ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

Čj. UOOU-04229/19-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle čl. 58 odst. 2 písm. i) 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 (obecné nařízení o ochraně osobních údajů), vydává dne 5. listopadu 2019 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, tento příkaz:

Je prokázáno, že účastník řízení: Společnost [redacted] se sídlem [redacted], jako správce osobních údajů svých zákazníků podle čl. 4 bodu 7 nařízení (EU) 2016/679,

I. tím, že nezajistil, aby databáze, kterou v souvislosti s žádostí [redacted] a [redacted] vytvořil a dne 14. a 28. března a 11. dubna 2019 předal těmto subjektům, neobsahovala osobní údaje přibližně 40.000 zákazníků odebírajících pouze plyn, a to v rozsahu u fyzických osob jméno, příjmení, datum narození, adresa trvalého bydliště, adresa odběrného místa, a dále u fyzických osob podnikajících osobní údaje v rozsahu jméno, příjmení, příp. obchodní firma, IČ, adresa sídla a adresa odběrného místa,

porušil povinnost stanovenou čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost správce provést vhodná technická a organizační opatření,

II. za což se mu v souladu s čl. 83 odst. 4 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 40.000 Kč
(slovy čtyřicet tisíc korun českých)

splatná do 30 dnů ode dne nabytí právní moci tohoto příkazu bezhotovostním převodem na účet vedený u ČNB, č. ú. 19-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání tohoto příkazu je spisový materiál shromážděný v rámci kontroly sp. zn. UOOU-02949/19-9 provedené Úřadem pro ochranu osobních údajů (dále jen „Úřad“) u účastníka řízení ve dnech ve dnech 6. srpna 2019 až 2. října 2019.

K aplikaci právních předpisů je nezbytné uvést, že dne 24. dubna 2019 nabyl účinnosti zákon č. 110/2019 Sb., o zpracování osobních údajů, který navazuje na přímo použitelný předpis Evropské unie, tj. nařízení (EU) 2016/679. Podle čl. 40 odst. 6 Listiny základních práv a svobod se trestnost činu posuzuje a trest se ukládá podle zákona účinného v době, kdy byl čin spáchán. Pozdějšího zákona se použije, jestliže je to pro pachatele příznivější. Správní orgán posoudil obě právní úpravy a dospěl k závěru, že novější právní úprava obsažená v zákoně č. 110/2019 Sb. není pro účastníka řízení příznivější, proto celou věc posuzoval podle nařízení (EU) 2016/679.

Ze spisového materiálu vyplývá, že účastník řízení v souladu s ustanovením čl. 33 nařízení (EU) 2016/679 ohlásil dne 27. června 2019 Úřadu porušení zabezpečení osobních údajů. K tomu došlo na základě žádosti České televize a Českého rozhlasu podle § 8 odst. 10 zákona č. 348/2005 Sb., o rozhlasových a televizních poplatcích, kdy měl účastník řízení vygenerovat příslušné sestavy obsahující požadovaná data, tedy soupis osobních údajů zákazníků odebírajících elektřinu. U fyzických osob to byly osobní údaje v rozsahu jméno, příjmení, datum narození, adresa trvalého bydliště a adresa odběrného místa. U fyzických osob podnikajících se jednalo o údaje v rozsahu jméno, příjmení, příp. obchodní firma, IČ, adresa sídla a adresa odběrného místa.

Dne 24. června 2019 účastník řízení zaevidoval incident, kdy se na něj obrátila [redacted] s žádostí o potvrzení, že není odběratelem elektřiny. Dále k tomu uvedla, že se na ni obrátil [redacted] s výzvou určenou pro odběratele elektřiny, kteří nejsou poplatníky koncesionářských poplatků. Následnou analýzou účastník řízení zjistil, že do generované databáze obsahující osobní údaje o odběratelích elektřiny byli zařazeni i odběratelé plynu, kteří ale nemají současně smlouvu na dodávku elektřiny. Dále bylo zjištěno, že takovýchto sad s osobními údaji bylo přibližně 40.000. Dle zjištění účastníka řízení k pochybení došlo u zaměstnance, který nesprávně pracoval s databázemi zákazníků odebírajících elektřinu i plyn, přestože zadání na základě žádosti se týkalo pouze zákazníků odebírajících elektřinu. Tato vytvořená databáze byla uložena na CD a zaheslována. Následně došlo k výmazu databáze z úložiště účastníka řízení. Toto CD spolu s hesly bylo dne 14. a 28. března a 11. dubna 2019 předáno přímo žadatelům.

Bezodkladně po zjištění incidentu účastník řízení kontaktoval zástupce [redacted] a [redacted] kdy je požádal o součinnost, výmaz nebo anonymizaci osobních údajů, zastavení procesu upomínání a vymáhání koncesionářských poplatků ve vztahu k neoprávněně předaným osobním údajům. Současně uskutečnil pohovor s odpovědným zaměstnancem a předal mu upozornění na porušení povinností vyplývajících z právních předpisů vztahujících se k zaměstnancem vykonávané práci. Dále bylo provedeno školení zaměstnanců z úseku segmenty a marketing. Protože v době vytvoření databáze neexistovaly interní předpisy upravující jednorázové exporty dat, řídil se zaměstnanec účastníka řízení pouze obecnými předpisy [redacted]),

které ale, jak se později ukázalo, byly nedostatečné. Proto po zjištění incidentu účastník řízení přijal závazná pravidla pro tuto oblast (pokyn ředitele úseku segmenty a marketing), aby se situace neopakovala. Tato nová pravidla obsahovala např. kontrolu čtyř očí a zdokumentování.

K předmětu řízení lze konstatovat, že dle čl. 4 bodu 1 nařízení (EU) 2016/679 se osobním údajem rozumí veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); 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. Informace o odběratelích pouze plynu, které účastník řízení protiprávně zahrnul do vytvářené databáze, jsou nepochybně osobními údaji, neboť na jejich základě je subjekt údajů jednoznačně identifikován a vztahují se k němu. Účastník řízení tak nepochybně zpracovával osobní údaje této skupiny svých zákazníků.

Dle čl. 4 bodu 2 nařízení (EU) 2016/679 se zpracováním rozumí jakákoliv operace nebo soubor operací, které jsou prováděny s osobními údaji nebo soubory osobních údajů 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. Účastník řízení v rámci své podnikatelské činnosti v souvislosti s poskytováním dodávky elektřiny a plynu nepochybně zpracovává osobní údaje zákazníků, neboť je shromažďuje, uchovává a v případě potřeby dále používá (a to včetně jejich zpřístupnění třetím subjektům). Je tedy i správcem údajů svých zákazníků ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své podnikatelské činnosti určil účel a prostředky zpracování.

Jako správce osobních údajů je účastník řízení povinen dodržet veškeré relevantní povinnosti stanovené tímto nařízením pro zpracování osobních údajů. Jedna z těchto povinností je vyjádřena v zásadě integrity a důvěrnosti stanovené v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, která stanoví, že osobní údaje musí být zpracovány způsobem, který zajistí náležité zabezpečení osobních údajů, včetně jejich ochrany pomocí vhodných technických nebo organizačních opatření před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením. Na tuto zásadu pak navazuje čl. 32 odst. 1 nařízení (EU) 2016/679, dle kterého musí správce, popř. zpracovatel s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob provést vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně opatření uvedených pod písm. a) až d) tohoto článku. Z dokumentů, které účastník řízení v rámci kontroly předložil a které upravují ochranu osobních údajů, vyplývá, že v době porušení měl účastník řízení zpracovaná technická a organizační opatření pouze obecně. Pokud se týká opatření, která by zajišťovala přesnost zpracovávaných osobních údajů pro účely vytvoření databáze pro Českou televizi a Český rozhlas, toto účastník řízení upravil až následně po incidentu vydáním pokynu ředitele úseku segmenty a marketing, kterým mj. zavedl několikerou kontrolu obsahu vytvořené databáze (kontrola čtyř očí, zdokumentování). Lze tedy konstatovat, že z důvodu nedostatečně upravených pravidel zpracování došlo k pochybení zaměstnance účastníka řízení, které tím

pádem nemohlo být před předáním databáze podchyceno. K tomuto správní orgán pro úplnost doplňuje, že povinnost zpracovávat osobní údaje může zaměstnanec pouze na pokyn správce, tedy svého zaměstnavatele, viz čl. 29 nařízení (EU) 2016/679. S touto povinností ovšem koresponduje především povinnost správce přijmout opatření k zajištění dodržování tohoto ustanovení podle čl. 32 nařízení (EU) 2016/679, které bylo v daném případě nedostatečné.

Podle čl. 83 odst. 2 nařízení (EU) 2016/679 se při rozhodování o uložení sankce a její výši přihlédne zejména k povaze, závažnosti a délce trvání porušení, k povaze, rozsahu a účelu dotčeného zpracování, k počtu dotčených subjektů údajů a míře škody, která jim byla způsobena a k dalším okolnostem porušení stanoveným v tomto článku.

Při stanovení sankce tak správní orgán přihlédl, jako k okolnosti zvyšující závažnost jednání, zejména k tomu, že se protiprávní jednání týkalo velkého počtu dotčených subjektů. Další přitěžující okolnost správní orgán shledal ve skutečnosti, že se o neoprávněném zpracování dozvěděl účastník řízení až na základě dotazu jednoho dotčeného subjektu. Správní orgán shledal jako polehčující okolnost ojedinělost události, a též následné jednání účastníka řízení s cílem, aby se situace neopakovala. Po souhrnném zhodnocení všech okolností byla pokuta uložena při samé dolní hranici sazby, kterou nařízení (EU) 2016/679 stanoví a která činí 10 000 000 eur.

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním povinnost stanovenou v čl. 32 odst. 1 nařízení (EU) 2016/679, tedy povinnost správce provést vhodná technická a organizační opatření, a proto rozhodl podle § 150 odst. 1 správního řádu ve spojení s § 90 odst. 1 zákona č. 250/2016 Sb. ve věci příkazem.

Poučení: V souladu s § 150 odst. 3 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto příkazu podat ve lhůtě 8 dnů ode dne jeho doručení odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz je doručen dnem převzetí stejnopisu, nejpozději ale desátým dnem od jeho uložení na poště. V případě doručování do datové schránky je dnem doručení okamžik přihlášení oprávněné osoby do datové schránky, nejpozději ale desátý den ode dne dodání příkazu do datové schránky.

Praha 5. listopadu 2019

otisk
úředního
razítka

Mgr. Martina Šnajderová, Dis.
pověřená řízením přestupkové agendy