

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Některé problematické aspekty předávání osobních údajů do třetích zemí

Požadavky na zpracování osobních údajů v členských státech Evropské unie patří momentálně k těm nejpřísnějším na světě. Hlavním pramenem práva v této oblasti je obecné nařízení o ochraně osobních údajů (GDPR)[1]. Právě díky tomu je v rámci EU zaručen také volný pohyb osobních údajů, který nesmí být nijak omezován ani zakazován. Podmínkou však zůstává, že správce osobních údajů musí mít pro předání dat dalšímu správci právní důvod (titul).

To je logicky vyžadováno i v případě předávání osobních údajů do třetích zemí. Zjevný rozdíl však spočívá v tom, že při předávání osobních údajů mimo EU/EHP jsou na správce, či další organizaci „vyvážející osobní data“, kladeny vyšší nároky z hlediska institucionálního zabezpečení, což znamená, že nelze (až na výjimky) předávat osobní údaje do států, kde není zajištěna jejich dostatečná právní ochrana. Tato posílená (institucionální) ochrana zahrnuje mimo jiné i rozhodnutí Komise o odpovídající úrovni ochrany v příslušné zemi nebo poskytnutí dostatečných záruk.

V tomto článku se zaměříme na některé problematické aspekty předávání osobních údajů do třetích zemí a zhodnotíme nedávný přezkum rozhodnutí Komise o dostatečné úrovni ochrany dat v některých třetích zemích.

Správce a zpracovatel, nebo vývozce a dovozce dat?

V kontextu zpracování dat jsme zvyklí rozlišovat mezi různými rolí, a to buď správce nebo zpracovatele. Avšak, pokud jde o předání osobních údajů mimo EU/EH/, toto rozlišení ztrácí do velké míry na významu, protože přísná pravidla platí bez ohledu na tuto distinkci. Jinými slovy, není klíčové, jestli dochází k předávání od správce k správci, od správce k zpracovateli nebo od zpracovatele k subzpracovateli.

Při předávání údajů hraje klíčovou roli zásada odpovědnosti, která vyžaduje aktivní snahu vývozce dat zajistit, že údaje přenesené do třetí země budou chráněny na úrovni srovnatelné s ochranou poskytovanou v EU. Což v sobě zahrnuje i schopnost toto kdykoliv prokázat a doložit. Jakým způsobem to tedy může v praxi vypadat?

Institucionální záruky za ochranu osobních údajů

Jedním z nejčastějších prostředků pro zajištění ochrany práv dotčených osob jsou záruky ve formě dodatečných smluvních ujednání či doložek[2]. V praxi však může tento typ záruk často získat pouze formální podobu, což bylo kritizováno i Soudním dvorem EU v případě Schrems II[3]. V tomto rozhodnutí Soudní dvůr EU potvrdil, že standardní smluvní doložky samy o sobě dostačující nejsou, a jejich podstatným rysem by měla být spíše doplňující povaha, a to vedle dalších opatření. Ta musí být vždy učiněna individuálně na základě obsahu či rozsahu datových toků, kategorií subjektů údajů nebo úrovně citlivosti a rizikovosti předání.

Dalším způsobem zajištění ochrany může být přijetí tzv. závazných podnikových pravidel („*Binding Corporate Rules*“). Ty přicházejí do hry v případě, kdy správce má pobočky v různých částech světa. Tyto normy mohou být následně schváleny vedoucím dozorovým orgánem podle hlavního sídla

správce v Evropské unii, avšak v praxi, kvůli administrativně náročnému procesu, tato možnost zajištění bezpečnosti předání dat téměř není využívána.[\[4\]](#)

Pro některé další země Evropská komise již vydala stanovisko o odpovídající úrovni ochrany, které může podstatně usnadnit proces předání. Komise totiž tímto rozhodnutím deklaruje, že míra ochrany osobních údajů v dané zemi odpovídá unijním pravidlům a že do ní mohou být osobní údaje vyváženy bez dalších formálních požadavků. Právě tyto tzv. rozhodnutí o adekvátnosti („*data protection adequacy decisions*“) Komise na začátku letošního roku přezkoumávala, a potvrdila, že předávání osobních údajů z Evropské unie do

- Andory,
- Argentiny,
- Kanady,
- Faerských ostrovů,
- Guernsey,
- ostrova Man,
- Izraele,
- Jersey,
- Nového Zélandu,
- Švýcarska
- a Uruguaye

stále vycházejí z dostatečných záruk ochrany. Poskytování údajů do těchto zemí by tedy nemělo být zatíženo požadavky další institucionální ochrany. Můžeme říci, že připravenost Komise využít své pravomoci k úpravě rozhodnutí o přiměřenosti svědčí o jejím závazku udržovat vysoké standardy ochrany osobních údajů při mezinárodním oběhu dat.

Dodatečné záruky pro ochranu dat předávaných mimo EU/EHP

Je však nutné zopakovat, že při zpřístupnění osobních údajů jakémukoliv dalšímu subjektu, je správce či další vývozce dat povinen vždy zvážit, zda je předání v souladu s GDPR (klíčovou je zásada zodpovědnosti) a jaká jsou rizika pro dotčené osoby. **O smluvní doložky či rozhodnutí o adekvátnosti by se tedy neměl automaticky (bez dalšího) opírat.**

Vedle těchto institucionálních opatření existuje řada dalších praktických kroků, která přispívají ke zvýšení bezpečnosti při předávání informací, jako například:

- pseudonymizace (nahrazení identifikačních údajů falešnými nebo alternativními údaji),
- anonymizace (zajištění úplného odstranění osobních identifikátorů z dat),
- rozdělení mezi více příjemců,
- zkrácení doby uschování,
- šifrování vlastním klíčem.

Důležité jsou i pravidelné kontroly, zda jsou zavedená opatření stále dostačující a funkční a dostatečně reagují na všechna rizika pro práva a svobody dotčených osob.

Při nastavení konkrétních opatření by pak měl vývozce osobních údajů vždy vycházet právě ze zmíněné rizikovosti přenosu dat. Svoje rozhodnutí o dodatečných opatřeních by měl dokumentovat a měl by také být schopen jej odůvodnit, jinak jen obtížně doloží soulad svojí činnosti s požadavky obecného nařízení o ochraně osobních údajů (GDPR).



Ostap Denys,

student Právnické fakulty Univerzity Karlovy v Praze



Mgr. František Nonnemann,

konzultant v oblasti ochrany osobních údajů, compliance a řízení rizik, externí vyučující na Právnické fakultě Univerzity Karlovy v Praze

e-mail: nonnemann@volny.cz

Článek vyjadřuje osobní názory autorů a odráží právní a skutkový stav ke dni 23. února 2024

[1] 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).

[2] Vzorové smluvní doložky jsou vydány jako Prováděcí rozhodnutí Komise 2021/914 ze dne 4. června 2021 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení Evropského parlamentu a Rady (EU) 2016/679, dostupné >>> [zde](#).

[3] Rozsudek Soudního dvora EU ze dne 16. července 2020, Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems, věc C-311/18, dostupné >>> [zde](#).

[4] Srov. seznam schválených závazných podnikových pravidel >>> [zde](#).

Další články:

- [Mimosmluvní odměna při společném zastupování více osob](#)
- [Nepřiznané koalice](#)
- [Společnost s podíly 50:50 – právní rizika patových situací a jejich smluvní řešení](#)
- [Byznys a paragrafy, díl 34: Jednání za společnost – prokura](#)
- [Jak nastavit smlouvy s dodavateli podle nové právní úpravy kybernetické bezpečnosti?](#)
- [Vada koupené věci – kdy zjištěné nedostatky zakládají kupujícímu práva z vadného plnění a kdy nikoliv?](#)
- [Smluvní autonomie vs. ochrana slabší strany v moderním kontraktačním právu](#)
- [Reklamáce vad stavby](#)
- [Konec „severních ateliérů“? Nový stavební zákon otevírá dveře k rekolaudaci ubytovacích jednotek na plnohodnotné byty](#)
- [Oceňování nemovitosti a přiměřená náhrada při zrušení spoluvlastnictví](#)
- [Byznys a paragrafy, díl 33.: Prevence střetu zájmů \(jednatel × společnost\)](#)