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-00706/20-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 64 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, a 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 13. února 2020 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád, a § 90 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich, tento příkaz:

[redacted]

I. se uznává vinným ze spáchání přestupku podle § 62 odst. 1 písm. b) zákona č. 110/2019 Sb., neboť porušil některou ze základních zásad pro zpracování osobních údajů podle čl. 5 až 7 nebo 9 nařízení (EU) 2016/679, kterého se, jako správce osobních údajů dlužníků podle čl. 4 bodu 7 nařízení (EU) 2016/679, dopustil tím, že nezajistil, aby z elektronické adresy [redacted] nebyly ve dnech 5. prosince 2018, 12. července 2019, 20. srpna 2019 a 6. září 2019 zaslány neoprávněné osobě na e-mailovou adresu [redacted] finanční reporty obsahující osobní údaje přibližně 2 000 dlužníků, a to v rozsahu jméno, příjmení, rodné číslo, spisová značka exekučního řízení a názvy věřitelů,

čímž porušil povinnost stanovenou čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy povinnost zpracovávat osobní údaje 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 („integrita a důvěrnost“),

II. za což se mu podle § 35 písm. b) zákona č. 250/2016 Sb. a v souladu s čl. 83 odst. 5 nařízení (EU) 2016/679 ukládá

pokuta ve výši 20.000 Kč
(slovy dvacet 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 protokol o kontrole čj. UOOU-03232/19-14 ze dne 9. prosince 2019 pořízený podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád) a spisový materiál shromážděný v rámci kontroly vedené u [redacted], se [redacted] (dále jen „účastník řízení“), ve dnech 26. září 2019 až 9. prosince 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. Dle § 7 zákona č. 250/2016 Sb. se jednáním, jehož jednotlivé dílčí útoky vedené jednotným záměrem naplňující skutkovou podstatu stejného přestupku, jsou spojeny stejným nebo podobným způsobem provedení, blízkou souvislostí časovou a souvislostí v předmětu útoku, rozumí pokračování v přestupku. Vzhledem ke skutečnosti, že během páchání protiprávního jednání účastníka řízení došlo ke změně právní úpravy, musel správní orgán s ohledem na pokračující charakter porušení specifikovaných ve výroku tohoto příkazu posuzovat odpovědnost účastníka řízení za jeho protiprávní jednání dle právní úpravy účinné v době, kdy došlo k poslednímu dílčímu jednání. Je přitom zjevné, že tímto posledním jednáním bylo zaslání e-mailové zprávy dne 6. září 2019. Správní orgán tedy posuzoval jednání účastníka řízení podle zákona č. 110/2019 Sb.

Ze spisového materiálu vyplývá, že kontrola byla zahájena na základě podnětu postoupeného Krajským ředitelstvím policie [redacted], ze dne 16. července 2019, ve věci neoprávněného nakládání s osobními údaji [redacted] který vede [redacted] a dále na základě doplnění tohoto podnětu stěžovatelkou [redacted] doručeném na výzvu Úřadu dne 17. září 2019. Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených nařízením (EU) 2016/679 v souvislosti se zpracováním osobních údajů při výkonu činnosti exekutorského úřadu se zaměřením na dodržování povinností dle čl. 5, 6, 24, 32 a 33 nařízení (EU) 2016/679.

Ze shromážděné dokumentace vyplývá, že zaměstnankyně účastníka řízení [redacted] v rámci své pracovní náplně vypracovávala na žádost některých věřitelů měsíční finanční reporty obsahující jméno a příjmení jejich dlužníků, rodná čísla těchto osob, a další údaje důležité pro výkon rozhodnutí, včetně názvu věřitele. Předmětné reporty pracovnice exekutorského úřadu [redacted] následně zasílala z elektronické adresy [redacted] určeným věřitelům na základě jejich požadavku kontroly plateb dlužníků. [redacted] takto vypracovávala též měsíční finanční reporty určené pro společnost [redacted], které následně zasílala na e-mailovou adresu společnosti [redacted], k rukám paní [redacted] Z důvodu pochybení zaměstnankyně [redacted] nicméně opakovaně došlo k odeslání těchto reportů namísto na e-mailovou adresu paní [redacted] ze společnosti [redacted] na e-mailovou adresu stěžovatelky

[redacted]. Přestože stěžovatelka zaslala [redacted] dne 12. července 2019 e-mailovou zprávu, ve které zaměstnankyni exekutorského úřadu upozornila, že odesílá předmětné dokumenty na nesprávnou e-mailovou adresu, obdržela následně další 2 reporty. Celkem zaslala [redacted] neoprávněné osobě 4 finanční reporty určené společnosti [redacted] a to report za měsíc listopad 2018 (který stěžovatelka obdržela dne 5. prosince 2018), finanční report za měsíc červen 2019 (který stěžovatelka obdržela dne 12. července 2019), finanční report za měsíc červenec 2019 (který stěžovatelka obdržela dne 20. srpna 2019) a dále finanční report za měsíc srpen 2019 (který stěžovatelka obdržela dne 6. září 2019). Měsíční finanční reporty obsahovaly v měsíci listopadu 2018 celkem 16 stran, v měsíci červnu 2019 celkem 18 stran, v měsíci červenci 2019 celkem 18 stran a v měsíci srpnu 2019 celkem 18 stran. Jedna stránka reportu má 57 řádků, jednotlivý řádek obsahuje jméno a příjmení dlužníka, jeho rodné číslo, a další údaje důležité pro výkon rozhodnutí, včetně názvu věřitele. Některé subjekty údajů se na jednotlivých stránkách i v jednotlivých reportech opakují, nicméně i tak se jedná o závažný únik většího množství osobních údajů cca 2 000 subjektů.

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; 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. Ze shromážděné dokumentace vyplývá, že účastník řízení v rámci své činnosti (činnost exekutorského úřadu) nakládá s osobními údaji dlužníků, a to minimálně v rozsahu jméno, příjmení, datum narození, rodné číslo, adresa bydliště, místo trvalého pobytu, telefonní číslo, elektronická adresa, číslo bankovního účtu, údaje o majetku, tj. nemovitých a movitých věcech a údaje o příjmech a spořeních. Tyto informace, které účastník řízení zpracovává, jsou nepochybně osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, neboť se jedná o informace o identifikovaných osobách.

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 činnosti exekutorského úřadu nepochybně zpracovává osobní údaje dotčených dlužníků, neboť je shromažďuje, uchovává a v případě potřeby dále používá. Současně je tedy v této souvislosti i správcem údajů výše uvedených subjektů ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své činnosti určil účel (nucený výkon exekučních titulů a další činnost podle zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti), i prostředky zpracování.

Zpracování osobních údajů musí být vždy v souladu se základními zásadami, které jsou zakotveny v čl. 5 nařízení (EU) 2016/679. Tyto zásady představují základní pravidla, od nichž se odvíjejí všechny procesy zpracování, a zároveň jsou též nejdůležitějšími principy, které správci určují, jak má s osobními údaji nakládat. Jednou z těchto zásad je zásada integrity a důvěrnosti stanovená v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, podle kterého musí být osobní údaje zpracovávány 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.

Výše uvedená zásada integrity a důvěrnosti je pak podrobněji specifikována v dalších ustanoveních nařízení (EU) 2016/679, zejména v čl. 32 tohoto nařízení, kde jsou stanoveny konkrétní požadavky na zabezpečení osobních údajů. Dle čl. 32 odst. 1 nařízení (EU) 2016/679 správce, popř. zpracovatel musí 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 zajistil úroveň zabezpečení odpovídající danému riziku, případně včetně opatření uvedených pod písm. a) až d) tohoto článku.

Je tedy zřejmé, že správce musí nejprve posoudit pravděpodobnost a závažnost rizik, která při zpracování osobních údajů hrozí, a následně s přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování vybrat a následně zavést vhodná technická a organizační bezpečnostní opatření ke zmírnění těchto rizik. Riziko pro práva a svobody fyzických osob přitom lze považovat za kritérium, na němž závisí uplatnění nebo míra uplatnění řady institutů upravených v nařízení (EU) 2016/679. 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. Pro posouzení bezpečnostních rizik a volbu vhodných opatření k jejich zmírnění platí stejné zásady jako pro posuzování obecného rizika zpracování. Posouzení by nemělo být jednorázovým procesem, nýbrž by se mělo jednat o pravidelný proces vyhodnocování vnitřních a vnějších okolností, které mohou mít na míru rizika vliv, a v případě změny rizika pak musí správce bezpečnostní opatření zrevidovat a případně přijmout vhodnější.

Lze tedy shrnout, že splnění této povinnosti, tj. povinnosti provést vhodná technická a organizační opatření, aby byla zajištěna úroveň zabezpečení odpovídající danému riziku, aby osobní údaje nebyly vystaveny riziku neoprávněného zpracování či využití, předpokládá, že účastník řízení důsledně zváží veškerá rizika, která jsou s jím prováděným zpracováním osobních údajů spojená, a přijme odpovídající opatření k jejich maximálnímu vyloučení.

Z výše uvedeného je zřejmé, že účastník řízení nedodržel základní zásadu integrity a důvěrnosti stanovenou v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, když ze strany jeho zaměstnankyně [redacted], která nejspíš neučinila kontrolu zadané e-mailové adresy věřitele, byly opakovaně zaslány finanční reporty obsahující osobní údaje dlužníků neoprávněné osobě, a to i přesto, že pracovnice exekutorského úřadu byla upozorněna na chybu v osobě adresáta.

Podle § 5 zákona č. 250/2016 Sb. je přestupkem škodlivý protiprávní čin, který je v zákoně za přestupek výslovně označen a který vykazuje znaky stanovené zákonem, nejde-li o trestný čin.

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 správního trestu tak správní orgán přihlédl jako k okolnosti zvyšující závažnost jednání zejména k tomu, že jednáním účastníka řízení byla porušena základní zásada, která představuje základní principy, na jejichž řádném dodržování spočívá každé zpracování osobních údajů. Přitěžující okolností je též samotný charakter dotčených osobních údajů, který představuje vyšší riziko pro práva a svobody subjektů těchto údajů, neboť reporty obsahovaly i rodná čísla, která slouží jako obecný identifikátor občanů. Správní orgán shledal jako přitěžující okolnost rovněž fakt, že porušení zabezpečení trvalo delší dobu a docházelo k němu i po upozornění stěžovatelky, že předmětné reporty jsou zasílány na nesprávnou e-mailovou adresu. Přitěžující okolností je též skutečnost, že jednáním účastníka řízení byl dotčen vysoký počet subjektů údajů (cca 2 000 osob). Dále však správní orgán při rozhodování o uložení sankce a její výši, jako k okolnosti snižující závažnost jednání, přihlédl k tomu, že předmětné osobní údaje byly, ač opakovaně, zaslány pouze jedné neoprávněné osobě, a tedy riziko jejich zneužití nebylo pravděpodobné. Správní orgán shledal jako polehčující okolnost rovněž skutečnost, že účastník řízení během kontroly spolupracoval a učinil kroky k nápravě protiprávního stavu. Po souhrnném zhodnocení všech okolností byla pokuta uložena při samé dolní hranici sazby, kterou nařízení (EU) 2016/679 stanoví a která činí 20 000 000 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. 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy povinnost zpracovávat osobní údaje 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 („integrita a důvěrnost“), 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, 13. února 2020

otisk
úředního
razítka

Mgr. Lucie Lakatošová
pověřená řízením přestupkové agendy
(podepsáno elektronicky)