4. 7. 2019

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

Rok po účinnosti GDPR – pravomocná rozhodnutí a příkazy za porušení tohoto nařízení

Píše se konec roku 2017. Do účinnosti nového 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 (dále také jako „GDPR“) zbývá už jen půl roku. Ve velkých médiích se začínají množit články o tom, že správcům osobních údajů již nezbývá mnoho času, aby dali do souladu veškeré procesy ve svých společnostech.

Články jsou různorodé – odborné, pro laiky, praktické, teoretické. Každý článek však obsahuje (nejlépe tučným písmem) jednotící prvek, a tím je informace o astronomické pokutě.

V současné době je GDPR již rok účinné, účinnosti nabyl rovněž nový zákon o ochraně osobních údajů, a také byly uděleny první pokuty. Jsou astronomické? Jaký je důvod udělených pokut? To jsou otázky, na které bych chtěl v tomto článku odpovědět. Rovněž bych chtěl poukázat na skutečnost, že ochrana osobních údajů není potřebná z důvodu „dalšího zla“, které musí správce či zpracovatel dodržovat, aby se vyhnul pokutě. Všechny níže uvedené příklady totiž poukazují na fakt, že k uložení pokuty často vede naprostá bezohlednost při nakládání s osobními údaji.

SEDLAKOVA LEGAL

Úřad pro ochranu osobních údajů (dále také jako „**Úřad**“) na žádost zveřejnil anonymizovaná pravomocná rozhodnutí a příkazy za porušení GDPR[1]. Pokusím se srozumitelným a stručným způsobem shrnout nejzajímavější příkazy a rozhodnutí, které byly zveřejněny.

Bývalý zaměstnanec a fotografie na Facebooku

První příkaz rozebraný v tomto článku byl vydán dne 10. 1. 2019 v souvislosti s Facebookovým profilem školy (zaměstnavatele), která zde měla zveřejněny fotografie bývalé zaměstnankyně společně s jejím jménem[2]. Zaměstnankyně školu žádala, aby došlo k odstranění fotografií, přičemž škola na žádost nereagovala. Zaměstnankyně tak podala stížnost k Úřadu, který se rovněž pokusil vyzvat školu k odstranění fotografie. Ani na opakované žádosti Úřadu však škola nereagovala, a tak Úřad udělil pokutu ve výši 10 000 Kč.

Úřad rovněž zdůraznil, že zveřejnění fotografie o bývalém zaměstnanci společně s uvedením jeho jména, příjmení a titulu je možné pouze na základě předchozího souhlasu. Jiný právní důvod nepřichází v úvahu. Jedná se tak o typický příklad toho, že Úřad v prvé řadě nechce udělovat pokuty, nýbrž chce napravit závadný stav. Kdyby škola s Úřadem spolupracovala a fotografie odstranila, udělení pokuty by bylo mnohem méně pravděpodobnější.

Jednu otázku však daný příkaz vyvolává, a to, zda se opravdu v daném případě jedná o zpracování osobních údajů. V příkazu je totiž uvedeno, že se jedná o osobní údaje ve smyslu čl. 4 bodu 1 GDPR a že škola je jejich správcem, už však není rozebráno, zda se jedná o zpracování či nikoliv. Ve stanovisku č. 12/2012 Úřadu, které bylo v říjnu 2017 aktualizováno, je uvedeno, že: *„pokud z příležitostně pořízených fotografií nebo záznamů nejsou při jejich použití vytvářeny evidence o fyzických osobách ani nejsou k zobrazeným či zaznamenaným osobám kromě běžné identifikace jménem a příjmením systematicky přiřazovány další osobní údaje, jinak řečeno,* ***pokud nedochází k jejich zpracování ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. nebo čl. 4 odst. 2 GDPR.[3]****"*

Ze stanoviska tak vyplývá, že by se v daném případě nemuselo vůbec jednat o zpracování osobních údajů. Samozřejmě lze namítat, že v tomto případě mohlo jít o portrétní fotografii, která nezachycuje pouze určitou společenskou, kulturní a jinou akci. Odůvodnění však nepovažuji za velmi šťastné.

Překročil jste rychlost a já to vím

Další příkaz Úřadu ze dne 4. 2. 2019 se týká GPS lokátorů, které byly umístěny ve vozidlech a tato následně společnost pronajímala[4]. Zákazníci o GPS lokátorech v autech vůbec nevěděli. Jeden zákazník na skutečnost přišel náhodou při hádce se zaměstnancem společnosti poskytujících nájem vozidel. Zaměstnanec zákazníkovi totiž sdělil, že ví, že překročil rychlost, a proto byla zákazníkovi udělena smluvní pokuta. Tuto informaci měl zaměstnanec společnosti právě z GPS lokátoru umístěného v autě.

Nedošlo tedy k informování subjektů údajů o tomto zpracování dle čl. 13 GDPR a správce tak porušil zásadu zákonnosti, korektnosti a transparentnosti. Za toto porušení udělil Úřad pokutu 30 000 Kč. V tomto případě správce spolupracoval s Úřadem a činil kroky k nápravě protiprávního stavu, a tak byla pokuta udělena při samé dolní hranici sazby.

Smlouvy o spotřebitelských úvěrech u kontejneru[5]

Malá společnost poskytovala v rámci výkonu své činnosti služby spočívající ve zprostředkování úvěrů, při kterých se uzavíraly smlouvy o spotřebitelských úvěrech. Tyto smlouvy se následně kopírovaly a společnost si kopie ponechávala. Smlouvy obsahovaly osobní údaje jako jméno, příjmení, rodné číslo, číslo občanského průkazu, informace o úvěru či telefonní číslo. Nutno podotknout, že se jedná o velký rozsah osobních údajů, který by mohl stačit ke krádeži identity.

Jednatelka společnosti převezla přes 300 smluv k sobě domů v úmyslu, že je následně uloží do skladu. Smlouvy však jednatelka uložila v papírové krabici do garáže, kam měli přístup všichni obyvatelé domu. Následně byla papírová krabice nalezena u kontejneru, kam ji odnesla neznámá osoba. Společnost tak nepřijala dostatečná bezpečnostní opatření k ochraně osobních údaje před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Společnost oznámila tento bezpečností incident (odcizení smluv) Úřadu, ovšem uvedla, že se jednalo jen přibližně o 80 smluv.

K oznámení bezpečnostního incidentu bylo přihlíženo jako k přitěžující okolnosti, neboť obsahovalo hrubě zavádějící informace týkající se počtu odcizených dokumentů. Na druhou stranu se však jednalo o velmi malou společnost, proto (aby nebyla pokuta likvidační) udělil Úřad pokutu ve výši 30 000 Kč. Úřad v rozhodnutí shrnuje, že správce osobních údajů musí vždy vyhodnotit pravděpodobnost a závažnost rizik, která při zpracování hrozí.

Jak je uvedeno v samotném rozhodnutí: *„Riziko pro práva a svobody fyzických osob musí být hodnoceno na základě objektivního posouzení, kdy východiskem pro jeho posouzení je hrozba narušení důvěrnosti a integrity zpracování."*

Na rozhodnutí je nejzajímavější, že i když došlo k oznámení bezpečnostního incidentu, bylo na něj pohlíženo jako na přitěžující okolnost, neboť neodpovídalo skutečnosti. Každý správce musí vzít v potaz pravdivost tvrzení, které poskytuje Úřadu.

Únik dat z online hry

Velmi zajímavý je rovněž příkaz ze dne 28. 2. 2019, ve kterém šlo o únik dat v rozsahu e-mailové adresy, hesla k uživatelskému účtu a IP adresy, a to v nejmenované online hře[6]. Únik dat způsobil programátor společnosti. Zajímavostí je, že k úniku došlo v noci na 25. května 2018, tedy dne počátku účinnosti GDPR, což dle účastníka řízení bylo učiněno schválně.

Programátor byl společností najat na zhotovení webové aplikace, jako doplněk k online hře, přičemž mu byla zpřístupněna celá databáze, kde byly uloženy soubory ke hře a databáze hráčů se všemi osobními údaji. Programátor se rozhodl, dle názoru účastníka řízení, omezit přístup k databázi jen na svou osobu a zveřejnil celou databázi na internetu. Společnost vyvíjející hru oznámila porušení ochrany osobních údajů na své Facebookové stránce prostřednictvím videa a únik byl oznámen také každému hráči při přihlášení do hry, společně s upozorněním, aby došlo ke změně hesla i na jiných portálech. Problémem v daném případě byl rovněž fakt, že data byla uložena na cloudových uložištích a s poskytovateli nebyly uzavřeny zpracovatelské smlouvy[7] dle čl. 28 GDPR. Programátor se také nacházel v pozici zpracovatele osobních údajů a rovněž s ním nebyla uzavřena zpracovatelská smlouva dle čl. 28 GDPR.

Rovněž společnost nepřijala dostatečná bezpečnostní opatření k zabezpečení osobních údajů, a tak Úřad uložil účastníku řízení pokutu ve výši 15 000 Kč. Výše pokuty byla uložena v samé dolní hranici sazby, neboť učinil kroky směřující k následnému zabezpečení zpracování osobních údajů a současně činil kroky, jejichž cílem bylo informovat dotčené subjekty údajů a poučit je, jak mají dále postupovat.

Jedná se o velmi zajímavý příkaz, který byl Úřadem velmi důsledně anonymizován, tudíž jsou z něj nečitelná některá bezpečnostní opatření, která byla přijata pro zamezení přístupu. V tomto případě došlo k porušení více povinností, což se projevilo jako přitěžující okolnost. Z udělené pokuty je však patrné, že se nejednalo o nikterak závratnou pokutu.

Biometrický podpis a ukládání nahrávek hovorů

Nejvyšší pokuta ze zveřejněných příkazů a rozhodnutí byla uložena v rozhodnutí Úřadu ze dne 21. 3. 2019, a to ve výši 250 000 Kč[8].

Zjednodušeně šlo v dané věci o porušení dvou zásad, a to k porušení zásady minimalizace údajů a porušení zásady omezení uložení dle GDPR.

Společnost poskytující úvěry zpracovávala kromě údajů potřebných ze zákona rovněž biometrické údaje z podpisu (při uzavírání smluv v elektronické podobě), jako například rychlost a tlak pohybu pera[9]. K tomuto zpracování byl od subjektů údajů vyžadován souhlas se zpracováním pro účely uložení a uchování smluvní dokumentace a zjednodušení procesu. K tomuto Úřad uvedl následující: *„[…] ani souhlas subjektu údajů se zpracováním konkrétních osobních údajů nezbavuje účastníka řízení povinnosti dodržovat všechny základní zásady zpracování osobních údajů, neboť soulad sledovaného účelu a k němu se vztahujícího minimálního rozsahu osobních údajů je nutno hodnotit objektivně, nikoli subjektivně.“*[10] Zároveň Úřad uvedl, že identifikovat subjekt lze i prostřednictvím jiných identifikátorů, než dle biometrického podpisu (postačí grafický sken podpisu). Tímto zpracováním biometrického podpisu tak společnost nedodržela zásadu minimalizace údajů.

V informačním systému společnost rovněž ukládala nahrávky hovorů, a to po dobu trvání smluvního

vztahu a následně po dobu 10 let od ukončení. Společnost měla povinnost, dle § 21 odst. 2 zákona č. 21/1992 Sb., uchovávat některé nahrávky, ovšem žádným způsobem nerozlišovala, zda jde o hovory informativního charakteru, servisního poradenství atp. Tímto tak došlo k porušení zásady omezení uložení.

Jako přitěžující okolnost bylo vnímáno porušení více povinností a uchovávání biometrických údajů jako zvláštní kategorie osobních údajů (zneužití by znamenalo značný zásah do soukromí). Souhlas se zpracováním a spolupráce s Úřadem byly považovány jako skutečnosti snižující závažnost jednání.

Závěr

Z výše uvedených rozhodnutí a příkazů je patrné, že pokuty nemají mít likvidační charakter, na druhou stranu musí být určitým způsobem odstrašující. Určitě se v oblasti ochrany osobních údajů neděje revoluce co do výše uložených pokut. Na druhou stranu se děje revoluce v počtu ohlášených incidentů a počtu subjektů údajů zajímajících se o svá práva. Správci osobních údajů si rovněž v některých případech začínají uvědomovat, že je potřeba brát osobní údaje v potaz a v případě problémů tyto problémy řádné ohlásit.

Výše jsem rozebral některé typické situace, které mohou nastat naprosto v jakémkoliv odvětví podnikání. V bezpečnostních incidentech hraje velkou roli lidský faktor, tudíž je vhodné vždy dobře proškolit všechny zaměstnance, odpovědné osoby a další subjekty pracující s osobními údaji.

A výše pokuty? Pokud bude správce (zpracovatel) spolupracovat, bude se snažit odstranit závadný stav, s osobními údaji bude pracovat svědomitě, není se čeho obávat. Neodpustím si však závěrem připomenout, že žádný správce by neměl být motivován ke správnému dodržování nakládání s osobními tím, že mu hrozí pokuta. Mnohem důležitější je si uvědomit, že práce s osobními údaji je velmi důležitá, neboť případná škoda, která může vzniknout, se nedá v některých případech vyčíslit penězi.

Mgr. Jiří Hradský,
advokátní koncipient

SEDLAKOVA LEGAL
Budova TITC
Purkyňova 648/125
612 00 Brno

Tel: +420 733 555 958
E-mail: office@sedlakovalegal.com

Zdroje:

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
Pravomocná rozhodnutí zveřejněná na stránkách Úřadu pro ochranu osobních údajů. K dispozici >>> zde.
Příkaz Úřadu pro ochranu osobních údajů ze dne 10. 1. 2019, č. j. UOOU-08244/18-15. K dispozici >>> zde.
Příkaz Úřadu pro ochranu osobních údajů ze dne 4. 2. 2019, č. j. UOOU-00178/19-3. K dispozici >>> zde.
Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 4. 2. 2019, č. j. UOOU-09571/18-14. K dispozici >>> zde.
Příkaz Úřadu pro ochranu osobních údajů ze dne 28. 2. 2019, č. j. UOOU-00163/19-3. K dispozici >>> zde.
Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. 3. 2019, č. j. UOOU-10138/18-8. K dispozici >>> zde.

_____
[1] Pravomocná rozhodnutí jsou k dispozici >>> zde.
[2] Příkaz Úřadu pro ochranu osobních údajů ze dne 10. 1. 2019, č. j. UOOU-08244/18-15. K dispozici >>> zde.
[3] Stanovisko je k dispozici >>> zde.
[4] Příkaz Úřadu pro ochranu osobních údajů ze dne 4. 2. 2019, č. j. UOOU-00178/19-3. K dispozici >>> zde.
[5] Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 4. 2. 2019, č. j. UOOU-09571/18-14. K dispozici >>> zde.
[6] Příkaz Úřadu pro ochranu osobních údajů ze dne 28. 2. 2019, č. j. UOOU-00163/19-3. K dispozici >>> zde.
[7] Skutkový stav byl poměrně složitější, kdy se jednalo o takzvané řetězení zpracovatelů bez předchozího souhlasu správce.
[8] Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. 3. 2019, č. j. UOOU-10138/18-8. K dispozici >>> zde.
[9] Jedná se o tzv. citlivé údaje dle čl. 9 GDPR
[10] Rozhodnutí Úřadu pro ochranu osobních údajů ze dne 21. 3. 2019, č. j. UOOU-10138/18-8. Str. 12 rozhodnutí

© EPRAVO.CZ – Sbírka zákonů, judikatura, právo | www.epravo.cz

Další články:

- Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí
- Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše

- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory