V Y J Á D Ř E N Í ÚOOÚ

k využívání cloudových služeb z pohledu ochrany osobních údajů a povinnostem správce a zpracovatele podle obecného nařízení

Obecná východiska

Zavádění cloudových služeb má dopad i do oblasti ochrany osobních údajů a může obnášet i rizika pro práva a svobody fyzických osob v souvislosti se zpracováním jejich osobních údajů. Specifická rizika dálkových služeb jsou dána mj. tím, že správce nemá data plně (fyzicky) pod kontrolou. Může jít především o nedostatek kontroly nad osobními údaji a nedostatečné informace o tom, kde a kým jsou údaje zpracovávány či dále zpracovávány, po jakou dobu, nekontrolovaný přístup k datům, absence účinné cizozemské právní ochrany subjektu údajů. Správce proto musí provést důkladnou analýzu rizik, do níž zahrne i umístění serverů, na kterých se údaje zpracovávají, a zvážit rizika a přínos cloudové služby z hlediska ochrany údajů.[1]

Úřad doporučuje, aby analýza rizik byla zpracována i v případě, že se povinnost vypracovat posouzení vlivu na správce nevztahuje, zejména v případě veřejné správy. Úřad to považuje za potřebné z toho důvodu, že výjimka z této povinnosti se mj. vztahuje na široký okruh orgánů veřejné moci, které při zpracování osobních údajů postupují podle předpisů, k nimž příslušná odpovědná ministerstva žádné posouzení vlivu nevypracovala a ani později posouzení vlivu nové technologie cloudu dodatečně neprovedla.

Při využití cloudových služeb dochází zpravidla i ke zpracování osobních údajů a je tak nutné aplikovat Nařízení evropského parlamentu a rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále „obecné nařízení“ nebo „GDPR“). Z pohledu obecného nařízení leží primární odpovědnost za zpracování na zákazníkovi (uživateli) služby, který se nachází v pozici správce osobních údajů. Poskytovatel cloudových služeb bude ve většině případů vystupovat v pozici zpracovatele osobních údajů. V rámci poskytování služby často dochází ke zpracování dalších osobních údajů spojených s evidencí zákazníků, účtování služeb, komunikace se zákazníkem a osobních údajů spojených s provozem (logy, přihlášení apod.), kde se již poskytovatel cloudu nachází v pozici správce.

Povinnosti správce vyplývající ze zásady transparentnosti – čl. 13 a 14 GDPR

- Správce musí subjektu údajů poskytnout stručným, transparentním, srozumitelným a snadno přístupným způsobem základní informace o zpracování (účel, rozsah, dobu uchování, příjemce údajů, případný úmysl předat osobní údaje do třetí země). Správce musí umožnit výkon práv subjektu údajů a na jeho žádost mu poskytnout podrobnosti o jednotlivých operacích zpracování.

[1] Podrobně popsaná rizika jsou k dispozici v dokumentu ENISA Cloud computing – Benefits, Risks and Recommendations for Information Security. https://www.enisa.europa.eu/activities/riskmanagement/files/deliverables/cloud-computing-risk-assessment.

- K naplnění této povinnosti musí správce, jako primární subjekt odpovědný za zpracování, mít možnost efektivně řídit, dohlížet a kontrolovat objem dat předávaných do cloudu a mít tak dostatečnou kontrolu nad tím, jaká data byla odesílána, kam, za jakým účelem a na jak dlouhou dobu, komu byla nebo by mohla být dále zpřístupněna či předávána. Pokud hlavní zpracovatel hodlá zapojit do zpracování dalšího (dílčího) zpracovatele, musí o tom správce vždy předem informovat.

Povinnost správce aplikovat zásadu záměrné a standardní ochrany – čl. 25 GDPR

- Správce musí zavézt vhodná technická a organizační opatření v co nejranějších fázích koncipování operací zpracování tak, aby již od začátku byly respektovány zásady ochrany soukromí a ochrany osobních údajů („záměrná ochrana osobních údajů“). Opatření musí dodržovat a aktualizovat po celou dobu zpracování až do doby, kdy jsou údaje zlikvidovány. Správci musí zároveň zajistit, aby osobní údaje byly zpracovávány s co nejvyšší ochranou soukromí (např. by měly být zpracovávány pouze nezbytné údaje, krátká doba uchovávání, omezená přístupnost), aby osobní údaje standardně nebyly zpřístupněny neomezenému počtu osob („standardní ochrana osobních údajů“).

- Ačkoliv se čl. 25 přímo na zpracovatele nevztahuje, je nutné s nimi počítat jako s důležitými aktéry v procesu zavádění záměrné a standardní ochrany. Zpracovatelé si musí být vědomi toho, že správci jsou povinni zpracovávat osobní údaje pouze se systémy a technologiemi, které mají integrovanou ochranu údajů. Při zpracování jménem správců by zpracovatelé měli využívat své odborné znalosti a navrhovat správcům řešení, která integrují ochranu dat do zpracování.

<u>Povinnosti správce provést posouzení vlivu na ochranu osobních údajů – čl. 35 GDPR</u>

- Správce osobních údajů hodlající využívat cloudové služby musí provést analýzu, z které vyplyne, zda se na něj vztahuje povinnost provést posouzení vlivu na ochranu osobních údajů podle **čl. 35 GDPR**.[2] Posouzení vlivu musí provést postupem podle **čl. 35 odst. 7 GDPR** dříve, než bude zpracování zahájeno (data vložena do cloudu).

- Obecné nařízení požaduje [**čl. 32 odst. 1 písm. d) a čl. 35 odst. 11],** aby monitorování a přezkoumávání rizik pro práva a svobody subjektů údajů probíhalo nepřetržitě na základě aktuální situace. V souvislosti s cloudovou službou lze za takovou situaci považovat i rozsudek Evropského soudního dvora C-311/18, kterým bylo zrušeno rozhodnutí Komise o štítu soukromí a upřesněno používání standardních smluvních doložek. Obecně vzato vznik nové situace spojené s riziky vždy vyžaduje, aby proběhla revize uvažovaných hrozeb, hodnocení správnosti a účinnosti uplatněných opatření (technických a organizačních) včetně revize smluvních ujednání (zpracovatelská

[2] Za tím účelem Úřad vydal Seznam druhů operací zpracování (ne)podléhajících požadavku na posouzení vlivu na ochranu osobních údajů dostupné zde: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940.

smlouva) i nástrojů používaných správcem pro bezpečné předávání osobních údajů do třetích zemí (standardní smluvní doložky, závazná podniková pravidla).

Povinnosti správce uzavřít se zpracovatelem zpracovatelskou smlouvu - čl. 28 GDPR

- Pokud při využívání cloudových služeb bude rovněž docházet ke zpracování osobních údajů, musí být mezi správcem a zpracovatelem uzavřena zpracovatelská smlouva, která musí obsahovat všechny náležitosti podle **čl. 28 GDPR**.
- Správce může využít pouze takového zpracovatele, který poskytuje dostatečné záruky zavedení vhodných technických a organizačních opatření **- čl. 28 odst. 1 GDPR**.
- Zpracovatel musí správci poskytnout veškeré informace k doložení toho, že byly splněny povinnosti stanovené v čl. 28.
- Zpracovatel musí správci umožnit provedení auditu - **čl. 28 odst. 5 písm. h).**
- Poskytovatelé cloudových služeb musí svým zákazníkům podávat informace nezbytné ke správnému posouzení výhod a nevýhod (rizik či omezení) spojených s přijetím této služby. Hlavními elementy, o něž by se nabídka cloudových služeb měla opírat, aby byly aplikovatelné požadavky ochrany osobních údajů, by měla být bezpečnost, transparentnost a právní jistota pro zákazníky.[3]

Povinnosti správce přijmout vhodné záruky v případě předání údajů do třetích zemí – kapitola V GDPR

- V případě využívání cloudových služeb zpravidla dochází rovněž k předání osobních údajů (zákaznická data, metadata, provozní záznamy) do třetích zemí, přičemž obvykle je vývozce údajů správce (uživatel) a dovozce údajů zpracovatel (poskytovatel cloudové služby). Pokud k předání do třetích zemí dochází, musí být splněny podmínky, které jsou stanoveny v kap. V GDPR. V případě, že (dílčí) zpracovatel je usazen ve třetí zemi, musí správce osobních údajů zajistit osobním údajům v třetí zemi přiměřenou úroveň ochrany tím, že přijme některé z vhodných záruk podle čl. 46 a 47 obecného nařízení pro všechny kategorie dat. Vhodné záruky mohou poskytovat např. standardní smluvní doložky podle rozhodnutí Komise nebo závazná podniková pravidla.

- V případě použití standardních smluvních doložek uzavřených mezi vývozcem a dovozcem údajů rozhodnutí Komise nezbavuje pravomoci dozorový úřad dočasně nebo trvale zakázat nebo pozastavit předání údajů v konkrétních případech, kdy by předání mohlo mít nepříznivý dopad na práva jednotlivců v souvislosti se zpracováním jejich osobních údajů. Ustanovení článku 58 odst. 2 písm. f) a j) obecného nařízení pravomoci dozorového úřadu potvrzují. Významnou roli dozorového úřadu v tomto případě zdůrazňuje i rozsudek ESD ve věci C-311/18 (odst. 113, 114, 115).

Předávání do třetích zemí po rozsudku Evropského soudního dvora

[3] Stanovisko WP 29 č. 05/2012 ke cloud computingu z 1. července 2012, které je i po změnách právní úpravy ochrany osobních údajů stále aktuální.

- ESD ve svém rozsudku C-311/18 došel k závěru, že je i nadále možné využívat pro předávání do třetích zemí standardní smluvní doložky. Jejich použití však podmiňuje testem přiměřenosti přijatých opatření v závislosti na okolnostech předání a na zemi dovozce údajů. V zásadě tedy požaduje, aby v případě, že se správce rozhodne pro předání údajů do konkrétní třetí země použít standardní smluvní doložky, sám prověřil, zda vhodné záruky a ochranná opatření v doložkách skutečně zajišťují úroveň ochrany, která musí být „v zásadě rovnocenná" úrovni ochrany zaručené v Unii obecným nařízením a Listinou. Při posuzování úrovně by měl brát v úvahu rovněž i relevantní prvky právního řádu třetí země. Pokud správce dojde k závěru, že vlastní doložky samy o sobě nezajišťují „v zásadě rovnocennou" úroveň ochrany osobních údajů, které hodlá předat do třetí země, musí přijmout (ve spolupráci s dovozcem) doplňková opatření, která požadovanou úroveň ochrany zajistí.

- K dopadům rozsudku ESD se vyjádřil Evropský sbor formou často kladených otázek.[4] Úřad o problematice informuje na svých stránkách.[5] Současně byla vytvořena pracovní skupina při Evropském Sboru, která se věnuje dopadům rozsudku a problematice doplňkových opatření k již existujícím bezpečným nástrojům pro přenos dat do třetích zemí. Evropská Komise připravuje revizi standardních smluvních doložek.

Předávání do USA po rozsudku Evropského soudního dvora

- Rozsudek Evropského soudního dvora C-311/18, kterým bylo zrušeno rozhodnutí Komise o štítu soukromí a upřesněno používání standardních smluvních doložek, se mj. týká cloudových služeb zahrnujících předávání a následné uložení nebo dalším zpracováním osobních údajů na území USA. Soud konstatoval, že právní předpisy USA se vztahují na všechny „poskytovatele elektronických komunikačních služeb", a tudíž i na poskytovatele cloudových služeb, přičemž nezajišťují účinnou právní ochranu subjektům údajů a umožňují „plošný" přístup státních orgánů USA k osobním údajům obyvatel EU.

- Dodavatelé cloudový sloužeb a správci využívající cloudových služeb musí v rámci posouzení vlivu na ochranu osobních údajů vždy zohlednit i závěry, ke kterým v souvislosti s předáváním údajů do USA dospěl Evropský soudní dvůr. Dodavatelé služeb i správci, kteří v návaznosti na rozsudek přehodnocují nastavení cloudových služeb, se mohou obrátit na Úřad se žádostí podloženou konkrétními podklady o předběžnou konzultaci postupem dle čl. 36 GDPR.

[4] Dostupné zde: https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en.
[5] O dopadech rozsudku ÚOOÚ informoval zde https://www.uoou.cz/uoou-k-nbsp-dopadum-zruseni-stitu-soukromi-eu-usa-na-spravce/d-43874.

Závěr

Obecné nařízení ukládá správci (uživateli cloudové služby) postupovat samostatně a odpovědně při přípravě i samotném provozu zpracování a zohlednit předem všechny zásady ochrany osobních údajů (zásadu odpovědnosti, zásadu záměrné a standardní ochrany apod.). Zásada odpovědnosti je trvalým závazkem správce, který musí v pravidelných intervalech posuzovat rizika v závislosti na aktuální situaci. Nakonec musí sám vyhodnotit, zda rizika spojená s vložením údajů do cloudu jsou přijatelná, případně může požádat Úřad o konzultaci.

Správce musí dostát požadavkům na transparentnost zpracování, čili být schopen vysvětlit, co se s daty děje, kde jsou uložena, komu zpřístupněna nebo předávána apod. Všichni správci, kteří uvažují o cloudovém řešení nebo v cloudu svá data již mají, by měli být za současné situace uvážliví a pokud možno volit datová úložiště plně a jasně podléhající evropskému právu. Od svých zpracovatelů (poskytovatelů cloudových služeb) by měli žádat jasné a vymahatelné záruky.

Uživatel cloudové služby by měl po poskytovateli nad rámec smluvních doložek vyžadovat návrhy řešení v podobě dalších bezpečnostních záruk (např. uložení dat včetně metadat pouze na území EU, šifrování bez zadních vrátek, pseudonymizaci, garanci nesdílení dat s orgány veřejné moci státu dovozce údajů apod.).[6] Vhodná doplňková opatření pro zajištění požadované úrovně ochrany mohou mít právní, technickou a organizační povahu a lze je různě kombinovat. Pokud by správce (uživatel) cloudové služby nepřijal žádná opatření směřující k tomu, aby zpracování probíhalo v souladu s úrovní ochrany stanovené právními předpisy EU o ochraně údajů a výkladem ESD, bylo by nutné považovat předávání do třetích zemí z pohledu požadavků ESD za protiprávní.

V oblasti veřejné správy pak musí být respektována zásada legality státní moci. Přípustnost cloudu jako nezbytného prostředku zpracování musí být jasně dovoditelná z právních předpisů, které upravují kompetenci a postupy veřejné správy. Nasazení technických prostředků zpracování je nezbytné provádět v souladu s prováděcími a metodickými předpisy a aplikovat přitom i nové nástroje ochrany osobních údajů.

[6] Na vytvoření podrobného seznamu možných doplňkových opatření v současné době pracuje za tím účelem vytvořená pracovní skupina při Evropském Sboru