Legal Update z oblasti

Zima 2021/2022

Weinhold Legal

Pokyny k místní příslušnosti a předávání osobních údajů

Evropský sbor pro ochranu osobních údajů („EDPB“) vydal Pokyny 5/2021 o vzájemném působení mezi aplikací čl. 3 a ustanovení o předávání osobních údajů do třetích zemí mimo EU/EHP dle kapitoly V. obecného nařízení o ochraně osobních údajů („GDPR“). Do 31. ledna 2022 probíhala k pokynům veřejná diskuze.

Cílem pokynů je pomoci správcům a zpracovatelům v EU při identifikaci, zda zpracovatelská operace představuje předávání osobních údajů do třetích zemí, jelikož GDPR neposkytuje právní definici pojmu „převod osobních údajů do třetí země nebo mezinárodní organizaci". Kritéria jsou tři a musí být splněna současně:

1. Vývozce údajů, tedy správce nebo zpracovatel, podléhá GDPR pro dané zpracování;
2. Tento vývozce předává nebo zpřístupní osobní údaje dovozci dat (jiný správce, společný správce nebo zpracovatel);
3. Dovozce se nachází (je usazen) ve třetí zemi nebo je mezinárodní organizací.

Zpracování bude považováno za předávání, bez ohledu na to, zda dovozce usazený ve třetí zemi podléhá GDPR podle čl. 3.

EDPB se však domnívá, že shromáždění údajů mimo EU/EHP přímo od subjektů údajů na základě jeho vlastní iniciativy nepředstavuje předávání osobních údajů mimo EU/EHP.

Pokyny k právu na přístup k osobním údajům

EDPB vydal Pokyny k právu na přístup 1/2022. Analyzují různé aspekty práva subjektu údajů na přístup k údajům o něm zpracovávaných a poskytují vodítka, jak má správce osobních údajů přístup subjektu údajů poskytnout v různých situacích. Pokyny mimo jiné objasňují rozsah práva na přístup, informace, které musí správce poskytnout subjektu údajů, formát žádosti o přístup, hlavní způsoby poskytování přístupu a pojem zjevně neopodstatněné nebo nepřiměřené žádosti. Do 11. března 2022 probíhá k pokynům veřejná diskuze.

Pokyny k příkladům porušení zabezpečení osobních údajů

EDPB vydal Pokyny 1/2021 k příkladům porušení zabezpečení po veřejné diskuzi. Pokyny mají pomoci správcům osobních údajů při rozhodování, jak zacházet s porušením zabezpečení osobních údajů a jaké faktory musí vzít v úvahu při posuzování rizik.

Postavení subjektů při poskytování zprostředkování finančních služeb

(rozsudek Nejvyššího správního soudu ČR ze dne 7. října 2021, sp. zn. 7 As 146/2021)

Nejvyšší správní soud ČR („NSS“) v řízení rozhodl o kasační stížnosti společnosti SMS finance, a.s. („žalobce“ nebo „stěžovatel“) proti rozhodnutí Městského soudu v Praze („městský soud“), ve kterém pro nedůvodnost zamítl správní žalobu žalobce proti rozhodnutí Úřadu pro ochranu osobních údajů („ÚOOÚ“). Zabýval se zde otázkou, zda správní orgány oprávněně považovaly stěžovatele za správce osobních údajů dle čl. 4 bod 7 GDPR. V tomto ohledu se NSS ztotožnil s názorem městského soudu. Tedy s názorem, že žalobce byl v dané věci **v postavení správce osobních údajů, neboť určil účely a prostředky zpracování osobních údajů**. Stěžovatel určil osobu Ing. L. Š., jakožto vázaného zástupce ve smyslu § 15 zákona č. 170/2018 Sb., o distribuci pojištění a zajištění, která zprostředkovávala služby žalobce, v rámci čehož docházelo i ke shromažďování osobních údajů potenciálních klientů, které

Legal Update z oblasti

Zima 2021/2022

Weinhold Legal

shromažďovala a zpracovávala právě pro účely stanovené žalobcem. Již zpracování osobních údajů před představením nabídky služeb stěžovatele je přitom vedeno za účelem nabídnutí těchto služeb. Stěžovatel měl s Ing. L. Š. uzavřenou pouze smlouvu o obchodním zastoupení, nikoliv smlouvu zpracovatelskou a argumentoval, že jde o nezávislou podnikatelku a že v prvotní fázi oslovení klienta zpracovává osobní údaje subjektů údajů za účelem vybudování si své vlastní zákaznické sítě, které následně bude v rámci své podnikatelské činnosti nabízet své vlastní služby (služby finančního poradenství), přičemž k nabízení služeb stěžovatele dochází až následně, a nikoli vždy.

Rozkladem žalobce brojil proti právnímu názoru ÚOOÚ, že je správcem osobních údajů. ÚOOÚ uložil žalobci nápravná opatření, konkrétně povinnost zajistit právní tituly pro zpracování osobních údajů všech subjektů údajů, vůči kterým je v postavení správce, tedy tam, kde sám určil účel a prostředky zpracování v souladu s čl. 6 GDPR, přičemž v případě, že by takové zajištění nebylo u některého subjektu údajů možné, potom má provést výmaz osobních údajů takového subjektu údajů, a to ve lhůtě 3 měsíců od právní moci tohoto rozhodnutí. ÚOOÚ také uložil žalobci uzavřít zpracovatelskou smlouvu se subjekty, které pro něj plní úkoly spojené se zpracováním osobních údajů tak, aby tyto disponovaly řádným právním titulem pro úkoly spojené se zpracováním osobních údajů.

Rozklad byl zamítnut a žalobce napadl rozhodnutí o rozkladu správní žalobou. Rozhodnutí bylo následně potvrzeno v rámci správního řízení i městským soudem, proti čemu podal stěžovatel kasační stížnost. NSS připomíná, že důvodem **pro úpravu vztahů mezi správcem a zpracovatelem** (a to především na základě specifické smlouvy podle čl. 28 odst. 3 GDPR) je právě skutečnost**, že se jedná o vztah dvou jinak na sobě nezávislých subjektů**. Právní úprava za správce považuje toho, kdo určuje účely a prostředky zpracování osobních údajů. Zpracovatelem je pak ten, kdo zpracovává osobní údaje pro správce. Jde přitom pouze k tíži stěžovatele, že si efektivně nezajistil, aby mu Ing. L. Š. předávala osobní údaje.

NSS tak potvrdil závěr ÚOOÚ, že **stěžovatel je v postavení správce i ve vztahu k osobním údajům, jež pro něj zpracovává tzv. samostatný zprostředkovatel finančních služeb, neboť určil účel tohoto zpracování.**

Odpovědnost za únik údajů není vždy absolutní

(rozsudek Nejvyššího správního soudu ČR ze dne 11. listopadu 2021, sp. zn. 1 As 238/2021)

NSS posuzoval otázku, zda se žalobce dopustil přestupku podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. o ochraně osobních údajů („ZOOÚ") tím, že nepřijal opatření pro zajištění bezpečnosti zpracovávaných osobních údajů dle ustanovení § 13 odst. 1 ZOOÚ, které stanoví, že správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů. V projednávané věci uznal ÚOOÚ žalobce, společnost Internet Mall, a.s. („žalobce" nebo „stěžovatel"), vinnou ze spáchání přestupku, když nepřijala opatření pro zajištění bezpečnosti zpracovávaných osobních údajů. Konkrétně nezabezpečila osobní údaje nejméně 735.956 zákazníků (v rozsahu jméno, příjmení, e-mailová adresa, heslo uživatelského účtu, případně telefonní číslo) před neoprávněným přístupem v období minimálně od 31. prosince 2014 do srpna 2017, v důsledku čehož došlo v době od 27. července 2017 do 25. srpna 2017 k jejich zpřístupnění neznámým hackerem na internetových stránkách www.ulozto.cz. Za spáchání uvedeného přestupku uložil ÚOOÚ pokutu ve výši 1.500.000 Kč. Žalobce podal proti prvostupňovému rozhodnutí rozklad, který byl zamítnut.

Následně se žalobce bránil podáním správní žaloby, kterou městský soud zamítl. V kasační stížnosti podané u NSS žalobce (stěžovatel) argumentoval*, že městský soud vycházel ze skutečnosti, že přestupek podle citovaného ustanovení je konstruován jako odpovědnost za následek, jímž je ohrožení bezpečnosti*

zpracovávaných osobních údajů. Uvedený výklad je v rozporu s textem zákona a úmyslem zákonodárce. Dotčené ustanovení vychází z norem evropského práva, jejichž autoři si byli vědomi toho, že veškerá bezpečnostní opatření jsou vždy pozadu za jakýmikoliv hrozbami, pročež antivirové, ani jiné softwarové prostředky nikdy neposkytnou 100% ochranu. Výklad aplikovaný městským soudem by znamenal, že veškeré subjekty, které byly obětí takových [kybernetických] útoků, by se dopustily přestupku, bez ohledu na to, jaká opatření reálně přijaly. Stěžovatel tvrdil, že podle § 13 zákona ZOOÚ **není povinností správce údajů přijmout za účelem jejich ochrany všechna myslitelná opatření**. Tento výklad dle stěžovatele koresponduje i s textem GDPR, které nepožaduje přijetí veškerých možných opatření ale v čl. 24 a čl. 32 GDPR hovoří o *vhodných opatřeních* a *vhodné úrovni bezpečnosti*.

Dle NSS v posuzované věci nebylo sporné, že stěžovatel nezabránil neoprávněnému přístupu k osobním údajům více než 700 tisíc jeho zákazníků. Odcizení údajů pak odhalil až se značným časovým odstupem, a to v návaznosti na jejich zveřejnění na internetových stránkách. Domníval se však, že jak žalovaný ÚOOÚ, tak i městský soud interpretovali ustanovení ZOOÚ chybně a trval na tom, že bylo povinností ÚOOÚ zkoumat, **jaká opatření stěžovatel za účelem předejití neoprávněného přístupu k osobním údajům přijal**.

NSS dovodil, že **odpovědnost správců a zpracovatelů osobních údajů není bezbřehá, ale klade důraz na to, aby dotčené subjekty vynaložily za účelem ochrany osobních údajů náležité úsilí a nelze na ně přenášet neomezenou odpovědnost za jakoukoliv (mnohdy i protiprávní či dokonce trestnou) činnost jiných subjektů**. Stěží lze očekávat, že přijatá bezpečnostní opatření budou natolik silná, aby byla schopná odrazit případně i sofistikovaný a cílený kybernetický útok. Kasační soud připomíná, že **pro vznik odpovědnosti za přestupek není rozhodující, zda se osobní údaje v konečném důsledku podaří ochránit či nikoliv, ale zda je zjištěn deficit v přijetí náležitých opatření za účelem jejich ochrany**. V daném případě k neoprávněnému přístupu k osobním údajům došlo zjevně v důsledku cíleného protiprávního jednání jiného subjektu. Stěžovatel přitom sice musí obdobné jednání předvídat, nemůže však za něj nést automaticky odpovědnost bez ohledu na to, jaká opatření za účelem ochrany osobních údajů přijal, a nakolik promyšlený a propracovaný byl útok neznámého subjektu, který údaje z databáze odcizil. NSS tedy souhlasil se stěžovatelem a přikročil ke zrušení napadeného správního rozhodnutí. Bude tak na ÚOOÚ, aby zohlednil všechna stěžovatelem **přijatá opatření** a zabýval se tím, jestli byla **s ohledem na dostupnou úroveň ochrany v rozhodném období, charakter činnosti stěžovatele a rozsah jím zpracovávaných údajů dostatečná**.

O dalších novinkách z oblasti GDPR pravidelně informujeme na sociálních sítích. Sledujte nás na LinkedIn a Facebooku.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Tereza Hošková
Vedoucí advokát
Tereza.Hoskova@weinholdlegal.com