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-09571/18-14

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, jako věcně příslušný orgán podle § 46 odst. 1 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a 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) v řízení o porušení povinností podle nařízení (EU) 2016/679, vedeném podle zákona č. 500/2004 Sb., správní řád, rozhodl dne 4. února 2019 takto:

I. Je prokázáno, že společnost , se sídlem , IČO: jako správce osobních údajů svých klientů při zprostředkování úvěru, tím, že nezajistila osobní údaje cca 300 klientů v rozsahu jméno, příjmení, rodné číslo, číslo občanského průkazu, adresa bydliště, telefonní číslo a informace o úvěru, které byly obsaženy ve smlouvách o spotřebitelském úvěru, které byly volně uloženy v papírové krabici v prostorách společných garáží bytového domu v po dobu minimálně 14 dnů a následně nalezeny dne 23. srpna 2018 v kontejneru u v ,

porušila základní zásadu zpracování osobních údajů stanovenou čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být 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,

II. za což se jí podle čl. 83 odst. 5 písm. a) nařízení (EU) 2016/679 ukládá

pokuta ve výši 30.000 Kč
(slovy třicet tisíc korun českých)

III. a dále podle § 79 odst. 5 správního řádu povinnost nahradit **náklady řízení ve výši 1.000 Kč**,

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

Odůvodnění

Řízení ve věci podezření z porušení povinnosti stanovené v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679 v souvislosti se zabezpečením osobních údajů klientů bylo zahájeno oznámením Úřadu pro ochranu osobních údajů (dále jen „Úřad“), které bylo účastníkovi řízení, společnosti , doručeno dne 11. prosince 2018. Podkladem pro zahájení řízení byl spisový materiál Krajského ředitelství policie , obvodní oddělení , čj. postoupený správnímu orgánu dne 19. října 2018.

Ze spisového materiálu vyplývá, že účastník řízení uzavíral v rámci výkonu své činnosti, zprostředkování úvěrů, smlouvy o spotřebitelských úvěrech na svých pobočkách prostřednictvím svých zprostředkovatelů. Kopie smluv uzavřených na pobočkách v a v přivezla jednatelka účastníka řízení, paní v blíže neurčený den (dle podání vysvětlení na Policii České republiky ze dne 24. srpna 2018 asi tři týdny nebo 14 dny před podáním vysvětlení) k sobě domů v úmyslu, že je převeze do skladu v Smlouvy byly uloženy v papírové krabici, u osobního automobilu jednatelky, v . Do prostoru garáží mají volný přístup všichni obyvatelé domu. Jednatelka nechtěla z důvodu manipulovat s krabicí. Dne 23. srpna 2018 byla v kontejneru u točny autobusu nalezena krabice obsahující výše uvedené kopie smluv uzavřené s 308 žadateli o úvěr. Předmětné smlouvy obsahovaly osobní údaje v rozsahu jméno, příjmení, rodné číslo, číslo občanského průkazu, adresa bydliště, telefonní číslo a informace o úvěru.

Ze spisového materiálu dále vyplývá, že Úřadu bylo dne 28. srpna 2018 doručeno ohlášení porušení zabezpečení osobních údajů zaslané účastníkem řízení. Z oznámení porušení, kromě popisu skutečností zjištěných Policií České republiky, vyplývá, že kopie smluv byly pořízeny pro případ, že by některý z věřitelů smlouvu postrádal. Krabice se smlouvami se měla nacházet v rohu garáží jednatelky a měla obsahovat cca 80 kusů smluv uzavřených převážně v roce 2017. Po zjištění nálezu smluv od Policie České republiky provedla jednatelka společnosti kontrolu, zda se v okolí popelnic, kde k nálezu smluv došlo, nenachází žádné další smlouvy. Účastník řízení dále uvedl, že v současné době odpadla povinnost pořizovat kopie smluv, které by musela shromažďovat, tudíž se uvedená událost již nemůže opakovat.

Dne 21. prosince 2018 bylo správnímu orgánu doručeno vyjádření účastníka řízení k předmětu řízení, ve kterém doplnil informace poskytnuté Policii České republiky a v oznámení porušení. Od 1. března 2018 při zprostředkování úvěru obdrží klient jeden výtisk smlouvy a druhý výtisk je odeslán poskytovateli úvěru v předepsaném termínu.

Všechny dokumenty, které účastník řízení shromáždil do 1. března 2018, byly neprodleně skartovány. Závěrem účastník řízení uvedl, že je malou společností se zaměstnanci s malým zdanitelným ziskem, což doložil daňovým přiznáním za rok 2016 a 2017.

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, které zpracovává účastník řízení o fyzických osobách, tedy jméno, příjmení, rodné číslo, číslo občanského průkazu, adresa bydliště, telefonní číslo a informace o úvěru, jsou osobními údajů 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 shromažďuje osobní údaje zájemců o úvěr pro účely uzavření smlouvy o úvěru, používá tyto údaje, uchovává kopie smluv s osobními údaji atd.; provádí tedy zpracování osobních údajů.

Dle čl. 4 bodu 7 nařízení (EU) 2016/679 se správcem rozumí fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů; jsou-li účely a prostředky tohoto zpracování určeny právem Unie či členského státu, může toto právo určit dotčeného správce nebo zvláštní kritéria pro jeho určení. Dle těchto kritérií je účastník řízení v postavení správce osobních údajů, protože určil účel (zprostředkování finančních služeb) a prostředky (dokumenty v listinné formě vedené za účelem evidence klientů, kterým byl poskytnut spotřebitelský úvěr) předmětného zpracování osobních údajů.

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 údajů nakládat. Jednou z těchto zásad je zásada integrity a důvěrnosti stanovená 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.

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 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 zajistili 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.

Správní orgán musí konstatovat, že v daném případě nebyly osobní údaje klientů účastníkem řízení zpracovávány způsobem, který by zajistil jejich náležité zabezpečení. Účastník řízení nedostatečně vyhodnotil rizika pro práva a svobody svých klientů, a tedy ani nepřijal odpovídající bezpečnostní opatření k jejich ochraně před neoprávněným či protiprávním zpracováním a před náhodnou ztrátou, zničením nebo poškozením, když ponechal krabici s dokumenty pocházejících z jeho činnosti obsahující osobní údaje klientů při zprostředkování úvěru volně uloženou v prostorách společných garáží bytového domu, přestože mu muselo být více než zřejmé, že k nim může mít přístup kdokoli z obyvatel daného domu, který s nimi mohl libovolně disponovat. To potvrzuje i skutečnost, že krabice s dokumenty byla následně nalezena v kontejneru u , kam ji odnesla neznámá osoba. Účastník řízení, jak vyplývá z podání vysvětlení jeho jednatelky, přitom ztratil nad listinami i osobními údaji dispozici minimálně po dobu 2 týdnů, než byly následně nalezeny na veřejném prostranství.

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním zásadu stanovenou v čl. 5 odst. 1 písm. f) nařízení (EU) 2016/679, tedy zásadu, že osobní údaje musí být 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.

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 výše sankce bylo přihlédnuto jako k okolnosti zvyšující závažnost jednání účastníka řízení k tomu, že osobní údaje se týkaly většího počtu subjektů údajů a dále ke skutečnosti, že nalezené listiny obsahovaly také rodná čísla, která slouží jako obecný identifikátor občanů. Při stanovení sankce správní orgán přihlédl, jako k okolnosti přitěžující, že účastník řízení v rámci ohlášení porušení zabezpečení uvedl hrubě zavádějící informaci týkající se počtu odcizených dokumentů s osobními údaji (účastník řízení ohlásil ztrátu přibližně 80 smluv, ale ve skutečnosti odcizená krabice obsahovala smluvní dokumentaci více jak 300 klientů). Jako ke skutečnosti snižující závažnost jednání účastníka řízení správní orgán přihlédl k tomu, že ze strany účastníka řízení byla přijata od 1. března 2018 opatření k zamezení opětovného porušení zákonem uložené povinnosti,

Správní orgán při stanovení výměry sankce přihlédl též k majetkovým poměrům účastníka řízení, které účastník řízení doložil prostřednictvím svých daňových přiznání za roky 2016 a 2017.

Po zhodnocení uvedených okolností případu a s ohledem na skutečnost, že sankce má být uložena v takové výši, aby pro delikventa znamenala dostatečnou újmu – ať už na majetku, či na jiných hodnotách, avšak přitom nesmí mít tzv. likvidační charakter (viz nález pléna Ústavního soudu sp. zn. Pl. ÚS 3/02 ze dne 13. srpna 2002), uložil správní orgán sankci při samé dolní hranici stanovené sazby, která činí 20 miliónů eur.

Podle § 156 odst. 1 zákona č. 280/2009 Sb., daňový řád, může účastník řízení požádat ve lhůtě pro zaplacení uložené pokuty (30 dnů od právní moci tohoto rozhodnutí) Úřad pro ochranu osobních údajů, jakožto příslušného správce daně podle § 10 odst. 2 zákona č. 280/2009 Sb., o povolení rozložení její úhrady na splátky, pokud mu svědčí některý z důvodů uvedených v § 156 odst. 1 písm. a) až e) zákona č. 280/2009 Sb.

S ohledem na výše uvedené, bylo rozhodnuto, jak je uvedeno ve výroku tohoto rozhodnutí.

Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z § 79 odst. 5 správního řádu, který správnímu orgánu ukládá uložit účastníkovi řízení, který řízení vyvolal porušením své povinnosti, náklady řízení paušální částkou, a z § 6 odst. 1 vyhlášky č. 520/2005 Sb., o rozsahu hotových výdajů a ušlého výdělku, které správní orgán hradí jiným osobám, a o výši paušální částky nákladů řízení, podle kterého paušální částka nákladů správního řízení, které účastník vyvolal porušením své právní povinnosti, činí 1.000 Kč.

Poučení: V souladu s § 152 odst. 1 správního řádu lze u Úřadu pro ochranu osobních údajů proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedkyni Úřadu pro ochranu osobních údajů.

Rozhodnutí je doručeno 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 rozhodnutí do datové schránky.

Praha, 4. února 2019

otisk
úředního
razítka

Mgr. Vanda Foldová
ředitelka odboru kontrolního