ZNALECKÝ POSUDEK

č. 145-2017

Posouzení, zda splňuje cloudová služba Microsoft Azure poskytovaná společností Microsoft jakožto zpracovatelem osobních údajů požadavky nařízení GDPR

Objednatel:	**MICROSOFT s.r.o.** **IČ: 47123737** **Vyskočilova 1561/4a** **140 00 Praha 4**
Zhotovitel:	**Ústav kvalifikovaný pro znaleckou činnost** **Cetag, s.r.o.** **IČ: 27451925** **Na Poříčí 1070/19** **110 00 Praha 1**
Účel posudku:	**Právní úkony objednatele**

V Praze, dne 15. dubna 2017

Znalecký posudek se vydává písemně ve třech vyhotoveních, dvě vyhotovení se předávají objednateli a jedno vyhotovení se ukládá do digitálního archívu znaleckého ústavu. Posudek má celkem -42- stran, z toho -40- stran textu a -2- strany příloh.

OBSAH

1 Objednatel

MICROSOFT s.r.o.

IČ: 47123737

Vyskočilova 1561/4a

140 00 Praha 4

Posudek je vydáván na základě objednávky #97865027 ze dne 1. 3. 2017

Kontaktní osoba: Ing. Zdeněk Jiříček

Tel.: +420 725517517

Email: zdenekj@microsoft.com

2 Zhotovitel

Ústav kvalifikovaný pro znaleckou činnost

Cetag, s.r.o.

Na Poříčí 1070/19

Praha 1 – 110 00

(dále také jen „Znalec")

IČ: 27451925

OR: C 114044 společnost vedená u rejstříkového soudu v Praze

Telefon: 222 314 164

Mobil: 724 871 197

Email: info@cetag.com

ŘEŠITELSKÝ TÝM ZNALECKÉHO POSUDKU		
1.	**Hlavní řešitel:**	**Ing. Jaroslav Mráz**
	Kvalifikace:	Soudní znalec
2.	**Řešitel:**	**Ing. René Piták**
	Kvalifikace:	Soudní znalec
3.	**Řešitel:**	**Jan Vojtěch Binder**
	Kvalifikace:	ICT expert

3 Zadání znaleckého posudku

Objednávka č.: 97865027

Vystavena: 1. března 2017

Kontaktní osoba: Zdeněk Jiříček

email: zdenekj@microsoft.com

Otázka na Znalce:

Zadavatel požaduje ověření vlastností cloudu AZURE dle následující otázky:

Splňuje cloudová služba Microsoft Azure poskytovaná společností Microsoft jakožto zpracovatelem osobních údajů na základě čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů („nařízení") požadavky na vhodná opatření a záruky, včetně bezpečnostních opatření a mechanismů, které je správce osobních údajů povinen přijmout v souladu s čl. 32 a čl. 35 odst. 7 nařízení, a to pro automatizované zpracování údajů o zdravotním stavu a jiných zdravotnických dat odpovídajícímu přiložené studii (tj. pro zpracování zvláštních kategorií osobních údajů)?

Termín vyhotovení: 15. dubna 2017

4 Dokumenty, ze kterých Znalec čerpal

- CELEX_32016R0679_CS_TXT.pdf
  - zdroj: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1489484200339&uri=CELEX:32016R0679
  - 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)
- CELEX_32016L0680_CS_TXT.pdf
  - zdroj: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1489533632400&uri=CELEX:32016L0680
  - SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV
- CELEX%3A32014R0910%3ACS%3ATXT.pdf
  - zdroj: http://eur-lex.europa.eu/legal-content/CS/TXT/?qid=1490709179993&uri=CELEX:32014R0910
  - NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES
- sb0039-2012-98-2012.pdf
  - Zdroj: https://www.psp.cz/sqw/sbirka.sqw?cz=98&r=2012
  - VYHLÁŠKA ze dne 22. března 2012 o zdravotnické dokumentaci
- S.ICZ_MICR01451-Healthcare_AR_SecControls_Azure_130_Final.pdf
  - Analýza rizik a bezpečnostní opatření zdravotnických IS v cloudu
- Priloha 1 - Metodika analyzy rizik.pdf
  - Metodika analýzy rizik Verze: 1.2
- Priloha 2 - AR pro scenar 1.pdf
- Priloha 3 - AR pro scenar 2.pdf
- Priloha 4 - AR pro scenar 3.pdf
- Priloha 5 - AR pro scenar C.pdf
- S.ICZa.s.-Protecting_Data_in_MS_Cloud_202_Final.pdf
  - Protecting Data in Microsoft Online Services
- Microsoft Corporation: Microsoft Security Policy, 6. 1. 2016
- Zákon č. 181/2014 Sb.
- (M434)EnrAmend(GDPRTerms)(WW)(CZE)(Apr2017)(IU).docx
  - GDPR podmínky - Dodatek M434
- Archív Znalce (znaleckého ústavu)

- Veřejně dostupné zdroje

Upozornění: *Ačkoliv mám jako znalec za to, že informace, na jejichž základě je znalecký posudek zpracován, byly nashromážděny ze spolehlivých zdrojů, zároveň ale upozorňuji, že nepřebírám žádnou odpovědnost za pravdivost a přesnost jakýchkoliv takto získaných informací. Neprováděl jsem tudíž žádná šetření směřující k ověření pravosti, správnosti a úplnosti předložených dokumentů, ze kterých jsem ve svém znaleckém posudku vycházel. V posudku jsem vycházel pouze z výše uvedených dokumentů.*

5 Nález

Zadavatel poskytuje zákazníkům v České republice celou řadu produktů a služeb. Od 25. května 2018 vstoupí v účinnost Nařízení Evropského parlamentu a Rady (EU) 2016/679 General Data Protection Regulation (dále též GDPR), které mění a zpřísňuje některé stávající opatření pro ochranu osobních dat, například zákon č. 101/2000 sb.

Zadavatel požaduje ověření vlastností cloudu AZURE dle následující otázky: *Splňuje cloudová služba Microsoft Azure poskytovaná společností Microsoft jakožto zpracovatelem osobních údajů na základě čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů („nařízení") požadavky na vhodná opatření a záruky, včetně bezpečnostních opatření a mechanismů, které je správce osobních údajů povinen přijmout v souladu s čl. 32 a čl. 35 odst. 7 nařízení, a to pro automatizované zpracování údajů o zdravotním stavu a jiných zdravotnických dat odpovídajícímu přiložené studii (tj. pro zpracování zvláštních kategorií osobních údajů)?*

5.1 Rozhodné datum

Znalec určil jako Rozhodné datum **15. dubna 2017** (datum vyhotovení)

5.2 Definice pojmů

dle Zákona č. 181/2014 Sb. je popsána role:

Správce - správcem informačního systému je orgán nebo osoba, kteří určují účel zpracování informací a podmínky provozování informačního systému

dle Zákona č. 101/2000 Sb. je popsána role:

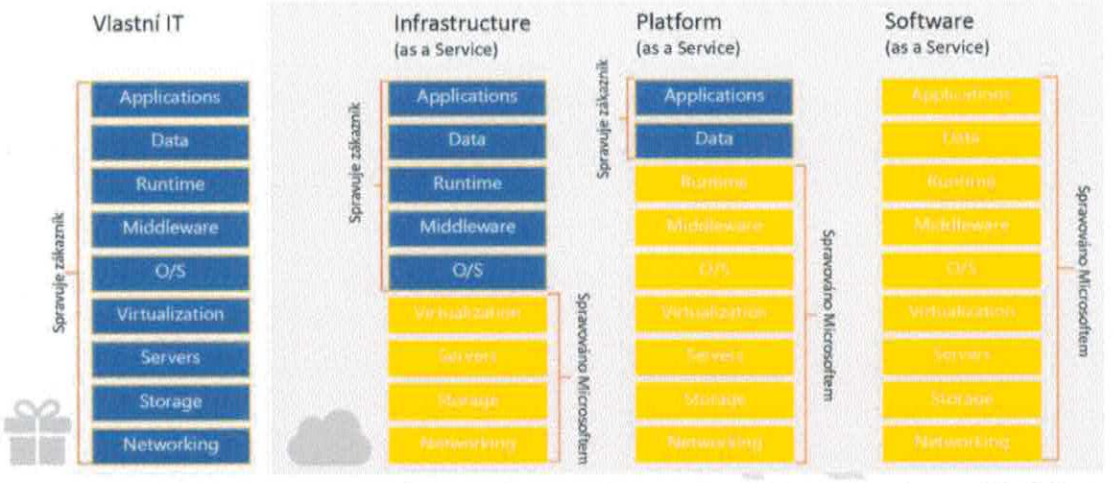
Zpracovatel - zpracovatelem je každý subjekt, který na základě zvláštního zákona nebo pověření správcem zpracovává osobní údaje podle tohoto zákona

5.3 Microsoft cloud – AZURE

Microsoft Azure je otevřené a flexibilní cloudové prostředí pro tvorbu, nasazení a správu aplikací provozovaných v síti datových center společnosti Microsoft rozmístěných po celém světě. Principem cloudové služby je poskytování hardwarových nebo softwarových prostředků formou služby, bez fyzického přístupu k samotnému hardwaru (k serverům, síťovým prvkům a podobně). Aplikace a servery v cloudu je možné propojit s již existujícími servery a aplikacemi v prostředí zákazníka.

Cloudové služby jsou služby informačních technologií poskytované prostřednictvím zabezpečeného internetového propojení, případně vyhrazeným privátním síťovým spojením s datovým centrem. Umožňují využívat aplikace bez nutnosti jejich instalace v prostředí zákazníka na lokálních serverech. Mezi řadu výhod patří například snadno rozšiřitelný výpočetní výkon, automatické navýšení výkonu dle potřeb zákazníka nebo

vytížení serverů, zpoplatnění pouze aktuálně využívaného výpočetního výkonu a podobně. Cloudové služby se dělí, dle úrovně správy v odpovědnosti poskytovatele, na **Infastructure as a Service (IaaS)** – tj. infrastruktura jako služba, kdy poskytovatel cloudových služeb zodpovídá na provoz HW vybavení, sítí a systémů pro provoz operačních systémů), dále na **Platform as a Service (PaaS)** – platforma jako služba, kdy poskytovatel cloudových služeb nad výše uvedený rámec IaaS provozuje a spravuje i operační systém s požadovanou platformou (např. webový nebo aplikační server, SQL databáze - bez nutnosti aby zákazník instaloval a provozoval server) až po **Software as a Service (SaaS)** – aplikace jako služba, kdy poskytovatel služby nabízí hotová řešení na úrovni aplikací (u Microsoftu např. elektronická pošta - Exchange online, Uložiště dokumentů - SharePoint Online, hlasové a video konference - Skype for Business a další).



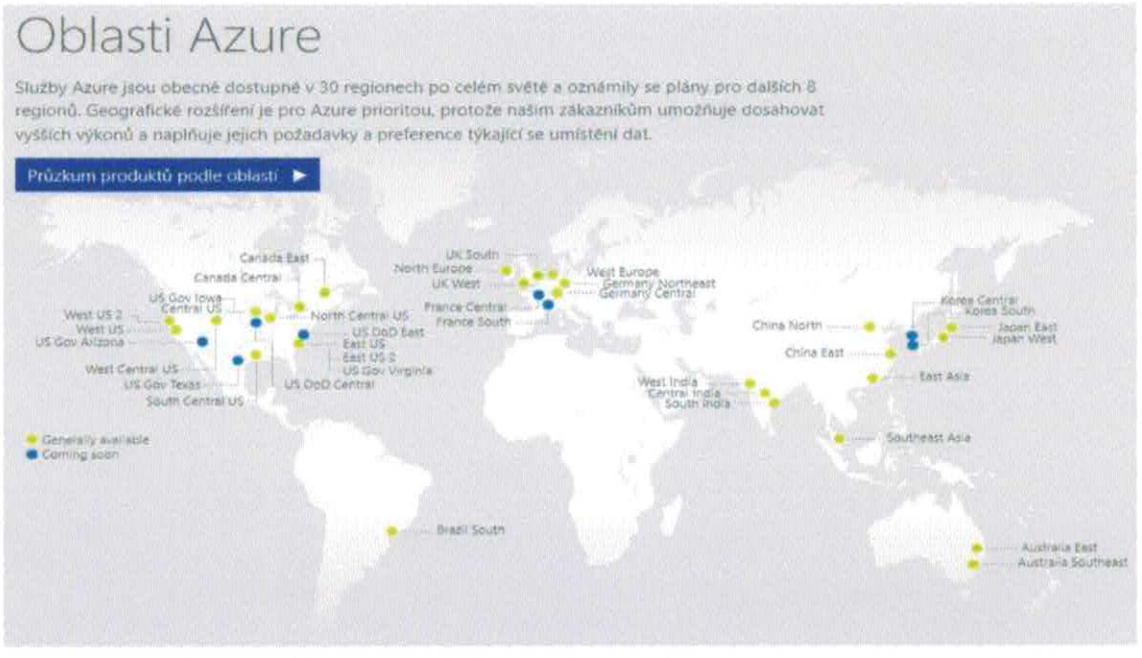
Provozovatelé Cloudových služeb bývají specializované subjekty, které vytvářejí často komplexní řešení geograficky rozložené ve více oblastech.

Z hlediska vlastnictví lze jednotlivé modely rozdělit na:

- Veřejný cloud (public cloud) – služby jsou nabízeny na společném HW základě pro otevřenou množinu zákazníků. Jednotliví zákazníci jsou bezpečně odděleni, aby nemohli navzájem nahlížet do dat a aplikací.
- Soukromý (privátní) – služby jsou poskytovány v rámci jedné organizace nebo pro přesně vymezenou související množinu subjektů. V tuto chvíli nejsou technologie velkých provozovatelů Cloudu na toto uzpůsobeny, a tak se obvykle jedná o proprietární řešení.
- Hybridní cloud – je kombinace obou výše uvedených přístupů.

5.3.1 Umístění datových center

Vlastní poskytování služeb Microsoft Azure, probíhá z datových center, která jsou nyní umístěna v 38 regionech na 3 kontinentech viz obrázek *(zdroj: https://azure.microsoft.com/cs-cz/regions/)*:



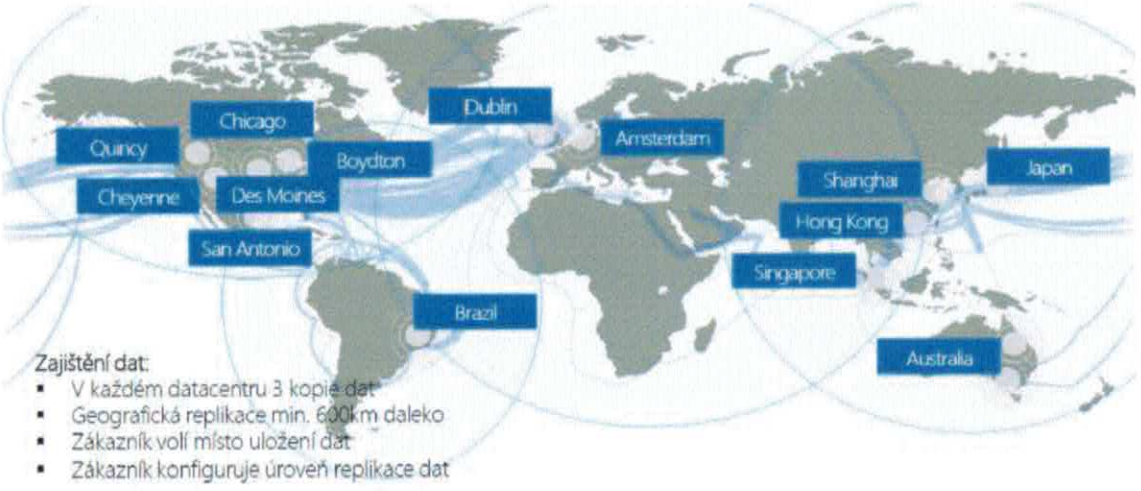
Obrázek 2 -oblasti Microsoft Azure

Datová centra umístěná v Evropě jsou v těchto státech:

Oblast	Umístění
Severní Evropa	Irsko
Západní Evropa	Nizozemsko
Německo – střed[1]	Frankfurt
Německo – severovýchod	Magdeburg
Spojené království – západ	Cardiff
Spojené království – jih	Londýn
NOVĚ OZNÁMENO	
Francie – střed	Oznámí se
Francie – jih	Oznámí se

Podle dostupných podkladů byla datová centra zajišťující službu Azure už v roce 2014 umístěna v následujících lokalitách:

[1] datová centra v Německu jsou oddělená od zbytku infrastruktury a mají specifický režim provozu.



Takže již **k Rozhodnému datu** disponoval Microsoft v rámci členských států EU centry v **Dublinu** (Irsko) a **Amsterodamu** (Holandsko)

5.4 GDPR

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 (dále jen „obecné nařízení o ochraně osobních údajů" nebo „GDPR") vstoupí v účinnost 25. 5. 2018, a to plošně ve všech státech EU. GDPR stanoví obecná pravidla pro správu a zpracování osobních údajů a od chvíle, kdy vstoupí v účinnost, bude platit jako přímo aplikovatelná legislativa v České republice. Očekává se, že v rámci zákonodárného procesu na národní úrovni bude stávající zákon o ochraně osobních údajů této situaci přizpůsoben.

Klíčové části nařízení a směrnice pro zpracování zdravotních údajů jsou:

5.4.1 Odstavec 24 odůvodnění Směrnice EU 2016/680

(24) Mezi osobní **údaje o zdravotním stavu** by měly být zahrnuty **veškeré údaje související se zdravotním stavem subjektu údajů,** které vypovídají o minulém, současném či budoucím tělesném nebo duševním zdraví subjektu údajů. To zahrnuje informace o dané fyzické osobě shromážděné v průběhu registrace pro účely zdravotní péče a jejího poskytování dotčené fyzické osobě podle směrnice Evropského parlamentu a Rady 2011/24/EU (1); číslo, symbol nebo specifický údaj přiřazený fyzické osobě za účelem její jedinečné identifikace pro zdravotnické účely; informace získané během provádění testů nebo vyšetřování části těla nebo tělesných látek, včetně z genetických údajů a biologických vzorků, a jakékoliv informace například o nemoci, postižení, riziku onemocnění, anamnéze, klinické léčbě nebo fyziologickém či biomedicínském stavu subjektu údajů nezávisle na jejich původu, tedy bez ohledu na to, zda pocházejí například od lékaře nebo jiného zdravotníka, z nemocnice, ze zdravotnického prostředku či diagnostických testů in vitro.

5.4.2 *Článek 28* Zpracovatel

1. Pokud má být zpracování provedeno pro správce, využije správce pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby dané zpracování splňovalo požadavky tohoto nařízení a aby byla zajištěna ochrana práv subjektu údajů.

2. Zpracovatel nezapojí do zpracování žádného dalšího zpracovatele bez předchozího konkrétního nebo obecného písemného povolení správce. V případě obecného písemného povolení zpracovatel správce informuje o veškerých zamýšlených změnách týkajících se přijetí dalších zpracovatelů nebo jejich nahrazení, a poskytne tak správci příležitost vyslovit vůči těmto změnám námitky.

3. Zpracování zpracovatelem se řídí smlouvou nebo jiným právním aktem podle práva Unie nebo členského státu, které zavazují zpracovatele vůči správci a v nichž je stanoven předmět a doba trvání zpracování, povaha a účel zpracování, typ osobních údajů a kategorie subjektů údajů, povinnosti a práva správce. Tato smlouva nebo jiný právní akt zejména stanoví, že zpracovatel:

   a) zpracovává osobní údaje pouze na základě doložených pokynů správce, včetně v otázkách předání osobních údajů do třetí země nebo mezinárodní organizaci, pokud mu toto zpracování již neukládají právo Unie nebo členského státu, které se na správce vztahuje; v takovém případě zpracovatel správce informuje o tomto právním požadavku před zpracováním, ledaže by tyto právní předpisy toto informování zakazovaly z důležitých důvodů veřejného zájmu;

   b) zajišťuje, aby se osoby oprávněné zpracovávat osobní údaje zavázaly k mlčenlivosti nebo aby se na ně vztahovala zákonná povinnost mlčenlivosti;

   c) přijme všechna opatření požadovaná podle článku 32;

   d) dodržuje podmínky pro zapojení dalšího zpracovatele uvedené v odstavcích 2 a 4;

   e) zohledňuje povahu zpracování, je správci nápomocen prostřednictvím vhodných technických a organizačních opatření, pokud je to možné, pro splnění správcovy povinnosti reagovat na žádosti o výkon práv subjektu údajů stanovených v kapitole III;

   f) je správci nápomocen při zajišťování souladu s povinnostmi podle článků 32 až 36, a to při zohlednění povahy zpracování a informací, jež má zpracovatel k dispozici;

   g) v souladu s rozhodnutím správce všechny osobní údaje buď vymaže, nebo je vrátí správci po ukončení poskytování služeb spojených se zpracováním, a vymaže existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;

h) poskytne správci veškeré informace potřebné k doložení toho, že byly splněny povinnosti stanovené v tomto článku, a umožní audity, včetně inspekcí, prováděné správcem nebo jiným auditorem, kterého správce pověřil, a k těmto auditům přispěje. 4.5.2016 L 119/49 Úřední věstník Evropské unie CS Pokud jde o první pododstavec písm. h), informuje zpracovatel neprodleně správce v případě, že podle jeho názoru určitý pokyn porušuje toto nařízení nebo jiné předpisy Unie nebo členského státu týkající se ochrany údajů.

4. **Pokud zpracovatel zapojí dalšího zpracovatele, aby jménem správce provedl určité činnosti zpracování, musí být tomuto dalšímu zpracovateli uloženy na základě smlouvy nebo jiného právního aktu podle práva Unie nebo členského státu stejné povinnosti na ochranu údajů, jaké jsou uvedeny ve smlouvě nebo jiném právním aktu mezi správcem a zpracovatelem podle odstavce 3, a to zejména poskytnutí dostatečných záruk, pokud jde o zavedení vhodných technických a organizačních opatření tak, aby zpracování splňovalo požadavky tohoto nařízení.** Neplní-li uvedený další zpracovatel své povinnosti v oblasti ochrany údajů, odpovídá správci za plnění povinností dotčeného dalšího zpracovatele i nadále plně prvotní zpracovatel.

5. Jedním z prvků, jimiž **lze doložit dostatečné záruky** podle odstavců 1 a 4 tohoto článku, je skutečnost, že z**pracovatel dodržuje schválený kodex chování uvedených v článku 40** nebo **schválený mechanismus pro vydávání osvědčení uvedený v článku 42**.

6. Aniž jsou dotčeny individuální smlouvy mezi správcem a zpracovatelem, mohou být smlouvy nebo jiné právní akty podle odstavců 3 a 4 tohoto článku založeny zcela nebo částečně na standardních smluvních doložkách podle odstavců 7 a 8 tohoto článku, mimo jiné i v případě, že jsou součástí osvědčení uděleného správci či zpracovateli podle článků 42 a 43.

7. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky stanovit Komise přezkumným postupem podle čl. 93 odst. 2.

8. Pro záležitosti uvedené v odstavcích 3 a 4 tohoto článku může standardní smluvní doložky přijmout dozorový úřad v souladu s mechanismem jednotnosti uvedeným v článku 63.

9. Smlouva nebo jiný právní akt podle odstavců 3 a 4 musí být vyhotoveny písemně, v to počítaje i elektronickou formu.

10. Aniž jsou dotčeny články 82, 83 a 84, pokud zpracovatel poruší toto nařízení tím, že určí účely a prostředky zpracování, považuje se ve vztahu k takovému zpracování za správce.

5.4.3 *Článek 32* Zabezpečení zpracování

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel

vhodná technická a organizační opatření, **aby zajistili úroveň zabezpečení odpovídající danému riziku**, případně včetně:

a) **pseudonymizace a šifrování osobních údajů**; 4.5.2016 L 119/51 Úřední věstník Evropské unie CS

b) schopnosti **zajistit neustálou důvěrnost, integritu, dostupnost a odolnost** systémů a služeb zpracování;

c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

2. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.

3. Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je dodržování schváleného kodexu chování uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.

4. Správce a zpracovatel přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu.

5.4.4 *Článek 35 Posouzení vlivu na ochranu osobních údajů*

1. **Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.**

2. Při provádění posouzení vlivu na ochranu osobních údajů si správce vyžádá posudek pověřence pro ochranu osobních údajů, byl-li jmenován.

3. Posouzení vlivu na ochranu osobních údajů podle odstavce 1 je nutné zejména v těchto případech:

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

4. Dozorový úřad sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů podle odstavce 1. Dozorový úřad uvedené seznamy předá sboru.

5. Dozorový úřad může rovněž sestavit a zveřejnit seznam druhů operací zpracování, u nichž není posouzení vlivu na ochranu osobních údajů nutné. Dozorový úřad uvedené seznamy předá sboru.

6. Před přijetím seznamů podle odstavců 4 a 5 použije příslušný dozorový úřad mechanismus jednotnosti uvedený v článku 63, pokud tyto seznamy zahrnují činnosti zpracování související s nabídkou zboží či služeb subjektům údajů nebo s monitorováním jejich chování v několika členských státech, nebo jestliže dané seznamy mohou výrazně ovlivnit volný pohyb osobních údajů v rámci Unie. 4.5.2016 L 119/53 Úřední věstník Evropské unie CS

7. **Posouzení obsahuje alespoň:**

a) systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;

b) posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;

c) posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci 1

d) plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.

8. Dodržování schválených kodexů chování podle článku 40 příslušnými správci nebo zpracovateli se řádně zohlední při posuzování dopadu operací zpracování prováděných těmito správci či zpracovateli, zejména pro účely posouzení vlivu na ochranu osobních údajů.

9. Správce ve vhodných případech získá k zamýšlenému zpracování stanovisko subjektů údajů nebo jejich zástupců, aniž by byla dotčena ochrana obchodních či veřejných zájmů nebo bezpečnost operací zpracování.

10. Pokud má zpracování podle čl. 6 odst. 1 písm. c) nebo e) právní základ v právu Unie nebo členského státu, které se na správce vztahuje, a toto právo upravuje konkrétní operaci nebo soubor operací zpracování a pokud bylo posouzení vlivu na ochranu osobních údajů již provedeno jakožto součást obecného posouzení dopadů v souvislosti s přijetím uvedeného právního základu, odstavce 1 až 7 se nepoužijí, ledaže by členské státy považovaly provedení tohoto posouzení před činnostmi zpracování za nezbytné.

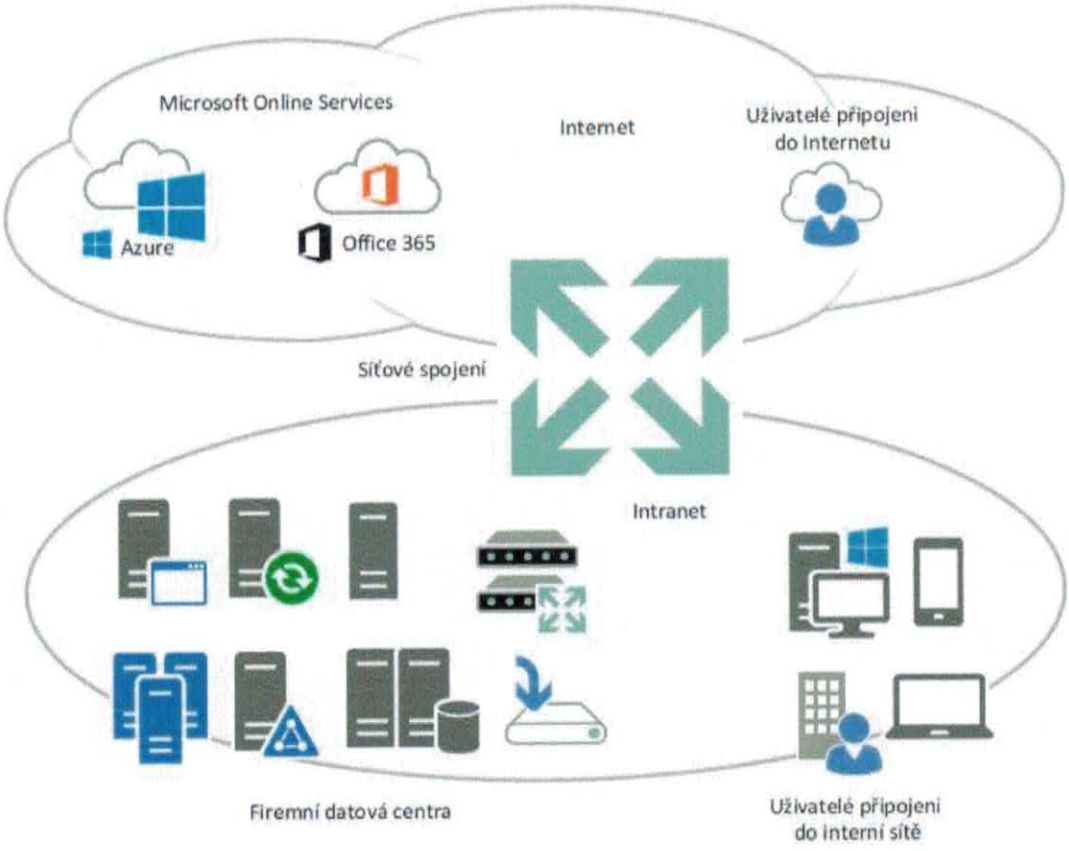
11. Správce případně provede přezkum s cílem posoudit, zda je zpracování prováděno v souladu s posouzením vlivu na ochranu osobních údajů alespoň v případech, kdy dojde ke změně rizika, jež představují operace zpracování.

5.5 Problematika umístění citlivých dat a aplikací v cloudu

Citlivá data je třeba chránit proti přístupu nepovolané osoby. Ochrana dat a aplikací může být buďto fyzickou formou, tj. ochranou prostředků s takovými daty a aplikacemi, a to včetně celé infrastruktury. V současnosti je ale většinou základním požadavkem i dostupnost prostřednictvím internetu. V takovou chvíli stejně musí nastoupit ochrana dat nějakým dalším opatřením. Standardně se používají metody šifrovaného (kryptovaného) přenosu. Pro útočníka, který sleduje provoz na síti, je pak taková komunikace nečitelná. V případě, že umístím data a aplikace do cloudu, tj. do úložiště poskytovatele cloudových služeb (viz: 5.3 Microsoft cloud – AZURE) je nutné je ochránit před zneužitím. To mohu zajistit šifrováním nebo pseudonymizací. Článek 3 odst. 5 Směrnice 2016/680 - „pseudonymizací" zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě.

5.6 Architektura řešení

Obecná řešení v Cloudu se obvykle stávají doplňkem firemního řešení. Zákazník cloudu si tak některé funkce ponechá u sebe. Do Cloudu umístí některé role. Typicky mail, firemní portál, služby na sdílení dokumentů apod. Následující obrázek zjednodušeně ukazuje zapojení Cloudu do stávajícího firemního řešení.



6 Posudek

6.1 Rizika zpracování informací v cloudu

6.1.1 Nedostatek kontroly

Umístění osobních údajů v cloudových úložištích včetně aplikací ztrácí Správce výlučnou kontrolu nad těmito údaji. Není jednoznačné, jak by mohl definovat plně organizační, technická a jiná opatření k plné kontrole na daty. Hrozí:

- Malá kontrola nad umístěním dat a obtížná přemístitelnost např. z lokality do lokality nebo případně k jinému poskytovateli cloudových služeb. Překážkou je propustnost linek, součinnost provozovatele, různé prostředí po technické stránce apod.
- Závislost na dalších zdrojích a dodavatelích – síťová infrastruktura internetu, tj. nutnost funkčního propojení mezi cloudem a Správcem.
- Nedostatečná integrita způsobená sdílením zdrojů: Cloud sestává ze sdílených systémů a infrastruktury. Poskytovatelé cloudových služeb zpracovávají osobní údaje pocházející z různých zdrojů, tj. od různých subjektů údajů či organizací, a může dojít ke střetu zájmů anebo zpracování může sloužit různým cílům.
- Nedostatek důvěrnosti ve smyslu žádostí o vymáhání práva adresovaných přímo poskytovateli cloudových služeb: osobní údaje zpracovávané v cloudu mohou být předmětem žádostí o vymáhání práva podaných donucovacími orgány členských států EU nebo třetích zemí. Existuje riziko, že osobní údaje mohou být sděleny (cizím) donucovacím orgánům bez platného právního základu EU, čímž by došlo k porušení právních předpisů EU pro ochranu údajů.
- Neschopnost intervence (práva subjektů údajů): Je možné, že poskytovatel cloudových služeb nezajistí nezbytná opatření a nástroje, jež by správci napomohly při správě údajů, např. pokud jde o přístup k údajům, jejich **výmaz** či opravu.
- Chybějící izolovanost: Poskytovatel cloudových služeb může využívat fyzickou kontrolu nad údaji od různých zákazníků k propojování osobních údajů.

6.1.2 Nedostatek informací o zpracování

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

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

- Řetězec zpracování zahrnuje více zpracovatelů a subdodavatelů.
- Osobní údaje jsou zpracovávány na různých místech v rámci EHP, což má přímý dopad na právní předpisy použitelné pro veškeré spory ohledně ochrany údajů, k nimž může dojít mezi uživatelem a poskytovatelem.

- Osobní údaje jsou předávány do třetích zemí mimo EHP. Třetí země nemusí zajišťovat odpovídající úroveň ochrany údajů a předávání údajů nemusí být spojeno s vhodnými ochrannými opatřeními (např. standardní smluvní doložky nebo závazná podniková pravidla), a mohlo by být tudíž nezákonné.

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

6.1.3 Výmaz dat

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

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

Znalec dospěl k závěru, že data jsou v Cloudu uložena na úložištích typu disková pole, kde vlastní informace jsou rozprostřeny na více discích. Jeden disk vlastně nese jen nepoužitelnou část informace, a tak jeho mazání demagnetizací nebo opakovaným přepisem není nutné. Na diskovém poli jsou navíc data uložena ve virtuálním prostoru a po jeho odstranění lze jen těžko identifikovat, kde a jak byla skutečně uložena a při případné kompromitaci takového zařízení z něj zpětně data sestavit. Jiná situace by mohla nastat u záloh, ale tam Znalec nepředpokládá, že by tyto byly realizovány jinak než šifrovaně.

6.1.4 Prostředí AZURE a bezpečnost

V prostředí Microsoft AZURE je implementováno množství bezpečnostních politik (a návazných bezpečnostních standardů), přičemž většina z nich je z bezpečnostních důvodů dostupná pouze pracovníkům společnosti Microsoft.

Pro zákazníky využívající služby Office 365 a Microsoft AZURE jsou k dispozici dokumenty popisující zavedená opatření a jejich úroveň s podrobností nabízející základní přehled o opatřeních, ale zároveň nezvyšující rizika služeb Microsoft. Zejména se jedná o následující dokumenty:

- Bezpečnostní politika „Microsoft Security Policy (External)"
- Dokument „Microsoft Online Services Controls as Aligned to ISO/IEC 27001:2013 with ISO/IEC 27018:2014"
- Zprávy z auditu podle normy ISO/IEC 27001

- Dodatek M434

Dále je zákazník Microsoft AZURE právně a provozně zajištěn zněním a implementací postupů dle dodatku M434, který detailně popisuje role a zodpovědnosti ve vztahu ke zpracovávaným a uchovávaným datům, a to s ohledem právě na požadavky GDPR

6.2 Povinnosti Správce VIS

6.2.1 Základní požadavky

- zavést organizaci řízení bezpečnosti informací,
- určit výbor pro řízení kybernetické bezpečnosti a
- určit bezpečnostní role (přiměřeně k rolím požadovaným po správci KII – viz dále) a jejich práva a povinnosti související s informačním systémem.
- Pro naplnění identifikovaných požadavků musí správce KII
- Zavést organizaci řízení bezpečnosti informací
- Určit výbor pro řízení kybernetické bezpečnosti a určit bezpečnostní role a jejich práva a povinnosti související s informačním systémem, konkrétně role:
  - manažer kybernetické bezpečnosti,
  - architekt kybernetické bezpečnosti,
  - auditor kybernetické bezpečnosti a garant aktiva.

6.2.2 Opatření v rámci řešení v cloudu

Správce musí zajistit takové zabezpečení, aby v celém procesu zpracování dat byly zajištěny veškeré požadavky dané pro příslušnou úroveň citlivosti informací. Vhodnými technikami zabezpečení jsou pseudonymizace a šifrování osobních údajů.

V případě šifrování dat má správce k dispozici několik způsobů ochrany šifrovacích klíčů. Nejnižší míru důvěry v cloudovou službu umožňuje šifrování, při kterém jsou klíče uloženy a vlastní šifrování a dešifrování dat prováděno uvnitř interní sítě Správce; v takovém případě jsou ale možnosti zpracování trvale šifrovaných dat v cloudu velmi omezené. V případě, že se šifrovací klíče a dešifrovaná data objeví během zpracování v cloudu, musí správce zajistit ve své smlouvě se zpracovatelem dodatečná bezpečnostní opatření, která riziko zneužití osobních údajů v cloudu minimalizují – viz podrobnější vysvětlení dále.

6.3 Problematika zpracování údajů o zdravotním stavu a jiných zdravotnických dat

Údaje o zdravotním stavu jsou z hlediska ochrany data, která vyžadují mimořádnou ochranu – tj. „zvláštní kategorie osobních údajů". Článek 9 odst. 3 GDPR doslova uvádí: *Osobní údaje uvedené v odstavci 1 mohou být zpracovávány pro účely uvedené v odst. 2 písm. h), jsou-li tyto údaje zpracovány pracovníkem vázaným služebním tajemstvím nebo na jeho odpovědnost podle práva Unie nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány nebo jinou osobou, na niž se rovněž vztahuje povinnost*

mlčenlivosti podle práva Unie nebo členského státu nebo pravidel stanovených příslušnými vnitrostátními orgány.

Odstavec 1, na který se odvolává uvádí:

Zakazuje se zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a ***zpracování genetických údajů, biometrických údajů*** *za účelem jedinečné identifikace fyzické osoby* ***a údajů o zdravotním stavu*** *či o sexuálním životě nebo sexuální orientaci fyzické osoby.*

Výjimka pro zpracování je vázána na Odstavec 2. pism. h):

2. Odstavec 1 se nepoužije, pokud jde o některý z těchto případů:

h) zpracování je nezbytné pro účely preventivního nebo pracovního lékařství, pro posouzení pracovní schopnosti zaměstnance, lékařské diagnostiky, poskytování zdravotní nebo sociální péče či léčby nebo řízení systémů a služeb zdravotní nebo sociální péče na základě práva Unie nebo členského státu nebo podle smlouvy se zdravotnickým pracovníkem a při splnění podmínek a záruk uvedených v odstavci 4;

6.3.1 Zajištění důvěrnosti ve službě Microsoft AZURE

Microsoft Pravidla služeb Online (dále též PSO) obsahují **obecný závazek, že Microsoft bude osobní údaje zpracovávat v souladu s veškerými zákony a předpisy**, které se vztahují k provozování služeb online. Na pracovníky společnosti Microsoft se proto vztáhne ustanovení článku 28 odst. 3 písm. b) GDPR, které stanoví povinnost zachovávat mlčenlivost. Tato povinnost je navíc reflektována v PSO, podle kterých musí pracovníci společnosti Microsoft uchovávat zpracovávaná data v bezpečí a v tajnosti. Ti pracovníci, kteří mají přístup k zákaznickým údajům, jsou dále vázaní závazky důvěrnosti.

A to konkrétně:

Pracovníci společnosti Microsoft (str. 10)

Pracovníci společnosti Microsoft nebudou zákaznická data zpracovávat bez svolení zákazníka. *Pracovníci společnosti Microsoft musí zákaznická data uchovávat v bezpečí a v tajnosti tak, jak je popsáno v podmínkách zpracování údajů, a tato povinnost platí i po ukončení jejich závazků.*

Organizace zabezpečení informací (str. 11)

Pracovníci společnosti Microsoft s přístupem k zákaznickým datům jsou vázáni závazky důvěrnosti.
Standardní smluvní doložky – Dodatek 2 (str. 33)
Pracovníci musí zachovávat důvěrnost zákaznických dat a tato povinnost platí i po ukončení jejich závazků.

6.3.2 Poskytnutí záruk ze strany Microsoft AZURE / Online služby

Microsoft implementoval technická a organizační opatření, která jsou specifikována v PSO v části „Podmínky zpracování dat – Zabezpečení" na str. 11–12 PSO. Prostředí MS AZURE naplňuje povinnosti požadavků GDPR pro Zpracovatele.

V konkrétním případě zpracování údajů má zákazník (správce údajů) právo vyžádat si další specifické záruky, které by musely být řešeny na individuální bázi.

Konkrétní opatření:

Zabezpečení (PSO str. 8)

Prioritou společnosti Microsoft je napomáhat při ochraně bezpečnosti informací zákazníka. Společnost Microsoft implementovala a bude uplatňovat a dodržovat příslušná technická a organizační opatření určená k ochraně zákaznických dat před náhodnou ztrátou či změnou, neoprávněným nebo nezákonným přístupem, zveřejněním, změnou, ztrátou nebo zničením.

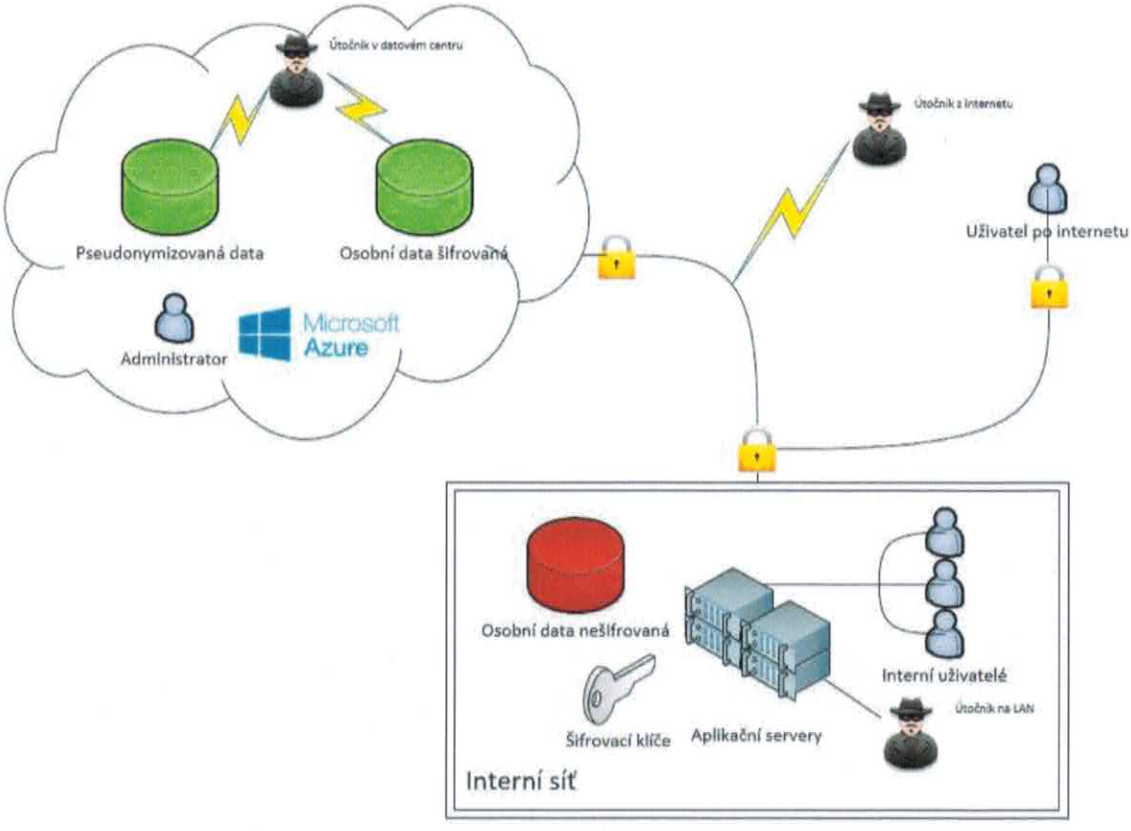
Zabezpečení (PSO str. 11)

Společnost Microsoft implementovala a pro služby online bude v souvislosti se závazky k zabezpečení uvedenými v podmínkách pro služby online udržovat a dodržovat následující bezpečnostní opatření, která představují jedinou odpovědnost společnosti Microsoft s ohledem na zabezpečení zákaznických dat.

6.4 Zajištění dat v cloudu

6.4.1 V Cloudu jsou jen šifrovaná a pseudonymizovaná data

Z hlediska stávajících požadavků GDPR je umístění dat i aplikací v cloudu Microsoft AZURE možné ve všech představitelných scénářích. Je třeba důsledně zabezpečit komunikaci po internetu, zvláště pokud v Cloudu budou umístěna pouze pseudonymizovaná nebo šifrovaná data (viz obrázek)

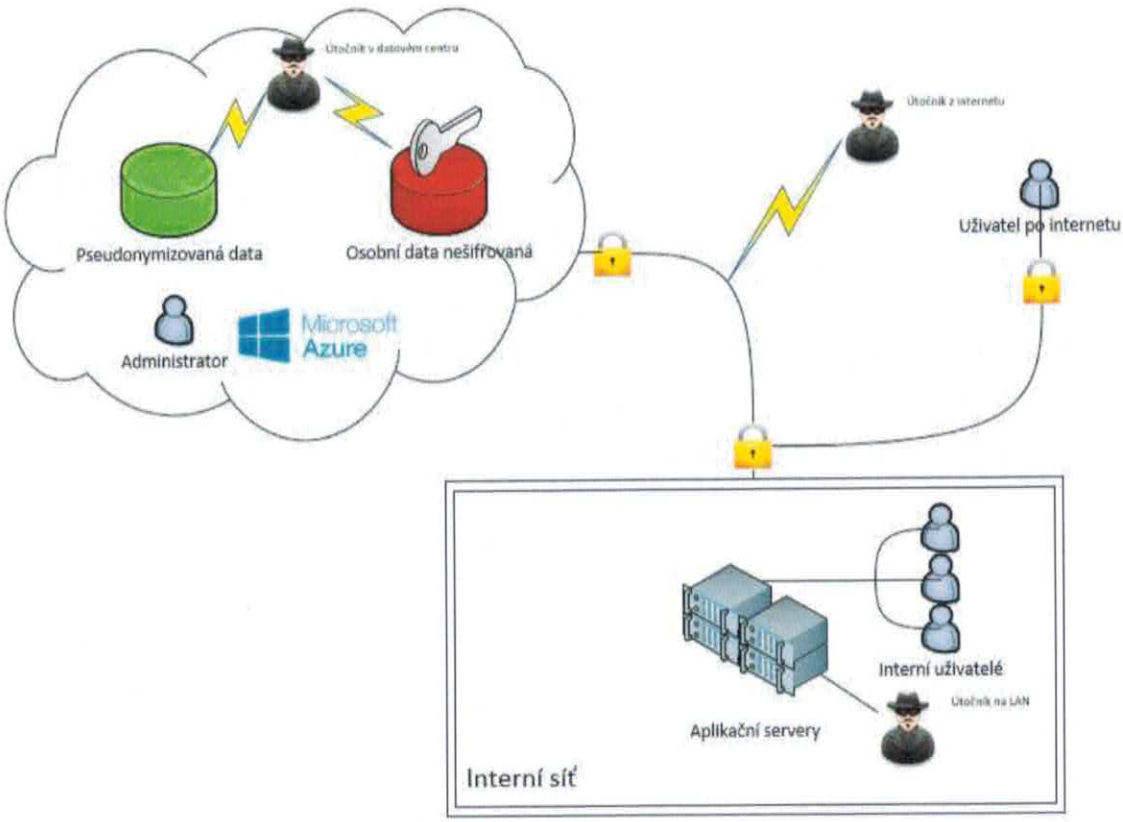


V takovém případě nejsou provozovateli Cloudu přístupná dešifrovaná data a tím je podstatně sníženo riziko kompromitace dat na jeho straně.

6.4.2 V Cloudu jsou dešifrovaná data nebo přítomen dešifrovací klíč v nechráněné podobě

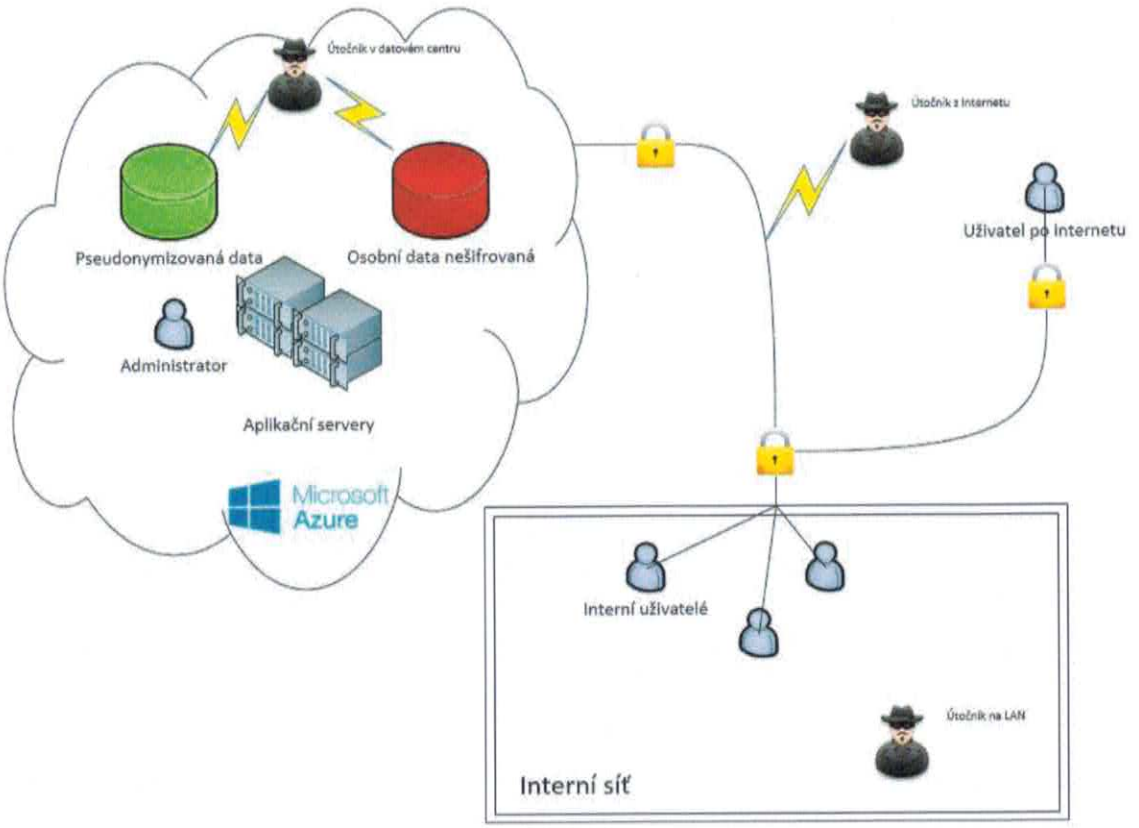
Pokud ale daný scénář vyžaduje zpracování dešifrovaných dat v Cloudu, pak je třeba zavést další bezpečnostní opatření, která výskyt dešifrovaných dat v cloudu omezí jen na nezbytně dlouhou dobu, a která zajistí ochranu šifrovacích klíčů před neoprávněným přístupem. Provozovatel Cloudu musí zajistit ochranu dat (např. udržovat je v šifrované podobě mimo okamžik jejich zpracování) i ochranu šifrovacích klíčů, a zavázat se k této ochraně smluvně Správci.

Umístíme-li v Cloudu nešifrovaná data, případně šifrovaná data, ale s dostupným klíčem, pak jsou provozovateli Cloudu přístupná a musí tak zajistit jejich ochranu a zavázat se smluvně Správci.



6.4.3 V Cloudu jsou dešifrovaná data nebo přítomen dešifrovací klíč v nechráněné podobě a jsou zde i aplikační servery

V případě že Správce umístí do Cloudu i Aplikační servery, je tak celý systém snadno spravovatelný odkudkoliv a dají se jeho funkce sdílet bez omezení na konkrétní lokalitu. V takové situaci musí poskytovatel Cloudu zajistit veškerou ochranu i dle dalších zákonných norem, jako je Zákon č. 181/2014 sb. O kybernetické bezpečnosti.



Scénář umístění v Cloudu nejen nešifrovaných dat, ale i aplikačních serverů, tedy programového vybavení, které umožní absolutní čitelnost takových dat, je pro plné využití výhod zpracování dat v Cloudu nejpravděpodobnější. V takovém případě mohou k dané službě přistupovat uživatelé odkudkoliv. Provozovatel Cloudu musí minimalizovat a zajistit sledování přístupů svých zaměstnanců k datům klientů. Toto zajišťuje společnost Microsoft takto (Relevantní ustanovení PSO):

Soukromí (str. 10)

Pracovníci společnosti Microsoft. Pracovníci společnosti Microsoft nebudou zákaznická data zpracovávat bez svolení zákazníka. Pracovníci společnosti Microsoft musí zákaznická data uchovávat v bezpečí a v tajnosti tak, jak je popsáno v podmínkách zpracování údajů, a tato povinnost platí i po ukončení jejich závazků.

Sdělení a správa operací (str. 11):

Společnost Microsoft protokoluje nebo umožňuje zákazníkovi protokolovat informační systémy obsahující zákaznická data, která registrují ID přístupu, čas, přidělené nebo zamítnuté oprávnění a příslušnou činnost, a k těmto informačním systémům přistupovat a používat je.

Řízení přístupu (str. 12)

Zásady přístupu. Společnost Microsoft uchovává záznam o oprávnění zabezpečení osob, které mají přístup k zákaznickým datům.

Oprávnění k přístupu

- *Společnost Microsoft uchovává a aktualizuje záznam pracovníků oprávněných k přístupu k systémům společnosti Microsoft, které obsahují zákaznická data.*
- *Společnost Microsoft deaktivuje pověření pro ověření, která nebyla používána po dobu maximálně šesti měsíců.*
- *Společnost Microsoft identifikuje pracovníky, kteří mohou udělovat, měnit nebo rušit autorizovaný přístup k datům a prostředkům.*
- *Společnost Microsoft zajistí, že pokud k systémům obsahujícím zákaznická data přistupuje více než jedna osoba, budou mít tyto osoby oddělená ID a přihlašovací údaje.*

Minimální oprávnění

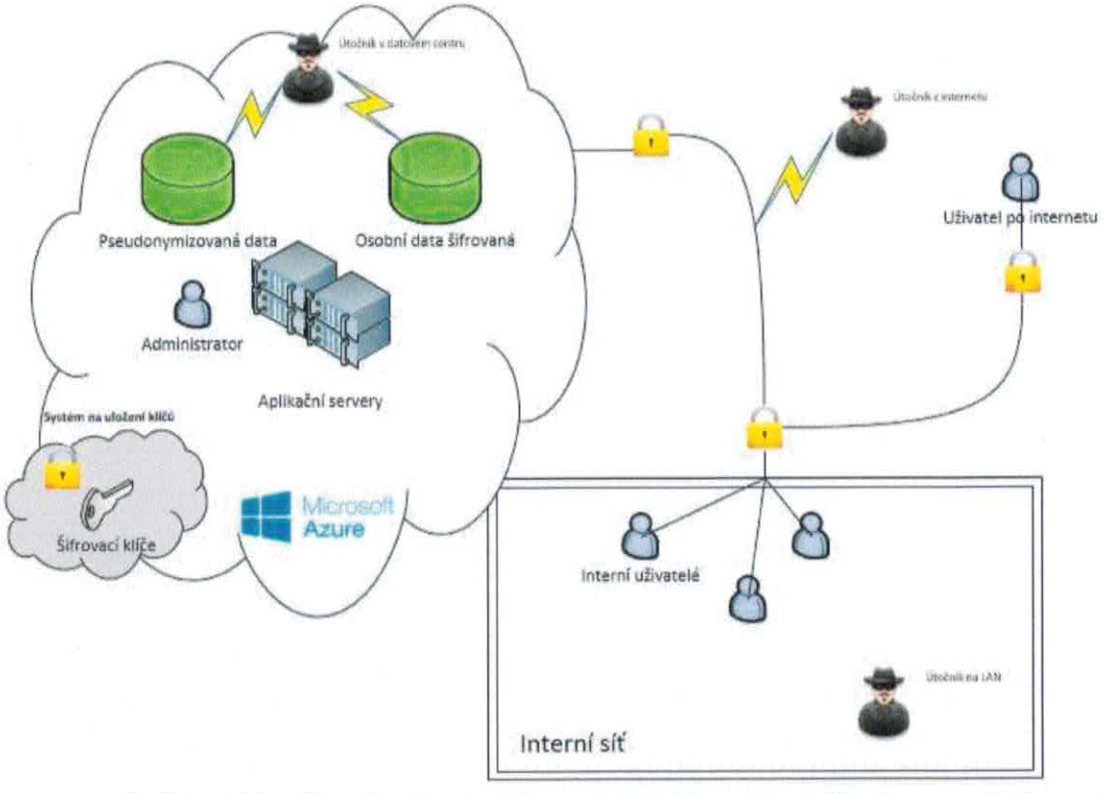
- *Pracovníci technické podpory mají přístup k zákaznickým datům pouze v případě potřeby.*
- *Společnost Microsoft omezuje přístup k zákaznickým datům pouze na osoby, které tento přístup vyžadují k vykonávání své funkce.*

Relevantní opatření:

V prostředí Microsoft Azure a Microsoft's Cloud Infrastructure and Operations jsou nasazeny mechanizmy identifikace, autentizace, řízení přístupu a jsou nasazeny mechanizmy záznamu činnosti.

A dále opatření: 9.3.3, 9.3.4, 9.3.6

6.4.4 V Cloudu jsou šifrovaná data i aplikační servery, ale klíč je chráněn speciálními technicko-organizačními opatřeními



V tomto scénáři platí veškeré výhody jako v předešlém, ale klíče jsou umístěny ve speciálním úložišti, které je chráněno a zabezpečeno oddělenými technickými prostředky. V případě Microsoft Azure se jedná o službu Azure Key Vault, která je popsána takto:

Azure Key Vault pomáhá chránit kryptografické klíče a tajné klíče používané cloudovými aplikacemi a službami. Pomocí Key Vault můžete šifrovat klíče a tajné klíče (např. ověřovací klíče, klíče účtu úložiště, šifrovací klíče dat, soubory PFX a hesla) pomocí klíčů chráněných moduly hardwarového zabezpečení (HSM). Pro zvýšené bezpečí můžete klíče importovat nebo generovat v modulech HSM. Pokud se tak rozhodnete, společnost Microsoft bude zpracovávat vaše klíče v modulech HSM ověřených podle standardu FIPS 140-2 Level 2 (hardware a firmware).

Key Vault zjednodušuje proces správy klíčů a zajišťuje vám kontrolu nad klíči, které se používají k přístupu a šifrování dat. Vývojáři můžou během pár minut vytvořit klíče pro vývoj a testování a potom je bez problémů migrovat na produkční klíče. Správci zabezpečení můžou klíčům podle potřeby udělovat (a odvolávat) oprávnění.

6.5 Splnění technických požadavků zákonných norem v Cloudu

Znalec vycházel z technických požadavků veškerých zákonných norem, které by se měly dotýkat zpracování lékařských záznamů. Jedinou problematickou oblast, kterou bude obtížné naplnit, je problematika Výmazu dat.

Podstatné je **vyjádření Úřadu pro ochranu osobních údajů**, který již 23.7.2014 prostřednictvím pana PhDr. Davida Pavláta zveřejnil toto stanovisko:

Lze využít cloud computing pro zpracování osobních údajů?

Na ochranu osobních údajů v rámci využití „cloud computingu" musíme nahlížet zejména z pozice správce osobních údajů, tedy z pozice subjektu, který s údaji primárně nakládá a rozhoduje o druzích prostředků, které budou pro zpracování osobních údajů použity. Jedním z technických prostředků může být právě varianta cloud computingu, tedy jakéhosi pronájmu výpočetního výkonu či úložného prostoru poskytovatele této služby. Z hlediska správce osobních údajů lze důrazně doporučit přistupovat k poskytovateli cloud computingu jako ke zpracovateli ve smyslu § 4 písm. k) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. To však nezbavuje správce osobních údajů (tedy subjekt, který si cloud najímá) povinností, které jsou na něj zákonem č. 101/2000 Sb. kladeny, a v této souvislosti je nutné zmínit zejména povinnost stanovenou v § 13 zákona č. 101/2000 Sb., která se týká zabezpečení osobních údajů. Je tak na správci, aby analyzoval dopady řešení využití cloud computingu (analýza rizik), zajistil adekvátní opatření na své straně (např. šifrování dat) a aby si uzavřením smluvních vztahů s případným poskytovatelem služeb cloud computingu ošetřil veškeré podmínky zpracování (zajištění odpovídající úrovně zabezpečení; odpovědnost poskytovatele služeb / zpracovatele za jeho případná selhání s dopady do oblasti ochrany osobních údajů, garantování nevratné likvidace údajů apod.).

Z hlediska zákonných pravidel a záruk požadovaných pro předávání osobních údajů lze doporučit využívat pouze webové služby a cloudová úložiště, které se nacházejí na území EU a jsou plně pod jurisdikcí evropského práva, v takovém případě by pak měly být splněny i požadavky zákona o ochraně osobních údajů

6.5.1 Dodatek M434

V rámci ustanovení tohoto dodatku Microsoft přijímá roli Zpracovatele a zavazuje se k dalším povinnostem (např. procesu při použití dalšího Dílčího zpracovatele) a tím naplňuje požadavky článků 28, 32 a 33 dle GDPR.

7 Doporučení

7.1 Architektonická doporučení

Znalec doporučuje, před převodem do Cloudu zpracovat kompletní popis operací zpracování a kompletní analýzu rizik. Dokument „Analýza rizik a bezpečnostní opatření zdravotnických IS v cloudu" je dobrým základem zpracování vlivu na ochranu osobních údajů dle článku 35 GDPR, s tím, že povinná osoba musí dle bodu 7. Vypracovat posouzení, které:

obsahuje alespoň:

a) *systematický popis zamýšlených operací zpracování a účely zpracování, případně včetně oprávněných zájmů správce;*

b) *posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelů;*

c) *posouzení rizik pro práva a svobody subjektů údajů uvedených v odstavci 1; a*

d) *plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob.*

Výše zmíněný dokument postihuje písmeno c) a d). Na Správci tak je dopracování bodů a) a b). Zárukou pro použitelnost řešení v Microsoft Azure jsou také tyto mezinárodně uznávané certifikace:

Zdroj: Veřejně publikovaná specifikace Microsoft Azure (https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings) ukazuje soulad s mezinárodními standardy bezpečnosti informačních systémů:

- ISO/IEC 27001:2013 Information Security Management Standards
- ISO/IEC 27017:2015 Code of Practice for Information Security Controls (cloud-specific information security threats and risks referring to clauses 5 to 18 in ISO/IEC 27002:2013)
- ISO/IEC 27018:2014 International code of practice for cloud privacy, based on EU data-protection laws.
- ISO/IEC 22301:2012 International Business Continuity Management Standard

Soulad s výše uvedenými standardy byl auditován akreditovanými společnostmi British Standards Institute (BSI) a Coalfire ISO Inc. (pouze ISO/IEC 27017).
Účinnost zavedených bezpečnostních opatření byla dále ověřena auditní společností Deloitte & Touche LLP formou mezinárodně uznávaných auditních zpráv:

- SOC 1 Type II (rovněž známa jako SSAE 16 nebo ISAE 3402)
- SOC 2 Type II (rovněž známa jako AT 101)
- SOC 3 Report for the Security, Availability, Processing Integrity and Confidentiality Trust Principles.

Soulad s těmito mezinárodními standardy a související auditní zprávy mohou poskytnout správcům osobních údajů a případně i dozorovému úřadu dostatečné záruky účinného zavedení bezpečnostních opatření pro zabezpečení zpracování osobních údajů. Další garancí jsou ustanovení Dodatku M434 a jeho Příloha 1. a to zejména v těchto ustanoveních:

4. Zabezpečení

Společnost Microsoft je povinna (i) dodržovat postupy a zásady zabezpečení za účelem ochrany osobních údajů, jak je blíže stanoveno v písemných zásadách zabezpečení dat („zásady zabezpečení informací"), a to pro každou ze služeb online, a dále (ii) poskytnout zákazníkovi zásady zabezpečení informací společně s popisy bezpečnostních opatření zavedených pro služby online a dalšími informacemi, které mohou být zákazníkem rozumně vyžadovány v souvislosti s postupy a zásadami zabezpečení společnosti Microsoft.

5. Porušení zabezpečení osobních údajů

Společnost Microsoft je povinna vynaložit přiměřené úsilí, aby pomohla zákazníkovi s plněním povinností zákazníka ohlásit příslušným orgánům dozoru a subjektům údajů, že došlo k porušení zabezpečení osobních údajů podle článků 33 a 34 GDPR.

Dále v bodě C odstavce 5. až 8.

5. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou zákazník a společnost Microsoft vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

(a) pseudonymizace a šifrování osobních údajů;

(b) schopnosti zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

(c) schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů; a

(d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování. (Článek 32(1))

6. Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim. (Článek 32(2))

7. Zákazník a společnost Microsoft přijmou opatření pro zajištění toho, aby jakákoliv fyzická osoba, která jedná z pověření zákazníka nebo společnosti Microsoft a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn zákazníka, pokud jí jejich zpracování již neukládá právo Unie nebo členského státu. (Článek 32(4))

8. Jakmile společnost Microsoft zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu zákazníkovi. (Článek 33(2))

7.2 Posouzení vlivu

Správce dat zvláštních kategorií dále musí zajistit dle Článku 35 (GDPR) odstavec 3 písmeno b)

Článek 35 ***Posouzení vlivu na ochranu osobních údajů***

1.Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro práva a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

2.Při provádění posouzení vlivu na ochranu osobních údajů si správce vyžádá posudek pověřence pro ochranu osobních údajů, byl-li jmenován.

3.Posouzení vlivu na ochranu osobních údajů podle odstavce 1 je nutné zejména v těchto případech:

a) systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad;

b) rozsáhlé zpracování zvláštních kategorií údajů uvedených v čl. 9 odst. 1 nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů uvedených v článku 10; nebo

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Zpracovaná studie „Analýza rizik a bezpečnostní opatření zdravotnických IS v cloudu", bude i zde dobrým vodítkem.

7.3 Výmaz dat

Vzhledem k tomu, že Správce nemá v případě zpracování dat v Cloudu dostupné fyzické hardware tak, aby mohl zajistit veškeré požadavky na bezpečný výmaz dat, měl by zvážit všude tam, kde budou uložena nešifrovaná data, sepsání procesu takového bezpečného výmazu dat v součinnosti s provozovatelem Cloudu, aby postup bezpečného výmazu naplnil. Vzhledem k tomu, že v prostředí Microsoft AZURE jsou data umístěna na diskových svazcích, je však velmi nepravděpodobná možnost obnovy dat po jejich smazání. Jednotlivá část (pevný disk) nenese takové informace, z kterých by byla obnova možná.

Výmaz dat je dostatečně definován v Dodatku M434 a to v bodech C. 3(g), Příloha 1 M434 2. (a), Příloha 1 M434 3. (e) – a to v tomto znění:

(g) Společnost Microsoft je povinna zejména v souladu s rozhodnutím zákazníka všechny osobní údaje buď vymazat, nebo je vrátit zákazníkovi po ukončení poskytování služeb spojených se zpracováním, a vymazat existující kopie, pokud právo Unie nebo členského státu nepožaduje uložení daných osobních údajů;

(a) Po dobu účinnosti prováděcí smlouvy společnost Microsoft zpřístupní zákazníkovi osobní údaje subjektů údajů způsobem, který je v souladu s funkčností služeb online a podmínkami prováděcí smlouvy. V rozsahu, v jakém při svém užívání a správě služeb online po dobu účinnosti prováděcí smlouvy není zákazník sám schopen opravit, pozměnit nebo vymazat osobní údaje v prostředí služeb online (jak vyžaduje GDPR), poskytne společnost Microsoft zákazníkovi součinnost ve vztahu k přiměřeným požadavkům z jeho strany a bude zákazníkovi nápomocna při provedení takovýchto úkonů a při reakcích zákazníka na žádosti od subjektů údajů. Zákazník odpovídá za veškeré přiměřené náklady vzniklé společnosti Microsoft v souvislosti s poskytnutím takovéto asistence.

(e) Po uplynutí doby účinnosti nebo ukončení užívání služeb online zákazníkem společnost Microsoft osobní údaje buď vymaže, nebo je vrátí v souladu s podmínkami a ve lhůtách uvedených pro každou jednotlivou službu online v příslušných OST, ledaže právo Unie, právo členského státu anebo jiné aplikovatelné právo požaduje uchování daných osobních údajů.

8 Závěr – výrok Znalce

Otázka na Znalce:

Splňuje cloudová služba Microsoft Azure poskytovaná společností Microsoft jakožto zpracovatelem osobních údajů na základě čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů („nařízení") požadavky na vhodná opatření a záruky, včetně bezpečnostních opatření a mechanismů, které je správce osobních údajů povinen přijmout v souladu s čl. 32 a čl. 35 odst. 7 nařízení, a to pro automatizované zpracování údajů o zdravotním stavu a jiných zdravotnických dat odpovídajícímu přiložené studii (tj. pro zpracování zvláštních kategorií osobních údajů)?

Výrok znalce:

ANO - K Rozhodnému datu lze v prostředí cloudové služby Microsoft Azure realizovat informační systém a uložení dat tak, aby odpovídal technickým požadavkům na zpracování zvláštních kategorií osobních údajů.

9 Oprávnění znaleckého ústavu

JUDr. Daniela Kovářová
ministryně spravedlnosti

V Praze dne - 4 -03- 2010
Čj. 309/2009-OD-ZN

R o z h o d n u t í

Na základě žádosti a v souladu s ustanovením § 21 odst. 3 zákona č. 36/1967 Sb., o znalcích a tlumočnících, a ustanovením § 6 odst. 1 vyhlášky č. 37/1967 Sb., k provedení zákona o znalcích a tlumočnících, ve znění pozdějších předpisů, se do prvého oddílu seznamu ústavů kvalifikovaných pro znaleckou činnost zapisuje:

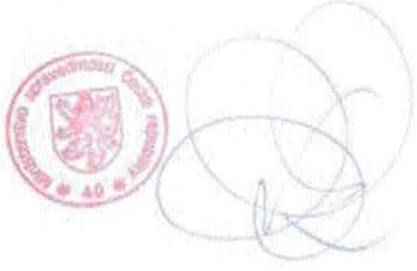
Cetag, s.r.o.,

se sídlem Na Poříčí 1070/19, Praha 1, PSČ 110 00, IČ: 274 51 925

pro obor kybernetika

s rozsahem znaleckého oprávnění výpočetní technika.

Zápis bude publikován v Ústředním věstníku České republiky.



MINISTERSTVO SPRAVEDLNOSTI
ČESKÉ REPUBLIKY

V Praze dne 24 -04- 2013
Čj. 14/2013-OSD-SZN/15

Rozhodnutí

Ministerstvo spravedlnosti ČR rozhodlo podle § 21 odst. 2 zákona č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů, ve věci žádosti ze dne 14. 1. 2013 účastníka řízení - znaleckého ústavu Cetag, s.r.o., se sídlem Na Poříčí 1070/19, 110 00 Praha 1, IČ: 27451925, o rozšíření dosavadního rozsahu znaleckého oprávnění u jmenovaného znaleckého ústavu zapsaného v I. oddílu seznamu znaleckých ústavu pro obor kybernetika takto:

Rozsah znaleckého oprávnění u znaleckého ústavu **Cetag, s.r.o.,** se mění takto:

I. oddíl

v oboru ekonomika s rozsahem znaleckého oprávnění:

- oceňování hardware a software;

v oboru kybernetika s rozsahem znaleckého oprávnění:

- výpočetní technika.

Odůvodnění:

Podle ustanovení § 68 odst. 4 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, není odůvodnění rozhodnutí třeba, jestliže správní orgán prvního stupně všem účastníkům v plném rozsahu vyhoví.

Poučení:

Proti tomuto rozhodnutí je možné podat k ministru spravedlnosti rozklad, a to do 15 dnů ode dne oznámení rozhodnutí na adresu Ministerstva spravedlnosti ČR, Vyšehradská 16, 128 10 Praha 2. O rozkladu rozhoduje ministr spravedlnosti.

Po právní moci tohoto rozhodnutí budou změny v zápisu do seznamu znaleckých ústavů vyznačeny v Ústředním věstníku ČR a na webových stránkách Ministerstva spravedlnosti ČR.

JUDr. Pavel Blažek, Ph.D.
ministr spravedlnosti

Cetag, s.r.o.
Na Poříčí 1070/19
110 00 Praha 1

10 Oprávnění a certifikace hlavního řešitele

Spr 892/2014

Předseda
Krajského soudu v Českých Budějovicích

R o z h o d n u t í

Předseda Krajského soudu v Českých Budějovicích se sídlem Zátkovo nábřeží 2 , 370 01 České Budějovice, jako správní orgán příslušný na základě pověření ministra spravedlnosti podle § 3 zákona č. 36/1967 Sb., o znalcích a tlumočnících, ve znění pozdějších předpisů (dále jen „zákon o znalcích a tlumočnících"), rozhodl o žádosti „Ing. Jaroslav Mráz nar. 30.3.1960 trvale bytem Strměchy 46, 393 01 Pelhřimov , / dále jen „žadatel"/, doručené dne 12.6.2014.

t a k t o
Ing. Jaroslava Mráze
jmenuji znalcem

oboru: **Ekonomika,** odvětví **cena a odhady,** specializace **softwer, hardware, komplexních řešení v oblasti IT, telekomunikací a duševních vlastností.**
oboru: **Kybernetika,** odvětví **výpočetní technika, posuzování technologické neutrality**

Odůvodnění:

Předseda krajského soudu tímto rozhodnutím žadateli vyhověl v plném rozsahu. Bližší odůvodnění tohoto rozhodnutí není třeba, protože podle § 68 odst. 4 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, není odůvodnění rozhodnutí třeba, jestliže správní orgán prvního stupně všem účastníkům v plném rozsahu vyhoví.

Poučení o opravném prostředku: Proti tomuto rozhodnutí lze podat odvolání do 15 dnů ode dne jeho oznámení k ministru spravedlnosti prostřednictvím předsedy Krajského soudu v Českých Budějovicích.

V Českých Budějovicích dne 25. 9. 2014

JUDr. Milan Tripes
předseda krajského soudu

KRAJSKÝ SOUD • ČESKÉ BUDĚJOVICE

Slib složen dne: 25.9.2014
Vyznačeno v knize slibů pod poř. číslem: 1996/z

Převzal : .....
Kolek: 1 000,-Kč

11 Prohlášení o nezávislosti

Tímto prohlašujeme, že k zúčastněným subjektům (stranám smluv) nejsme ve vztahu finanční nebo personální závislosti nebo v zaměstnaneckém či jiném obdobném poměru.

Znalecký ústav zpracoval znalecký posudek podle podmínek na trhu v době jeho provádění a neodpovídá za případné změny v podmínkách trhu, ke kterým by došlo po předání znaleckého posudku.

Znalecký posudek je vypracován v souladu se zákonem č. 36/1967 Sb., o znalcích a tlumočnících, v platném znění a vyhláškou č. 37/1967 Sb., k provedení zákona o znalcích a tlumočnících.

Zpracovaný znalecký posudek zohledňuje všechny nám známé skutečnosti, které by mohly ovlivnit dosažené závěry nebo posuzované hodnoty.

Znalecký posudek je zpracován s vědomím následků vědomě nepravdivého znaleckého posudku ve smyslu § 346 zákona č. 40/2009 Sb., trestní zákoník. Znalecký ústav si je vědom následků vědomě nepravdivého posudku ve smyslu § 110a zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád) a § 127a zákona č. 99/1963 Sb., občanský soudní řád, v platném znění.

12 Znalecká doložka

ZNALECKÁ DOLOŽKA

Znalecký posudek vypracoval ústav kvalifikovaný pro znaleckou činnost Cetag, s.r.o., se sídlem Na Poříčí 1070/19, Praha 1 – 11000, IČ: 27451925, společnost vedená u rejstříkového soudu v Praze, C 114044, jmenovaný Ministryní spravedlnosti dne 4. března 2010, č.j.: 309/2009 –OD-ZN a zapsaný do prvního oddílu seznamu ústavů kvalifikovaných pro znaleckou činnost v oboru kybernetika – výpočetní technika podle ustanovení par. 21., odst. 3 zákona č. 36/1967 Sb., o znalcích a tlumočnících a ustanovení par. 6., odst. 1 vyhlášky č. 37/1967 Sb., ve znění pozdějších předpisů. Dne 24. dubna 2013 byla činnost znaleckého ústavu rozšířena o obor ekonomika s rozsahem znaleckého oprávnění oceňování hardware a software na základě rozhodnutí Ministra spravedlnosti JUDr. Pavla Blažka, Ph.D., č.j. 14/2013-OSD-SZN/15.

Hlavní řešitel: Ing. Jaroslav Mráz

(kontaktní osoba ve věci znaleckého posudku)

Znalecký posudek je zapsán ve znaleckém deníku pod pořadovým číslem **145-2017**

V Praze, dne 15. dubna 2017

.....

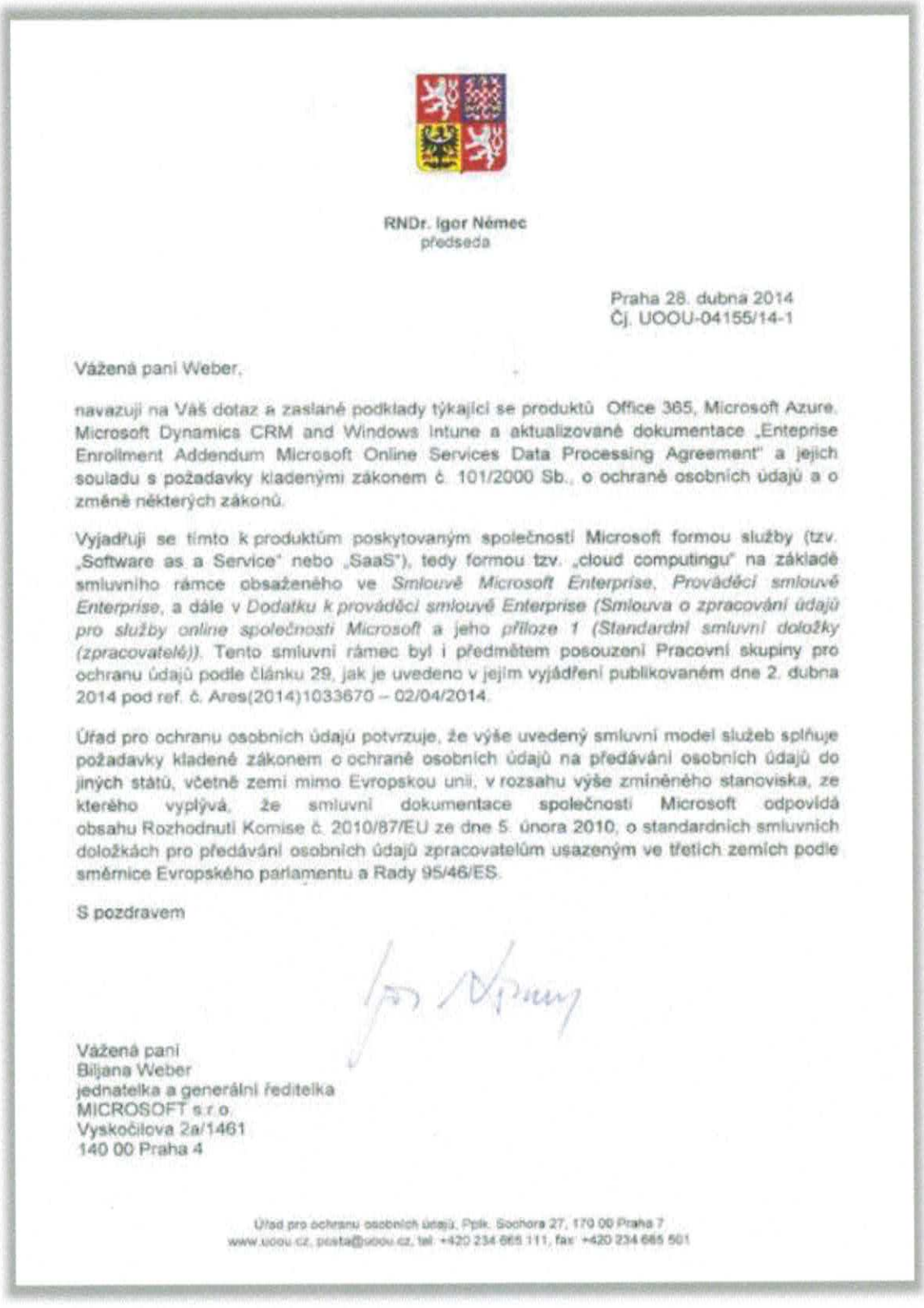
Ing. Jaroslav Mráz

Jednatel společnosti, soudní znalec

Cetag, s.r.o. Ústav kvalifikovaný pro znaleckou činnost v oboru kybernetika a ekonomika

13 Přílohy

13.1 Vyjádření ÚOOU



RNDr. Igor Němec
předseda

Praha 28. dubna 2014
Čj. UOOU-04155/14-1

Vážená paní Weber,

navazuji na Váš dotaz a zaslané podklady týkající se produktů Office 365, Microsoft Azure, Microsoft Dynamics CRM and Windows Intune a aktualizované dokumentace „Enteprise Enrollment Addendum Microsoft Online Services Data Processing Agreement" a jejich souladu s požadavky kladenými zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

Vyjadřuji se tímto k produktům poskytovaným společností Microsoft formou služby (tzv. „Software as a Service" nebo „SaaS"), tedy formou tzv. „cloud computingu" na základě smluvního rámce obsaženého ve *Smlouvě Microsoft Enterprise*, *Prováděcí smlouvě Enterprise*, a dále v *Dodatku k prováděcí smlouvě Enterprise (Smlouva o zpracování údajů pro služby online společnosti Microsoft* a jeho *příloze 1 (Standardní smluvní doložky (zpracovatelé))*. Tento smluvní rámec byl i předmětem posouzení Pracovní skupiny pro ochranu údajů podle článku 29, jak je uvedeno v jejím vyjádření publikovaném dne 2. dubna 2014 pod ref. č. Ares(2014)1033670 – 02/04/2014.

Úřad pro ochranu osobních údajů potvrzuje, že výše uvedený smluvní model služeb splňuje požadavky kladené zákonem o ochraně osobních údajů na předávání osobních údajů do jiných států, včetně zemí mimo Evropskou unii, v rozsahu výše zmíněného stanoviska, ze kterého vyplývá, že smluvní dokumentace společnosti Microsoft odpovídá obsahu Rozhodnutí Komise č. 2010/87/EU ze dne 5. února 2010, o standardních smluvních doložkách pro předávání osobních údajů zpracovatelům usazeným ve třetích zemích podle směrnice Evropského parlamentu a Rady 95/46/ES.

S pozdravem

Vážená paní
Biljana Weber
jednatelka a generální ředitelka
MICROSOFT s.r.o.
Vyskočilova 2a/1461
140 00 Praha 4

Úřad pro ochranu osobních údajů, Pplk. Sochora 27, 170 00 Praha 7
www.uoou.cz, posta@uoou.cz, tel: +420 234 665 111, fax: +420 234 665 501

13.2 Zkratky

Zkratka	Popis
AD	Active Directory
ASW	Aplikační software
AZURE	Windows Azure Platform je cloudová platforma společnosti Microsoft
BYOK	Bring Your Own Key
Cloud	Prostředí v internetu na hostování služeb
DR	Disaster recovery
GDPR	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
HW	Hardware - hmotná část ICT systémů
IaaS	Infrastructure as a Service - infrastruktura jako služba
ICT	Informační a telekomunikační technologie
IPS	Intrusion Prevention System
IRM	Information Rights Management
IS	Informační systém
IT	Informační technologie
IZIP	společnost pro Internetové Zdravotnictví pro využití Informací Pacienta
JŘBU	Jednací řízení bez uveřejnění
MCIO	Microsoft's Cloud Infrastructure and Operations
MS	Microsoft s.r.o.
MS SQL	Microsoft SQL
Multi-tenant prostředí	Prostředí, které je poskytováno množství subjektů a které zajišťuje, aby činnost jednoho subjektu neovlivňovala činnost ostatních subjektů
MySQL	Relační databáze primárně šířená jako Open Source
NAT	Network Address Translation
PaaS	Platform as a Service - Platforma jako služba
PSO	Podmínky pro služby online
SaaS	Software as a Service - Software jako služba
SaaS	Service as a Service
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SW	Software - programy
VZ	Veřejná zakázka
VZP	Objednatel - Všeobecná zdravotní pojišťovna ČR
ZVZ	Zákon o veřejných zakázkách 137/2006 Sb.

Cetag, s.r.o.
Na Poříčí 1070/19
11000 Praha 1
IČ: 27451925
DIČ: CZ27451925
www.cetag.com