Služby veřejného cloudu společnosti Microsoft: zpracování osobních údajů, kybernetická bezpečnost a ochrana soukromí

Soulad s požadavky Zákona o ochraně osobních údajů

Společnost Microsoft se snaží své služby nabízet tak, aby umožnily splnění požadavků, které jsou kladeny na subjekty, které nakládají s osobními údaji (tedy např. státní orgány, banky, atd.) v České republice. Je vhodné zmínit, že zákazník, který bude ukládat osobní údaje (svých zákazníků, zaměstanců, občanů komunikujících se státní správou) do cloudové služby Microsoftu, bude zpravidla v postavení správce ve smyslu zákona č. 101/2000 Sb., o ochraně osobních údajů (dále jen Zákon). Společnost Microsoft, poskytující cloudové služby jako jsou Windows Azure, Office 365 a CRM Online, zde vystupuje v roli smluvního zpracovatele osobních údajů ve smyslu Zákona. Postavení správce a zpracovatele ovlivňuje i rozdělení povinností dle Zákona.

Využití cloud computingu pro zpracování osobních údajů je samozřejmě v zásadě možné. Pro posouzení cloudu se podmínky příliš neliší od outsourcovaných informačních systémů veřejné správy, které zpracovávají osobní údaje. Zákazník cloudových služeb (správce osobních údajů ve smyslu Zákona) však musí provést analýzu rizik, nezbytná technická opatření na své straně, a ošetřit podmínky zpracování dat uzavřením smluvních vztahů se zpracovatelem směrem k zajištění odpovídající úrovně zabezpečení, viz §13 výše citovaného zákona č. 101/2000 Sb.[1]

Požadavky Zákona jsou ze strany Microsoftu adresovány ve smluvní dokumentaci společnosti Microsoft k výše uvedeným cloudovým službám, kdy Microsoft uzavře se zákazníkem smlouvu o zpracování údajů, tak aby zákazník (správce osobních údajů) byl schopen doložit splnění svých povinností dle Zákona. Microsoft též splňuje požadavky norem ISO 27001, ISO 27018 a ISAE 3402, které jdou nad rámec požadavků Zákona. S ohledem na požadavky Zákona ohledně zpracování osobních údajů lze podmínky pro užívání služeb cloudu splnit následujícími způsoby:

1) V rámci EU je to možné bez omezení a není nutné splňovat další podmínky. Toto je v cloudových službách společnosti Microsoft pro zákazníky se sídlem v ČR splněno ve většině případů výběrem hlavního a záložního datacentra na území EU (dle znění nových Podmínek pro služby online[2], kapitola „Umístění pro uchování zákaznických dat), nicméně vzhledem k určitým technickým podmínkám jako např. zajištění kontinuální správy a servisu mohou nastat případy zpracovávání osobních údajů i mimo oblast EU.[3]

2) Aplikací standardních smluvních doložek („EU model clauses")[4], tj. smluvního ujednání mezi vývozcem a dovozcem osobních údajů. Podpis standardních smluvních doložek je způsob, který poskytuje nejvyšší formu záruk pro zákazníka, a v souladu s §27[5] Zákona už není nutné splňovat další podmínky. Standardní smluvní doložky jsou nyní součástí Podmínek pro služby online jako Příloha 3 smlouvy.

Toto je cesta, kterou správci dat v ČR mohou dosáhnout nejvyšší úrovně zabezpečení při zpracování osobních údajů, ve smyslu Zákona.

1 - Viz webové stránky ÚOOÚ – sekce „Často kladené otázky", http://uoou.cz/uoou.aspx?menu=14&loc=331; zde odpověď na otázku „Lze využít cloud computing pro zpracování osobních údajů?"

2 - Viz Microsoft Onlie Services Terms (OST) (URL)

3 - Viz Centrum zabezpečení služeb Office 365 (URL), odtud „Zeměpisné hranice" (URL)

4 - V minulosti také principem Safe Harbour Agreement, který však byl v říjnu 2015 zrušen rozhodnutím Evropského soudního dvora.

5 - Viz webové stránky ÚOOÚ - „Přehled případů předávání osobních údajů do zahraničí, u nichž není nutno žádat Úřad o povolení" – případ EU standardní smluvní doložky dole na stránce http://uoou.cz/uoou.aspx?menu=41&submenu=44

Výše deklarovaný soulad online služeb může společnost Microsoft doložit těmito dokumenty:

- **Stanovisko EU „Article 29 Working Party“:** Microsoft získal souhlasné stanovisko asociace úřadů na ochranu osobních údajů v celé EU (tzv. „Article 29 Working Party“) o tom, že implementace „Standardních smluvních doložek“ (zajišťujících dostatečnou míru ochrany soukromí při předání osobních údajů do třetích zemí, i mimo EU), které Microsoft poskytuje na přání k Enterprise Agreementu obsahujícímu cloudové služby, je v souladu s příslušným opatřením EU „Standard Contractual Clause 2010/87/EU“.
  Viz blog z 10. 4. 2014 nebo přímo zmíněné stanovisko. (Veřejná informace)
- **Vyjádření ÚOOÚ:** Úřad na ochranu osobních údajů ČR sdělil dopisem ze dne 28. 4. 2014 pod č.j. UOOU-04155/14-1 společnosti Microsoft ČR stanovisko, že smluvní model cloudových služeb společnosti Microsoft (Office 365, Azure, CRM Online) splňuje požadavky kladené zákonem o ochraně osobních údajů 101/2000 Sb. na předávání osobních údajů do jiných států, včetně zemí mimo Evropskou unii. Jedná se o smluvní model Enterprise Agreement, Dodatek k prováděcí smlouvě Enterprise, a Smlouva o zpracování údajů pro služby online společnosti Microsoft včetně Přílohy 1 - Standardní smluvní doložky.

Soulad s požadavky Zákona o kybernetické bezpečnosti

Microsoft obdržel v červnu 2015 vyjádření Národního bezpečnostního úřadu (NBÚ), které stanoví rozsah dokumentace, které poskytovatelé cloudových služeb musí poskytnout povinným osobám ze **Zákona o kybernetické bezpečnosti č. 181/2014 Sb.** (a jeho Vyhlášky o kybernetické bezpečnosti č. 316/2014 Sb.) tak, aby povinné osoby mohly splnit požadavky vyplývající z tohoto zákona. Microsoft může tyto podklady povinným osobám poskytnout za podmínek předávání důvěrných informací (Non-Disclosure Agreement). Podklady k certifikaci ISO 27001 jsou součástí této dokumentace.

Závěr:

Cloudové služby Microsoft Office 365, CRM Online, a jejich podkladová vrstva Windows Azure získaly všechny běžně vyžadované certifikace (viz přehled níže), a svým zákazníkům nabízí takové smluvní podmínky včetně „Smlouvy o zpracování dat“ případně se zahrnutím standardních smluvních doložek („EU Model Clauses“), které umožní **splnění podmínek zákona č. 101/2000 Sb. o ochraně osobních údajů.**

Právní doložka: Tento dokument byl vytvořen za účelem shrnutí klíčových požadavků ohledně ochrany osobních údajů v prostředí Cloudu a způsobu, jakým se s nimi vypořádává společnost Microsoft. Tento dokument nevyjadřuje stanovisko společnosti Microsft ohledně vhodnosti použití cloudu pro konkrétní prostředí a nenahrazuje právní posouzení, které musí učinit subjekt, který službu bude užívat.

Reference a dodatečné informace

Přehled certifikací cloudových služeb společnosti Microsoft – stav k 1.1.2016

Standard - certifikace	**Office 365**	**Microsoft Dynamics CRM**	**Microsoft Azure**	**Windows Intune**	**Yammer**	**GFS (Global Foundation Services – infra-struktura dato-vých center)**
ISO 27001:2005 nebo ISO 27001:2013, se zahrnutím ISO 27018	Yes	Yes	Yes	Yes	Yes	Yes, US Datacenters EU/Intl datacenters
EU Model Clauses (Standardní smluvní doložky Evropské unie, ověřen „soulad")	Yes	Yes	Yes	Yes	No	Yes
PCI DSS (Payment Card Industry Data Security Standard)	N/A	N/A	N/A	N/A	N/A	Yes
SOC 1 Type 2[6] (Service Organization Controls - SSAE 16 / ISAE 3402)	Yes	Yes	Yes	Yes	No	Yes
SOC 2 Type 2 (AT Section 101)	Yes	Yes	Yes	Yes	No	N/A
UK G-Cloud	Yes	Yes	Yes	No	No	Yes
FedRAMP (US) (Moderate)	Yes	No	Yes	No	No	Yes
FERPA (US – Education)	Yes	N/A	Yes	N/A	Yes	N/A
HIPPA/BAA (US - Healthcare)	Yes	Yes	Yes	Yes	No	Yes
IPv6	Yes	No	No	No	No	N/A
CJIS (US - Criminal Justice)	Yes	No	No	No	No	N/A

6 - Service organization controls – viz Wikipedia

ISO 27001: Microsoft Azure obdržel ISO/IEC 27001:2005 a později ISO/IEC 27001:2013 certifikaci od BSI Group (UK) www.bsigroup.com, pod číslem 577753. Certifikace pokrývá širokou škálu služeb Windows, viz výčet na vlastní stránce certifikátu. Tento certifikát je uznávaný globálně, a osvědčuje, že Microsoft zavedl specifické prvky řízení informační bezpečnosti, definované v tomto standard. Samostatné certifikace ISO 27001:2005 nebo novější ISO 27001:2013 obdržely i služby Microsoft Office 365, Dynamics CRM Online, Microsoft Intune, a Globální infrastruktura datových center Microsoft (viz tabulka výše).

Stávající nebo potenciální zákazníci online služeb společnosti Microsoft mohou pro svoje interní analýzy rizik získat za podmínky předávání důvěrných informací (Non-Disclosure Agreement) auditní zprávu k certifikaci ISO 27001 zmíněných online služeb společnosti Microsoft.

V únoru 2015 Microsoft ohlásil přijetí nového standardu ISO 27018 na ochranu soukromí v cloudových službách. Jeho audit probíhá společně s certifikací ISO 27001, a 25 nových opatření ISO 27018 na ochranu soukromí je nyní zdokumentováno v novém Prohlášení o aplikovatelnosti k certifikátu ISO 27001.

SSAE 16 (USA) / **ISAE 3402** (ostatní státy) – „Statement on Standards for Attestation Engagements No. 16" – je nezávislé ověření souladu pravidel řízení bezpečnosti, a účinnosti řízení bezpečnosti v organizaci. Tento nový standard nahradil původní standard SAS 70 od června 2011. Jedná se vlastně o zprávu auditora, který potvrzuje:

- Jestli popis řízení bezpečnosti u dodavatele služeb je správně prezentován
- Jestli řízení bezpečnosti u dodavatele služeb je nastaveno účinně
- Jestli postupy řízení bezpečnosti u dodavatele služeb byly skutečně zavedeny k uvedenému datu.
- Jestli postupy řízení bezpečnosti u dodavatele služeb byly účinně v provozu v průběhu daného časového intervalu.

Tyto audity jsou ve společnosti Microsoft prováděny nezávislou auditní firmou pravidelně každý rok. Stávající nebo potenciální zákazníci online služeb společnosti Microsoft mohou pro svoje interní analýzy rizik získat za podmínky mlčenlivosti (Non-Disclosure Agreement) auditní zprávy Microsoft SOC 1 (SSAE 16/ISAE 3402) Type II report, a dále SOC 2 (AT 101) Type II report.

SOC (Service Organization Controls) jsou mezinárodně uznávané zprávy nezávislého auditora, které mají pevně danou strukturu, a varianta „Type II" ověřuje, jestli příslušná opatření byla účinná po dobu 6 měsíců (nejen k jednomu určitému datu).

Webové stránky Centrum zabezpečení služeb (Trust Center), pro produkty:

Office 365[7]; CRM Online[8]; Windows Azure[9] (poslední pouze v angličtině). Tyto stránky jsou průběžně aktualizovány a poskytují i linky k podrobným vyjádřením na téma „Omezení přístupu správců k zákaznickým datům", „Přenositelnost dat", „Zeměpisné hranice", a podrobný výpis auditů a certifikátů. Najdete je také zadáním „Office 365 Trust Center" nebo „Centrum zabezpečení služeb Office 365" do vašeho vyhledávače.

Certifikace služby Microsoft Azure jsou uvedeny v aktuálním stavu na stránce http://azure.microsoft.com/en-us/support/trust-center/compliance/

Standardní odpovědi společnosti Microsoft na otázky pro výběrová řízení cloudových služeb, dle doporučené matice „Cloud Control Matrix“, publikované nezávislou asociací Cloud Security Alliance (CSA) https://cloudsecurityalliance.org/

Najdete zde obsáhlé odpovědi pro všechny tři hlavní cloudové služby - Office 365, CRM Online, a Windows Azure. Odpovědi jsou podpořeny výsledky auditů ISO 27001, ISAE 3402 a dalšími. Publikováno na webu:

Standard Response to Request for Information- Windows Azure- Privacy & Security [10]

7 - http://www.microsoft.com/cs-cz/office365/trust-center.aspx

8 - http://www.microsoft.com/en-gb/dynamics/crm-trust-center.aspx

9 - http://www.windowsazure.com/en-us/support/trust-center/

10 - http://www.microsoft.com/en-us/download/details.aspx?id=26647