17. 9. 2020

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

Rozsudek Schrems II dva měsíce poté: Lze předávat osobní údaje do USA?

Soudní dvůr EU ve svém rozsudku ve věci C-311/18 Data Protection Commissioner v. Facebook Ireland Limited a Maximillian Schrems[1] (dále jen „rozsudek Schrems II“) ze dne 16. 7. 2020 zneplatnil bez jakéhokoliv přechodného období tzv. Privacy Shield[2] (také „Štít soukormí“), který představoval významný právní základ předávání osobních údajů do USA.

V dnešní době je téměř nepředstavitelné, aby podnikatel nespoléhal na žádné (zejména IT) služby či nástroje, při jejichž provozu dochází k předávání osobních údajů do USA (např. služby od společností jako Google, Microsoft, Facebook, Amazon, Mailchimp apod.). Většina zpracovatelů měla předávání údajů do USA založené právě na Privacy Shield, což není nadále možné. Je tedy možné je nadále používat ke zpracování osobních údajů?

Odpověď na tuto otázku není jednoduchá. Je totiž třeba posuzovat každý případ individuálně. Dle **čl. 46 GDPR** mohou být osobní údaje předány do třetí země pouze pokud správce nebo zpracovatel poskytl vhodné záruky a za podmínky, že jsou k dispozici vymahatelná práva subjektu údajů a účinná právní ochrana subjektů údajů. Tento příspěvek si klade za cíl předestřít aktuálně dostupné možnosti řešení vzniklé situace a informovat o souvisejícím dění.

Každý správce osobních údajů by měl nejprve s využitím záznamů o činnostech zpracování vedených dle **čl. 30 GDPR** zjistit, zda v rámci svých aktivit předává osobní údaje zpracovatelům do USA. V případě, že k takovému předávání údajů dochází, může být nezbytné (vzhledem k tomu, že nebylo dáno přechodného období) jej alespoň dočasně pozastavit, a to z důvodu absence právního podkladu předávání.

Většina velkých poskytovatelů služeb již z vlastní iniciativy vyvíjí snahu o řešení situace. Jejich řešení jsou zpravidla založená na standardních smluvních doložkách dle rozhodnutí 2010/87/EC [3] (neboli také Standard Contractual Clauses, SSD či SCC). Zásadní však z tohoto pohledu je, zda jsou standardní smluvní doložky doplněny o nějaká další opatření. Vzhledem k tomu, že zákony USA umožňují státním autoritám plošný přístup k předávaným osobním údajům[4], nebudou samotné doložky jako dvoustranná ujednání bohužel zřejmě stačit[5]. Vždy totiž musí být zajištěna úroveň ochrany údajů v zásadě rovnocenná s tou v EU.

Správce osobních údajů se tedy musí zabývat tím, jaká legislativa USA na jím předávané údaje dopadá a s jakými důsledky, jak poskytovatel nakládá s případnými požadavky státních autorit na zpřístupnění údajů a jak běžné tyto požadavky jsou. V každém případě je totiž třeba provést zhodnocení rizik pro práva a svobody subjektů, jakož i rozhodnutí, zda je předávání osobních údajů do USA možné, resp. za jakých podmínek.

Nejobvyklejším řešením budou nepochybně právě již zmiňované **standardní smluvní doložky uzavírané mezi správcem a zpracovatelem**. Otázkou zůstává, o jaká další opatření mají být standardní smluvní doložky případně doplněny a zda tímto způsobem vůbec lze v případě USA docílit dostatečné úrovně ochrany. V daném ohledu rozsudek Schrems II bohužel příliš sdílný nebyl. Nabízí se např. **pseudonymizace**, **šifrování**[6], další zvláštní smluvní ujednání apod. EDPB (European Data

Protection Board) by měl v tomto ohledu v nejbližší době vydat doporučení[7].

Pokud není řešení založené na standardních smluvních doložkách z jakýchkoliv důvodů možné, pak je k dispozici ještě čl. 49 GDPR (tzv. závaznými podnikovými pravidly, resp. BCR, dle čl. 47 GDPR se článek pro nízký praktický význam nezabývá). Je však třeba podotknout, že právní základy předávání osobních údajů obsažené v tomto ustanovení by se měly využívat pouze výjimečně, jak ostatně vyplývá i z pokynů EDPB[8]. Teoreticky použitelnými se jeví např. předávání na základě výslovného souhlasu subjektu (dle čl. 49 odst. 1 písm. a) GDPR), případně předávání nezbytné pro splnění smlouvy mezi správcem a subjektem údajů (dle čl. 49 odst. 1 písm. b) GDPR), či uzavřené v zájmu subjektu údajů (dle čl. 49 odst. 1 písm. c) GDPR).

Neprávním řešením situace pak může být změna nastavení služeb tak, aby byly osobní údaje uchovávány pouze na serverech v EU/EEA. Tato možnost je ze strany zpracovatelů stále častěji nabízena, ale zpravidla je zpoplatněna. Pokud není změna nastavení možná, pak lze zvážit využití alternativních služeb či nástrojů, které uchování osobních dat výhradně v EU/EEA nabízí.

Z výše uvedeného je zjevné, že situace je komplikovaná. Není však reálné, aby se tok dat mezi USA a EU zastavil. Mnoho podnikatelů proto bude nepochybně volit postup s akceptováním určité míry rizika. Jako nejpoužitelnější (nikoliv ideální) řešení se jeví předávání na základě standardních smluvních doložek doplněných o některá konkrétní opatření, zejména pak proti „odposlouchávání“ internetového provozu (např. **silné šifrování a pseudonymizace**). Za doplňkové opatření se dá považovat i **certifikace Privacy Shield** na straně zpracovatele (Privacy Shield již nemůže být základem pro předávání, ale certifikace nadále zavazuje). Takové řešení se dá v současnosti pokládat za „best-effort“ postup. Lze očekávat, že v případě důsledného zhodnocení rizik a realizace obdobného řešení, bude přístup regulátorů alespoň v nejbližší době přinejmenším shovívavý. A to jak s ohledem na počet správců, kterých se problém způsobený zrušením Privacy Shield týká, tak i na právní nejistotu a aktuálně dostupné možnosti řešení.

Závěrem je vhodné zmínit, že není vyloučeno, že regulátoři přistoupí k **zákazu předávání osobních údajů do USA**[9]. Není to však příliš pravděpodobné. V každém případě lze doporučit i nadále sledovat vývoj. V nejbližší době by mělo přijít výše zmiňované doporučení EDPB (ohledně doplňujících opatření k **SCC**). Kromě toho **Evropská komi**se v červnu oznámila záměr aktualizovat znění standardních smluvních doložek[10]. A možná se dočkáme i Privacy Shield 2.0, o němž byly zahájeny debaty[11].

Mgr. Štěpán Kubát,
advokát

Mgr. Štěpán Kubát, advokát

Kořenského 1025/7,
150 00 Praha

Tel.: +420 735 530 300
e-mail: office@justask.cz

---

[1] Celé znění rozsudku k dispozici >>> zde.

[2] Více informací o frameworku Privacy Shield >>> zde.

[3] Rozhodnutí dostupné >>> zde.

[4] Např. FISA 702 či EO 12.333

[5] Viz body 133-135 rozsudku Schrems II

[6] Uvedeno i ve stanovisku ÚOOÚ dostupném >>> zde.

[7] Viz bod 10 dokumentu „FAQ“ vydaného EDPB, který je dostupný zde.

[8] Pokyny EDPB jsou dostupné >>> zde.

[9] Viz bod 113 rozsudku Schrems II

[10] Viz Sdělení Komise o implementaci GDPR dostupné >>> zde.

[11] Viz společná tisková zpráva dostupná >>> zde.

Další články:

- Evropská unie mění pravidla plateb: více odpovědnosti, intenzivnější zpracování dat, více kontrol
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Novinky z české a evropské regulace finančních institucí za měsíc květen 2026
- Sport versus EU – aktuální sportovní kauzy rozhodované Soudním dvorem EU
- Postavení finančního arbitra v kontextu nařízení Brusel I bis - Funkční pojetí „soudu“, osvědčení podle čl. 53 a možnost výkonu nálezu v jiných členských státech EU
- ESG Simple jako praktická opora pro ESG reporting malých a středních podniků
- Novinky z české a evropské regulace finančních institucí za měsíc duben 2026

- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Novinky z české a evropské regulace finančních institucí za měsíc březen 2026