31. 3. 2021

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

Rozesílání obchodních sdělení a GDPR

Za spam zatím padají vyšší pokuty než za porušení GDPR. Úřad pro ochranu osobních údajů (ÚOOÚ) kromě ochrany osobních dat vykonává i řadu dalších, zdánlivě menších či alespoň méně viditelných agend. Jednou z nich je i dozor nad rozesíláním obchodních sdělení, jehož pravidla upravuje zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů.

ÚOOÚ je dozor nad agendou obchodních sdělení svěřen již od počátku platnosti uvedeného zákona. V poslední době bylo publikováno několik kontrolních závěrů a rozhodnutí ÚOOÚ, které vyvolaly zájem odborné veřejnosti. Tato pozornost byla do značená míra spojena st tím, že za porušení pravidel pro zasílání obchodních sdělení ÚOOÚ zatím uložil vyšší pokuty, než za porušení obecného nařízení o ochraně osobních údajů (GDPR).

Podle mého názoru si s ohledem na aktuální rozhodovací praxi ÚOOÚ bližší analýzu zaslouží tyto dva body

- Meze odpovědnosti objednatele rozesílání obchodních sdělení, kterou ÚOOÚ vykládá poměrně široce
- Jak je při výkonu dozoru posuzována současná aplikace zákona č. 480/2004 Sb. a GDPR, když řešené materie jsou si do velké míry blízké.

Kdo je odpovědný za protiprávní rozesílání obchodních sdělení?

Posunem výkladové praxe spočívající v odpovědnosti objednatele obchodních sdělení, nejen jejího faktického rozesílatele, jsem se již zabýval v předchozím článku.[1] S jistým odstupem si však bližší analýzu, či možná spíše jen formulování konkrétních otázek, zaslouží i meze takto vyložené odpovědnosti.

Stručně si shrňme, že v ÚOOÚ již několik let vykládá odpovědnost dle zákona č. 480/2004 Sb. za rozesílání obchodních sdělení tak, že za jeho legalitu rozesílání není odpovědný jen ten, kdo obchodní sdělení fakticky rozesílá, ale i na toho, kdo si jejich rozesílku objednal či v jehož prospěch je činěna.

V posuzovaném případě, kdy výklad ÚOOÚ potvrdil i Městský soud v Praze[2], si společnost se sídlem v České republice objednala rozesílku obchodních sdělení u společnosti se sídlem na Ukrajině. Ve smlouvě i v následující komunikaci se česká společnost snažila zajistit, aby rozesílání bylo prováděno v souladu s právními předpisy, nicméně i tak docházelo k rozesílání obchodních sdělení v její prospěch v rozporu se zákonem.

Jaké kroky objednatel učinil? Ve smlouvě s faktickým rozesílatelem si sjednal, že rozesílatel ručí za zákonnost posílání obchodních sdělení. V okamžiku, kdy se dozvěděl, že někteří z adresátů obchodních sdělení tvrdí, že byli kontaktování protiprávně, o tom informoval rozesílatele a vyzval ho k vyjádření či nápravě.

Podle názoru ÚOOÚ, potvrzeného následně i správním soudem první instance, to bylo málo. Bohužel ani dozorový úřad, ani soud nenaznačily, jaká opatření nebo jaké druhy opatření by v obdobném

obchodním modelu bylo možné považovat za dostatečné k vyvinění objednatele.

Jak zajistit legalitu rozesílání obchodních sdělení při využití dodavatele?

ÚOOÚ a správní soud v uvedeném případě rozhodly, jaká opatření k zajištění legality rozesílání obchodních sdělení za dostatečná nepovažují. Jaká další opatření či kroky by tedy objednatel měl či mohl přijmout?

Možnost vyvinění z odpovědni za přestupek a jeho podmínky upravuje § 21 zákona č. 250/2016 Sb., podle kterého:

(1) Právnická osoba za přestupek neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby přestupku zabránila.

(2) Právnická osoba se nemůže odpovědnosti za přestupek zprostit, jestliže z její strany nebyla vykonávána povinná nebo potřebná kontrola nad fyzickou osobou, která se za účelem posuzování odpovědnosti právnické osoby za přestupek považuje za osobu, jejíž jednání je přičitatelné právnické osobě, nebo nebyla učiněna nezbytná opatření k zamezení nebo odvrácení přestupku.

V kontextu tohoto případu, resp. shora uvedené otázky odpovědnosti, je relevantní především možnost dle prvého odstavce. Jaká opatření lze, zejména s ohledem na standardy v oblasti řízení rizik včetně compliance rizik, pro vyvinění dle tohoto ustanovení zákona doporučit? Jaké úsilí lze považovat za „veškeré“, které lze po objednateli rozeslání obchodních sdělení spravedlivě požadovat?

Při zohlednění okolností konkrétního vztahu a z něj vyplývajících rizik lze doporučit především následující opatření:

- Pečlivý výběr dodavatele a jeho alespoň základní prověření (zápis ve veřejném rejstříku, historie atd.)
- Řádné smluvní nastavení celého vztahu obsahující nejen záruky za legalitu procesu na straně dodavatele, ale i určení odpovědnosti obou stran, smluvní ujednání o zabezpečení dat či nastavení komunikace o stížnostech klientů a procesu pro jejich řešení; smlouvy by měla obsahovat i pravidla pro zpracování osobních údajů dle čl. 28 odst. 3 GDP, který zahrnuje mj. právo na audit u zpracovatele, v tomto případě toho, kdo fakticky rozesílá obchodní sdělení
- Nastavení pravidelného reportingu dodavatele objednateli o realizaci rozesílky obchodních sdělení, např. kolik obchodních sdělení bylo rozesláno, jaký je poměr nedoručených zpráv a tedy nefunkčních elektronických adres, kolik rozesílatel obdržel stížností na zasílání obchodních sdělení či odvolaných souhlasů s dalším zasíláním atd.
- Případná kontrola vzorku odesílaných obchodních sdělení z pohledu jejich souladu se zákonem
- Případný audit na místě u dodavatele k ověření toho, jak fakticky rozesílání obchodních sdělení probíhá

Pokud by objednatel takováto opatření, samozřejmě v individualizované a ne šablonovité formě, aplikoval a v rámci řízení vedeného ÚOOÚ doložil, musel by se ÚOOÚ podle mého názoru zabývat možným vyviněním objednatele. Pokud by zavedená opatření podle jeho závěru k vyvinění nestačila, musel by odůvodnit, proč je takto nastavený systém nedostatečný.

Mohu dostat pokutu za rozesílání spamu a porušení GDPR zároveň?

V teoretické rovině elektronické zasílání obchodních nabídek nemusí vždy nutně představovat zpracování osobních údajů tak, jak je definováno v čl. 4 bod 1)[3] a 2)[4] GDPR. Zejména

v případech, kdy jsou obchodní sdělení zasílána na generické kontaktní údaje, např. e-mailové adresy, právnických osob, se obvykle nejedná o osobní data.

Na druhou stranu, pojem osobní údaj je českými i unijními soudy vykládán široce a obvykle zahrnuje i jakýkoliv údaj, který umožní přímo kontaktovat fyzickou osobu.[5] V případě generických elektronických adres právnických osob se může jednat o zaměstnance, která má k této adrese přístup a pravidelně z ní komunikuje.

Ještě důležitějším hlediskem je však skutečnost, že v praxi obvykle dochází ke společné evidence, společnému zpracování elektronických kontaktů pro účely marketingu, ať už jsou personalizované nebo nikoliv. I kdyby rozesílatel obchodních sdělení cíleně oslovil pouze generické adresy, již samotný proces evidence, vyhledání a třídění v databázi, která obsahuje i e-mailové adresy fyzických osob, představuje zpracování osobních údajů.

Jestliže tedy ÚOOÚ kontroluje splnění podmínek pro rozesílání obchodních sdělení podle zákona č. 480/2004 Sb., nezbytně musí ve velkém počtu případů získat i informace o souvisejícím zpracování daných osobních údajů, elektronických kontaktů, ať už jde o jejich získání, způsob zpracování, způsob zabezpečení, dobu uchování, plnění informační povinnosti vůči subjektům údajů atd.

Z výše uvedeného vyplývá několik poměrně důležitých následků?. Tím pro praxi zřejmě nejhmatatelnějším je skutečnost, že pokud ÚOOÚ při kontrole rozesílání obchodních sdělení zjistí i související porušení GDPR, je z moci úřední povinen jej řešit[6]. A zatímco za porušení pravidel pro šíření obchodních sdělení zákon č. 480/2004 Sb. stanoví maximální sankci ve výši 10 milionů korun, sankce za porušení GDPR se mohou vyšplhat až ke 20 milionů euro či 4 % z ročního obratu skupiny podniků za předchozí rok. Pokud by tedy ÚOOÚ zahájil kontrolu na základě stížností na zasílání nevyžádaných obchodních sdělení a při ní zjistil závažné nedostatky týkající se souvisejícího zpracování osobních údajů, sankce, hranice sankce, kterou by za to mohl uložit, by se významně zvýšila.

Jak je tedy souběžná aplikace zákona č. 480/2004 Sb. a předpisů upravujících zpracování osobních údajů v současné době v praxi řešena?

Správní soudy souběh (zatím) neřešily

České soudy se přímo touto otázkou často nezabývají. Zmínit lze rozsudek Městského soudu v Praze z dubna roku 2020 v kauze, která se týkala primárně odpovědnosti za rozesílání obchodních sdělení při zapojení dalších subjektů[7]. Soud sice v tomto případě aplikoval v době správního řízení účinný zákon č. 101/2000 Sb., nicméně jednalo se o instituty či normy, které v GDPR zůstaly prakticky nezměněné; daný rozsudek je tedy relevantní i pro výklad současné právní úpravy.

Městský soud se však v daném rozsudku, z pohledu naší otázky bohužel, zabývá zejména obecnou odpovědností účastníka řízení. Ten byl správcem osobních údajů využitých k rozesílání obchodních nabídek, proto byl odpovědný i za legalitu jejich rozesílání, ač k němu využil služeb dodavatele. Otázkou souběhu deliktů podle odlišných předpisů se však soud nezabýval.[8]

Trestání za porušení obou regulací v praxi ÚOOÚ

ÚOOÚ na svém webu zveřejňuje výsledky svých kontrol, ať už se týkají zpracování osobních údajů nebo zasílání obchodních sdělení.[9]

V roce 2020 zveřejnil informace o celkem 8 kontrolách týkajících se zasílání nevyžádaných obchodních sdělení. Ve dvou z nich se ÚOOÚ blíže zabýval aplikací pravidel pro zpracování osobních údajů jako takových. V prvé z nich se úřad řešil i nedostatečné informování subjektů údajů o

zpracování jejich dat za účelem marketingu dle čl. 12 a aplikaci práva na námitku podle čl. 21 GDPR. Kontrolovaná osoba však tato porušení odstranila již v průběhu kontroly, proto souběh deliktů řešen nebyl.[10] Ve druhém případě ÚOOÚ při kontrole zaměřené především na obchodní sdělení posuzoval, obdobně jako v předchozím případě, i související plnění informační povinnosti a uplatnění práva na námitku a nad to rovněž uplatnění práva na výmaz podle čl. 17 GDPR. V tomto případě úřad došel k závěru, že kontrolovaný subjekt tyto povinnosti plní v souladu s GDPR.[11] Obdobně při další kontrole uzavřené v roce 2019 konstatoval, že kontrolovaný porušil informační povinnost dle § 11 v době kontroly účinného zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákona, nicméně svoje pochybení v průběhu kontroly napravila.[12]

Prvostupňová rozhodnutí ÚOOÚ ve strukturované formě nezveřejňuje.

Za rok 2020 úřad na svém webu zveřejnil toliko tři druhostupňová rozhodnutí, z nichž žádné se aplikací zákona č. 480/2004 Sb. nezabývá.[13]

Za rok 2019 ÚOOÚ publikoval 26 druhostupňových rozhodnutí předsedkyně úřadu. Z nich 7 bylo vydání v řízení, jehož předmětem byla aplikace zákona č. 480/2004 Sb. Současnou aplikaci tohoto předpisu a úpravy zpracování osobních údajů částečně řeší jen jedno z nich a to pouze ve vztahu k souhlasu se zasíláním obchodních sdělení a jeho hodnocení z pohledu GDPR.[14]

Z dostupných informací o výkladové praxi ÚOOÚ vyplývá, že ÚOOÚ se i při kontrolách zahájených na základě stížnosti na obchodní sdělení zabývá souvisejícím zpracováním osobních údajů a aplikací GDPR. Jednalo se zejména o plnění informační povinnosti o zpracování osobních údajů dotčených osob, uplatnění práva na námitku proti zpracování osobních údajů či práva na výmaz, stejně tak by ovšem ÚOOÚ mohl posuzovat i plnění dalších povinností, pokud by to v konkrétním případě bylo s ohledem na okolnosti důvodné.

Z dostupné rozhodovací praxe však bohužel není zcela jasné, jak se ÚOOÚ staví, resp. jak by uchopil souběžné porušení zákona č. 480/2004 Sb. a GDPR.

Jakou sankci by ÚOOÚ mohl uložit?

Zasílání nevyžádaných obchodní sdělení a protiprávní zpracování osobních údajů, adresátů či potencionálních adresátů obchodních sdělení, lze jistě považovat za porušení povinností vyskytujících se ve stejné oblasti veřejné správy. K projednání obou z nich je příslušný ÚOOÚ. Podle mého soudu jsou tak splněny obě podmínky dle § 88 odst. 1 zákona č. 250/2016 Sb. a ÚOOÚ by v takovémto případě měl dané přestupky automaticky projednat ve společném řízení.[15]

Jestliže by ÚOOÚ dospěl k závěru, že skutečně došlo k porušení jak zákona č. 480/2004 Sb., tak GDPR, horní hranici sazby pokuty by určil podle absorpční zásady, tzn. že by účastníka řízení potrestal podle sazby za nejpřísněji trestný delikt.[16] Jak je výše uvedeno, za zasílání nevyžádaných obchodních sdělení dle současné úpravy hrozí pokuta až 10 milionů korun, za porušení základních pravidel pro zpracování osobních údajů, např. informační povinnosti č postupu při uplatnění práv subjektů údajů pokuta do výše 20 milionů euro nebo 4 % z ročního obratu skupiny podniků. Právě tato částka by v případě společného řízení byla tou, která by ohraničila možnou výši sankce.

Pro úplnost dodejme, že v úvahu by přicházela i tzv. zásada asperační, podle které se v případě společného řízení horní hranice nejpřísnějšího (nejvyššího) trestu zvyšuje a to až o polovinu této sazby, resp. až do výše součtu horních hranic za jednotlivé projednávané delikty.[17] V našem případě by se tak horní hranice pokuty 20 milionů euro zvýšila o 10 milionů korun. Dle názoru autorů se však jedná o v tuto chvíli spíše teoretickou hrozbu, resp. hrozbu za skutečně mimořádně rozsáhlé protiprávní zpracování osobních údajů a související zasílání nevyžádaných obchodních sdělení .

Na obzoru je výrazné zvýšení pokut

Vztah regulace elektronického zasílání obchodních sdělení a pravidel pro zpracování osobních údajů není zcela jednoznačný. Dozor nad oběma oblastmi vykonává ÚOOÚ a organizacím reálně hrozí, že budou postiženy za chyby svého dodavatele, resp. že při kontrole týkající se zasílání obchodních sdělení jim v případě zjištění souvisejícího porušení GDPR uložena výrazně vyšší pokuta. Proto je důležité věnovat náležitou pozornost nejen výběru dodavatele, který bude obchodní sdělení fakticky rozesílat, ale i nastavení smluvního vztahu a procesu spolupráce včetně nezbytných kontrol. Jen dostatečná kontrolní opatření mohou objednatele rozesílky obchodních sdělení případně vyvinit z odpovědnosti za chyby či nedostatky na straně jeho dodavatele.

Pro úplnost dodejme, že na úrovni Evropské unie je již několik let projednáván návrh nařízení o soukromí a elektronických komunikacích, tzv. ePrivacy nařízení, které by mělo nahradit současnou směrnici. Návrh nařízení, které by snad mohlo být schváleno v rámci portugalského předsednictví do června tohoto roku, pravidla pro elektronické zasílání obchodních sdělení ponechává prakticky stejná, jako nyní známe ze zákona č. 480/2004 Sb. Co by se však mělo výrazně změnit, je možná sankce za zasílání nevyžádaných obchodních sdělení. Návrh ePrivacy nařízení totiž počítá se sankcemi až do výše až do výše 10 milionů euro nebo 2 % ročního celosvětového obratu skupiny. Riziko spojené s možným porušením pravidel pro zasílání obchodních sdělení se tak v případě, že ePrivacy nařízení v této podobě bude schváleno, výrazně zvýší.

Mgr. František Nonnemann

Autor je zaměstnancem MallPay s.r.o. a členem Výboru Spolku pro ochranu osobních údajů.

Článek vyjadřuje osobní názor autora.

e-mail: nonnemann@volny.cz

---

[1] Srov. Nonnemann, F. Kdo může dostat pokutu za spam? Publikováno na epravo.cz dne 1. června 2020, k dispozici >>> zde.

[2] Rozsudek Městského soudu v Praze ze dne 7. dubna 2020, č. j. 14 A 242/2018 – 29, k dispozici >>> zde.

[3] Osobními údaji se rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě…; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.

[4] Zpracováním údajů ve smyslu GDPR je jakákoliv operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.

[5] K výkladu pojmu osobní údaj srov. Nulíček, M., Donát, J., Nonnemann, F., Lichnovský, B., Tomíšek, J., Kovaříková, K. GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář. 2. vydání. Praha: Wolters Kluwer ČR, 2018.

[6] Jak vyplývá především ze zásady ochrany veřejného zájmu upravené v § 2 zákona č. 500/2004 Sb., správní řád.

[7] Jedná se o rozsudek Městského soudu v Praze ze dne 7. dubna 2020 č. j. 14 A 242/2018 – 40.

[8] Srov. body 51-54 rozsudku.

[9] K dispozici >>> zde.

[10] Kontrolní závěr k dispozici >>> zde.

[11] Kontrolní závěr k dispozici >>> zde.

[12] Kontrolní závěr k dispozici >>> zde.

[13] K dispozici >>> zde.

[14] K dispozici >>> zde.

[15] Srov. Jemelka, L., Vetešník P. Zákon o odpovědnosti za přestupky a řízení o nich. Zákon o některých přestupcích. Komentář. 2. vydání. Praha: C. H. Beck, 2020. Komentář k § 41.

[16] Srov. § 41 odst. 1 zákona č. 250/2016 Sb.

[17] Srov. § 41 odst. 2 zákona č. 250/2016 Sb.

Další články:

- Právní due diligence nemovitostí: na co se v praxi skutečně zaměřit
- Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie
- Zákon Lugového: jak Rusko přepisuje pravidla mezinárodních arbitráží
- Novelizace nařízení EU o odlesňování (EUDR)
- Prekluze důvodu neplatnosti VH
- Jak zahájit provoz mezinárodní letecké linky do České republiky (EU): právní požadavky pro aerolinky ze třetích zemí
- TOP 5 judikátů z korporátního práva za rok 2025
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- SCHEJBAL& PARTNERS stáli u získání jedné z prvních licencí dle MiCA v ČR
- Proč dnes více než polovina M&A transakcí ve střední Evropě nekončí podpisem