Digital Legal Update

Červenec 2024

Weinhold Legal

Pokuta ÚOOÚ za neoprávněné zpracování osobních údajů

Společnosti Avast Software s.r.o. byla Úřadem pro ochranu osobních údajů („ÚOOÚ“, „Úřad“) pravomocně uložena pokuta ve výši 351 milionů Kč za neoprávněné zpracování osobních údajů uživatelů jejího antivirového programu a jeho rozšíření internetových prohlížečů (Browser Extensions) v roce 2019.

Úřad uložil pokutu, protože Avast neoprávněně předával pseudonymizovanou historii prohlížení internetu přibližně 100 milionů uživatelů společnosti Jumpshot, INC. Tato společnost poskytovala data marketérům pro sledování online chování spotřebitelů. Ačkoli Avast tvrdil, že údaje byly anonymizovány, bylo dle Úřadu prokázáno, že předávaná data mohla vést k identifikaci uživatelů, což znamená, že nebyly skutečně anonymizované.

Úřad pro ochranu osobních údajů zdůraznil, že jako přední odborník na kybernetickou bezpečnost, by Avast neměl předávat údaje, které by mohly odhalit totožnost uživatelů či jejich soukromé informace, jako jsou zájmy, bydliště, majetkové poměry a další. Vzhledem k tomu, že se jednalo o případ přeshraničního zpracování osobních údajů v rámci celé EU, byla věc řešena také s ostatními dozorovými úřady v EU v rámci mechanismu One Stop Shop.

Kontrola souhlasu se zpracováním osobních údajů pro marketingové účely

Úřad provedl kontrolu zaměřenou na nastavení souhlasu se zpracováním osobních údajů pro marketingové účely u obchodní korporace nabízející zasílání zboží. Tato společnost umožňovala zákazníkům objednávat zboží poštou, prostřednictvím objednávkových kupónů, přičemž podpisem objednávky zákazník automaticky souhlasil se zpracováním osobních údajů pro marketingové účely. Nebylo možné provést objednávku bez tohoto souhlasu.

Úřad kontrolou zjistil, že se jednalo o systémově špatné nastavení udělování souhlasu se zpracováním osobních údajů. Navíc, pokud zákazník chtěl využít svého práva na opravu osobních údajů, musel použít formulář „Vyjádření souhlasu o změnu údajů v adrese“, který rovněž obsahoval souhlas se zpracováním osobních údajů pro marketingové účely. Tento postup byl pro subjekty údajů překvapivý a v rozporu s GDPR.

Zjištěná praxe nesplňovala podmínky článků 4 bodu 11 a článku 7 odst. 4 GDPR, jelikož souhlas nebyl svobodný, a tudíž nebyl platný. Společnost tak neměla platný právní titul pro zpracování osobních údajů pro marketingové účely. Navíc dokumenty neobsahovaly informaci o právu souhlas kdykoliv odvolat, což bylo další porušení nařízení. Společnost rovněž neinformovala subjekty údajů o právním základu zpracování jejich osobních údajů.

EDPB k modelům „pay or OK“

Na základě žádosti nizozemského, norského a hamburského úřadu pro ochranu údajů, Evropský sboru pro ochranu osobních údajů („EDPB“) přijal stanovisko 08/2024, které se zabývá platností souhlasu se zpracováním osobních údajů pro účely behaviorální reklamy v kontextu modelů „pay or OK“ (tedy „platba nebo souhlas“) zaváděných velkými online platformami.

Klíčové body stanoviska:

- Modely „pay or OK“ často uživatele nutí buď souhlasit se zpracováním osobních údajů, nebo zaplatit poplatek, což uživatelům neposkytuje skutečnou možnost volby;

Digital Legal Update

Červenec 2024

Weinhold Legal

- Nabídnutí pouze placené alternativy k službám zpracovávajícím osobní údaje pro behaviorální reklamu není adekvátní a správci by měli zvážit poskytnutí „rovnocenné alternativy“ bez nutnosti platby;
- Velké online platformy by měly zajistit, že jakýkoli účtovaný poplatek nebude uživatele tlačit k nechtěnému souhlasu;
- Souhlas musí být informovaný, konkrétní a jednoznačný, jak ukládá GDPR; uživatelé by měli být plně informováni o důsledcích své volby.

EDPB nyní pracuje na detailnějších pokynech k modelům „pay or OK“.

Evropská komise k modelu „pay or OK“ společnosti Meta

Evropská komise (Komise, „EK“) zahájila řízení dle čl. 8 nařízení o digitálních trzích (Digital Markets Act, „DMA“) a informovala společnost Meta o prozatímních zjištěních týkajících se jejího reklamního modelu „pay or OK“ („platba nebo souhlas“), protože dle Komise tento model nesplňuje požadavky nařízení o digitálních trzích.

Nový model „pay or OK“ zavedla Meta v listopadu 2023, kdy si uživatelé Facebooku a Instagramu v EU museli vybrat mezi placeným předplatným bez reklam nebo bezplatným přístupem s personalizovanými (behaviorálními) reklamami.

Komise zastává prozatímní názor, že reklamní model společnosti Meta "pay or OK" není v souladu s DMA, protože nesplňuje nezbytné požadavky stanovené v čl. 5 odst. 2 DMA. Model společnosti Meta zejména:

- neumožňuje uživatelům zvolit si službu, která využívá méně jejich osobních údajů, ale jinak je rovnocenná službě založené na personalizované reklamě;
- neumožňuje uživatelům uplatnit jejich právo na svobodný souhlas s kombinací jejich osobních údajů mezi určenými službami základní platformy a jinými službami.

V průběhu svého šetření Komise koordinovala svou činnost s příslušnými dozorovými úřady pro ochranu osobních údajů.

Meta má nyní možnost uplatnit své právo na obhajobu a vyjádřit se k prozatímním zjištěním Komise. Komise plánuje uzavřít své šetření do 12 měsíců od zahájení řízení, tj. do konce března 2025. Pokud setrvá na závěrech svých prozatímních zjištěních i v samotném rozhodnutí o nesouladu, může společnosti Meta uložit pokutu až do výše 10 % celkového celosvětového obratu, což by v přepočtu mohlo činit přibližně 315 miliard korun.

Komise má také pravomoc přijmout další nápravná opatření, jako je např. povinnost prodat podnik nebo jeho části.

Šetření EDPS o používání Microsoft 365 Evropskou komisí

V květnu 2021 zahájil Evropský inspektor ochrany údajů (European Data Protection Supervisor, „EDPS“) šetření ohledně používání Microsoft 365 Evropskou komisí v návaznosti na rozsudek Schrems II. Cílem bylo ověřit, zda EK dodržuje doporučení EDPS týkající se používání produktů a služeb společnosti Microsoft orgány EU.

EDPS dovodil, že EK porušila několik ustanovení nařízení EU 2018/1725 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány, institucemi a jinými subjekty Unie a o volném pohybu těchto údajů a o zrušení nařízení (ES) č. 45/2001 a rozhodnutí č. 1247/2002/ES, když EK neposkytla vhodné záruky pro ochranu osobních údajů předávaných mimo EU/EHP, což je v rozporu s požadavky na odpovídající úroveň ochrany. Dále smlouvy EK se

Digital Legal Update

Červenec 2024

Weinhold Legal

společností Microsoft dostatečně nespecifikovaly, jaké údaje budou shromažďovány a pro jaké účely. EDPS proto nařídil Komisi, aby

- pozastavila veškeré datové toky vyplývající z používání služby Microsoft 365 společnosti Microsoft a jejím přidruženým společnostem a dílčím zpracovatelům nacházejícím se v zemích mimo EU/EHP, na které se nevztahuje rozhodnutí o odpovídající ochraně a
- uvedla operace zpracování vyplývající z používání služby Microsoft 365 do souladu s nařízením EU 2018/1725.

Splnění obou podmínek musí Komise prokázat do 9. prosince 2024.

Proti rozhodnutí EDPS podala Evropská komise dne 17. května žalobu k Soudnímu dvoru Evropské unie („SDEU“) (Věc T-262/24) a učinila tak i společnost Microsoft dne 21. května 2024 (Věc T-265/24).

Návrh zákona o kybernetické bezpečnosti

Legislativní rada vlády (LRV) doporučila vládě ke schválení návrh zákona o kybernetické bezpečnosti, kterým se do českého právního řádu implementuje směrnice o kybernetické bezpečnosti (Network and Information Security Directive, „NIS2“). Tento krok následuje po úpravách, které Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) zapracoval na základě předchozích podnětů LRV.

Pro lepší orientaci v zapracovaných úpravách připravil NÚKIB přehled hlavních provedených změn. Cílem tohoto dokumentu je zjednodušit veřejnosti a budoucím adresátům vznikajícího zákona orientaci v aktuální verzi dokumentu.

Vláda nyní projednává návrh zákona, přičemž bude zohledňovat také připomínky z mezirezortního připomínkového řízení. Po schválení vládou bude návrh předložen Poslanecké sněmovně Parlamentu ČR. Transpoziční lhůta dle směrnice NIS2 požaduje účinnost nového zákona k 18. říjnu 2024. V závislosti na průběhu legislativního procesu se předpokládá účinnost zákona koncem roku 2024 či dokonce až v roce 2025. Termíny pro plnění dalších povinností pak budou záležet na finálním datu účinnosti zákona.

Nařízení o umělé inteligenci publikováno v Úředním věstníku EU

Dne 12. července 2024 bylo v Úředním věstníku EU zveřejněno Nařízení Evropského parlamentu a Rady (EU) 2024/1689, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (nařízení o umělé inteligenci, „AI Act“). Toto nařízení přináší zásadní změny v regulaci umělé inteligence. AI Act stanovuje jasná pravidla pro využití umělé inteligence s cílem maximalizovat její přínosy a minimalizovat nežádoucí dopady na společnost. Firmy se nyní musí adaptovat na nová pravidla a začít je zavádět do praxe.

Klíčové body AI Act:

- klasifikace: AI systémy jsou klasifikovány podle jejich rizikovosti, přičemž některé jsou pro nepřijatelné riziko zcela zakázány;
- pravidla pro užívání AI: stanovuje jednotná pravidla pro vývoj, uvádění na trh, uvádění do provozu a používání systémů AI v souladu s pravidly EU týkajícími se bezpečnosti, základních práv občanů EU a etickými zásadami;
- bezpečnost, spolehlivost a transparentnost: zavádí přísné požadavky na systémy AI, včetně přesnosti, snižování rizik a povinnosti informovat uživatele, že komunikují s AI systémem;

Digital Legal Update

Červenec 2024

Weinhold Legal

- inovace: podporuje výzkum a vývoj v oblasti AI prostřednictvím bezpečných a regulovaných postupů.

Nařízení je závazné a přímo použitelné ve všech členských státech EU. Povinnosti se liší podle rizika jednotlivých AI systémů a vztahují se i na subjekty mimo EU, pokud je výstup systému AI používán v EU.

Klíčové termíny a povinnosti:

- 2. února 2025: vstoupí v účinnost obecná ustanovení nařízení o umělé inteligenci (články 1–5) a začnou platit zákazy pro nepřijatelné riziko AI (zakázané AI). Doporučujeme, aby firmy začaly s přípravou již nyní, aby splnily nové povinnosti, například v oblasti školení zaměstnanců.
- 2. května 2025: Kodexy správné praxe by měly být již připraveny, aby poskytovatelé mohli včas prokázat soulad. Kodexy správné praxe by měly představovat ústřední nástroj pro řádné dodržování povinností stanovených tímto nařízením pro poskytovatele obecných modelů AI a jejich vypracování zajišťuje Úřad pro AI.
- 2. srpna 2025: členské státy musí zřídit oznamující orgány a určit orgány dozoru nad trhem. Začnou platit povinnosti poskytovatelů obecných modelů AI. Již bude možné použít ustanovení o sankcích.
- 2. srpna 2026: AI Act začne být účinný v plném rozsahu (kromě článku 6 odst. 1, který vstoupí v platnost 2. srpna 2027).

Výroční zpráva ÚOOÚ 2023

Úřad předložil Senátu Parlamentu České republiky Výroční zprávu za rok 2023, která představuje ucelený přehled a shrnutí nejdůležitějších výsledků dozorové činnosti Úřadu v oblasti zpracování osobních údajů. Její klíčové body jsou:

- Cookies

  V roce 2023 Úřad významně zvýšil počet rozhodnutí týkajících se zpracování osobních údajů prostřednictvím souborů cookies. Někteří správci totiž nedostatečně reagovali na vytýkací dopisy, které Úřad zasílal. Úřad se bude této problematice nadále intenzivně věnovat, protože zpracování osobních údajů prostřednictvím cookies může být pro uživatele internetu velmi nebezpečné.

- Evropský návrh procesního nařízení doplňujícího GDPR

  V červenci 2023 představila Evropská komise návrh nařízení, kterým se stanoví další procesní pravidla pro prosazování nařízení (EU) 2016/679 (obecné nařízení o ochraně osobních údajů, GDPR) a nyní návrh postupuje legislativním procesem a je projednáván Evropským parlamentem. Návrh reaguje na zkušenosti s aplikací GDPR v přeshraničních případech (např. když má subjekt osobních údajů bydliště v jiném státě než správce) a jeho cílem je zlepšit spolupráci mezi vnitrostátními dozorovými úřady při prosazování GDPR.

- Návrh zákona o digitální ekonomice

  Ministerstvo průmyslu a obchodu začalo intenzivně připravovat adaptaci nařízení o digitálních službách (Digital Services Act, „DSA“) a nařízení o správě dat (Digital Governance Act, „DGA“) do českého právního řádu v podobě návrhu zákona o digitální ekonomice a o změně některých souvisejících zákonů.

  Návrh zákona o digitální ekonomice má zajistit správné fungování vnitřního trhu v oblasti digitální a datové ekonomiky prostřednictvím vytvoření jasného a předvídatelného právního rámce pro vymáhání povinností plynoucích ze souvisejících právních předpisů EU. To zahrnuje jednak určení příslušných

Digital Legal Update

Červenec 2024

Weinhold Legal

orgánů, které odpovídají za vymáhání nařízení o správě dat a nařízení o digitálních službách Hlavním dozorovým úřadem bude Český telekomunikační úřad; ÚOOÚ bude spolupracovat zejména na dozoru elektronické reklamy.

Návrh též stanoví pravidla týkající se sankcí za porušení DSA a DGA.

- Pravomocná pokuta za aplikaci Karanténa

Úřad udělil první pravomocnou pokutu za porušení předpisů upravujících ochranu osobních údajů v režimu tzv. trestněprávní směrnice, konkrétně za neoprávněné zpracování osobních údajů osob, jimž byla nařízena izolace Policií ČR v rámci databáze Karanténa.

Za účelem získání dalších informací kontaktujte, prosím, partnera / manažera, s nímž jste obvykle ve spojení.

Martin Lukáš
Partner
Martin.Lukas@weinholdlegal.com

Tereza Hošková
Vedoucí advokát
Tereza.Hoskova@weinholdlegal.com

Daša Aradská
Advokátka
Dasa.Aradska@weinholdlegal.com