27. 9. 2019

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

Na co se ÚOOÚ zaměřil v kontrolách za první pololetí 2019?

Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („GDPR“) v článku 57 odst. 1 písm. a) a h) ukládá dozorovým úřadům monitoring a šetření o uplatňování GDPR. Tyto aktivity Úřad pro ochranu osobních údajů („ÚOOÚ“) provádí zejména prostřednictvím kontrol. ÚOOÚ tento týden zveřejnil přehled kontrol za první polovinu roku 2019.

Z počtu provedených kontrol a jejich závěrů je přitom zřejmé, že ÚOOÚ nepostupuje příliš aktivisticky a namísto represivního chování vůči správcům osobních údajů se snaží spíše poskytovat vodítka a v případě neprodlených náprav porušení GDPR nepřistupuje k vysokým sankcím. Současně je zřejmé, že ÚOOÚ postupuje v souladu vydaným plánem kontrol a další aktivity jsou soustředěny pouze na podněty související s porušováním GDPR. S ohledem na pravomoci ÚOOÚ pak kontroly mimo dodržování GDPR zahrnují i kontroly v oblasti dodržování zákona č. 480/2004 Sb., o některých službách informační společnosti („ZoIS“) v oblasti zasílání nevyžádaných obchodních sdělení.

Jakkoli závěry zveřejněných kontrol neobsahují nic, co by bylo příliš překvapivé, je vhodné na některé z nich upozornit a současně poukázat na to, na co se ÚOOÚ při kontrolách zaměřuje nejvíce, což může přispět k lepší připravenosti osob zpracovávajících osobní údaje.

Kontroly v oblasti ochrany osobních údajů

- **Kontrola provedení balančního testu**

Při zpracování osobních údajů na základě oprávněného zájmu je správce je povinen provést tzv. balanční test pro každé zpracování osobních údajů, které hodlá vykonávat na základě právního důvodu oprávněného zájmu. V praxi vidíme, že správci vykonání tohoto testu proporcionality často opomíjejí. ÚOOÚ se přitom na v rámci kontrol zaměřil i na kontrolu vypracování tohoto balančního testu (např. kontrola provedená ve společnosti Student Agency). Při kontrole TOP 09 přitom ÚOOÚ konstatoval, že „*v rámci tohoto posouzení (balančního testu) je nutné vzít do úvahy více faktorů, a to především váhu samotného oprávněného zájmu, možné negativní či pozitivní důsledky pro subjekty údajů, rozumné očekávání subjektů údajů ohledně zpracování či vztah správce a subjektu údajů. I výsledek balančního testu lze nakonec ovlivnit ve prospěch správce také přijetím vysokých záruk bezpečnosti zpracování či vyšší transparentností zpracování. Posouzení oprávněného zájmu je zároveň nutné pečlivě dokumentovat a být připraven jej v souladu se zásadou odpovědnosti předložit ÚOOÚ ke kontrole*.“ Správci by tak neměli zapomínat na záznam balančního testu vyhotovený před započetím zpracování osobních údajů na základě oprávněného zájmu. Tento test by měl zejména obsahovat analýzu odpovědí na otázky následujícího typu: (i) jaký je vztah mezi správcem a

subjektem údajů, (ii) je rozumným očekáváním subjektu údajů, že jeho osobní údaje budou užity zamýšleným způsobem, (iii) jaký vliv má na subjekty údajů zpracování údajů zamýšleným způsobem, (iv) lze zavést dostatečné záruky, aby se minimalizoval vliv na subjekty údajů, či (v) zdali jsou zpracovávány zvláštní kategore údajů ve smyslu čl. 9 GDPR, údaje dětí, či údaje zvláště citlivé. Pouze na základě vyhodnocení takového testu může správce dospět k závěru, zdali nemají před jeho zájmy přednost zájmy subjektů údajů a tedy, zdali vůbec může osobní údaje na základě oprávněného zájmu zpracovávat.

- **Kontrola zavedení technicko-organizačních opatření**

Z provedených kontrol je zřejmé, že se ÚOOÚ zaměřuje (a tendence v EU naznačují, že se do budoucna dozorové úřady patrně budou více zaměřovat) na dodržování povinností stanovených v čl. 5 odst. 1 písm. e) a čl. 32 GDPR o přijetí dostatečných technicko-organizačních opatření při zpracování osobních údajů (např. kontrola společností BOHEMIA ENERGY, České školní inspekce či KAPITOL pojišťovací a finanční poradenství).

ÚOOÚ například kontroloval provozovatele on-line hry, vůči němuž byly úspěšně provedeny DDoS útoky. Provozovatel se s útočníkem dohodl na tom, že útočník upraví zdrojový kód, aby byl vůči útokům odolnější. Útočník však nahrál do zdrojového kódu backdoor, jehož prostřednictvím mohl získat osobní údaje hráčů. Více jak čtyři tisíce účtů s osobními údaji tak bylo po krátkou dobu zveřejněno na internetu. Toto jednání provozovatele ÚOOÚ shledal jako porušení GDPR (nepřijetí dostatečných technických a organizačních opatření pro zabezpečení osobních údajů) a uložil provozovateli pokutu ve výši 25.000 Kč.

ÚOOÚ rovněž provedl kontrolu zabezpečení osobních údajů při jejich zpracování Českou školní inspekcí. Došlo k tomu, že v inspekčním systému elektronického testování bylo možné získat osobní údaje stovek žáků, protože údaje nebyly náležitě zabezpečeny. Česká školní inspekce poté, co se o porušení zabezpečení dozvěděla, zajistila zastavení provozu systému a úpravu aplikace tak, aby osobní údaje byly náležitě zabezpečeny. S ohledem na spolupráci s ÚOOÚ a neprodlenou nápravu ÚOOÚ upustil od uložení pokuty.

V Evropě jsme však svědky mnohem závažnějších porušení zabezpečení a mnohem drakoničtějších pokut. Kupříkladu maltský dozorový úřad udělil pokutu 5.000 Euro tamějšímu katastrálnímu úřadu v důsledku neexistence vhodných bezpečnostních opatření na webových stránkách.[1] Tím došlo k zpřístupnění více, než 10 GB osobních údajů sestávajících se primárně z korespondence s katastrálním úřadem. Vyšší pokuty z důvodů nedostatečných bezpečnostních opatření byly uděleny v Norsku. Bergenský městský úřad byl sankcionován pokutou 170.000 Euro[2] za to, že umožnil přihlášení do různých informačních systémů školy, a tím získal přístup k různým kategoriím osobních údajů týkajících se žáků a zaměstnanců. Pokutou ve výši 203.000 Euro pak byl sankcionován městský úřad v Oslo[3] za chyby v zabezpečení mobilní aplikace umožňující komunikaci rodičů a zaměstnanců školy, díky nimž se neoprávněné osoby mohly přihlásit jako oprávnění uživatele a získat přístup k osobním údajům o studentech, zákonných zástupcích a zaměstnancích. Prozatím nejvyšší sankce v oblasti nedostatečného zabezpečení byly uděleny britským ICO společnostem Marriott International (110.390.200 Euro) a British Airways (204.600.000 Euro), avšak tyto pokuty jsou prozatím nepravomocné.

- **Zveřejnění osobních údajů dlužníků**

V případě kontrol Všeobecné zdravotní pojišťovny České republiky a Oborové zdravotní pojišťovny zaměstnanců bank, pojišťoven a stavebnictví ÚOOÚ zopakoval, že zveřejnění osobních údajů dlužníků považuje za nátlakové jednání a takové je možné činit pouze s jejich souhlasem. Zveřejňování jmen či fotografií subjektů - dlužníků, či těch porušujících práva je dnes již

učebnicovým příkladem porušování práv subjektů, ke kterému se vyjádřil již Nejvyšší správní soud ČR v notoricky známém případu ve věci ekolo, kdy soud konstatoval, že takovým jednáním se nepřiměřeně zasahuje do soukromí osob.[4]

Kontroly v oblasti nevyžádaných obchodních sdělení

- **Neudělení souhlasu odesílatele**

Jedním z nejčastějším prohřešků identifikovaným ÚOOÚ je porušení § 7 odst. 4 písm. b) ZoIS - neuvedení identifikace odesílatele, jehož jménem se komunikace uskutečňuje (např. kontrola spol. Hadys corp. s.r.o., PETLAS CZ s.r.o. a spol., La Fruteria s.r.o. a DIREKTO s.r.o.). Důvodem často bývá skutečnost, že správce osobních údajů zpracovává osobní údaje ve prospěch celé skupiny a obchodní sdělení zasílá ve prospěch různých společností a opomene uvést jejich totožnost. V této souvislosti je třeba připomenout, že podle ust. § 7 odst. 3 ZoIS má fyzická nebo právnická osoba možnost šířit obchodní sdělení elektronickými prostředky bez souhlasu pouze svým zákazníkům a ve vztahu k vlastním výrobkům nebo službám, které jsou obdobné jako výrobky a služby poskytnuté zákazníkovi. Ve vztahu k ostatním členům skupiny je šiřitel povinen si obstarat souhlas.

- **Nedoložení souhlasu se zasíláním obchodních sdělení**

Dalším opakovaným porušením ZoIS je nedostatečné doložení udělení souhlasů uživatelů se zasíláním marketingových zpráv. ÚOOÚ např. v kontrole spol. Hadys corp. s.r.o. poukázal na to, že nepostačí prokázání udělení souhlasu prostřednictvím snímků obrazovky systému, ve kterých byl ke každé e-mailové adrese uveden pouze čas registrace a uživatelské jméno, ale součástí musí být uvedena i internetová stránka, na které měla registrace proběhnout. Byť ZoIS neobsahuje obdobné ustanovení jako čl. 7 odst. 1 GDPR, tedy výslovnou povinnost správce být schopen doložit, že subjekt údajů udělil souhlas se zpracováním svých osobních údajů, jelikož je ÚOOÚ oprávněn kontrolovat, zdali jsou obchodní sdělení šířena v souladu se ZoIS, tedy v některých případech se souhlasem adresáta, je kontrolovaný subjekt povinen tento souhlas prokázat stejně jako podle GDPR. Ostatně v řadě případů se získává při jedné aktivitě subjektu jeden souhlas se zpracováním osobních údajů a jeden se zasíláním obchodních sdělení. U elektronicky získávaných souhlasu je přitom nezbytné zajistit možnost prokázání, kdo souhlas udělil, kdy, co souhlas obsahoval a jak byl udělen. Je tedy nutné zajistit autenticitu a současně integritu dokumentu, na kterém je souhlas zachycen. Autenticitu lze zajistit např. žádostí o ověření zaslanou na e-mail, nebo prostřednictvím sms. Zpětnou vazbu je však zapotřebí řádně uložit pro případnou nutnost prokázání. Integritu lze přitom zajistit pořízením kopie webové stránky, na které je uveden souhlas (včetně jeho textu) opatřené časovým razítkem, nebo hashem takového dokumentu.[5] Přestože některé dozorové orgány nepovažují uložení data, IP adresy a linku na webové stránky obsahující souhlas za možnost zajistit souhlas (podle GDPR),[6] domnívám se, že v českém právu možné využít metodu odpovídající záznamům údajů splňujícím formu ust. § 562 odst. 2 zák. 89/2012 Sb., občanský zákoník, kterou docílíme spolehlivosti takového záznamu.

Lze předpokládat, že ÚOOÚ bude pokračovat v kontrolách dle plánu pro rok 2019. ÚOOÚ se tak bude patrně zaměřovat na kontrolu zpracování osobních údajů při používání cookies, zpracování osobních údajů společností vyvíjející a provozující mobilní aplikace, nebo kontrolu zpracování osobních údajů žadatelů o uzavření smlouvy o úvěr při jejím sjednávání online.

JUDr. Zdeněk Kučera, Ph.D.,
vedoucí praxe IT práva a litigací Kinstellar a vyučující Právnické fakulty Univerzity Karlovy v Praze

Kinstellar, s.r.o., advokátní kancelář

Palác Myslbek
Na příkopě 1096/19
110 00 Praha 1

Tel.: +420 221 622 111

---

[1] GVHZ advocates. *IDPC FINES LANDS AUTHORITY FOR DATA BREACH*. [online]. [vid. 26. 9. 2019]. K dispozici >>> zde.

[2] Datatilsynet. *Administrative fine of 170.000 € imposed on Bergen Municipality*. [online]. [vid. 26. 9. 2019]. K dispozici >>> zde.

[3] Datatilsynet, případ č. AR279591351.

[4] Viz rozsudek Nejvyššího správního soudu z 8. června 2016 sp. zn. 3 As 118/2015-34.

[5] Obdobně též ICO. *How should we obtain, record and manage consent?* [online]. [vid. 26. 9. 2019]. K dispozici >>> zde.

[6] *Ibid*.

Další články:

- „Za každou kauzou je živý příběh“
- Přehnaná, nebo důvodná prevence? Zajištění a utvrzení závazků v praxi
- Spoluvlastnictví a správa společné věci
- Doručování soudních písemností ze zahraničí do ČR
- Návrh nového zákona o digitální ekonomice
- Byznys a paragrafy, díl 30.: Jednání za s.r.o. – zápis jednatelského oprávnění do obchodního rejstříku
- Předběžné opatření a další instituty k ochraně věřitelů při přeměnách
- Promlčení zápůjčky bez určení splatnosti v judikatuře Nejvyššího soudu
- Rozvod s mezinárodním prvkem a související otázky péče o děti a výživného
- Příkaz a příkaz na místě v přestupkovém řízení vedeném orgány inspekce práce
- Letiště a letecké stavby