, vyškolené techniky a obrovská zálohovací centra, neboť ztrátu důvěry uživatelů si nemohou dovolit, proto by snad i *bezpečnost dat*[12] měla být v cloudu vyšší než u vlastní IT struktury. Při používání aplikací provozovaných jako cloudové řešení se dá též *zamezit možnosti obchodování s použitým softwarem.*[13]

Bezpečnost dat a systému může však být i součástí problematické části cloudového řešení společně s ochranou osobních údajů, interoperabilitou a určením odpovědnosti mezi poskytovatelem a uživatelem.

Kritické oblasti pro Cloud computing spočívají v roztříštěnosti jednotného digitálního trhu, která vyplývá z odlišných vnitrostátních právních rámců a tím způsobené nejistoty ohledně rozhodného práva. Dále se mohou vyskytovat problémy se smluvní úpravou přenositelnosti dat, jejich kontroly a vlastnictví. Množství norem a jejich nepřehlednost podporuje zmatek a nejistotu ohledně otázky úrovně interoperability formátů dat umožňující jejich přenositelnost.[14]

## 1.1 Modely nasazení cloudu

Cloud computing rozlišujeme podle fyzického umístění jeho jednotlivých technologických prostředků a vlastnictví k nim ze strany jak uživatele tak poskytovatele, či rozsahem těchto technologií, které má uživatel ve vlastnictví či které mu jsou poskytnuty jako služba.

*Privátní cloud* představuje cloudovou infrastrukturu poskytovanou výhradně jediné organizaci s několika uživateli (např. obchodními provozovnami). Tato infrastruktura může být vlastněna, řízena a provozována samotnou organizací, třetí stranou nebo kombinací obou, a může být umístěna i mimo obchodní prostory.[15]

[12] Tamtéž, s. 311-312.
[13] Tamtéž, s. 312.
[14] Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru Regionů: Uvolnění potenciálu cloud computingu v Evropě. COM(2012) 529 final ze dne 27.09.2012. In: *Úřední věstník EU*. EUR-Lex, 2012. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52012DC0529&from=EN
[15] BADGER, Lee, Tim GRANCE, Robert PATT-CORNER a Jeff VOAS. Cloud Computing Synopsis and Recommendations *Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-146 [online]. U.S. Department of Commerce: National Institute of Standards and

Privátní cloud má potenciál přinést organizaci větší kontrolu nad infrastrukturou, výpočetními zdroji a i cloudovými uživateli než u veřejného cloudu.[16]

*Veřejný cloud* naopak poskytuje svou cloudovou infrastrukturu otevřeně pro užití širokou veřejností. Může být vlastněn, řízen a provozován obchodní společností, akademickou institucí nebo vládní organizací či kombinací některých z nich. U veřejného cloudu platí, že je umístěn v prostorách poskytovatele daného cloudu.[17] Jeho infrastruktura a výpočetní zdroje, které cloud tvoří, jsou zpřístupněny veřejnosti přes Internet. Poskytovatel a provozovatel cloudu poskytuje uživatelům cloudové služby a už z definice vyplývá, že stojí vně uživatelské organizace.[18]

*Community cloud* disponuje cloudovou infrastrukturou poskytovanou pro výhradní užití určitého společenství (komunity) uživatelů z organizací, které mají společné zájmy (týkající se například otázky bezpečnostních požadavků, poslání, politiky compliance apod.). Tato infrastruktura může být vlastněna, řízena a provozována jednou nebo více organizací na území daného společenství, třetí stranou, anebo kombinací těchto s tím, že je buď umístěna na nebo mimo prostory dané komunity.[19] Komunitní cloud je víceméně něco mezi privátním a veřejným cloudem přičemž se rozlišuje s ohledem na cíl stanovený uživateli. Tímto se podobá cloudu privátnímu, ale infrastrukturu a výpočetní zdroje sdílí dvě či více entit se stejnými

---

Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

[16] WAYNE Jansen Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, s. 3.

[17] BADGER, Lee, Tim GRANCE, Robert PATT-CORNER a Jeff VOAS. Cloud Computing Synopsis and Recommendations *Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-146 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

[18] WAYNE Jansen Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, s. 3.

[19] BADGER, Lee, Tim GRANCE, Robert PATT-CORNER a Jeff VOAS. Cloud Computing Synopsis and Recommendations *Recommendations of the National Institute of Standards and Technology.* NIST Special Publication 800-146 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

bezpečnostními a regulatorními aspekty, tudíž tímto se podobá spíše veřejnému cloudu.[20]

*Hybridní cloud* je složitějším modelem než ostatní, neboť se skládá z kompozice složené ze dvou nebo více odlišných cloudových infrastruktur (privátní, veřejné nebo komunitní, které zůstávají samostatné jednotky, ale jsou navzájem propojeny standardizovanou nebo patentovanou technologií, která umožňuje přenositelnost dat a aplikací.[21]

I když volba modelu nasazení přináší důsledky pro bezpečnost a soukromí systému, model sám o sobě neurčuje jejich úroveň co se týče jednotlivých nabízených cloudových služeb. Tato míra bezpečnosti a soukromí závisí především na solidnosti bezpečnostních pravidel a ochrany osobních údajů, důkladnosti bezpečnostních kontrol a rozsahu transparentnosti v řízení a správě cloudového prostředí, které vytváří poskytovatel cloudu nebo jsou převzaty nezávisle od organizace provozující cloud.[22]

## 1.2 Distribuční modely cloudu

Stejně jako modely nasazení jsou i distribuční modely důležitým faktorem cloudu. Servisní model, kterému cloud odpovídá, určuje rozsah a kontrolu organizace nad výpočetním prostředím a charakterizuje míru abstrakce jeho užití. Distribuční model může být nasazen jako veřejný cloud anebo kterýkoli z ostatních modelů nasazení.[23] Tři nejznámější a nejpoužívanější servisní modely jsou následující:

[20] WAYNE Jansen Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.p, s. 3.
[21] BADGER, Lee, Tim GRANCE, Robert PATT-CORNER a Jeff VOAS. Cloud Computing Synopsis and Recommendations *Recommendations of the National Institute of Standards and Technology.*
[22] WAYNE Jansen Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, s. 4.
[23] WAYNE Jansen Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing, op. cit., s. 4.

*Infrastructure as a Service* („IaaS“) je model distribuce služeb, kde základní výpočetní infrastruktura serverů, softwaru a síťových zařízení je poskytována jako služba na vyžádání, na které může být vytvořena platforma k vývoji a provádění aplikací. Jeho hlavním účelem je vyhnout se nákupu, skladování a správě základních součástek hardwarové a softwarové infrastruktury a namísto toho získat tyto prostředky jako virtualizované objekty ovladatelné na dálku skrze servisní rozhraní. Uživatel cloudu má celkově značnou volnost ve výběru operačního systému a vývojového prostředí, které má být hostitelem. Všechna bezpečnostní opatření nad rámec základní infrastruktury jsou pak zpravidla prováděna uživatelem cloudu.[24] IaaS se týká relativně nízko-úrovňových funkcí vyžadujících větší sofistikovanost uživatele a jeho odborných znalostí včetně důkladnějšího mikrořízení zdrojů. Nicméně IaaS poskytuje uživateli větší flexibilitu a naprostou kontrolu. Sloučené výpočetní zdroje v IaaS se používají hlavně ke zpracování dat, skladování a síťování či jiným službám připojení. Aplikace určitých právních předpisů týkajících se umístění, zabezpečení dat a nakládání s nimi může být ovlivněna zvláštními opatřeními pro zpracování a ukládání a přenos dat.[25] Poskytovatelé této cloudové služby jsou například Amazon Web Services, Windows Azure, Google Compute Engine, Rackspace Open Cloud, IBM SmartCloud Enterprise či HP Enterprise Converged Infrastructure.[26]

*Platform as a Service* („PaaS”) je distribuční model pro poskytování počítačové platformy jako služby na vyžádání, na které mohou být aplikace jak vyvinuty tak nasazeny. Poskytovatel této služby poskytuje uživateli svůj hardware, operační systém, vývojovou platformu, včetně souvisejících služeb (hosting, dostupnost platformy, upgrade softwaru a další). Záměrem tohoto modelu je snížit náklady a složitost nákupu, skladování a správu podkladových hardwarových a softwarových komponentů platformy, včetně všech potřebných nástrojů na programování a vývoj databáze. Vývojové prostředí je typicky určeno pro zvláštní účely poskytovatelem cloudu a přizpůsobeno návrhu a architektuře své platformy. Cloudový uživatel má kontrolu nad aplikacemi a nastavením aplikačního prostředí platformy. Bezpečnostní opatření sdílí

[24] Tamtéž, s. 4.
[25] (ed.). Cloud Technologies and Services. MILLARD, Christopher a W Kuan HON. *Cloud Computing Law*. Oxford University Press, 2013, s. 448. ISBN 978-0-19-967167-0, s. 5-6.
[26] IaaS Providers List: Comparison And Guide. *Tom'sIT PRO* [online]. [cit. 2016-08-13]. Dostupné z: http://www.tomsitpro.com/articles/iaas-providers,1-1560.html

poskytovatel společně s uživatelem.[27] U PaaS jsou uživatelé ušetřeni potřeby spravovat zpracování surových dat nebo aktivní ukládání zdrojů a mohou se tak zaměřit na programování aplikací, které mají být hostované prostřednictvím dané služby. Hranice mezi IaaS a PaaS může být až nerozeznatelná. Zatímco uživatelé IaaS musí spravovat své vlastní virtuální výpočetní zdroje, PaaS zahrnuje to, co technologové označují jako tzv. vyšší úroveň abstrakce, neboť tato platforma poskytuje integrovanou výpočetní infrastrukturu a programování, obvykle včetně služeb databází a webových serverů. Uživatelé PaaS se nemusí zabývat správou virtuálních a výpočetních zdrojů při nízké úrovni, ale mohou se soustředit na programování aplikačních počítačových programů vyjádřených v podobě zdrojových kódů[28]. Poté, co je počítačový program v podobě kódu dle volby uživatele nasazen na PaaS jako aplikace, ta může být na žádost uživatele spuštěna přes Internet, například jako SaaS. Platforma poskytovatele se automaticky zabývá řízením a vyrovnáváním zatížení výpočetních zdrojů, virtualizovaných i jiných, aby poskytla a měřila aplikace podle potřeby, včetně ukládání dat a replikace.[29] Poskytovatelé PaaS jsou například Engine Yard, Red Hat OpenShift, Google App Engine, Heroku, AppFog, Windows Azure Cloud Services, Amazon AWS, Caspio nebo Mobile App Development Platforms.[30]

*Software as a Service* („SaaS“) je model poskytování služeb, kde jeden nebo více aplikačního softwaru a výpočetní zdroje k jejich spuštění jsou poskytovány pro užití na vyžádání jako služba na klíč. Smyslem této služby je snížit celkové náklady na hardware a vývoj softwaru, jeho údržby a provozu. Bezpečnostní opatření jsou prováděna především poskytovatelem cloudu. Uživatel nespravuje ani nekontroluje základní cloudovou infrastrukturu nebo jednotlivé aplikace kromě preferenčních voleb a

[27] WAYNE Jansen, Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, s. 4.

[28] Zdrojový kód představuje zápis instrukcí počítačového programu v programovacím jazyce. Zdrojový kód následně slouží jako kompilátor, neboli softwarový nástroj, k přeložení do strojového kódu, jenž je souhrnem instrukcí v binárním tvaru a přímo zpracováván počítačem. Zdroj: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 32.

[29] (ed.). Cloud Technologies and Services. MILLARD, Christopher a W Kuan HON. *Cloud Computing Law*. Oxford University Press, 2013, s. 448. ISBN 978-0-19-967167-0, s.12.

[30] PaaS Providers List: Comparison And Guide. *Tom'sIT PRO* [online]. [cit. 2016-08-13]. Dostupné z: http://www.tomsitpro.com/articles/paas-providers,1-1517.html

limitních administrativních nastavení aplikací.[31] SaaS poskytuje sofistikované funkcionality a obecně vyžaduje méně technických znalostí uživatele, ale současně mu nabízí méně kontroly. SaaS nabízí ještě vyšší míru abstrakce než PaaS, navíc se uživatelé nemusí zabývat vytvářením aplikace, neboť využijí tu vytvořenou poskytovatelem. Nasazení základních výpočetních zdrojů, je spravováno poskytovatelem. Někteří SaaS poskytovatelé vystavěli své služby na IaaS nebo PaaS infrastrukturách jiných poskytovatelů, zatímco další zase využívají vlastní fyzickou a softwarovou infrastrukturu. I když uživatelé mohou nastavit předvolby svých SaaS aplikací a kontrolovat, jak je jejich kvóta infrastruktury používána (např. paměťový prostor), jsou omezeni v možnosti přizpůsobit konkrétní aplikaci a nemohou ani kontrolovat, jak poskytovatelé spravují hlavní výpočetní zdroje. Podstatou SaaS služby je používat jedinou funkční aplikaci, která pak slouží vícero uživatelům. Údaje od různých uživatelů mohou být uloženy ve stejné databázi, což přináší potenciální bezpečnostní rizika. Uživatelé se musí spolehnout na SaaS software, který by měl být nastaven tak, aby v něm byla data jednotlivých zákazníků oddělena. Zatímco SaaS aplikace často pocházejí od poskytovatele této služby, může se stát, že jsou na infrastruktuře poskytovatele, nebo na privátním cloudu pro interní použití, nainstalovány aplikace třetích stran, které jsou nabízeny jako služba.[32] SaaS je nejčastěji používaný typ cloudové služby, zejména mezi spotřebiteli. Systém totiž umožňuje uživatelům získat aplikační software rychle, aniž by museli instalovat specifický software. Podle průzkumu byly v předešlých letech nejčastější SaaS aplikace email, zálohování, obnovení po ztrátě, úschovna a web hostingové služby.[33] Poskytovateli SaaS modelu jsou SaaS Customer Service Providers, SaaS Office Suite Providers (pod něž patří například Google Apps for Business a Microsoft Office 365), SaaS Project Management Providers, SaaS Help Desk Providers, SaaS Network Monitoring Buyer's Guide, SaaS IT Security Buyer's Guide, SaaS Application Monitoring Buyer's Guide.[34]

[31] WAYNE Jansen, Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, s. 4.
[32] (ed.). Cloud Technologies and Services. MILLARD, Christopher a W Kuan HON. *Cloud Computing Law*. Oxford University Press, 2013, s. 448. ISBN 978-0-19-967167-0, s.13.
[33] (ed.). Cloud Technologies and Services. MILLARD, Christopher a W Kuan HON. *Cloud Computing Law*. Oxford University Press, 2013, s. 448. ISBN 978-0-19-967167-0, s.5.
[34] SaaS Providers List: Comparison And Guide. *Tom'sIT PRO* [online]. [cit. 2016-08-13]. Dostupné z: http://www.tomsitpro.com/articles/saas-providers,1-1554.html

Právě Google Apps a Microsoft Office aplikace budou obsahem třetí kapitoly a úprava ochrany osobních údajů u těchto poskytovaných smluv předmětem analýzy. Blíže k SaaS z právního hlediska v druhé kapitole.

## 1.3 Právní rámec Cloud computingu

Ochrana a dispozice s počítačovými programy jsou obsaženy v autorském zákoně, občanském zákoníku v rozsahu úpravy licenčních smluv a směrnici 2009/24/ES. Podle směrnice 2009/24/ES se softwarem rozumí počítačový program v jakékoli formě, které jsou součástí technického vybavení (tj. hardwaru). Pod pojem software spadají i přípravné koncepční práce, které vedou k vytvoření počítačového programu za podmínky, že jejich povaha umožní vytvoření takového programu. Ochrana autorským právem (zákon č. 121/2000 Sb., zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) se dotýká jen výsledného vyjádření počítačových programů a neuplatní se vůči myšlenkám a zásadám, na nichž jsou jednotlivé prvky programu založeny včetně myšlenek a zásad jednotlivých rozraní. Podle občanskoprávní úpravy (zákona č. 89/2012 Sb., občanský zákoník) je software tzv. jinou věcí bez hmotné podstaty.[35]

Autorská práva k softwaru nabývá programátor nebo každý člen z týmu programátorů, pokud se jedná o zakázku IT firmy, která vývoj daného softwaru iniciovala, vedla a financovala. Autorská práva jsou nepřevoditelná, což však nevylučuje převod výkonu těchto práv. U případu vypracované zakázky IT firmou dochází ze zákona k přenosu výkonu autorských práv z jednotlivých programátorů na danou IT firmu. Autorská práva se rozdělují na osobnostní a majetková. Osobností jsou vázána na osobnost autora softwaru (např. programátora), který se jich nemůže vzdát a ani je nemůže převést na jinou osobu, může však dát souhlas k zásahu do nich (viz níže např. u open source softwaru). Mezi osobnostní autorská práva patří právo na zveřejnění, právo osobovat si autorství nebo právo na nedotknutelnost (což může být opsáno také jako právo udělit souhlas se změnou softwaru, například zásahem do zdrojového kódu). Majetková autorská práva jsou spojena s majetkovými dispozicemi

[35] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 31-32.

se softwarem. Základem majetkových práv je právo užít software nehledě na to, zda samotným programátorem nebo jinou osobou. Autorský zákon stanovuje, že mezi způsoby užití patří právo na rozmnožování (tj. vytváření kopií softwaru), právo na rozšiřování rozmnoženiny (tj. uvádění kopií softwaru na trh), právo na pronájem rozmnoženiny (čímž může být úplatné poskytnutí časově omezené licence), právo na půjčování rozmnoženiny (tj. bezúplatné licencování) anebo právo na sdělování softwaru veřejnosti (čímž se myslí například zpřístupnění softwaru na Internetu). Tento výčet způsobů užití softwaru není taxativní, a není proto vyloučena možnost užít software i jiným způsobem (například formou SaaS).[36] Autorský zákon stanovuje v § 66 omezení, která se vztahují na práva autora nebo vykonavatele majetkových práv softwaru. Mezi zásah do autorských práv programátorů nebo IT firem, které software licencují, nepatří jednání oprávněného uživatele, pokud jedná za účelem zajištění běžného provozu softwaru, dosažení interoperability s dalším softwarem nebo zkoumání podstaty funkčnosti (jeho interpretace).[37]

Software je možno licencovat (tj. udělit právo užít software) anebo převést výkon majetkových práv k němu. U licencování softwaru dochází k jeho prodeji či bezúplatnému šíření rozmnoženiny, která je nedílnou součástí licence. Při užití softwaru dochází k vzájemnému propojení softwaru a hardwaru, proto dokumentace k softwaru obsahuje často minimální požadavky ohledně hardwaru. Pokud je dodavatel softwaru zároveň dodavatelem hardwaru (což je převážně server) nebo pokud odpovídá i za serverovou infrastrukturu, odpovídá pak i za splnění daných požadavků. Počítačový program stejně jako jeho jednotlivé části je chráněn jako dílo literární podle autorského zákona a směrnice 2009/24/ES. Týká se to jak dokončeného softwaru tak jeho jednotlivých vývojových fází a částí. Ochrany požívají i samotné výstupy softwaru jako jsou například data v podobě databáze[38], jeho vzhled nebo název.[39]

[36] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 40-42.
[37] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT, op. cit., s. 43-45.
[38] Databáze je z pohledu autorského zákona souborem dat, údajů nebo jiných prvků (např. fotografií, grafických prvků apod.), které jsou systematicky nebo metodicky uspořádány. Databáze jsou buď součástí softwaru nebo jeho výstupem. Za předpokladu, že je databáze součástí softwaru, je potřeba udělit licenci i dané databázi. Zdroj: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 49.

Cloud computing představuje novou formu outsourcingu IT zdrojů (pokud se samozřejmě nejedná o vlastní cloudovou infrastrukturu, kterou si majitel spravuje nezávisle sám), která se od tradičního outsourcingu v některých aspektech liší. Co se týče SaaS, tam je outsourcovaným zdrojem aplikační software, u IaaS je to výpočetní hardware (servery, úložiště apod.) a u PaaS to jsou hardware a vývojářská a hostingová software platforma. Existuje však několik klíčových rozdílů mezi tradičním outsourcingem a Cloud computingem. Navíc problematickou oblastí je i právní úprava, kdy dosavadní zákony upravující tradiční outsourcing IT služeb či samostatných databází nejsou aplikovatelné na cloudové služby, neboť nezohledňují rozdílnost služeb a jejich jednotlivých vrstev a vysokou míru abstrakce. Zásadní rozdíly mezi těmito dvěma způsoby dodání IT služeb spočívají v míře aktivní participace uživatele při zpracování dat, časovém postupu zapojování subdodavatelů nebo standardizaci cloudových služeb (zejména u veřejných cloudů) a míře kontroly a přizpůsobení služby prováděné uživatelem podle úrovně dané abstrakce a vrstvení. Na rozdíl od tradičního outsourcingu se poskytovatelé cloudové infrastruktury aktivně nezapojují do zpracování dat uživatele, jen pasivně poskytují zdroje, na kterých je uživatel ukládá, z kterých je může kdykoli vyjmout, a které také užívá ke zpracování dat na samoobslužném principu. V otázce služeb subdodavatelů se tradiční outsourcing liší od cloudu tím, že se subdodavatelé zapojují až po uzavření smlouvy mezi poskytovatelem a uživatelem, zatímco u cloudu má poskytoval zpravidla předem nakontraktované své subdodavatele, zejména v případě SaaS služeb poskytovatele IaaS či PaaS podle míry vrstvení. Cloudové služby se také liší od těch tradičních tím, že jsou většinou poskytovány ve standardizované formě jako finální produkt, který si uživatel už nemůže měnit podle vlastních požadavků s výjimkou privátních cloudů, které nabízejí velký prostor pro individuální úpravy.[40] Co se týče kontroly uživatelů nad jednotlivými zdroji a kapacitami poskytovanými v rámci cloudové služby, tabulka (viz Obrázek 1 níže) pracovní skupiny Cloud Security Aliance vyjadřuje nejlépe míru kontroly a tím i odpovědnosti uživatele v závislosti na modelu služby veřejného cloudu.

---

[39] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 32-35.

[40] HON, W Kuan a Christopher MILLARD. *Cloud Computing vs Traditional Outsourcing – Key Differences* [online]. Computers & Law, Vol. 23, Issue 4, 2012 [cit. 2016-08-15]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200592, s. 3.

Obrázek 1[41]: Rozdělení kontroly nad zdroji podle typu služeb

| Service owner | SaaS | PaaS | IaaS |
|---|---|---|---|
| Data | Joint | Tenant | Tenant |
| Application | Joint | Joint | Tenant |
| Compute | Provider | Joint | Tenant |
| Storage | Provider | Provider | Joint |
| Network | Provider | Provider | Joint |
| Physical | Provider | Provider | Provider |

Jak vidíme v grafickém znázornění, model SaaS umožňuje sdílenou kontrolu nad daty a aplikací, ale nad výpočetními zdroji, úložišti, sítí a fyzickou infrastrukturou cloudu připisuje kontrolu jen poskytovateli. U PaaS má výlučnou kontrolu nad daty uživatel (nájemce), který dále sdílí kontrolu s poskytovatelem nad aplikací a výpočetními zdroji. Úložiště, síť a fyzickou infrastrukturu má pak pod dohledem jen poskytovatel. Model služby IaaS následně nabízí uživateli výlučně kontrolovat a odpovídat za data, aplikaci a výpočetní kapacity, dále sdílet kontrolu s poskytovatelem nad úložištěm a sítí a posledně poskytovateli samostatně dohlížet jen nad fyzickou infrastrukturou cloudu.

Z právního hlediska uchopit Cloud computing není tak jednoduché. Mezi poskytovatelem a uživatelem dochází ke vzniku závazkového vztahu podle soukromoprávní úpravy, který však nemá konkrétní podobu mezi smluvními typy. Smlouva o poskytování cloudových služeb bude proto inominátní, nepojmenovanou, smlouvou (podle § 1746 zákona č. 89/2012 Sb.), ve které si strany musí konkrétně stanovit práva a povinnosti (včetně otázky vlastnického práva k hmotnému majetku jako je například fyzická infrastruktura, předměty práv duševního vlastnictví a oprávnění k jejich užití, dále ochrany osobnosti a osobních údajů v souvislosti se zpracováním dat, náhrady škod při vzniku škodné události či základních elementů závazkových vztahů jako je jejich vznik, zánik a změna).

[41] HON, W Kuan a Christopher MILLARD. *Cloud Computing vs Traditional Outsourcing – Key Differences,* op. cit., s. 4.

Vztah mezi poskytovatelem a uživatelem (označován také jako objednatel) se může vyskytnout ve třech formách, a to i) kdy je objednatel fyzickou osobou nepodnikatelem, ii) podnikatelem nebo iii) podnikatelem, který nabízí cloudové služby třetím osobám. V případě, kdy je uživatel nepodnikatelem, a je tedy i koncovým uživatelem, vzniká smlouva mezi poskytovatelem a danou fyzickou osobou, která se dostává do pozice spotřebitele. Podmínky vzniku smlouvy na dálku prostřednictvím elektronických prostředků jsou v tomto případě upraveny spotřebitelským právem, které zajistí ochranu slabší strany spotřebitele tím, že stanoví povinnosti týkající se poskytování informací, nepřípustnosti ustanovení znevýhodňující spotřebitele aj. Typickým příkladem objednatele fyzické osoby je uživatel SaaS aplikací Google Apps. V jiné situaci, kde je objednatel podnikatelem, který využívá cloudové služby pro vlastní účely, je též i koncovým uživatelem. Tento scénář je nejvyužívanějším a nejzajímavějším modelem, blíže k němu v následující kapitole. A v posledním případě je objednatelem podnikatel, který užívá služby Cloud computingu a jejich výstupy ve formě nějakého produktu či služby nabízí třetím osobám, kteří teprve figurují jako koncoví uživatelé. Příkladem je situace, kdy objednatel vytvoří na vývojové platformě PaaS aplikaci a začne umožňovat SaaS přístup k této aplikaci koncovým uživatelům. Ve vztahu k zákazníkům by si měl objednatel ošetřit otázku autorských práv a možnosti zpřístupnění, odpovědnosti za škodu způsobenou například nedostupností služby či ztrátou či poškozením dat apod.[42]

Na vztahy vznikající v cloudovém prostředí se budou muset uplatnit i instituty zvláštních právních odvětví jako ochrana práv duševního vlastnictví, a to především autorskoprávní ochrana počítačových programů (softwaru) a databází aj., podle ustanovení § 65 a násl. a § 88 a násl. autorského zákona a oprávnění k jejich užití formou licenčních smluv podle § 2358 a násl. občanského zákoníku a ochrana průmyslového vlastnictví v podobě ochranných známek nebo patentového práva apod. Součástí cloudového rozhraní jsou také služby hostingu, jehož podoba se bude lišit podle jednotlivých modelů cloudového řešení (IaaS, PaaS, SaaS). Hosting je zpravidla standardizovanou službou a smluvní dokumentace mezi datovým centrem a uživatelem

[42] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 314.

bývá postavena na koncepci *„hostingové smlouva + obchodní podmínky“*[43]. Při zpracovávání dat se samozřejmě také vyskytuje otázka jejich přenosu a ochrany, ať už se to týká osobních údajů, citlivých osobních údajů, citlivých obchodních údajů či údajů chráněných zvláštními právními předpisy jako je například bankovní tajemství, státní tajemství, či údajů podléhajících mlčenlivosti lékařů, advokátů aj. V těchto případech je uživatel povinen uvážit, zda poskytované cloudové řešení nabízí konformní a dostatečná bezpečnostní opatření. Ochraně osobních údajů v cloudovém modelu SaaS se dále věnuje třetí kapitola práce.

### 1.3.1 Právní úprava a regulace cloudových služeb na úrovni EU

V současné době není Cloud computing sám o sobě upraven žádným právním aktem. Jeho jednotlivé aspekty však spadají podle unijní legislativu v oblastech například práv duševního vlastnictví, jak již zmíněno, elektronických komunikací, ochrany osobních údajů, ochrany spotřebitele a mnoho dalších. Cloud computing je však předmětem tzv. soft law Evropské unie (EU), kde se jeho problematice věnuje hned několik pracovních skupin.

Dokument Evropské komise *Uvolnění potenciálu cloud computingu v Evropě*[44] z roku 2012 je základním kamenem strategie v oblasti Cloud computingu v EU a slouží i jako podklad pro další iniciativy. Toto sdělení navrhovalo klíčové kroky s cílem podpořit na jedné straně rozvoj norem, technických specifikací a certifikačních systémů, na druhé straně vytvořit bezpečné a spravedlivé smluvní podmínky, včetně podmínek týkajících se dispozice a ochrany osobních údajů a posledně podpořit přijetí cloudového řešení ze strany široké veřejnosti.[45] Těmto jednotlivým úsekům se věnují jednotlivé pracovní skupiny.

---

[43] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 327.

[44] Sdělení Komise Evropskému Parlamentu, Radě, Evropskému Hospodářskému A Sociálnímu Výboru A Výboru Regionů Č. COM(2012) 529 Final: Uvolnění Potenciálu Cloud Computingu V Evropě. In: *Úřední věstník EU*. EUR-Lex, Brusel, 2012. Dostupné také z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:CS:PDF

[45] DAVIES, Ron. Computing: An overview of economic and policy issues. In: *European Parliamentary Research Service* [online]. European Parliament, 2016, s. 23 [cit. 2016-08-15]. ISBN 978-92-823-9206-5.

*Cloud Select Industry Group on Service Level Agreements Subgroup*[46] (C-SIG SLA) je jednou z nich, která pracovala na rozvoji standardizačních pokynů pro dohody o garantované úrovni služeb (SLA) mezi poskytovatelem a uživatelem cloudových řešení. V červnu 2014 skupina dokončila svou práci a připravila pokyny pro cloudové SLA *(Cloud Service Level Agreement Standardisation Guidelines)*[47], které obsahují standardizované parametry pro cloudové služby, zejména v oblasti jejich výkonnosti, bezpečnosti, správy dat nebo ochrany osobních údajů..

Protože v rámci iniciativy o uvolňování potenciálu Cloud computingu byla vyjádřena podpora i certifikačním systémům, vytvořila se pod skupinou C-SIG podskupina pro certifikaci *Subgroup on Certification Schemes (SIG-Cert)*[48] , která byla založena s podporou agentury European Union Network and Information Security Agency (ENISA). SIG-Cert a ENISA společně vytvořily seznam dobrovolných certifikačních systémů pro cloudová řešení (cloud computing certification list, CCSL[49]), čímž zajistily potenciálním uživatelům větší přehled o certifikačních systémech a o tom, jak souvisejí s cloudovými řešení.

V neposlední řadě je třeba zmínit i pracovní skupinu *Cloud Select Industry Group on Code of Conduct*[50], ve které výbory na digitální záležitosti Evropské komise spolupracují s těmito expertními složkami, aby vypracovaly kodex chování pro poskytovatele služeb Cloud computingu (Data protection Code for Conduct for Cloud Services Providers). Kodex má podporovat jednotné uplatňování pravidel v oblasti ochrany osobních údajů ze strany poskytovatelů cloudových služeb. Kodex je od listopadu 2015 přepracováván podle připomínek předložených pracovní skupinou

---

Dostupné z: http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf, s.17.

[46] Cloud Select Industry Group on Service Level Agreements. *DIGITAL SINGLE MARKET* [online]. European Commission [cit. 2016-08-15]. Dostupné z: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-service-level-agreements

[47] Dostupné z: https://ec.europa.eu/digital-single-market/en/news/cloud-service-level-agreement-standardisation-guidelines

[48] Cloud Select Industry Group on Certification Schemes (SIG - Cert). *DIGITAL SINGLE MARKET* [online]. European Commission [cit. 2016-08-15]. Dostupné z: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-certification-schemes

[49] Dostupné z: https://resilience.enisa.europa.eu/cloud-computing-certification

[50] Cloud Select Industry Group on Code of Conduct. *DIGITAL SINGLE MARKET* [online]. European Commission [cit. 2016-08-15]. Dostupné z: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct

zřízenou na základě čl. 29 Směrnice o ochraně osobních údajů (Article 29 Working Party)[51].

Pracovní skupina Article 29 Working Party vydává řadu stanovisek a doporučení k jednotlivým oblastem. Mezi ta týkající se Cloud computingu, a která jsou relevantní pro tuto práci, patří Stanovisko 02/2015 o kodexu chování pro Cloud computing pracovní skupiny C-SIG (Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing)[52], Stanovisko 5/2012 o Cloud computingu (Opinion 05/2012 on Cloud Computing)[53] a Stanovisko 8/2010 o rozhodném právu (Opinion 8/2010 on applicable law)[54].

V červnu 2013 Komise dále zřídila expertní skupinu na smluvní ujednání cloudových služeb (Expert Group on Cloud Computing Contracts)[55]. Skupina odborníků byla založena s cílem pomoci Komisi při stanovování právních aspektů bezpečných a spravedlivých všeobecných smluvních podmínek používaných poskytovateli cloudových služeb pro spotřebitele a malé firmy. Výstupy probíhaly formou krátkých pracovních dokumentů v otázce přenosu dat v případě ukončení smluvního vztahu, kontroly a použití obsahu, odpovědnosti, dostupnosti služby, zpřístupnění a integrity dat, přesunu údajů v rámci cloudu, auditu a oznamovacích povinností poskytovatele cloudu, sjednávání subdodavatelů, nepříznivých podmínek v cloudových smlouvách, změn cloudových smluv, umístění dat a jejich bezpečnosti, odpovědnosti za nedodržení podmínek ochrany údajů či informační předsmluvní povinnosti.

A nakonec v oblasti závazkových vztahů Cloud computingu lze zmínit Návrh Směrnice Evropského Parlamentu a Rady o některých aspektech smluv o poskytování digitálního obsahu z roku 2015, který má plně harmonizovat soubor základních pravidel týkajících se smluv o poskytování digitálního obsahu, do něhož spadá mimo jiné ukládání do cloudu. Směrnice by měla obsahovat pravidla týkající se souladu digitálního obsahu se smlouvou, případně prostředky nápravy pro spotřebitele, pokud

[51] Více informací dostupné z: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm
[52] Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf
[53] Dostupné z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf
[54] Dostupné z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf
[55] Expert Group on Cloud Computing Contracts. *JUSTICE* [online]. European Commission [cit. 2016-08-15]. Dostupné z: http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm

by došlo k jejich nesouladu, dále právních aspektů práva ukončit dlouhodobou smlouvu a změnit digitální obsah.[56]

[56] Návrh Směrnice Evropského Parlamentu A Rady o některých aspektech smluv o poskytování digitálního obsahu č. COM(2015) 634 final. In: *Úřední věstník EU*. EUR-Lex, Brusel, 2015. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52015PC0634&from=EN

# 2 SaaS jako forma cloudových služeb

Software as a Service se stal základním modelem Cloud computingu. Předcházel mu však jiný nadějný model, Application Service Providing (ASP), který spočíval v provozování aplikací ve vzdáleném datovém centru poskytovatelem, k němuž měl objednatel přístup pomocí Internetu nebo virtuální privátní sítě (VPN). I u tohoto modelu poskytovatel nabízel komplexní zajištění provozu aplikací, včetně samotné aplikace, IT infrastruktury a další služby nezbytné pro zajištění dostupnosti aplikace. V modelu ASP je poskytována jedna standardizovaná aplikace v režimu one-to-many, což znamená, že více koncových uživatelů sdílí jednu a tu samou aplikaci. Model je tím tak velice úsporný pro poskytovatele a schopný nabídnout nižší ceny zákazníkům, ale z hlediska uživatele je limitující, neboť skoro nedovoluje tzv. customizaci (tj. přizpůsobení aplikace podle požadavků konkrétního zákazníka). Tento pojem byl proto téměř bez výjimky nahrazen pojmem Cloud computing, potažmo SaaS.[57] Na rozdíl od ASP lze SaaS využít jak na poli aplikačního tak systémového softwaru, právě kvůli minimální míře customizace ASP. Pro oba modely je však často používán pojem hostovaný software, neboť software je umístěn na serverech poskytovatele, který zároveň provádí jeho správu a údržbu a poskytuje licenci k jeho užívání. Jak již zmíněno, ani na jeden model se nedá vztáhnout konkrétní smluvní typ dle našich právních předpisů. Protože se jedná o virtuální služby, kde předmětem vztahu je závazek poskytovatele zpřístupnit infrastrukturu a software objednateli, a nikoli jeho nájem konkrétních serverů v konkrétním housingovém centru, nemůže se jednat o nájem[58] jako smluvní typ. V českém právu se tedy vztah mezi poskytovatelem a objednatelem bude upravovat inominátní smlouvou, jejímž předmětem je zmiňovaný závazek poskytovatele zpřístupnit příslušný software, udělit příslušná oprávnění k jeho

[57] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 308.

[58] Srov. s rozhodnutím německého Spolkového soudního dvora XII ZR 120/04, který stanovil, že pro model ASP je nájemní smlouva použitelným smluvním typem. Soud se ve svém tvrzení opřel o výklad předmětu závazkového vztahu vyplývajícího z ASP smlouvy ve smyslu, že software pokládá za hmotnou věc, neboť na jeho poskytování se aplikuje kupní smlouva. Z tohoto titulu je předmětem závazku přenechání užívání softwaru prostřednictvím Internetu. Vychází z toho, že za software považuje ten, co není vytvořen na objednávku, tedy standardní software, který je zachycen na hmotném nosiči. V tomto kontextu je tedy vlastníkem standardního softwaru poskytovatel, a pronajímá jej objednateli, aniž by záleželo na tom, zda ten jím skutečně disponuje či nikoli. Dostupné z: http://lexetius.com/2006,3202

užívání (licenci), tam, kde to připadá do úvahy, a zajistit jeho dostupnost. Co se týče garance dostupnosti služeb, je nezbytné ve smlouvě uzavřít i SLA (Service Level Agreement), případně též SSLA (Security Service Level Agreement), která by se měla dotýkat bezpečnostních opatření a garance s ohledem na citlivost dat uložených v cloudu. Závazkem objednatele je pak zaplatit sjednanou cenu za danou službu, přičemž modelů stanovení ceny a platby této ceny je mnoho, u cloudových řešení je však obecným principem stanovení ceny a její platba v závislosti na faktickém využívání služeb.[59]

## 2.1 Základní náležitosti smlouvy o poskytování SaaS

Smlouva o poskytování softwaru jako služby (SaaS) obsahuje buď v jednotlivých svých ustanoveních, nebo jako doplněná o smluvní dokumentaci ve formě příloh smlouvy, vedle jiných popis činností poskytovatele (scope/statement of work), dohodu o garantované úrovni služeb (SLA), platební podmínky (payment terms), politiku ochrany soukromí (privacy policy), dohodu o postupování při ztrátě dat (disaster recovery), technické specifikace pro podporu softwarových služeb (support services), specifikace subdodavatelů s uznáním jejich odpovědnosti (contractor agreement and certification), a případně i pojistné krytí (insurance coverage).

Mezi hlavní náležitosti smlouvy o poskytování softwaru jako služby patří *úvodní ustanovení*, kde se stanoví smluvní strany a nadefinují se pojmy používané v textu smlouvy, případně se v rámci těchto ustanovení vyskytne preambule (tzv. recitals), ve které strany prohlásí záměr a důvod pro uzavření dané smlouvy.

Dále následuje vymezení *předmětu smlouvy*, což je, jak z názvu smlouvy vyplývá, poskytování softwaru jako služby. V rámci těchto ujednání se vymezí souhrn a rozsah služeb ze strany poskytovatele za sjednání protiplnění ze strany objednatele ve formě platby. Tento seznam činností by měl být konkrétní, a jednoznačně by měl korelovat s ujednanou cenou, výčet by však neměl být taxativní, aby se předešlo situacím, kdy poskytovatel je povinný poskytnout jen činnosti uvedené ve smlouvě a

[59] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 315.

v případě potřeby tak není povinen poskytnout sužbu nad rámec tohoto seznamu. V takových případech by jen záleželo na vůli smluvních stran či výkladových pravidel, které si sjednají pro tuto smlouvu.[60]

Další ustanovení výše již zmíněné se týká *popisu práce* (statement of work), které slouží pro specifikaci činností vykonávaných poskytovatelem v souvislosti s poskytováním služby. Má charakter podrobného plánu týkajícího se zejména činností poskytovatele v rámci počáteční implementace, je-li možná, tzn. před poskytnutím hlavní služby. Míra specifikace požadované v popisu práce se bude odvíjet od množství zdrojů, služeb a nástrojů, které poskytovatel potřebuje k realizaci hostovaného systému. V případě, kdy SaaS aplikace nevyžaduje konverzi dat, počáteční upload, konfiguraci sítí a sestav či uživatelskou odbornou přípravu, bude stačit v ustanoveních sjednat splátkový kalendář, stručný implementační plán, kde probíhá implementace a akceptační kritéria.[61]

Mezi klíčová ustanovení patří i *rozsah uživatelů*, respektive oprávněných osob objednatele k užívání poskytované služby v rámci rozsahu licence objednatele. Ve smlouvě a objednávkovém formuláři se tak prvně vymezí prvotní okruh autorizovaných uživatelů na straně objednatele, kterým je služba a přístup poskytován v rámci objednatele souvisle za stejnou cenu stanovenou poměrně k délce užívání, ale zpravidla se upravuje i případná změna jejich počtu. Objednatel je oprávněn požádat o navýšení kapacity v souvislosti s navýšením počtu autorizovaných uživatelů nad sjednaný smluvní limit formou dodatečného objednávky v rámci konkrétní licence objednatele.[62]

V otázce úpravy rozsahu úrovně poskytovaných služeb je jednoznačně nejdůležitější součástí smluvní dokumentace SaaS *smlouva/dohoda o garantované úrovni služeb* (SLA). Základem této smlouvy je definice garance rozsahu, úrovně a intenzity poskytovaných služeb společně s monitoringem a měřením sjednaných

[60] GUTH, Stephen. *Contract Negotiation Handbook: Software As a Service*. Guth Ventures LLC, 2013, 250 s. ISBN: 0988830809.
[61] Exhibit X – Statement Of Work for Software as a Service Contracts, Contract For City of Seattle (vzor). Dostupné z: http://cdn.ttgtmedia.com/searchSecurity/downloads/SAASSOW.pdf
[62] Master SubscriptionAgreement Salesforce.com, Dostupné z: http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf

parametrů na proaktivní a průběžné bázi. Součástí smlouvy je požadavek na dosažení určité úrovně dostupnosti. Dostupností se myslí stav, kdy jsou sjednané funkce k dispozici objednateli ve sjednané míře a kvalitě. V otázce dostupnosti je klíčová úprava toho, jak se tato vypočítává a co se do ní zahrnuje. U SLA pro výpočet dostupnosti známe tzv. tvrdé a měkké metriky. Mezi ty tvrdé patří a) dostupnost služeb softwaru vyjádřená v procentech jako poměr času plné dostupnosti k době užívání softwaru, b) průměrná a mezní doba odezvy na požadavek uživatele při sjednaném způsobu zatížení softwaru, či c) doba odstranění incidentu stanovená v hodinách. Mezi měkké metriky řadíme např. akceptaci, protokoly, zápis, potvrzení a hodnocení realizovaného školení. V souvislosti s dostupností se v SLA zpravidla stanovuje tzv. servisní úroveň, jež má tři úrovně (standardní servisní úroveň – dostupnost 98%, minimální servisní úroveň – dostupnost 95%, motivační servisní úroveň – dostupnost 99% a vyšší). Pokud SLA uvádí 99,9% dostupnost, fakticky to ale neznamená skutečných 99,9%. Do úrovně dostupnosti se totiž započítávají i situace jako stoprocentní plnění, i když je v nich software fakticky nedostupný[63].[64]

Předmětem smlouvy SLA je závazek poskytovatele vyvíjet činnosti tak, aby zajišťoval po celou dobu trvání smlouvy garantovanou úroveň služeb a dostupnosti. Z hlediska technické specifikace úrovně dostupnosti se dají měřit a vyjádřit například servisní parametry, jako doba reakce na nahlášený incident a doba odstranění vady, procentuální poměr reklamací skutečných vad k ostatním požadavkům na podporu, doba odezvy jednotlivých funkcí aplikačního softwaru a rychlost zpracování dat, nebo dostupnost celého aplikačního nebo systémového softwaru, přičemž při výpočtu dostupnosti jsou jednotlivým parametrům přiděleny priority podle jejich důležitosti v rámci IT procesů objednatele. Dalšími důležitými body, které musí být v smlouvě upraveny v otázce měření úrovně dostupnosti, jsou období, za jaká se úroveň měří (kalendářní týden, měsíc, rok či jiné) a provozní doba. Garantovaná úroveň dostupnosti je zpravidla zaručena jen na tuto dobu (stanovenou v časovém rozmezí). U

[63] Jedná se např. o situace, kdy poskytovatel provádí údržbu a nastavení v předem sjednaných termínech, což označujeme jako odstávku nebo servisní okno. U těchto by mělo být smluvně stanoveno, zda a případně v jaké lhůtě je poskytovatel povinen ohlásit využití servisního okna. Dále případy, kdy výpadek je zaviněn objednatelem nebo jinými dodavateli služeb, softwaru či hardwaru relevantními pro fungování softwaru, jehož dostupnost poskytovatel zajišťuje.

[64] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 299-300.

sofistikovanějších systémů se může také smluvně stanovit způsob, jakým bude poskytovatel dokládat svá měření. Výjimkou z úrovně dostupnosti jsou tzv. výluky[65]. [66]

Při tak rychlém vývoji v IT oblasti je u poskytování softwarových služeb těžké udržet požadované úrovně dostupnosti bez průběžných úprav a rozvoje, což se vztahuje i na aplikační software. Pokud by tomu tak nebylo, hrozilo by, že poskytovatel nebude schopen dostát svému závazku zajistit sjednanou úroveň dostupnosti. Toto tzv. změnové řízení, v rámci něhož probíhá sjednávání uvedených změn, je čtyřfázové. Žádost o změnu jedné ze smluvních stran se vyhodnotí a rozhodne se o požadavcích na změnu, pokud nejsou požadavky na změnu dostatečně odůvodněny a zdokumentovány, může rozhodnutí předcházet výzva na doplnění odůvodnění a podkladů. Ve finále následuje samotná realizace nebo odmítnutí požadované změny druhou smluvní stranou. U zásadnějších změn se může vypracovat i případová studie změny. Povinnost poskytovatele konzultovat a doporučovat objednateli vývojové změny je uvedena buď přímo v předmětu smlouvy nebo vyplývá z účelu smlouvy. Poskytovatel by měl tedy proaktivně provádět analýzy bezpečnostních rizik a analýzy strategického rozvoje IT infrastruktury objednatele a navrhovat případné změny a vylepšení softwaru. S těmito povinnostmi je spjata povinnost vést dokumentaci změnového řízení. Odmítnutí požadavku na změnu lze také smluvně upravit jako výpovědní důvod smlouvy.[67]

Smlouva SLA má povahu dlouhodobého závazku a smlouva se tedy uzavírá buď na dobu určitou s tím, že smlouvu nelze vypovědět, ledaže si to strany výslovně dohodnou, nebo na dobu neurčitou, přičemž lze smlouvu vypovědět i bez udání důvodu a smluvní strany si dohodnou konkrétní podmínky, stejně jako pro odstoupení od smlouvy, buď zákonné nebo smluvní. Velice důležitým aspektem smluvní úpravy je otázka povinností smluvních stran v případě výpovědi nebo odstoupení od smlouvy. Z perspektivy objednatele je při ukončení smluvního vztahu s poskytovatelem zásadní přechod k novému poskytovateli, a aby tento přechod byl plynulý a nový poskytovatel

[65] Výluky se nezapočítávají do měření úrovně dostupnosti a mohou jimi být například odstávky, tj. sjednaná občasná vyřazení systému z provozu, pravidelné vyřazení z provozu poskytovatelem ve sjednaných časech, změnová okna např. za účelem updatu softwaru, výpadky systému způsobené vadami technických zařízení či softwaru třetích stran, výpadky způsobené objednatelem v důsledku jím prováděných změn nastavení systému a jiných zásahů do systému, výpadky zapříčiněné průnikem virů do systému, výpadky zapříčiněné objednatelem nebo třetí stranou kvůli neposkytnutí součinnosti, či výpadky zapříčiněné okolnostmi vylučující odpovědnost apod.

[66] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 302-303.

[67] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 306.

převzal garance úrovně dostupnosti přijatelné pro objednatele. S tímto souvisí smluvní vymezení povinností poskytovatele týkající se předání pokynů a poskytnutí součinnosti novému poskytovateli. Nesplněním těchto povinností by mohl vzniknout objednateli nárok na smluvní pokutu nebo náhradu škody.[68]

Mezi další obsahové náležitosti SLA patří smluvní úprava ujednání o autorských právech, jak je již zmíněno v obecném právní popisu, cenových a platebních podmínkách, definic vad a stanovení reakčních dob a dob odstranění a případně sankcí, formy notifikace poskytovatelem, součinnosti smluvních stran, projektového řízení, mlčenlivosti a způsoby ukončení smlouvy.

Mezi další základní náležitosti smlouvy o poskytování softwaru jako služby patří *právo užívání softwaru,* který je umístěn na serverech poskytovatele. Protože u SaaS řešení se objednatel nezabývá otázkou hardwaru, je to poskytovatel, který za něj plně odpovídá. Právo užívání je zásadně umožněno udělením licence. [69] Někteří poskytovatelé však neposkytují licencování softwaru, aby se vyhnuli případným souvisejícím rizikům. Namísto toho nabízejí open source software, u kterého vyloučí odpovědnost za porušování práv k duševnímu vlastnictví. Uživatelé mohou požadovat po poskytovatelích záruku, že aplikační software jim poskytovaný v cloudu neporušuje žádná práva duševního vlastnictví třetích osob pod sankcí odškodnění. Pro zajištění odpovědnosti za právní vady může uživatel požadovat rozšíření odpovědnosti a záruky na všechny subdodavatele, kteří participují na dodání poskytované služby za to, že jimi poskytované služby neporušují práva duševního vlastnictví třetích osob. Někteří poskytovatelé se omezují na poskytnutí záruky co se týče duševního vlastnictví, nikoli však v oblasti patentů. Odpovědnost za porušení práv k duševnímu vlastnictví je často limitována typem škody a její výší s tím, že poskytovatelé jsou ochotni odpovídat jen za přímé škody.[70] V případě, že se uzavírá formulářová smlouva (§ 1798 a násl. zák. č. 89/2012 Sb.), objednatel nemá možnost její podobu ovlivnit. Stává se tedy, že je v ní upravena kombinace limitované odpovědnosti na pouhou škodu skutečnou, což

[68] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 307.
[69] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 316.
[70] HON, W. Kuan, Christopher MILLARD a Ian WALDEN. *Negotiating Cloud Contracts: Looking At Clouds From Both Sides Now*. Stanford Technology Law Review [online]. 2012, Num. 1 (Vol. 16) [cit. 2016-08-17]. Dostupné z: http://stlr.stanford.edu/pdf/cloudcontracts.pdf, s. 94.

znamená, že poskytovatel neodpovídá za ušlý zisk, s limitací na částku odpovídající částce, kterou objednatel uhradil za poskytovanou službu. Jedná se tedy o nerovný vztah. Pak jen záleží, které právo je rozhodné pro daný konkrétní případ, neboť český soud by s největší pravděpodobností k takové limitaci nepřihlížel právě z důvodu ochrany slabší strany.[71]

Dalším klíčovým ustanovením smluv o poskytování SaaS je *právo na využívání prostoru na serverech poskytovatele*, které stanoví, že objednatel musí mít vždy přístup ke svým datům, že data nebudou nijak zneužita a budou kdykoli převedena na jiné servery, pokud o to objednatel požádá. Poskytovatel je pod sankcí povinen tyto smluvně ujednané požadavky dodržet.[72] Odpovědnost poskytovatele cloudu je upravena zákonem č. 480/2004 Sb., o některých službách informační společnosti a obecně odpovědnost poskytovatele za škodu jakožto následku porušení smluvní povinnosti je obsažená v § 2913 občanského zákoníku, podle čehož poskytovatel při porušení smluvní povinnosti nahradí škodu objednateli a také osobě, které mělo splnění povinnosti sloužit. Za předpokladu, že by subdodavatel poskytovatele věděl, že poskytuje hostovanou službu konkrétní osobě v pozici zákazníka poskytovatele, vznikla by mu povinnost hradit škodu třetí osobě. Poskytovatel bude odpovědný vždy, neboť ve smluvních vztazích se nevyžaduje zavinění, ledaže prokáže, že mu dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na jeho vůli.[73] Mnoho poskytovatelů se vůči této odpovědnosti staví proaktivně a má dvě až tři zálohy dat, což ovšem neznamená, že jsou ochotni se k takové praxi smluvně zavázat. Mnoho z nich nechce odpovídat ani za integritu dat či jejich ztrátu. V případě, kdy poskytovaná SaaS služba zahrnuje i dodání určitých dat ze strany poskytovatele, mnoho z nich omezuje svou odpovědnost jen na dodatečnou náhradu ztracených dat. Zálohování dat pak poskytovatelé mnohdy nabízejí jako službu navíc za dodatečný poplatek ze strany uživatele. V takovém případě se pak poskytovatel zavazuje zálohovat

[71] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 317.
[72] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 316.
[73] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 338-339.

a přebírá odpovědnost[74] za integritu záloh a ztráty dat. Velcí poskytovatelé často zahrnují do svých smluv tzv. sdílenou odpovědnost mezi nimi a uživateli za integritu dat, zálohování a bezpečnost dat. Uživatelé SaaS služeb obecně disponují menší kontrolou než uživatelé IaaS nebo PaaS, neboť u těchto cloudových řešení jsou to uživatelé, kteří ovládají virtuální servery a rozhodují o tom, co za bezpečnostní opatření na ně nainstalují (například firewally, anti-malware aj.) a současně také rozhodují, jaké aplikace na ně nainstalují, respektive na nich budou hostovat. Navíc se jedná o aplikace vyvinuté uživatelem a tím pádem i jím kontrolované. Naproti tomu uživatelé SaaS používají standardizované aplikace poskytované v prostředí, které nemohou kontrolovat, a proto se často musí spolehnout na poskytovatele v otázce jak zabezpečení aplikace, tak celého prostředí. V tomto případě se mnoho technicky vybavených uživatelů uchyluje k průběžnému zálohování na vlastních kapacitách.[75]

Smlouva SaaS zpravidla garantuje objednateli téměř okamžitou *podporu softwarových služeb* ze strany poskytovatele, a to ve formě buď Help Desku poskytovaného non stop nebo ve stanoveném časovém rozhraní, anebo v podobě bezprostředního upgradu užívaného softwaru, který je k dispozici okamžitě po jeho uvolnění ze strany výrobce softwaru.[76] Technická podpora se poskytuje uživateli v oblasti otázek „jak na to“, instalace nebo v souvislosti se zdrojovým kódem apod. Podpora může být v podmínkách odstupňovaná podle závažnosti dopadu a tomu i odpovídající reakční doba (response time). Poskytovatelé mohou též nabízet nadstandardní péči, respektive podporu, která se může lišit dobou reakce a dostupnosti. Tato služba je vždy zpoplatněná navíc. Poskytovatelé též často v podmínkách stanovují povinnost uživatele součinnosti a způsoby této povinnosti.[77]

---

[74] Objednatel se může domáhat odpovědnosti za škodu způsobenou ztrátou dat vůči poskytovateli cloudu poskytujícímu současně i hostingové služby, vůči subdodavateli poskytovatele provozujícímu datové centrum nebo vůči poskytovateli hostingových služeb (tj. data center), pokud uživatel uzavře samostatnou smlouvu s poskytovatelem hostingu na jedné straně a na druhé straně s poskytovatelem cloudu. Zdroj: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580, s. 339.

[75] HON, W. Kuan, Christopher MILLARD a Ian WALDEN. *Negotiating Cloud Contracts: Looking At Clouds From Both Sides Now*, op. cit., s. 94-95.

[76] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 316.

[77] IBM Software as a Service (SaaS) Support Handbook (vzor). Dostupné z: https://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf

V rámci smlouvy o poskytování SaaS samozřejmě nesmí chybět ani ustanovení o *povinnosti hradit cenu SaaS* objednatelem a platební podmínky. Cenu lze stanovit v závislosti na typu cloudových služeb nebo úrovni garance dostupnosti podle SLA a sjednaného či požadovaného serverového prostoru. Platba zpravidla probíhá prostřednictvím nástroje umístěného v rámci internetového rozhraní.[78]

Pro poskytovatele služeb SaaS je nezbytností získat důvěru zákazníků. Každá smlouva o poskytování SaaS služeb musí obsahovat ustanovení o *mlčenlivosti a nakládání s daty objednatele*. Úprava osobních údajů hraje u smluv typu SaaS (i u IaaS) stěžejní roli, především v případě údajů třetích osob, kterými objednatel služby disponuje jakožto správce osobních údajů a za nakládání s nimi nese odpovědnost. Poskytovatel cloudových služeb pak jedná z pozice zpracovatele osobních údajů, které ukládá na vlastní nosiče a umožňuje podle pokynů správce přístup k nim, jejich šíření a mnoho dalších operací. Jak zpracovatelé tak správci jsou ze zákona povinni proaktivně zabraňovat neoprávněnému nebo nahodilému přístupu k osobním údajům. Jedná se o tzv. technickoorganizační opatření, jejichž splnění by měly obě strany být schopny prokázat. V rámci ustanovení o nakládání s osobními údaji by mělo být upraveno i jejich předávání mimo EU. Dále je často možné uzavřít se zpracovatelem samostatnou smlouvu o zpracovávání osobních údajů, které se v českém právu říká smlouva o zpracování dat.[79] Podrobněji se této problematice ochrany osobních údajů v rámci smluv o poskytování SaaS bude zabývat čtvrtá kapitola této práce, včetně smluvní úpravy osobních údajů a analýzy dvou ukázkových smluv.

## 2.2 Licence při poskytování SaaS

Užívání softwaru jinou osobou je umožněno na základě udělení licence ve formě licenční smlouvy dle občanského zákoníku (§ 2358 a násl.).[80] Jak již bylo řečeno v rámci definic pojmu, SaaS je provozován na infrastruktuře poskytovatele Cloud

[78] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 316.
[79] OTEVŘEL, Petr. Vybraná úskalí uzavírání smluv typu SaaS: Právní aspekty IT služeb typu cloud computing. *SystemOnLine: S přehledem ve světě informačních technologií* [online]. 2012, (4.) [cit. 2016-08-17]. Dostupné z: https://www.systemonline.cz/it-pravo/vybrana-uskali-uzavirani-smluv-typu-saas.htm
[80] Zákon č. 89/2012 Sb.

computingu. Znamená to, že se k zákazníkovi nepřenáší rozmnoženiny softwaru a nedochází tím tedy k jeho distribuci. SaaS tak rozvrátil tradiční způsob distribuce softwaru. Poskytuje stejné účinky užití softwaru, nikoli však distribucí jeho kódu - ať už fyzicky, nebo v podobě zdrojového kódu, nebo jiných forem - ale tím, že poskytuje vzdálený přístup k rozhraní a službám softwaru, který je spuštěn na serverech provozovanými třetími osobami nebo poskytovateli těchto služeb. Mezi výrobcem softwaru a uživatelem softwarové licence dochází ke vzniku autorskoprávního vztahu zakládající právo užití softwaru, zatímco mezi poskytovatelem softwarových služeb a uživatelem je vztah upraven servisní smlouvou (viz výše SLA) a její plnění se měří podle úrovně služeb a dostupnosti. V tomto vztahu nedochází k žádné výměně kódu, neexistuje přímý vztah s koncovým uživatelem kódu. Protože se u SaaS nejedná o distribuci softwaru, v praxi se to odráží často na tom, že většina poskytovatelů cloudových služeb používá modifikovaný open source[81] software, aniž by uživatel měl právo požadovat zdrojový kód, přičemž jsou distribuovány modifikované kopie softwaru pod tzv. copyleftovou[82] licencí. Byl to vývojář a podpůrce Free softwaru[83] Bradley Kuhn společně se svým kolegou Eben Moglen, kteří navrhli doplněk ke GPL

[81] Open Source software (OSS) je software s otevřeným zdrojovým kódem (opakem proprietárního softwaru s uzavřeným kódem). Patří do kategorie nekomerčního softwaru, který je nejčastěji šířen pod licencí GNU/GPL (General Public License, tzv. všeobecná veřejná licence). OSS je definován základními znaky: volné další šíření; dostupnost zdrojového kódu nabyvateli licence; možnost vytvářet odvozený software a povinnost distribuovat jej pod stejnou licencí; omezení z důvodu integrity autorova kódu; zákaz diskriminace osob nebo skupiny; zákaz diskriminace účelu použití; povinnost zachování typu softwaru; licence nesmí být vázána na produkt; licence nesmí zakazovat použití nebo distribuci jiného softwaru; technologická neutralita licence. Definiční vymezení Open Source softwaru je ve správě organizace Open Source Initiative, jež má za úkol zjišťovat a potvrzovat, zda konkrétní software spadá do kategorie Open source. Dostupné z: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 266-269.

[82] Copyleftové licence jsou modifikací základních licencí, které vznikly pro otevřený a svobodný typ softwaru (Open source a Free software). Copyleft (opak Copyright) je nástrojem, prostřednictvím něhož se přenáší práva původní licence na další uživatele. V rámci copyleftové licence se musí všechny svobody a práva udělené autore uživatelům přenést na další uživatele při dalším šíření (např. právo studovat a upravovat zdrojový kód nebo právo šířit kopie). Copyleftové licence jsou jak kompatibilní tak nekompatibilní s GPL licencí. Dělí se na silné (GNU GPL) a slabé (LGPL, Mozilla Public License). Dále lze rozlišit plný Copyleft (vztahuje se na všechny části softwaru) a částečný ( umožňuje některé části modifikovaného softwaru šířit pod jinou licencí). Dostupné z: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 269.

[83] Free software je společně s Open source označován jako FOSS (Free and Open source software), neboť mají mnoho společných základních prvků. Free software však klade důraz na svobodu užití samotnými uživateli, zatímco open source na otevřenost zdrojového kódu pro další šíření. Free software je postaven na projektu R. Stallmana GNU z r. 1984, jehož záměrem bylo vytvořit kompletní svobodný operační systém. Základem Free softwaru jsou svobody nabyvatele softwaru, mezi něž patří svoboda používat software za jakýmkoli účelem, svoboda studovat software a přizpůsobit ho svým potřebám, svoboda redistribuovat kopie softwaru a svoboda šířit kopie upravené verze ostatním. Předpokladem naplnění těchto svobod je zpřístupnění zdrojového kód k volnému nakládání. Dostupné z: JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 267-268.

licencím (k těmto viz níže) pod názvem tzv. Affero klauzule (GNU Affero General Public License verze 3, AGPL). V této klauzuli nebyl účinek copyleftové licence vyvolán distribucí, zakládal se totiž na právu na kontrolu změn. Přišli tedy s myšlenkou a realizací toho, že i když je software modifikován, a to i v případě, že není zdrojový kód distribuován, musí být v rámci síťového rozhraní vhodné zařízení, které bude obsahovat odpovídající zdrojový kód. Oba jmenovaní zpopularizovali koncept softwaru jako služby a v rámci licence GNU General Public Licence verze 2, později autorizované jako výše uvedené GNU AGPL v.3, zavedli pro jeho poskytování používání modifikovaného open source softwaru, u kterého nemusí poskytovatel zpřístupňovat zdrojové kódy.[84]

### 2.2.1 Licence GNU General Public License verze 2 vs. verze 3

Podle studie Johna Sullivana, výkonného ředitele nadace Free Software Foundation, a jím uváděných údajů se open source softwary licencují z přibližně 70% jen licencemi z rodiny GNU General Public License.[85] Vedle těchto však existují i další licence, slučitelné s GNU GPL licencí, kam patří vedle celé GPL rodiny i Mozilla Public License (MPL), Modifikovaná BSD Licence a European Union Public Licence (EUPL), a neslučitelní s GNU GPL licencí, kam se řadí Originální BSD licence a MIT licence. Všemi těmito licencemi lze šířit svobodný software a Open source.[86] Tato práce se však soustředí jen na rodinu GNU GPL licencí, kam patří GNU General Public License (GPL) v.2 a v.3, GNU Lesser General Public License (LGPL) a Affero General Public License (AGPL).

GNU General Public License verze 3 vznikla roku 2007, kdy dvě předchozí verze byly vydány v letech 1989 a 1991. Každá z verzí má svá specifika (práce se však zabývá jen těm relevantním k předmětu práce) s tím, že celá řada neproprietárního

[84] *Legal aspects of free and open source software*. In: European Parliament: Directorate General For Internal Policies, 2013. Dostupné z: http://www.europarl.europa.eu/document/activities/cont/201307/20130708ATT69346/20130708ATT69346EN.pdf

[85] GPL use in Debian on the rise: study. *ItWire.com* [online]. 2012 [cit. 2016-08-18]. Dostupné z: http://www.itwire.com/business-it-news/open-source/52838-gpl-use-in-debian-on-the-rise-study

[86] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 270-271.

softwaru[87] (FOSS) je šířena pod druhou verzí. Všechny verze GPL však vyžadují, aby byl odvozený software vždy šířen pod shodnou licencí, čímž je zajištěno to, že i modifikovaný software bude svobodným softwarem. Každý soubor se zdrojovým kódem musí obsahovat zejména označení jeho autora, rok jeho vývoje a případně varování ohledně autorských práv autora daného softwaru. S těmito informace by měl být software, byť i jako modifikovaný, i nadále šířen. Každý autor změny softwaru má autorská práva k provedeným změnám. Třetí verze navíc přináší zákaz tzv. tivoizace neboli hardwarového omezení modifikace softwaru a umožňuje autorům si účtovat poplatek za zhotovení kopie a za servis.[88]

GNU GPL v. 2 stanoví, že se vztahuje na kterýkoli program či jiné dílo, které obsahuje autorem umístěnou zmínku o tom, že může být šířeno podle ustanovení Obecné veřejné licence GNU. Programem se myslí každý takový program a dílem založeném na programu každé takové dílo z něj odvozené dle autorského zákona. Článek 0. dále výslovně stanovuje, že jiné činnosti než kopírování, šíření a úpravy programu nejsou licencí pokryty, že sahají nad její rámec. GPL verze 2 v čl. 3 stanovuje též povinnost šířit upravené zdrojové kódy, a to v kontextu s rozmnožováním a distribucí softwaru.[89] Naproti tomu třetí verze GPL licence v čl. 0 stanoví, že jakýkoli druh šíření, které dalším stranám umožňuje výrobu nebo pořízení kopií, představuje zveřejnění díla. Běžným použitím díla přes počítačovou síť, aniž by došlo k přenosu kopie k uživateli, však nedochází ke zveřejnění díla, a nevyžaduje se tak povinnost šířit upravený zdrojový kód.[90] V rámci GPL licencí není stanovená povinnost zveřejňovat zdrojový kód modifikovaných verzí. Modifikovanou verzi lze používat soukromě, či interně v rámci organizace, aniž by se zveřejnila. V případě, že by se modifikovaná verze jakkoli zveřejnila, GPL ukládá povinnost zveřejnit i zdrojový kód této změněné verze, tzn. že povinnost zveřejnit zdrojový kód je spojena až s distribucí softwaru.[91]

---

[87] Neproprietární software je opakem proprietárního, který je licencován zejména úplatně.
[88] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 270.
[89] *Obecná veřejná licence GNU v.2 (GNU GPL v.2)*. Free Software Foundation, 1991. Dostupné z: http://www.gnugpl.cz/v2/
[90] *Obecná veřejná licence GNU v.3 (GNU GPL v.3)*. Free Software Foundation, 2007. Dostupné z: http://www.gnugpl.cz/v3/
[91] Frequently Asked Questions about version 2 of the GNU GPL. GNU Operating System [online]. Free Software Foundation, 2015 [cit. 2016-08-18]. Dostupné z: https://www.gnu.org/licenses/old-licenses/gpl-2.0-faq.en.html#GPLRequireSourcePostedPublic

V kontextu zveřejňování zdrojového kódu vznikla modifikovaná verze GPL3, která se nazývá GNU Affero General Public License v. 3 (AGPL). Podstatou této licence je přístup ke kompletním zdrojovým kódům softwaru v rámci internetové sítě.[92] V případě, kdy tedy autor či držitel majetkových práv k softwaru jej šíří pod AGPL licencí, je zjevné, že chce tímto donutit potenciální poskytovatele softwaru jako služby ke sdílení zdrojového kódu a zamezit tak užití změn SaaS bez zveřejnění zdrojového kódu. Poskytovatelé, kteří integrují do svého řešení zdrojové kódy softwaru pod touto licencí, budou s největší pravděpodobností muset zveřejnit zdrojový kód celého systému.

V souvislosti s poskytováním SaaS je třeba se zabývat i otázkou distribuce, i když se může zdát, že se mnohdy u tohoto řešení o distribuci, či jiný relevantní pojem použitý v textu licence, nejedná.

GLP v. 2 pracuje s pojmem „distribution“, který vykládáme jako kopírování a šíření programu. Šíření pod touto verzí licence je prováděno pomocí zdrojového kódu, který se považuje za nejvhodnější formu pro případné úpravy programu. U verze 2 se pak za šíření považuje i nabídnutí přístupu ke kopírování zdrojového kódu z určitého místa.[93] GLP v. 3 zavádí nové pojmy „convey“ a „propagate“, které můžeme přeložit jako předávání/zveřejňování a šíření. Předávání díla značí jakýkoli druh šíření, které dalším stranám umožňuje výrobu či pořízení rozmnoženiny díla. Šíření díla pak vyjadřuje jakékoli nakládání s dílem, které musí být konformní s autorskoprávními ustanoveními dle konkrétního rozhodného práva, kromě spouštění díla na osobním počítači a vytváření rozmnoženin pro vlastní osobní užití. Šíření zahrnuje vytváření rozmnoženin, jejich distribuci (s nebo beze změn) a jejich zpřístupnění veřejnosti, případně další činnosti.[94] U pojmu distribuce ve verzi 2 GPL se diskutovalo o definici a jeho rozsahu, termín byl však přejat z copyrightového práva USA s tím, že se počítalo, že každý stát pro něj bude mít odchylnou interpretaci.[95]

---

[92] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 271.
[93] *Obecná veřejná licence GNU v.2 (GNU GPL v.2)*. Free Software Foundation, 1991. Dostupné z: http://www.gnugpl.cz/v2/
[94] *Obecná veřejná licence GNU v.3 (GNU GPL v.3)*. Free Software Foundation, 2007. Dostupné z: http://www.gnugpl.cz/v3/
[95] A Quick Guide to GPLv3. GNU Operating System [online]. Free Software Foundation, 2014 [cit. 2016-08-18]. Dostupné z: https://www.gnu.org/licenses/quick-guide-gplv3.html

Pokud bychom vzali v potaz úpravu evropského práva, vztahovala by se k této otázce Směrnice o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti. Ta v čl. 4 konkrétně zmiňuje právo na rozšiřování, což terminologicky odpovídá distribuci, ale článek je zjevně aplikovatelný jen na hmotné nosiče děl. Dalším nejbližším aplikovatelným ustanovením směrnice by pak byl čl. 3, který stanovuje právo na sdělování děl veřejnosti a právo na zpřístupnění jiných předmětů ochrany veřejnosti. V odstavci 1 uvádí, že *„členské státy poskytnou autorům výlučné právo udělit svolení nebo zakázat jakékoliv sdělení jejich děl veřejnosti po drátě nebo bezdrátově včetně zpřístupnění jejich děl veřejnosti takovým způsobem, že každý jednotlivec ze strany veřejnosti má k těmto dílům přístup z místa a v době, které si zvolí."*[96] V kontextu úpravy v autorském zákoně by právo užít způsobem zpřístupnění softwaru vytvořeného autorem v pracovněprávním nebo služebním poměru nemělo být chápáno jako distribucí či předáváním podle GPL licencí, neboť § 58 autorského zákona vztahuje v daném případě na počítačový program i databáze režim zaměstnaneckého díla. To se týká i díla vytvořeného daným autorem na objednávku, neboť v takovém případě se za objednatele považuje zaměstnavatel.[97]

Byznys model SaaS svým způsobem představuje jakési východisko z copyleftových licencí spadajících do rodiny GNU General Public License. SaaS model může být vystavěn na open source copyleftovém softwaru, aniž by se k poskytování softwarových služeb musely udělovat uživatelům copyleftové licence, přičemž jim je ale poskytována GPL licence. SaaS služby tak představují způsob, jak obejít (tzv. SaaS loophole) copyleftové restrikce, neboť poskytovatel SaaS nemusí distribuovat žádný binární či zdrojový kód uživatelům. Ti totiž využívají webového prohlížeče pro přístup k poskytované službě jen velice zřídka. SaaS je model založený na přístupu k síti a nikoli na rozmnoženinách softwaru. Tato teorie by však neplatila v případech, kdy poskytovatel poskytuje kopii SaaS aplikace pod copyleftovou licencí, nebo kdy poskytovatel přenese SaaS aplikaci společně se zdrojovým kódem do úschovy

[96] Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti. In: *Úřední věstník EU*. EUR-Lex, 2001. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32001L0029

[97] CHALOUPKOVÁ, Helena a Petr HOLÝ. *Autorský zákon Komentář*. 4. Praha: C. H. Beck, 2012. ISBN 978-80-7400-432-2.

(escrow[98]) a ten je následně převeden uživateli pod copyleftovou licencí, anebo v případě, kdy poskytovatel dodá SaaS aplikaci pod copyleftovou licencí prostředníkovi (distributorovi, prodejci) pro další implementaci. Tento SaaS loophole platí jen v situacích, kdy nejsou žádné kopie copyleftové licence softwaru jako služby SaaS distribuovány/ předávány pod adekvátní licencí. Co se týče customizace, neboli přizpůsobování softwaru požadavkům uživatele, zpravidla platí, že kód k těmto změnám bude vlastnit poskytovatel služby.[99]

[98] Pojmem „escrow" se myslí u nás známý institut notářské nebo advokátní úschovy mezi dvěma smluvními stranami.
[99] LANDY, Gene K. *The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP law*. Syngress Publishing, 2008. ISBN 978-1-59749-256-0.

# 3 Právní rámec ochrany osobních údajů v cloudu

Otázka ochrany osobních údajů je v českém prostředí garantována na ústavní úrovni Listinou základních práv a svobod. V čl. 7 tento dokument stanovuje nedotknutelnost soukromí jedince, což úzce souvisí s jeho osobními údaji. Dále v čl. 10 je výslovně stanoveno, že každý by měl být chráněn před neoprávněným shromažďováním, zveřejňováním anebo jiným zneužíváním údajů o své osobě jakožto právo na zachování lidské důstojnosti, osobní cti, dobré pověsti a dobrého jména stejně tak na ochranu před neoprávněným zasahováním do soukromého života. Ochrany osobních údajů se také dotýká čl. 12 Listiny, jenž zakotvuje právo na nedotknutelnost obydlí a čl. 13 v němž je stanoveno listovní tajemství[100]

Institut ochrany osobnosti a osobních údajů je upraven i nadnárodními evropskými dokumenty, které jsou součástí právního pořádku České republiky. Mezi tyto patří Všeobecná deklarace lidských práv a Úmluva o ochraně lidských práv a základních svobod, která v čl. 8 zakotvuje vedle práva na respektování soukromého a rodinného života, obydlí a korespondence i výjimky z tohoto práva, které představují zájmy nadřazené zájmům jednotlivce, mezi něž patří otázka národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, předcházení nepokojů a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných.[101]

Otázkou zpracování osobních údajů se zabývá i Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat[102], která zakotvuje na území ratifikujících států ochranu soukromí v souvislosti s automatickým zpracováním

[100] Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod.
[101] Sdělení 209/1992, Sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.
[102] Sdělení Ministerstva zahraničních věcí, č. 115/2011 Sb.m.s, Úmluva o ochraně osob se zřetelem a automatizované zpracování osobních dat.

osobních údajů. Česká republika je touto Úmluvou vázána od roku 2001, ale problematiku v ní obsaženou, rozvádí blíže směrnice EU[103].

Vnitrostátní právní úprava ochrany osobních údajů je obsažena v zákoně o ochraně osobních údajů[104], který je výsledkem transpozice mezinárodních závazků v této oblasti. V kontextu cloudových služeb a jejich jednotlivých řešení nelze však aplikovat jen národní právní řád, neboť cloudová řešení neznají geografických hranic a služby jimi poskytované jsou zprostředkovávány přes Internet. Hlavními právními prameny proto budou na úrovni evropské úpravy právní předpisy EU.

V primárním právu se jedná o Smlouvu o fungování EU, která konkrétně v čl. 16 přiznává všem jedincům, bez rozlišení národnosti, právo na ochranu osobních údajů.[105] Toto ustanovení rozšiřuje dále Listina základních práv Evropské unie v čl. 8, kde stanovuje, že každý má právo na ochranu osobních údajů, které se ho týkají a zároveň uvádí pravidla pro zpracování údajů, nad kterými mají dozorovat nezávislé orgány (jako je např. u nás Úřad na ochranu osobních údajů). Tato pravidla se týkají korektního zpracování údajů, k přesně stanovenému účelu a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu, který stanoví zákon. Navíc ustanovení přiznává právo na přístup k údajům, které byly o dotyčné osobě shromážděny, a právo na jejich případnou opravu.[106]

Sekundární právo v otázce ochrany osobních údajů se v současnosti zakládá na dvou základních dokumentech, směrnice Evropského parlamentu a Rady 95/46/ES (podle angl. Data Protection Directive označována jako DPD)[107], kterou však zruší a nahradí již výše zmíněné nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (z

[103] 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. In: *Úřední věstník EU*. EUR-Lex, 1995.
[104] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1.ledna 2015
[105] Smlouva o fungování Evropské unie, 9.5.2008, In: Úřední věstník Evropské unie.
[106] Listina Základních Práv Evropské Unie 2012/C 326/02. In: *Úřední věstník Evropské unie*. EUR-Lex, 2012.
[107] 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. In: *Úřední věstník EU*. EUR-Lex, 1995.

anglického překladu obecného nařízení o ochraně údajů označován pod zkratkou GDPR)[108]. Nařízení vstoupilo v platnost 24. května 2016 a bude aplikovatelné od 25. května 2018.[109] Tyto dva právní předpisy budou sloužit jako předloha požadavků na smluvní ujednání mezi poskytovatelem a uživatelem, čemuž se budou věnovat následující část práce. Vedle těchto se dále jednotlivé oblasti ochrany osobních údajů upravují pomocí směrnice o zpracování osobních údajů a ochraně soukromí v odvětvích elektronických komunikací[110] a rozhodnutí[111] Komise, kterými se zavádí standardní smluvní doložky pro případy, kdy dochází k předávání osobních údajů do třetích zemí, aby se zajistila jejich dostatečná právní ochrana i případně mimo území EU.

## 3.1 Požadavky na úpravu ochrany osobních údajů v SaaS

Vzhledem k tomu, že v oblasti ochrany osobních údajů se změnila legislativa, všechny smlouvy cloudových služeb budou muset být v rámci nastávajících dvou let upraveny podle platné právní úpravy, v tomto případě podle GDPR. Tato část práce se bude zabývat podmínkami, které smlouvy o zpracování osobních údajů v cloudových službách musí splňovat jak podle dosavadní úpravy, tj. směrnice DPD, tak i nově zavedené změny podle GDPR.

Nejprve je stěžejní si nadefinovat pojem **osobní údaje**, se kterým obě normy pracují. Osobními údaji se myslí v obou dokumentech veškeré informace o identifikované nebo identifikovatelné fyzické osobě (neboli subjektu údajů). Podle Stanoviska W136 vypracovaného pracovní skupinou Article 29 Working Party (A29WP) se slovem „veškeré“ míní co nejširší koncept osobních dat, který pokrývá jak objektivní tak subjektivní složky informací, názorů či konstatování. Dále uvádí, že na

[108] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.
[109] Reform of EU data protection rules. *European Commission: Justice* [online]. [cit. 2016-08-19]. Dostupné z: http://ec.europa.eu/justice/data-protection/reform/index_en.htm
[110] Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. In: *Úřední věstník EU*. EUR-Lex, 2002.
[111] Rozhodnutí Komise 2004/915/ES ze dne 27. prosince 2004, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavedení alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí (oznámeno pod číslem K(2004) 5271). In: *Úřední věstník EU*. EUR-Lex, 2004.

to, aby se jednalo o osobní údaj, nemusí se jednat nutně o pravdivou či prokázanou informaci. Pojem osobní data obsahuje údaje zahrnující osobní a rodinný život subjektu údajů *in stricto sensu*, ale zároveň pod něj spadají i informace ohledně jakékoli činnosti, kterou daný subjekt vykonává (v souvislosti se zaměstnáním, ekonomicko-sociálním chováním jedince apod.). K tomu, aby se z osobního údaje stala pouhá informace, je třeba jej anonymizovat nebo pseudonymizovat. Pseudonymizace je proces, kterým se skryje identita subjektu údajů. Záměrem tohoto procesu je sběr dodatečných informací ohledně stejné osoby bez toho, aniž by došlo k odhalení její identity.[112] Podle definičních ustanovení GDPR by neměly být „*osobní údaje, zpracované pseudonymizací, přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, a to pokud jsou tyto uchovány odděleně a vztahují se na ně technická a organizační opatření pro zajištění toho, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.“* Pseudonymizace tak může omezit rizika pro dotčené subjekty údajů a pomoci zpracovatelům či správcům údajů v jejich povinnosti ohledně ochrany osobních údajů.[113]

Mezi osobní údaje řadíme také jejich podkategorii, kterou podle české vnitrostátní úpravy zákona o ochraně osobních údajů označujeme jako tzv. citlivé údaje. V čl. 9 GDPR se jedná o zákaz zpracování zvláštní kategorie osobních údajů, přičemž její výčet obsahuje všechny složky obsažené v DPD a nově vedle rasového a etnického původu, politických názorů, náboženského vyznání a filosofického přesvědčení, členství v odborech, údajů týkající se zdraví a sexuálního života přibyly genetické údaje, biometrické údaje za účelem jedinečné identifikace fyzické osoby nebo údaje o sexuální orientaci dotyčné osoby.

**Subjektem údajů** je podle obou úprav identifikovaná nebo identifikovatelná fyzická osoba, Identifikovatelnou osobou se má podle DPD na mysli taková osoba, která může být přímo nebo nepřímo identifkována, a to na základě například jejího identifikačního čísla nebo jednoho či vícero zvláštních prvků fyziologické, psychické,

[112] Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136. *European Commission, Article 29 Data Protection Working Party*, 2007 [online]. Dostupné také z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[113] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

ekonomické, kulturní nebo sociální identity. GDPR rozvíjí tento koncept znaků o identifikátory jako je jméno, identifikační číslo, lokační údaje, síťový identifikátor a mezi prvky identity zařazuje nově fyzické a genetické aspekty fyzické osoby. Identifikovanou osobou je taková osoba, kterou lze v rámci skupiny lidí odlišit od zbytku. Identifikovatelnou osobou se pak má na mysli stav, kdy dotyčná osoba není ještě identifikovaná, ale je možné tak učinit - což je určujícím elementem při stanovování, zda je informace způsobilá identifikovat fyzickou osobu.[114]

**Zpracování dat** je v novém nařízení upraveno jen nepatrně odlišně od původní úpravy. Stále se však v ustanovení o zpracování údajů udržela myšlenka zahrnutí všech možných způsobů nakládání s údaji. GDPR tím označuje všechny operace s osobními údaji nebo soubory údajů na základě jak automatizovaných tak neautomatizovaných postupů, mezi které patří shromáždění, záznam, uspořádání, strukturování, uložení, přizpůsobení nebo změna, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření a jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.[115] Nařízení, jak je vidět, myslelo na budoucí vývoj v oblasti tzv. Big dat a pokrylo tímto ustanovením všechny možné formy nakládání s daty. V oblasti zpracování osobních údajů pomocí nebo bez pomoci automatizovaných postupů byla upravena i otázka, zda uvedení osobních údajů na internetové stránce lze považovat za zpracování podléhající úpravě ochrany osobních údajů. V rozsudku Soudního dvora ve věci Lindqvist soud dospěl k závěru, že uvedení informací na internetové stránky dle současně používaných technických a počítačových postupů uložení takovéto stránky na server a nezbytné další úkony pro zpřístupnění stránky uživatelům na Internetu je třeba považovat za zpracování přinejmenším zčásti automatizované. Odkaz na internetových stránkách na různé osoby, které jsou identifikovány pomocí jména, jiného prostředku, například

[114] Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136. *European Commission, Article 29 Data Protection Working Party*, 2007 [online]. Dostupné také z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

[115] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

telefonního čísla nebo údaji o pracovních poměrech a zálibách, je úkonem úplného nebo částečně automatizovaného zpracování osobních údajů.[116]

U SaaS služeb se o zpracování údajů dá hovořit v případě, kdy dochází na dané platformě i k ukládání údajů držitelem šifrovacího kódu, a nikoli jen ke zprostředkování operačních systémů a softwaru. Protože se ze zákona za zpracování považuje i ukládání, je v takovém případě poskytovatel SaaS řešení i zpracovatelem jím ukládaných údajů v cloudu. V jiném případě by tomu tak nebylo, neboť by se k ukládaným údajům na cloudových serverech přistupovalo jako k anonymizovaným údajům.[117]

Zákonnost zpracování údajů je pák dána podmínkami uvedenými v obou dokumentech s tím, že GDPR legitimizační důvody trochu zpřísnilo. Namísto původního nezpochybnitelného souhlasu subjektu údajů se zpracováním nařízení vyžaduje souhlas pro jeden či více konkrétních účelů. To je nezpochybnitelně ustanovení, které slouží k větší ochraně spotřebitele, ale v oblasti cloudových služeb může komplikovat procesy, neboť ne vždy jsou konečné či potenciální účely zpracování jasné a známé již ve stádiu výchozích údajů. Zpracování osobních údajů je dále zákonné v případě, že je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením takové smlouvy a na žádost daného subjektu údajů, nebo že je nezbytné pro splnění právní povinnosti, která se na správce vztahuje, nebo když je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo i nově podle GDPR jiné fyzické osoby. Dále je zpracování legitimizováno za situace, kdy je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce, ale už nikoli třetí osoba, jak tomu bylo v DPD. Zpracování je též zákonné nezbytných případech pro účely oprávněných zájmů příslušného správce a třetí strany s výjimkou těch případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů, které vyžadují ochranu osobních údajů, což je zejména tehdy, pokud je subjektem dítě.[118]

---

[116] Rozsudek Soudního Dvora ve věci C−101/01 Göta Hovrätt proti Bodil Lindqvist. In: *InfoCuria - Judikatura Soudního dvora*, 2003. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=cs&jur=C,T,F&num=C-101/01&td=ALL

[117] HON, W Kuan, Christopher MILLARD a Ian WALDEN. *The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated?: The Cloud of Unknowing, part 1* [online]. Queen Mary University of London, School of Law, 2011 [cit. 2016-08-20]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577

[118] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

**Správcem osobních údajů** je *„fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů“*.[119] Definice počítá s variantou zpracování těch samých údajů vícero správci společně. Zpravidla je to správce, který je primárně povinen splňovat zákonné podmínky právní úpravy ochrany osobních údajů, včetně registrace u relevantních národních orgánů před zpracováváním údajů. Správce odpovídá jako jeden z mála za zákonné zpracování osobních údajů.[120] Správce určuje účely a prostředky zpracování osobních údajů, zapojuje do procesu zpracování zpracovatele, respektive poskytovatele cloudových služeb, se kterými uzavírá smlouvu o zpracování osobních údajů. Správce má právo požadovat po zpracovateli, aby údaje zpracovával podle pokynů správce a zapojil jistá bezpečnostní opatření, za která následně i ručí.[121] V cloudovém prostředí je za správce považován zákazník – tedy objednatel, neboť je to on, který určuje konečný účel zpracování údajů a rozhoduje o předání části nebo celého procesu zpracování dalšímu subjektu. Poskytovatel cloudových služeb je pak v pozici zpracovatele, který poskytuje prostředky a platformu pro zpracování údajů správce. Situace se však částečně komplikuje v situacích, kdy dochází k propojování jednotlivých služeb a řetězení poskytovatelů cloudu, apod. Ve skutečnosti se dá poskytovatel cloudu označit za správce údajů, a to buď jako společný správce nebo samostatný za předpokladu, že například spravuje a zároveň zpracovává údaje pro vlastní potřebu.[122]

Podle čl. 5 GDPR, který vychází z původní verze úpravy, je to správce, jenž odpovídá za dodržení zásad zpracování osobních údajů. Tyto stanoví, že údaje musí být zpracovány korektně a transparentním způsobem ve vztahu k subjektu údajů, shromažďovány pro určité, výslovně vyjádřené a legitimní účely a k tomuto účelu musí

[119] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.
[120] HON, W Kuan, Christopher MILLARD a Ian WALDEN. *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, part 2* [online]. Queen Mary University of London, School of Law, 2011 [cit. 2016-08-20]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130
[121] HON, W Kuan. Open Season on Service Providers? The General Data Protection Regulation Cometh…. *The IT Law Community* [online]. 2015 [cit. 2016-08-20]. Dostupné z: http://www.scl.org/site.aspx?i=ed43376
[122] Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196, *European Commission, Article 29 Data Protection Working Party*, 2012 [online]. Dostupné také z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

být přiměřené, relevantní a omezené na nezbytný rozsah, dále přesné a v případě potřeby aktualizované, a v neposlední řadě musí být uloženy ve formě umožňující identifikaci subjektu údajů a zpracovány způsobem, který zajistí náležité zabezpečení osobních údajů.[123]

Otázce správce se věnuje i judikatura, z níž nejvýznamnější rozsudek padl u Soudního dvora EU (ESD) ve věci Google Spain. V daném sporu se státní příslušník Španělska M. Costeja González domáhal u Státního úřadu pro ochranu osobních údajů (AEPD), aby společnost La Vanguardia, která vydává vysokonákladový deník, odstranila nebo změnila stránky v deníku zmiňující jméno dotyčného v souvislosti s dražbou nemovitostí zabavených v důsledku dluhů na sociálním zabezpečení. Dále se domáhal, aby společnostem Google Spain a Google Inc. byla uložena povinnost vymazat nebo skrýt jeho osobní údaje, aby se dále neobjevovaly ve výsledcích vyhledávání. Své požadavky opíral o argument, že pohledávky byly již několik let uhrazeny a jejich uvádění je tedy irelevantní, a naopak pro jeho podnikání škodné. Soud na základě těchto žalobních nároků podal k ESD předběžné otázky týkající se jak teritoriální působnosti směrnice, které tento spor o ochraně osobních údajů podléhá, tak otázce postavení vyhledávačů jakožto poskytovatelů obsahu a definici práva být zapomenut,.[124]

ESD stanovil, že činnost vyhledávače, která spočívá ve vyhledávání informací umístěných na Internet třetími osobami, jejich indexování, ukládání a poskytování uživatelům Internetu má být považováno za zpracování osobních údajů podle ustanovení směrnice o ochraně osobních údajů, pokud dané informace obsahují osobní údaje. Soud dále rozhodl, že činnosti vyhledávače zahrnují zpracování údajů, které se liší od zpracování údajů na straně vydavatelů webových stránek, které spočívá jen v umístění uvedených údajů na internetové stránce. Proto určil, že provozovatel vyhledávače je správcem odpovědným za zpracování údajů, které provádí, protože on sám určuje účel a prostředky daného zpracování. V daném případě se tedy jednalo o informace vyhledané, indexované, uložené a poskytnuté svým uživatelům

[123] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

[124] Rozsudek Soudního Dvora ve věci C−131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González,. In: *InfoCuria - Judikatura Soudního dvora*, 2014. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=cs&jur=C,T,F&num=C-131/12&td=ALL

vyhledávačem, které navíc obsahovaly údaje o identifikované nebo identifikovatelné fyzické osobě, proto tedy šlo o osobní údaje. Podle soudu a předchozích rozhodnutí[125] se mají úkony vyhledávače v podobě shromažďování, vyhledávání, zaznamenávání a v rámci programu indexování uspořádávání, uchovávání, sdělování a zpřístupňování svým uživatelům považovat za zpracování, a to i v případě, kdy se jedná o zpracování již zveřejněných informací, například v médiích. Argument, že provozovatel vyhledávače nemá kontrolu nad osobními údaji zveřejněnými na webových stránkách třetích osob, by byl v rozporu s jasnou definicí správce podle právní úpravy. Mimoto je určující i fakt, že vyhledávače zpřístupňují údaje uživatelům na globální úrovni, kteří by jinak nenašli webovou stránku s uvedenými údaji. Provozovatel vyhledávače proto jakožto osoba, která určuje účely a prostředky této činnosti, musí zajistit, že činnost vyhledávače zajišťuje účinnou a úplnou ochranu dotčených osob, zejména jejich práv na soukromí.[126]

**Zpracovatelem osobních údajů** se má na mysli podle obou právních úprav fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce.[127] V cloudu je pak zpracovatelem ten subjekt, který poskytuje prostředky a platformu pro zpracování údajů jménem cloudového uživatele, neboli objednatele. Poskytovatel cloudových služeb však může být považován za zpracovatele a současně za správce, nebo alespoň společného správce, pokud například zpracovává údaje pro vlastní potřeby či za jiných okolností. Povinnosti a odpovědnost v souvislosti se zpracováním dat odpovídající platné právní úpravě však musí být napevno stanoveny ve smlouvě mezi oběma stranami, poskytovatelem a správcem. V současném cloudovém prostředí se uživatelům cloudových služeb nedostává vyjednávacích výhod s velkými poskytovateli, neboť smluvní podmínky jsou zpravidla uzavírány formou formulářových standardizovaných smluv na tzv. zakliknutí.

[125] Viz Rozsudek Soudního dvora ve věci C−73/07 Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy, Satamedia Oy. In: *InfoCuria - Judikatura Soudního dvora*, 2008. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/07

[126] Rozsudek Soudního Dvora ve věci C−131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González,. In: *InfoCuria - Judikatura Soudního dvora*, 2014. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=cs&jur=C,T,F&num=C-131/12&td=ALL

[127] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

V každém případě je to zákazník, objednatel, který rozhoduje o umístění části nebo všech úkonů spojených se zpracováním údajů poskytovatelem služeb.[128] Nerovnost smluvního vztahu mezi malým správcem a velkými poskytovateli cloudu by neměla být důvodem přijetí smluvních ujednání a podmínek, které nesplňují požadavky stanovené úpravou ochrany osobních údajů. Z tohoto důvodu je správce povinen zvolit takového poskytovatele cloudu, který je schopen zaručit všechny zákonné požadavky na ochranu osobních údajů a zavést vhodné technické a organizační opatření.[129]

Zpracovatel má podle právní úpravy na ochranu osobních údajů hned několik povinností, aby se zajistila míra bezpečnosti a soukromí při nakládání s osobními údaji. Mezi tyto povinnosti dále patří obstarání si konkrétního písemného povolení správce v případě, že zpracovatel chce zapojit dalšího zpracovatele. Formou obecného písemného povolení je zpracovatel navíc povinen informovat správce o všech zamýšlených změnách. Vztah mezi správcem a zpracovatelem musí být upraven smlouvou či jiným právním aktem se všemi náležitostmi stanovenými jak ve směrnici či nařízení. Ve smlouvě se stanoví, že osobní údaje zpracovává na základě pokynů správce, nebo že nově zavazuje oprávněné osoby ke zpracování údajů mlčenlivostí, nebo ty, na které se vztahuje mlčenlivost ze zákona, dále že nakládá s údaji podle rozhodnutí správce, kterého následně i o daných úkonech informuje, apod.[130]

Zpracovatelé budou odpovědni stejně jako správci především za bezpečnostní opatření, která musejí odpovídat bezpečnostním rizikům zpracování osobních údajů. Zpracovatelé budou povinni sestavit bezpečnostní vyhodnocení pro každého uživatele, což v cloudovém kontextu, kde jsou zákazníkům nabízeny standardizované výpočetní zdroje pro samoobslužné služby, půjde ztěžka. Zpracovatel jako je například poskytovatel cloudu nebude považován za správce, pokud by údaje zpracovával vysloveně jen pro vlastní potřebu, ale bude subjektem právní ochrany osobních údajů co do bezpečnostních opaření zpracování. Mezi další povinnosti zpracovatele patří

[128] Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196, *European Commission, Article 29 Data Protection Working Party*, 2012 [online]. Dostupné také z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

[129] Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 196, *European Commission, Article 29 Data Protection Working Party*, 2010 [online]. Dostupné také z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[130] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

ukládání záloh, ochrana údajů *by design* a *by default* a samozřejmě součinnost se správci ohledně bezpečnostních opatření, notifikací, vyhodnocení nebezpečí a předchozí konzultace s dozorčími národními orgány pro ochranu osobních údajů.[131]

Cloudové prostředí je typické nestálou lokalizací infrastruktury poskytovatele cloudu, proto je v otázce ochrany osobních údajů uživatelů cloudových služeb nezbytné definovat **místní působnost** evropské právní úpravy ochrany osobních údajů. Vzhledem k tomu, že cloudový uživatel jen zřídka dokáže určit umístění údajů v reálném čase, je to právě nová úprava v podobě GDPR, která překlenuje nedostatky zastaralé předchozí úpravy.[132]

Nařízení GDPR vymezuje vlastní územní působnost v souvislosti se zpracováním osobních údajů v rámci činností provozovny správce nebo zpracovatele v EU bez ohledu na to, zda samotné zpracování pak probíhá stále v EU či mimo ni. V tomto ustanovení lze vidět vývoj v chápání nejen kyberprostoru, ale i cloudové infrastruktury a jednotlivých modelů, neboť oproti předchozí úpravě je zde zahrnut i zpracovatel. Předchozí ustanovení DPD týkající se správce usazeného mimo EU stanovovalo, že tento bude podléhat směrnici v případě, že používá za účelem zpracování osobních údajů automatizovaných či neautomatizovaných prostředků umístěných na území konkrétního členského státu s výjimkou toho, kdy jsou tyto prostředky použity pouze pro účely tranzitu přes území EU.[133] GDPR situaci se správcem nesídlícím na území EU zjednodušuje stanovením dvou typů zpracování osobních údajů, které jsou v takovém případě možné. Nařízení se tedy aplikuje, když dochází ke zpracování osobních údajů subjektů údajů, které se nachází na území EU, správcem nebo zpracovatelem, který není usazen v EU, pokud činnosti zpracování souvisejí buď s nabídkou zboží nebo služeb daným subjektům údajů v EU, přičemž platba nehraje roli, anebo s monitorováním jejich chování, ke kterému dochází na území

---

131 HON, W Kuan. Open Season on Service Providers? The General Data Protection Regulation Cometh…. *The IT Law Community* [online]. 2015 [cit. 2016-08-20]. Dostupné z: http://www.scl.org/site.aspx?i=ed43376

132 Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196, *European Commission, Article 29 Data Protection Working Party*, 2012 [online]. Dostupné také z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

133 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. In: *Úřední věstník EU*. EUR-Lex, 1995.

EU. Třetí podmínka aplikovatelnosti nařízení nebo směrnice, jež je u obou stejná, se vztahuje na zpracování osobních údajů správcem, který není usazen na území EU, ale na místě, kde se právo členského státu uplatňuje na základě mezinárodního práva veřejného[134].[135] Nová ustanovení tak jasně posilují jistotu a bezpečnost údajů subjektů, které se pohybují v kyberprostoru se záměrem si pořídit zboží či služby od poskytovatelů mimo EU.

Otázkou usazení společnosti na území EU či mimo něj se zabývá i výše zmíněná judikatura ESD ve věci Google Spain, Google Inc. proti AEPD, M. C. González. Ve věci vystupuje společnost Google Spain SL, která je zřízená dle španělského práva na území Španělska. Její mateřská společnost Google Inc. se sídlem ve Spojených státech amerických provozuje vyhledávač Google Search, který zpřístupňuje v celosvětovém měřítku prostřednictvím webových stránek www.google.com i pod národními doménami. V tomto modelu je to dceřiná společnost Google Spain, která provozuje prodej produktů a služeb online reklamy třetím osobám včetně marketingu takové reklamy. Google Spain je zapsaným subjektem u AEPD, kde registrovala dva rejstříky s osobními údaji o zákaznících, kteří se společností Google Inc. uzavřeli smlouvu. ESD se v rozhodnutí zabýval předběžnou otázkou ohledně toho, jaká situace se dá považovat za existenci provozovny. I přestože se společnosti Google Spain společně s Google Inc. ohradily, že zpracování osobních údajů je prováděno výhradně druhou zmiňovanou společností, která provozuje Google Search, aniž by prvně zmiňovaná do toho jakkoli zasahovala, neboť její činnost se soustřeďuje na poskytování podpory reklamní činnosti skupiny Google, soud uznal, že pro zpracování stačí, aby bylo prováděno v rámci provozovny a nikoli samotnou provozovnou. Soud proto rozhodl, že *„zpracování osobních údajů prováděné pro potřeby služby vyhledávače (jako např. Google Search), který je provozován podnikem se sídlem ve třetím státě, avšak s provozovnou v členském státě, je prováděno v rámci činnosti této provozovny, pokud je určena k tomu, aby v daném členském státě zajišťovala podporu prodeje a prodej reklamního prostoru nabízeného uvedeným vyhledávačem, který slouží k zajištění výnosnosti služby nabízené*

[134] Poznámka k odst. 3 čl. 3 GDPR: Podle zásad MPV se tím mají na mysli např. paluby lodí, letadel (dopravních) či diplomatické mise, nebo území pod správou jiného státu. Zajímavostí však je, že v souvislosti s tímto ustanovením společnost Google v roce 2009 požádala o patent pro své plovoucí datové centrum.

[135] Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

*uvedeným vyhledávačem"*.[136] Soud shledal spojitost mezi provozovatelem vyhledávače a provozovnou umístěnou v členském státě v tom, že reklamní činnost představuje prostředek k dosažení hospodářské výnosnosti daného vyhledávače, a navíc k tomu je vyhledávač prostředkem k takovéto činnosti.[137]

V souvislosti s Cloud computingem je významná i problematika **předávání osobních údajů do jiných států**. Evropská právní úprava je založená na zásadě volného pohybu osobních údajů v rámci členských států EU s podmínkou zachování všech bezpečnostních opatření k jejich ochraně. Do třetích zemí mohou být údaje předány se souhlasem subjektu údajů a bez něj jen výjimečně. Předávání údajů je vázáno principem teritoriality práva osobních údajů, který se vztahuje na místo, kde jsou údaje zpracovávány. V rámci škálovatelnosti cloudové infrastruktury může dojít k uložení, byť jen dočasnému, údajů na serverech kdekoliv na světě, neboť výpočetní výkon je zajišťován využitím paralelních serverů a kapacit a nikoli jedním extrémně výkonným počítačem. Právní úprava se v takovém případě snaží zajistit, aby země, do kterých jsou údaje předávány, disponovaly dostatečnými zárukami ohledně záruky ochrany osobních údajů.[138]

Předávání osobních údajů do třetích zemí, čímž se má na mysli jakákoli země mimo EU a EHS, je možné bez omezení provádět se zeměmi, které jsou smluvními stranami Úmluvy č. 108[139]. Těmito zeměmi jsou takové, o kterých Evropská komise stanovila, že zabezpečují dostatečné bezpečnostní záruky, a proto zde neplatí žádné zvláštní omezení či povolení národních dozorčích orgánů. Česká republika je Úmluvou vázána a její aplikovatelnost je reflektována v zákoně o ochraně osobních údajů[140], kde se připouští výjimka z povinnosti žádat Úřad pro ochranu osobních údajů o povolení předat osobní údaje do třetích zemí, pokud tak vyplývá z mezinárodní smlouvy.

---

[136] Rozsudek Soudního Dvora ve věci C−131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González,. In: *InfoCuria - Judikatura Soudního dvora*, 2014. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=cs&jur=C,T,F&num=C-131/12&td=ALL

[137] Rozsudek Soudního Dvora ve věci C−131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González, op. cit.

[138] JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT., op. cit., s. 336.

[139] Úmluva Rady Evropy č. 108 z r. 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat. Rada Evropy, 28.1.1981. Dostupné také z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

[140] Viz § 27 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

Pro zajištění ochrany osobních údajů v rámci předávání údajů z EU do USA vznikl program Safe Harbour na základě rozhodnutí Komise[141], které bylo přijato v roce 2000. Prostřednictvím této dohody mezi EU a USA bylo možné ukládat osobní údaje v USA, neboť přistoupením k dohodě a tím i k zásadám v ní obsaženým se na americké společnosti dalo pohlížet jako na subjekty splňující adekvátní požadavky podle evropské právní úpravy na ochranu osobních údajů a nakládání s nimi. Nad výkonem těchto zásad dozorovaly americké dozorčí nezávislé státní orgány, mezi něž jak je uvedeno v příloze rozhodnutí, patřily Federal Trade Commission a Departement of Transportation. Pokud poskytovatel cloudové služby splňoval podmínky stanovené programem a osvědčil se, mohl se zapsat do veřejného rejstříku vedeném Ministerstvem obchodu USA.

Rozhodnutí Komise z roku 2000 bylo prohlášeno Soudním dvorem EU za neplatné v rámci rozsudku ve věci Schrems proti Data Protection Commissioner. Základem sporu byla stížnost irského státního příslušníka, Maximiliana Schremse, kterou podal k irskému orgánu dozoru týkající se nedostatečné ochrany osobních údajů předávaných do USA před sledováním ze strany státních orgánů veřejné moci ve Spojených státech. Stěžovatel se zabýval konkrétně údaji poskytnutými na Facebooku předávanými z irské dceřiné společnosti na servery mateřské společnosti umístěné na území USA, kde jsou i zpracovávány. ESD následně řešil otázku, zda národní dozorčí orgán má pravomoc přezkoumávat úroveň ochrany údajů u země, u níž rozhodnutím Komise bylo rozhodnuto, že požadavky dle evropské právní úpravy splňuje. Soud dospěl k závěru, že dané rozhodnutí Komise nemůže bránit osobám, jejichž osobní údaje byly předány do třetí země, a které tvrdí, že právo a praxe platné v dané třetí zemi nezajišťují odpovídající úroveň ochrany, aby se obrátily na vnitrostátní dozorčí orgány s žádostí přezkumu ohledně zpracování těchto údajů a současně nemůže rozhodnutí tyto pravomoci odepřít či omezit ani vnitrostátním orgánům dozoru. Dále Soudní dvůr rozhodoval o slučitelnosti rozhodnutí Komise s dostatečnou ochranou soukromí a základních práv a svobod osob. Nakonec konstatoval, že právní úprava, která nezadá

[141] Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států. In: *Úřední věstník* L 215/7 *EU*. EUR-Lex, 2000. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32000D0520&from=CS

subjektům žádnou možnost využít právních prostředků k získání přístupu k vlastním osobním údajům nebo dosažení opravy či výmazu těchto údajů, pak taková právní úprava zcela jasně nerespektuje podstatu základního práva na účinnou právní ochranu. Z tohoto mezi dalšími Soudní dvůr rozhodl, že rozhodnutí Komise 2000/520 je neplatné.[142]

V únoru 2016 bylo dosaženo politického konsenzu a přijala se nová úprava předávání údajů z EU do USA v reakci na prohlášení předchozího programu Safe Harbour za neplatný. Nový dokument EU-US Privacy Shields[143] zavádí v důsledku všech předchozích událostí (viz rozsudek ve věci Schrems a Snowdenovo odhalení o monitorování údajů orgány veřejné moci v USA) dokument, ve kterém jsou obsaženy nové důkladnější závazky pro americké společnosti podléhající tomuto ujednání. Na rozdíl od předchozí úpravy se Privacy Shield zabývá nejen komerční oblastí, ale i závazky v oblasti ochrany osobních údajů ve vztahu k orgánům veřejné moci včetně účelů národní bezpečnosti.[144]

Předávání údajů je také možné podle nové úpravy prostřednictvím využití závazných podnikových pravidel (Binding Corporate Rules, BCR), která se aplikují v nadnárodních korporacích v rámci jejich přeshraničních struktur, anebo založen na vhodných zárukách, které má poskytnout správce nebo zpracovatel a za podmínky, že jsou k dispozici vymahatelná práva subjektů údajů a účinná právní ochrana subjektů údajů.[145]

Mezi **nová ustanovení** doposud neupravených povinností, která GDPR přináší, patří například povinnost vést záznamy o činnostech zpracování, zabezpečit zpracování osobních údajů podle požadavků stanovených v čl. 32, dále vypracovat posouzení vlivu na ochranu osobních údajů nebo povinnost týkající se předchozí konzultace

[142] Rozsudek Soudního Dvora ve věci C-362/14 Maximillian Schrems proti Data Protection Commissioner. In: *InfoCuria - Judikatura Soudního dvora*, 2015. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?num=C-362/14

[143] New framework for transatlantic exchanges of personal data for commercial purposes: the EU-U.S. Privacy Shield

[144] *Communication From The Commission To The European Parliament And The Council: Transatlantic Data Flows: Restoring Trust through Strong Safeguards*. European Commission, 2016, COM(2016) 117 final. Evropská komise. Dostupné také z: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf

[145] Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

s dozorovým úřadem před zpracováním, u kterého hrozí vysoké riziko a posledně nová povinnost správce a zpracovatele jmenovat pověřence pro ochranu osobních údajů v případech, kdy zpracování provádí orgán veřejné moci, nebo kvůli svému rozsahu vyžaduje systematické monitorování subjektů údajů, anebo se týká zvláštních kategorií údajů anebo osobních údajů týkajících se rozsudků v trestních věcech.[146]

Další novinkou je v oblasti informací poskytovaných v případě, že osobní údaje byly získány od subjektu údajů. GDPR totiž zavádí vedla práva požadovat od správce přístup k osobním údajům týkajícím se daného subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování a vznesení námitky, i právo na přenositelnost údajů. Tyto osobní údaje má subjekt právo získat ve strukturovaném, běžně používaném a strojově čitelném formátu a může je předat jinému správci.[147]

V oblasti ochrany spotřebitele na Internetu GDPR přináší nová ustanovení týkající se záměrné a standardní ochrany osobních údajů, která stanovují povinnost správce zavést vhodná technická a organizační opatření, a to jak v době určení prostředků pro zpracování, tak při samotném zpracování, k tomu, aby standardně zpracovávaly jen ty nezbytné osobní údaje pro konkrétní účel, a to i v nezbytně nutném množství, rozsahu a po dobu jejich uložení a dostupnosti.[148]

V otázce zabezpečení zpracování se povinnost provést vhodnými technickými a organizačními opatřeními zabezpečení odpovídající danému riziku rozšiřuje i na zpracovatele. Daná opatření mají být volena s přihlédnutím ke stavu techniky, nákladům na jejich provedení, jejich povaze, rozsahu, kontextu a účelům zpracování a dokonce i k různě pravděpodobným rizikům pro práva a svobody fyzických osob.[149]

## 3.2 Analýza smluvních úprav zpracování osobních údajů v SaaS na smlouvách Google Apps for Work vs. Microsoft Office 365

[146-138] Nařízení Evropského Parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

Následující kapitola se bude věnovat analýze smluvních úprav zpracování osobních údajů ve smlouvách upravující poskytování softwaru jako služby. Vzhledem k tomu, že společnosti Google a Microsoft jsou se svými balíčky SaaS služeb pro podniky jedny z nejtypičtějších SaaS modelů, vybrala jsem si právě ony k této analytické části práce. Navíc obě služby poskytují relativně shodné produkty, neboli aplikace, v rámci svých služeb, a tudíž jsou relevantní k následné komparaci.

**Smluvní úprava.** Služby Google Apps Enterprise se uzavírají online smlouvou Google Apps Enterprise Agreement (GAEA)[150], k níž jsou dobrovolné dodatky Data Processing Amendment to a Google Apps Agreement (DPA)[151] nebo Model contract clauses for Google Apps (MCC)[152]. Uživatelé na evropském území tuto smlouvu uzavírají se společností Google Ireland, Ltd., založenou podle irských zákonů. Smlouva GAEA je právně závazná, jak pro uživatele, tak pro společnost Google jen ve své anglické verzi.

Služby Microsoft Office 365 jsou smluvně upraveny v Microsoft Online Subscription Agreement (MOSA)[153], která odkazuje na podmínky v Online Services Terms (OST)[154] obsahující podrobně jednotlivé nabízené online služby. V otázce ochrany dat pro území EHP a Švýcarsko je smlouva uzavírána se společností Microsoft Ireland Operations, Ltd., opět založenou podle irského práva. MOSA je dostupná jen v anglické verzi, zatímco OST v různých jazykových variací.

**Rozsah zpracování.** GAEA stanoví, že bude zpracovávat osobní zákaznická data v souladu s pokyny zákazníka, kterými se podle DPA myslí písemné pokyny Googlu ohledně poskytnutí organizační a technické podpory, pokyny dané zákazníkem, jeho zástupci nebo koncovými uživateli prostřednictvím administrátorské konzole a

[150] Google Apps Enterprise (Online) Agreement [online], Google, 2016 [cit. 2016-08-20]. Dostupné z: https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html
[151] Data Processing Amendment to Google Apps Agreement [online], Google, 2016 [cit. 2016-08-20]. Dostupné z: https://www.google.com/work/apps/terms/dpa_terms.html
[152] 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, 2016 [cit. 2016-08-20]. Dostupné z: https://www.google.com/work/apps/terms/mcc_terms.html
[153] Microsoft Online Subscription Agreement [online], Microsoft, 2016 [cit. 2016-08-20]. Dostupné z: https://www.microsoft.com/online/mosa/MOSA2014Agr(NA)(ENG)(Nov2014)(HTML).htm
[154] Microsoft Online Services Terms [online], Microsoft, August 2016 [cit. 2016-08-20]. Dostupné z: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31

jakékoli další písemné pokyny uznané Googlem. Pokyny navíc musí být v souladu s možnostmi a zásadami ochrany osobních údajů společnosti Google. DPA pak stanoví, že zákazník jakožto správce musí být autorizovanou osobou pro poskytnutí takovýchto pokynů, a to i když jedná jménem jiného zákazníka, na kterého se vztahují tyto smluvní podmínky. Dále uvádí, že Google zpracovává údaje zákazníka jen v nezbytném rozsahu podle jeho pokynů a zavazuje se, že je nebude zpracovávat k žádnému jinému účelu.

Microsoft upravuje použití zákaznických dat v OST, kde stanoví, že data budou použita jen pro poskytování služeb zákazníkovi včetně účelů, které souvisí s poskytováním těchto služeb. Společnost Microsoft se pak zavazuje, že data nebude používat ani z nich nebude odvozovat informace pro žádné reklamní či jinak komerční účely. Společnost tak nedrží žádná práva k zákaznickým datům kromě těch, které zákazník společnosti přidělil pro poskytování konkrétní online služby. Pojem služby online se v kontextu zpracování údajů vztahuje mimo jiné na služby Office 365 a zákaznická data zahrnují ta data, která jsou poskytována prostřednictvím služeb online.

**Bezpečnostní opatření.** Pro zabezpečení dat GAEA uvádí, že společnost Google podnikne a zavede příslušná technická a organizační opatření tak, aby se zajistila ochrana zákaznických dat před náhodným či nezákonným zničením, ztrátou, změnou či neoprávněným zveřejněním a přístupem. Poměrně skromnou a nedostatečnou úpravu zabezpečení údajů ve smlouvě vynahrazuje dobrovolný dodatek DPA, který v čl. 6.1 navíc stanoví, že společnost má čas od času modifikovat a aktualizovat tato opatření s cílem zachování adekvátního zabezpečení. Typy dat, která jsou předávána, uchovávána, posílána nebo přijímána zákazníkem nebo koncovým uživatelem, zahrnovaly podle přílohy 2 dodatku například uživatelská ID, emaily, dokumenty, prezentace, obrázky, kalendářní záznamy, úkoly a jiná elektronická data. Příloha 2 dodatku DPA pak stanovuje konkrétní bezpečnostní opatření týkající se zajištění bezpečnosti datových center a sítí, včetně dat a jejich ukládání a izolace, kontroly přístupu a zařízení, bezpečnosti mezi zaměstnanci a bezpečnosti ze strany dalších zpracovatelů. Zabezpečení systémů vykonávajících logickou a fyzickou bezpečnost a dostupnost systému společnost dokládá prostřednictvím certifikačních atestů SSAE 16 typ II/ ISAE 3402. Google se také zavazuje k vypracování zprávy o auditu jednou za 18 měsíců podle čl. 2.8 GAEA.

Microsoft udává podrobné podmínky zabezpečení v OST pod jednotlivými doménami jako je organizace zabezpečení informací, správy prostředků, zabezpečení lidských zdrojů, fyzického zabezpečení a bezpečnosti životního prostředí, sdělení a správy operací, řízení postupu, správě incidentů zabezpečení informace a správě kontinuity podnikání. Dodržování bezpečnostních opatření představují jedinou odpovědnost společnosti Microsoft v souvislosti se zabezpečením zákaznických dat. OST dále uvádí, že každá online služba se řídí zásadami zabezpečení dat, které odpovídají konkrétně u služby Microsoft 365 standardům uvedeným v normách ISO 27001 a 27002 a nově i podle ISO 27018, které se vztahují na ochranu osobních údajů v cloudových službách.

**Ukončení smlouvy**. Podle čl. 11.1 GAEA může zákazník smlouvu ukončit vedle důvodů platební neschopnosti také z důvodu porušení (včetně porušení bezpečnostních opatření). Za předpokladu, že se druhá strana dopustila závažného porušení smlouvy bez možnosti nápravy, nebo při opakovaném porušení bez ohledu na možnost nápravu či při závažném porušení smlouvy a bez nápravy do 30 dnů po obdržení písemného oznámení o tomto porušení druhé straně.

MOSA v čl. 3 stanoví, že smlouvu lze ukončit podle druhu poskytovaných služeb. U krátkodobých předplatných lze smlouvu ukončit kdykoli v průběhu, u dlouhodobých služeb online lze ukončit před koncem období a zákazník má právo na refundaci předplatného za zbývající část daného období s výjimkou částečně využitých měsíců. Smlouva MOSA se konkrétně nezmiňuje v souvislosti s ukončením o udání důvodů, proto nejspíše platí, že lze ukončit v daných případech bez udání důvodů. Právo odstoupit od smlouvy má zákazník podle doložky 5 přílohy 3 OST také tehdy, pokud by změna právních předpisů měla nepříznivý vliv na ochranná opatření a závazky stanovenými doložkami natolik, že by nebyl schopen plnit své povinnosti ze smlouvy a podle pokynů zákazníka.

**Odpovědnost.** Ve smlouvě GAEA je odpovědnost omezena pro obě smluvní strany co se týče ztrát druhé smluvní strany ohledně skutečného nebo předpokládaného zisku včetně ztráty zisků ze smluv, ztrát předpokládaných úspor, ztrát obchodní příležitosti, ztráty dobré pověsti nebo poškození dobrého jména anebo zvláštní, nepřímé

nebo následné ztráty. Odpovědnost smluvních stran za uvedené ztráty bude mít omezení ve výši 125% celkové částky zaplacené zákazníkem za předchozích 12 měsíců nebo fixní omezení ve výši 50 000 liber záleže na tom, která částka je vyšší. Odpovědnost za smrt, úraz, podvod, úmyslné uvedení nepravdivých údajů, porušení podmínek plynoucích z platných právních předpisů anebo zneužití důvěrných informací není podle čl. 13.1 smlouvy GAEA nijak omezena.

V případě porušení povinností ze smlouvy MOSA má zákazník právo na náhradu škody podle SLA[155], jak je uvedeno v čl. 4 smlouvy. Odpovědnost obou smluvních stran za škody vyplývající ze smlouvy MOSA je omezena přímou škodou a výší částky zaplacené zákazníkem za období předchozích 12 měsíců s tím, že částka v žádném případě nemůže převýšit sumu zaplacenou za celou dobu předplatného. U produktů poskytovaných zadarmo čl. 6 smlouvy MOSA dále stanoví limit odpovědnosti za přímou škodu ve výši 5 000 USD. Odpovědnost podle MOSA za ušlý zisk, nepřímé, zvláštní, nedbalostní nebo jiné škody, ztrátu zisku, narušení podnikání nebo ztrátu obchodních informací je u obou smluvních stran vyloučená, i za předpokladu, že tyto byly rozumně předvídatelné.

**Úpravy služeb.** Zákazníkova pravomoc v oblasti změn a úprav jednotlivých služeb je značně omezená, neboť společnost Google v čl. 1.2 smlouvy GAEA stanoví, že může příležitostně provádět obchodně přiměřené změny služeb, kterou následně zákazníkovi oznámí za předpokladu, že se k odběru takovýchto informací přihlásil. Podle čl. 1.3 může dále společnost provést obchodně přiměřené změny týkající se smluvních podmínek, které zákazníkovi oznámí na email nebo prostřednictvím administrátorské konzole. Dotyčné změny pak začnou platit 30 dnů od oznámení zákazníkovi. V případě dlouhodobých tarifů a nepříznivých dopadů změn na zákazníka, může se tento po upozornění společnosti řídit až do konce aktuálního období podle předchozích podmínek.

Smlouva MOSA neupravuje možnost změn služeb a smluvních podmínek. V čl. 2 d) smlouvy stanoví, že změněnými smluvními podmínkami se zákazník bude řídit až po ukončení dosavadní smlouvy o předplatném a od okamžiku obnovení, resp.

[155] Online Services Consolidated SLA [online], Microsoft, August 2016 [cit. 2016-08-20]. Dostupné z: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37

prodloužení této služby. Za předpokladu, že by zákazník nesouhlasil s danými změnami podmínek, může odmítnout obnovit předplatné, což se s největší pravděpodobností interpretuje jako možnost odstoupení od smlouvy.

**Zpracování dat subdodavateli**. V čl. 2.11 smlouvy GEAE společnost Google stanovuje, že zajišťuje zpracovávání zákaznických dat prostřednictvím subdodavatelů, od kterých však vyžaduje úplnou implementaci vhodných bezpečnostních opatření a zajištění důvěrnosti těchto dat. Podle čl. 11.2 DPA společnost Google zajišťuje, aby subdodavatelé byli vázáni písemnými dohodami stanovující minimální úroveň ochrany osobních dat v souvislosti s osvědčením podle Safe Harbour programu, podle MCC klauzulí uzavřených mezi společností a zákazníkem anebo podle jiného alternativního řešení stanoveného společností. Čl. 11.3 dále uvádí, že zákazník uzavřením dohody GAEA se společností Google souhlasí i s uzavřením subdodavatelských dohod, a pokud jsou uzavřena i MCC, tak že se tyto klauzule vztahují na subdodavatelský vztah. Podle čl. 5 přílohy 2 DPA je Google povinen provést audit týkající se bezpečnostních opatření subdodavatele předtím, než s ním uzavře smlouvu.

Microsoft využití subdodavatelů upravuje v OST, kde v sekci použití subdodavatelů stanovuje, že tito budou mít možnost získat zákaznická data jen za účelem poskytování služeb, jež jsou předmětem subdodavatelské smlouvy. Společnost Microsoft se prohlašuje odpovědnou za dodržování podmínek stanovených ve smlouvách se zákazníky na straně svých subdodavatelů. Zákazník vyjadřuje souhlas se zapojením subdodavatelů podpisem smlouvy MOSA. V sekci soukromí OST dále stanovuje, že každá online služba na vlastním webu uvádí aktualizovaný seznam subdodavatelů, jež mají přístup k zákaznickým údajům, a 14 dnů před udělením daného oprávnění novému subdodavateli k přístupu k zákaznickým datům má zákazník možnost schválit nového subdodavatele. Pokud jej neschválí, může danou službu bez postihu ukončit písemnou výpovědí s uvedenými důvody neschválení subdodavatele.

**Výmaz dat.** Společnost Google v čl. 7 dodatku DPA stanovuje svou povinnost vymazat data zákazníka ve lhůtě 180 dnů a to nehledě na to, zda se jedná o výmaz ze strany zákazníka nebo koncového uživatele, výmaz v souvislosti se standardním ukončením smlouvy GAEA, anebo výmaz v souvislosti s ukončením smlouvy

v důsledku nesplacení dlužné částky. Podle čl. 8 DPA je zákazníkovi také zaručen přístup a možnost opravy, zablokování a přenosu zákaznických dat.

Microsoft vymazání dat upravuje v sekci soukromí smluvních podmínek OST, ve kterých zaručuje vymazání nebo vrácení zákaznických dat nejpozději 180 dní od uplynutí doby účinnosti nebo od ukončení používané služby online zákazníkem. Dodatek 1 ke standardním smluvním doložkám v rámci podmínek OST dále stanoví, že zákazníkovi musí být umožněn přístup k zákaznickým datům a poskytnuta možnost je opravit, odstranit, zablokovat, nebo provádět takové opravy, odstranění nebo blokování jménem zákazníka.

**Předávání dat**. V čl. 10 dodatku DPA společnost Google stanovuje, že může ukládat a zpracovávat zákaznická data jak v USA nebo jiných zemích, kde se nachází zařízení jejích subdodavatelů. V případě, že předává data do zemí mimo EHS a Švýcarsko, zajišťuje aplikaci evropské právní úpravy na ochranu osobních údajů, a to konkrétně zajištěním předání v souladu s programem Safe Harbour, nebo v souladu s MCC, která uzavře společnost se zákazníkem, anebo zajištěním alternativního řešení, které je v souladu s požadavky evropské právní úpravy na ochranu osobních údajů při předávání do třetích zemí.

Společnost Microsoft upravuje lokalizaci dat v sekci umístění pro uchování zákaznických dat ve smluvních podmínkách OST tak, že stanovuje pro služby Office 365, že pokud zákazník poskytuje svého klienta na území EU, společnost bude daná zákaznická data uchovávat pouze v této oblasti. Týká se to obsahu poštovních schránek služby Exchange Online a obsahu serveru SharePoint Online a souborů uložených na daném serveru. Společnost zahrnuje ve svých podmínkách OST v příloze 3 standardní smluvní doložky, které by měly odpovídat evropské právní úpravě, a které jsou aplikovatelné pro případ umístění ostatních dat.

**Shrnutím** na základě analýzy obou smluvních úprav zpracování osobních údajů lze dojít k následujícím závěrům. Uzavřením smlouvy GAEA zákazník automaticky neuzavírá smlouvu o zpracování osobních údajů a tím tedy jednak nemá zaručenou ochranu údajů, ale porušuje tím i povinnosti stanovené evropskou právní úpravou ochrany osobních údajů. Smluvní rámec zpracování osobních údajů je upraven totiž

teprve dodatečnou dohodou Data Processing Agreement (DPA), ke které se uživatel může dostat prostřednictvím administrátorské konzole, ale na kterou primární smlouva GAEA automaticky neupozorňuje. V otázce odpovědnosti společnosti Google jsou ustanovení smlouvy poněkud nejasná a neurčují, zda se jedná o odpovědnost za úmyslná či nedbalostní porušení. Odpovědnost společnosti je značně omezená, a proto v rámci ochrany osobních údajů nese její značnou část samotný uživatel, jak vyplývá ze smlouva GAEA. Google si také vyhrazuje možnost jednostranně změnit bezpečnostní opatření, o kterých zákazníka jen informuje, a to ke všemu jen pokud zákazník projeví zájem o přijetí takovýchto informací. Zákazníkovi, za předpokladu, že nesouhlasí s danými změnami, však nevzniká právo na odstoupení od smlouvy. Ve volbě subdodavatelů nemá zákazník též žádný prostor vyjádřit své priority, neboť dává apriorní souhlas s jejich výběrem při uzavření smlouvy GAEA. V oblasti předávání dat do třetích zemí se smluvní úprava nestihla zaktualizovat a nereflektuje rozhodnutí Soudního dvora ve věci Schrems a prohlášení programu Safe Harbour za neplatné, neboť v ustanovení smlouva odkazuje na tento program osvědčení.

Co se týče smluvního rámce služby Microsoft Office 365, tak v oblasti odpovědnosti může být nepříznivé striktní vymezení omezení odpovědnosti, a to zejména ve vztahu škod způsobených porušením povinností ochrany osobních údajů. V otázce úpravy bezpečnostních opatření disponuje zákazník možností odstoupení od smlouvy, pokud se zavedenými změnami nesouhlasí, čímž toto ustanovení podporuje právně stanovenou povinnost uživatele jakožto správce údajů kontrolovat postupy zpracování údajů v souvislosti s adekvátními bezpečnostními podmínkami. Podobně je tomu v případě zapojování subdodavatelů do procesu zpracování údajů, s nimiž zákazník podle smluvního ujednání Microsoftu musí nejdříve souhlasit, a pokud tak neučiní, má právo bez postihu odstoupit od smlouvy. Tímto se opět potvrzuje autonomní postavení uživatele, správce údajů, a jeho povinností v rámci zpracování osobních údajů. Smluvní úprava Microsoftu je aktualizovaná, její smluvní podmínky jsou datovány k srpnu 2016, a reflektují tak aktuální vývoj v oblasti předávání údajů do třetích zemí, neboť neobsahují zmínku o programu Safe Harbour.

Komparací obou smluv z hlediska evropské úpravy ochrany osobních údajů se dojde k příznivějšímu výsledku u smlouvy služby Microsoft Office 365. Hlavním nedostatkem této smluvní úpravy je omezení odpovědnosti, ale i tak není v rozporu

s evropským právním rámcem ochrany osobních údajů. Další nedostatky jsou diskutabilní, a celkově smlouva společně se svými smluvními podmínkami splňuje požadavky dosavadní právní úpravy v podobě směrnice 95/46/ES a relevantních rozsudků a rozhodnutí Komise. Naproti tomu smluvní úprava Google Apps for Work obsahuje právní nedostatky většího a závažnějšího rozsahu, které částečně lze vyřešit dobrovolnou dohodou o zpracování dat, případně uzavřením standardních smluvních doložek, ale i tak zůstává řada problémů nevyřešena. Je proto možné, že v mnohých ustanoveních uživatelé služeb Google Apps for Work porušují zákonné požadavky na ochranu osobních údajů.[156]

Společnost Microsoft reflektuje změny na úrovni evropských právních předpisů a rozhodnutí, které se také snaží konformně zakomponovat do svého smluvního rámce pro poskytování online služeb. Úzce spolupracuje a konzultuje všechny nastalé změny i s pracovní skupinou WP29, která se následně vyjadřuje ke smluvním úpravám společnosti, viz například Letter for the Article 29 Working Party to Microsoft on the Microsoft Service Agreement[157] z roku 2014. Společnost Google ve svém smluvním rámci neobsahuje příliš kvalitní úpravu ochrany osobních údajů. Potvrzuje to i názor ve formě veřejného dopisu pracovní skupiny WP29 směrem ke společnosti Google ohledně jejích smluvních ustanovení, která údajně nesplňují požadavky evropských právních předpisů a jiných právních aktů týkající se ochrany osobních údajů.[158]

[156] TOMÍŠEK Jan. Office 365 V. Google Apps: Srovnání z hlediska ochrany osobních údajů. *Revue pro právo a technologie*, 6.ročník (11/2015), s. 174.
[157] Letter for the Article 29 Working Party to Microsoft on the Microsoft Service Agreement, *European Commission, Article 29 Data Protection Working Party*, 2014 [online]. Dostupné také z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf
[158] Letter from the Article 29 Working Party to Google on Google Privacy Policy, *European Commission, Article 29 Data Protection Working Party*, 2014 [online]. Dostupné také z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf

# Závěr

Cloud computing není novou technologií ve smyslu nového zařízení. Je to prostředí, které představuje spíše změnu v uvažování o poskytování služeb online a ve využívání výpočetních kapacit.

První kapitola ukázala, že myšlenka cloudu není nová, není otázkou neznámou, nýbrž jen technologie, ze které se cloud skládá, je otázkou 21. století. Jeho postupný vývoj a přizpůsobení se požadavkům uživatelů dalo vznik několika jeho vrstvám, neboli modelům služeb poskytovaných na cloudové infrastruktuře. Cloud je dnes poskytován i v několika různých formách odvislých od koncových uživatelů. Co se týče jeho právního ukotvení, jak je vidět v první kapitole, cloudové prostředí není zatím regulované jinak než prostřednictvím tzv. soft law na evropské úrovni.

Druhá kapitola poskytla vhled do licenčních způsobů poskytování služby SaaS, rámci níž je možné použít upravený open source software bez nutnosti dále šířit zdrojové kódy s výjimkou těch služeb, kde je modifikovaný software distribuován. Naproti tomu však stojí fakt, že pro využívání služeb SaaS však obecně zákazník licenci jakožto institut využívání duševního práva nepotřebuje. Smluvní úprava služeb SaaS ze zákona musí splňovat jisté požadavky na smlouvu tohoto druhu, jejímž středem zájmu je kvalitní úprava dohody o garantované úrovni služeb, neboli SLA.

Třetí kapitola se věnovala právnímu rámci ochrany osobních údajů na evropské úrovni, která se opírá o dosavadní směrnici 95/46/ES a nařízení GDPR. Nově přijatá úprava v porovnání s tou současnou přináší podstatné zlepšení co se týče úpravy postavení subjektu údajů a ochrany jeho osobních údajů, neboť přináší spoustu nových povinností pro správce, ale i zpracovatele údajů a zavádí nová práva subjektu údajů. V oblasti ochrany údajů zpřísňuje podmínky týkající se bezpečnostních opatření a to i v otázce předávání do třetích zemí nebo subdodavatelům. Na základě analýzy smluv o zpracování údajů dvou SaaS služeb Google Apps for Work a Microsoft Office 365 lze říci, že společnost Microsoft důkladněji reflektuje ve své smluvní úpravě požadavky

evropské právní úpravy na ochranu osobních údajů, přičemž společnost Google v mnohých ustanoveních své smluvní úpravy nesplňuje ani zákonné minium na ochranu zpracovávaných osobních údajů, včetně nedostatečné aktualizace.

V blízké budoucnosti se dá očekávat jak další vývoj technologický, tak i v oblasti ochrany osobních údajů, a to zejména některých zvláštních kategorií údajů. S tím, jak se Cloud computing rozšiřuje do jednotlivých sfér života, lze očekávat, že se budeme muset po právní stránce vypořádat i s ochranou velice citlivých údajů v rámci takto celosvětové infrastruktury na zpracování daných údajů. To je však tématem na další práci. Zajímavou myšlenkou nakonec je otázka dostupnosti cloudových služeb. Vývoj v cenové oblasti cloudu je otázkou budoucnosti, neboť s klesajícími cenami za jednotlivé technologické komponenty, ale s rostoucími cenami za poskytované služby, je otázka prozatím nezodpovězená.

# Seznam zkratek

| | |
|---|---|
| AEPD | Agencia Espanola de Proteccion de Datos |
| A29WP | Article 29 Working Party |
| AGPL | Affero General Public License |
| ASP | Application Service Providing |
| BCR | Binding Corporate Rules |
| CCSL | Cloud computing certification listopadu |
| C-SIG SLA | Cloud Select Industry Group on Service Level Agreements Subgroup |
| DPA | Data Processing Amendment |
| DPD | Data Protection Directive |
| EHP | Evropský hospodářský prostor |
| ENISA | European Union Network and Information Security Agency |
| ESD | Evropský Soudní dvůr |
| EU | Evropská unie |
| EUPL | European Union Public License |
| FOSS | Free and Open Source Software |
| GAEA | Google Apps Enterprise Agreement |
| GDPR | General Data Protection Regulation |
| LGPL | Lesser General Public License |
| GPL | General Public License |
| IaaS | Infrastructure as a Service |
| MCC | Model contract clauses |
| MIT | Massachusetts Institute of Technology |
| MOSA | Microsoft Online Subscription Agreement |
| NIST | National Institute of Standards and Technology |
| OST | Online Services Terms |
| PaaS | Platform as a Service |
| SaaS | Software as a Service |
| SIG-Cert | Subgroup on certification Schemes |

| | |
|---|---|
| SLA | Service Level Agreement |
| SSLA | Security Service Level Agreement |
| VPN | Virtual Private Network |
| WP29 | Working Party 29 |

# Použité prameny

## Právní předpisy a judikatura


1. Návrh Směrnice Evropského Parlamentu A Rady o některých aspektech smluv o poskytování digitálního obsahu č. COM(2015) 634 final. In: *Úřední věstník EU*. EUR-Lex, Brusel, 2015. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52015PC0634&from=EN
2. Zákon č. 89/2012 Sb., Občanský zákoník
3. Směrnice Evropského parlamentu a Rady 2001/29/ES ze dne 22. května 2001 o harmonizaci určitých aspektů autorského práva a práv s ním souvisejících v informační společnosti. In: *Úřední věstník EU*. EUR-Lex, 2001. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex%3A32001L0029
4. Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod.
5. Sdělení 209/1992, Sdělení federálního ministerstva zahraničních věcí o sjednání Úmluvy o ochraně lidských práv a základních svobod a Protokolů na tuto Úmluvu navazujících.
6. Sdělení Ministerstva zahraničních věcí, č. 115/2011 Sb.m.s, Úmluva o ochraně osob se zřetelem a automatizované zpracování osobních dat.
7. 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. In: *Úřední věstník EU*. EUR-Lex, 1995.
8. Smlouva o fungování Evropské unie, 9.5.2008, In: Úřední věstník Evropské unie.
9. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1.ledna 2015
10. Listina Základních Práv Evropské Unie 2012/C 326/02. In: *Úřední věstník Evropské unie*. EUR-Lex, 2012.
11. Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o

volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.

12. Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. 7. 2002, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. In: *Úřední věstník EU*. EUR-Lex, 2002.
13. Rozhodnutí Komise 2004/915/ES ze dne 27. prosince 2004, kterým se mění rozhodnutí 2001/497/ES, pokud jde o zavedení alternativního souboru standardních smluvních doložek pro předávání osobních údajů do třetích zemí (oznámeno pod číslem K(2004) 5271). In: *Úřední věstník EU*. EUR-Lex, 2004.
14. Nařízení Evropského Parlamentu A Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník EU*. EUR-Lex, 2016.
15. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů
16. Rozsudek Soudního Dvora ve věci C−101/01 Göta Hovrätt proti Bodil Lindqvist. In: *InfoCuria - Judikatura Soudního dvora*, 2003. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=cs&jur=C,T,F&num=C-101/01&td=ALL
17. Rozsudek Soudního Dvora ve věci C−131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mario Costeja González,. In: *InfoCuria - Judikatura Soudního dvora*, 2014. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=cs&jur=C,T,F&num=C-131/12&td=ALL
18. Rozsudek Soudního dvora ve věci C−73/07 Tietosuojavaltuutettu proti Satakunnan Markkinapörssi Oy, Satamedia Oy. In: *InfoCuria - Judikatura Soudního dvora*, 2008. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/07
19. Úmluva Rady Evropy č. 108 z r. 1981 o ochraně osob se zřetelem na automatizované zpracování osobních dat. Rada Evropy, 28.1.1981. Dostupné také z: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108
20. Rozhodnutí Komise 2000/520/ES ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované

podle zásad „bezpečného přístavu“ a s tím souvisejících „často kladených otázek“ vydaných Ministerstvem obchodu Spojených států. In: *Úřední věstník* L 215/7 *EU*. EUR-Lex, 2000. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32000D0520&from=CS

21. Rozsudek Soudního Dvora ve věci C□362/14 Maximillian Schrems proti Data Protection Commissioner. In: InfoCuria - Judikatura Soudního dvora, 2015. Dostupné také z: http://curia.europa.eu/juris/liste.jsf?num=C-362/14

## Monografie a časopisecké články

1. GUTH, Stephen. *Contract Negotiation Handbook: Software As a Service*. Guth Ventures LLC, 2013, 250 s. ISBN: 0988830809.
2. HON, W Kuan a Christopher MILLARD. *Cloud Computing vs Traditional Outsourcing – Key Differences* [online]. Computers & Law, Vol. 23, Issue 4, 2012 [cit. 2016-08-15]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2200592.
3. HON, W. Kuan, Christopher MILLARD a Ian WALDEN. *Negotiating Cloud Contracts: Looking At Clouds From Both Sides Now.* Stanford Technology Law Review [online]. 2012, Num. 1 (Vol. 16) [cit. 2016-08-17]. Dostupné z: http://stlr.stanford.edu/pdf/cloudcontracts.pdf.
4. HON, W Kuan, Christopher MILLARD a Ian WALDEN. *The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated?: The Cloud of Unknowing, part 1* [online]. Queen Mary University of London, School of Law, 2011 [cit. 2016-08-20]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1783577.
5. HON, W Kuan, Christopher MILLARD a Ian WALDEN. *Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, part 2* [online]. Queen Mary University of London, School of Law, 2011 [cit. 2016-08-20]. Dostupné z: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130.
6. CHALOUPKOVÁ, Helena a Petr HOLÝ. *Autorský zákon Komentář*. 4. Praha: C. H. Beck, 2012. ISBN 978-80 -7400-432-2.

7. JANSA, Lukáš; OTEVŘEL, Petr. Softwarové právo : praktický průvodce právní problematikou v IT. Aktualizované Vydání. Brno: Computer Press, 2014. 414 s. ISBN 9788025134580.
8. LANDY, Gene K. *The IT/Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet, Media and IP law*. Syngress Publishing, 2008. ISBN 978-1-59749-256-0.
9. MILLARD, Christopher a W Kuan HON. Cloud Technologies and Services. *Cloud Computing Law*. Oxford University Press, 2013, s. 448. ISBN 978-0-19-967167-0.
10. TOMÍŠEK Jan. Office 365 V. Google Apps: Srovnání z hlediska ochrany osobních údajů. *Revue pro právo a technologie*, 6.ročník (11/2015), s. 174.

## Ostatní literatura

1. A Quick Guide to GPLv3. GNU Operating System [online]. Free Software Foundation, 2014 [cit. 2016-08-18]. Dostupné z: https://www.gnu.org/licenses/quick-guide-gplv3.html
2. ARIF, Mohamed. A history of cloud computing. ComputerWeekly.com [online]. 2009 [cit. 2016-08-10]. Dostupné z: http://www.computerweekly.com/feature/A-history-of-cloud-computing
3. BADGER, Lee, Tim GRANCE, Robert PATT-CORNER a Jeff VOAS. Cloud Computing Synopsis and Recommendations Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-146 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
4. Cloud Computing: Benefits, risks and recommendations for information security [online]. European Network and Information Security Agency (ENISA), 2009 [cit. 2016-08-20]. Dostupné z: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

5. Cloud Select Industry Group on Service Level Agreements. DIGITAL SINGLE MARKET [online]. European Commission [cit. 2016-08-15]. Dostupné z: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-service-level-agreements
6. Cloud Select Industry Group on Certification Schemes (SIG - Cert). DIGITAL SINGLE MARKET [online]. European Commission [cit. 2016-08-15]. Dostupné z: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-certification-schemes
7. Cloud Select Industry Group on Code of Conduct. DIGITAL SINGLE MARKET [online]. European Commission [cit. 2016-08-15]. Dostupné z: https://ec.europa.eu/digital-single-market/en/cloud-select-industry-group-code-conduct
8. Communication From The Commission To The European Parliament And The Council: Transatlantic Data Flows: Restoring Trust through Strong Safeguards. European Commission, 2016, COM(2016) 117 final. Evropská komise. Dostupné také z: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-communication_en.pdf
9. DAVIES, Ron. Computing: An overview of economic and policy issues. In: European Parliamentary Research Service [online]. European Parliament, 2016, s. 23 [cit. 2016-08-15]. ISBN 978-92-823-9206-5. Dostupné z: http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_EN.pdf, s.17.
10. Data Processing Amendment to Google Apps Agreement [online], Google, 2016 [cit. 2016-08-20]. Dostupné z: https://www.google.com/work/apps/terms/dpa_terms.html
11. Expert Group on Cloud Computing Contracts. JUSTICE [online]. European Commission [cit. 2016-08-15]. Dostupné z: http://ec.europa.eu/justice/contract/cloud-computing/expert-group/index_en.htm
12. Exhibit X – Statement Of Work for Software as a Service Contracts, Contract For City of Seattle (vzor). Dostupné z: http://cdn.ttgtmedia.com/searchSecurity/downloads/SAASSOW.pdf

13. Frequently Asked Questions about version 2 of the GNU GPL. GNU Operating System [online]. Free Software Foundation, 2015 [cit. 2016-08-18]. Dostupné z: https://www.gnu.org/licenses/old-licenses/gpl-2.0-faq.en.html#GPLRequireSourcePostedPublic
14. GPL use in Debian on the rise: study. ItWire.com [online]. 2012 [cit. 2016-08-18]. Dostupné z: http://www.itwire.com/business-it-news/open-source/52838-gpl-use-in-debian-on-the-rise-study
15. Google Apps Enterprise (Online) Agreement [online], Google, 2016 [cit. 2016-08-20]. Dostupné z: https://www.google.com/intx/cs/work/apps/terms/2014/2/premier_terms_ie.html
16. HON, W Kuan. Open Season on Service Providers? The General Data Protection Regulation Cometh…. The IT Law Community [online]. 2015 [cit. 2016-08-20]. Dostupné z: http://www.scl.org/site.aspx?i=ed43376
17. IaaS Providers List: Comparison And Guide. Tom'sIT PRO [online]. [cit. 2016-08-13]. Dostupné z: http://www.tomsitpro.com/articles/iaas-providers,1-1560.html
18. IBM Software as a Service (SaaS) Support Handbook (vzor). Dostupné z: https://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf
19. Legal aspects of free and open source software. In: European Parliament: Directorate General For Internal Policies, 2013. Dostupné z: http://www.europarl.europa.eu/document/activities/cont/201307/20130708ATT69346/20130708ATT69346EN.pdf
20. Letter for the Article 29 Working Party to Microsoft on the Microsoft Service Agreement, European Commission, Article 29 Data Protection Working Party, 2014 [online]. Dostupné také z: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140922_letter_microsoft_service_agreement.pdf
21. Letter from the Article 29 Working Party to Google on Google Privacy Policy, European Commission, Article 29 Data Protection Working Party, 2014 [online]. Dostupné také z: http://ec.europa.eu/justice/data-protection/article-

29/documentation/other-document/files/2014/20140923_letter_on_google_privacy_policy.pdf

22. Master SubscriptionAgreement Salesforce.com, Dostupné z: http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf
23. MELL, Peter, Tim GRANCE,. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-145 [online]. U.S. Department of Commerce: National Institute of Standards and Technology, 2011 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
24. Microsoft Online Services Terms [online], Microsoft, August 2016 [cit. 2016-08-20]. Dostupné z: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=31
25. Microsoft Online Subscription Agreement [online], Microsoft, 2016 [cit. 2016-08-20]. Dostupné z: https://www.microsoft.com/online/mosa/MOSA2014Agr(NA)(ENG)(Nov2014)(HTML).htm
26. Obecná veřejná licence GNU v.2 (GNU GPL v.2). Free Software Foundation, 1991. Dostupné z: http://www.gnugpl.cz/v2/
27. Obecná veřejná licence GNU v.3 (GNU GPL v.3). Free Software Foundation, 2007. Dostupné z: http://www.gnugpl.cz/v3/
28. Online Services Consolidated SLA [online], Microsoft, August 2016 [cit. 2016-08-20]. Dostupné z: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37
29. Opinion 4/2007 on the concept of personal data, 01248/07/EN WP 136. European Commission, Article 29 Data Protection Working Party, 2007 [online]. Dostupné také z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf
30. Opinion 05/2012 on Cloud Computing, 01037/12/EN WP 196, European Commission, Article 29 Data Protection Working Party, 2012 [online].

Dostupné také z: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

31. Opinion 1/2010 on the concepts of "controller" and "processor", 00264/10/EN WP 196, European Commission, Article 29 Data Protection Working Party, 2010 [online]. Dostupné také z: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf
32. OTEVŘEL, Petr. Vybraná úskalí uzavírání smluv typu SaaS: Právní aspekty IT služeb typu cloud computing. SystemOnLine: S přehledem ve světě informačních technologií [online]. 2012, (4.) [cit. 2016-08-17]. Dostupné z: https://www.systemonline.cz/it-pravo/vybrana-uskali-uzavirani-smluv-typu-saas.htm
33. PaaS Providers List: Comparison And Guide. Tom'sIT PRO [online]. [cit. 2016-08-13]. Dostupné z: http://www.tomsitpro.com/articles/paas-providers,1-1517.html
34. Reform of EU data protection rules. European Commission: Justice [online]. [cit. 2016-08-19]. Dostupné z: http://ec.europa.eu/justice/data-protection/reform/index_en.htm
35. SaaS Providers List: Comparison And Guide. Tom'sIT PRO [online]. [cit. 2016-08-13]. Dostupné z: http://www.tomsitpro.com/articles/saas-providers,1-1554.html
36. Sdělení Komise Evropskému Parlamentu, Radě, Evropskému Hospodářskému A Sociálnímu Výboru A Výboru Regionů: Uvolnění potenciálu cloud computingu v Evropě. COM(2012) 529 final ze dne 27.09.2012. In: Úřední věstník EU. EUR-Lex, 2012. Dostupné také z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:52012DC0529&from=E
37. 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, 2016 [cit. 2016-08-20]. Dostupné z: https://www.google.com/work/apps/terms/mcc_terms.html
38. WAYNE Jansen Timothy GRANCE. Guidelines on Security and Privacy in Public Cloud Computing. NIST Special Publication 800-144 [online]. U.S.

Department of Commerce: National Institute of Standards and Technology, 2012 [cit. 2016-08-11]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf, s. 3.

# Seznam příloh

1. Příloha 1 – smlouva Google Apps Enterprise Online Agreement (GAEA), vybraná ustanovení
2. Příloha 2 – dodatek ke smlouvě Data Processing Amendment to Google Apps Agreement (DPA), vybraná ustanovení
3. Příloha 3 – smlouva Microsoft Online Subscription Agreement (MOSA), vybraná ustanovení
4. Příloha 4 – smluvní podmínky Online Services Terms datované k srpnu 2016, vybraná ustanovení o zpracování dat (OST).