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

Čj. UOOU-01129/22-14

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 64 odst. 1 zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále jen „zákon č. 110/2019 Sb.“) 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) [dále jen „nařízení (EU) 2016/679“], rozhodl dne 9. února 2024 v souladu s § 150 odst. 1 zákona č. 500/2004 Sb., správní řád (dále jen „zákon č. 500/2004 Sb.“), a § 90 odst. 1 zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich (dále jen „zákon č. 250/2016 Sb.“), takto:

[redacted] jako správce osobních údajů podle čl. 4 bodu 7 nařízení (EU) 2016/679 (dále jen „obviněná“),

I. je vinna, že nepřijala dostatečná opatření k zabezpečení osobních údajů, v důsledku čehož dne 10. března 2022 došlo k předání emailových adres [redacted] a [redacted], tedy osobních údajů třetích osob, spolu s osobními údaji zákazníka obviněné [redacted], následkem čehož došlo i ke zpřístupnění osobních údajů [redacted] (jméno, příjmení, telefonní číslo, e-mailová adresa a adresa bydliště) majitelům těchto dvou e-mailových adres,

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

a tím spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.,

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

pokuta ve výši 21.000 Kč
(slovy dvacet jedna 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 obviněné, konstantní symbol 1148.

Odůvodnění

[1] Podkladem pro vydání tohoto příkazu je stížnost ze dne 17. března 2022 doručená Úřadu pro ochranu osobních údajů (dále jen „Úřad“) a spisový materiál čj. UOOU-01129/22 shromážděný v rámci prověření podané stížnosti.

[2] Dne 17. března 2022 byla Úřadu doručena stížnost, ve které stěžovatel [redacted] (dále jen „stěžovatel“) popsal, že v souvislosti s nesprávně vyřízenou reklamací u obviněné došlo k vymáhání peněz za zboží, které mu bylo zasláno navíc. Jeho osobní údaje obviněná dne [redacted] předala [redacted] (dále jen „společnost [redacted], která dne [redacted] zaslala e-mailovou zprávu týkající se vymáhané pohledávky na e-mailovou adresu stěžovatele, a to včetně faktury (obsahující jméno, příjmení, e-mailovou adresu a telefonní kontakt stěžovatele), na další dvě e-mailové adresy [redacted] a [redacted], které nenáleží stěžovateli (stěžovatel v rámci podané stížnosti uvedl, že se jedná o e-mailovou adresu cizích lidí).

[3] Dne 12. července 2022 zaslal Úřad obviněné výzvu označenou jako „Upozornění správci osobních údajů na možné porušení obecného nařízení o ochraně osobních údajů“. Ve vyjádření ze dne 3. srpna 2022 obviněná uvedla, že k předání e-mailových adres [redacted] z její strany došlo. Obviněná uvedla, že pokud nedovede vymoct dlužnou částku sama, obrací se na [redacted], která jí asistuje s vymáháním pohledávek. Obviněná stěžovatele eviduje jako registrovaného zákazníka pod číslem [redacted] s e-mailovou adresou [redacted] a s telefonním číslem [redacted]. Obviněná uvedla, že aby zvýšila šanci na vymožení pohledávky, vždy se snaží najít k zákazníkům více kontaktů, tj. kontroluje ve svém interním systému, zda k příslušné e-mailové adrese nebo telefonnímu číslu zákazníka neeviduje ještě další kontaktní údaje, protože je běžné, že zákazník nakupuje z více než jedné e-mailové adresy, popř. u zákazníka může evidovat různá telefonní čísla. U telefonního čísla stěžovatele byly evidovány další dvě registrace, a to pod číslem [redacted] e-mailová adresa [redacted] a u čísla [redacted] e-mailová adresa [redacted], proto tyto kontaktní údaje byly též předány [redacted] jako možné kontaktní údaje. Z náhledu do interního systému obviněné je zřejmé, že všechny výše uvedené tři e-mailové adresy jsou evidovány ke shodnému telefonnímu číslu (tj. číslu [redacted]. K tomu obviněná dále uvedla, že e-mailová adresa [redacted] zřejmě patří příbuznému stěžovatele (pozn. správního orgánu: z náhledu do interního systému je zřejmé, že k tomuto e-mailu je evidována [redacted], a to na shodné adrese s [redacted]. V případě e-mailové adresy [redacted] došlo k pochybení zaměstnance, který tento údaj nevyhodnotil jako nesouvisející se stěžovatelem, když patřil [redacted] (pozn. správního orgánu: tj. zcela odlišné osobě). V souvislosti s tímto pochybením se obviněná rozhodla aktualizovat pokyny vůči zaměstnancům, aby bylo pro ně srozumitelnější, které údaje lze předat v rámci vymáhání pohledávek, a zároveň poučila příslušného zaměstnance a upozornila jej na případné následky, pokud by se pochybení mělo opakovat. Závěrem obviněná uvedla, že se nejednalo o hromadnou e-mailovou zprávu a že adresátem byla jen jedna osoba,

která ale měla více e-mailových adres. K tomu doplnila, že pro rozesílání hromadných e-mailových zpráv má obviněná zavedena pravidla postupu, kdy jsou zaměstnanci povinni použít funkci e-mailového klienta „skrytá kopie“ nebo nástroj „mail merge“.

[4] Z vyjádření obviněné ze dne 13. března 2023 vyplývá, že údaje stěžovatele byly [redacted] předány prostřednictvím systému [redacted] dne [redacted]

[5] 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 zpracovávala obviněná o zákaznících, kdy se jednalo o údaje v rozsahu jméno, příjmení, telefonní číslo, adresa bydliště a e-mailová adresa, jsou osobními údaji ve smyslu čl. 4 bod 1 nařízení (EU) 2016/679, neboť se jedná o informace o identifikovaných osobách.

[6] 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. Obviněná v rámci své činnosti uchovává osobní údaje svých registrovaných zákazníků, které využívá v procesu objednávky a dodání zboží, ale dále např. i pro účely vymožení pohledávky, čímž nepochybně zpracovává jejich osobní údaje, neboť je shromažďuje, uchovává a v případě potřeby dále používá. Je tedy i správcem údajů svých zákazníků ve smyslu čl. 4 bodu 7 nařízení (EU) 2016/679, neboť v rámci své podnikatelské činnosti určila účel a prostředky zpracování.

[7] K výroku I. tohoto příkazu správní orgán uvádí, že podle čl. 32 odst. 1 nařízení (EU) 2016/679, má správce povinnost s přihlédnutím ke stavu techniky, nákladů 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.

[8] Obviněná v rámci vedení zákaznického účtu zpracovávala (uchovávala a dále používala) základní osobní údaje svého zákazníka. Když nastala situace, kdy u tohoto zákazníka evidovala pohledávku, kterou se ji nepodařilo vymoct, pokračovala dle své zavedené praxe a pohledávku k vymožení předala spolupracující [redacted] Než došlo k předání osobních údajů, které u zákazníka měla uložené, pokusila se ve své databázi najít další kontaktní údaje, které měly též patřit danému zákazníkovi. Nicméně si takto zjištěné údaje nijak dále neověřila a rovnou je přiřadila k danému zákazníkovi. Takto se stalo i u stěžovatele, kdy k jeho osobním údajům připojila i další dvě e-mailové adresy, které mu ale nepatřily, týkaly se dalších dvou osob, jiných zákazníků. Ze skutkových zjištění je tedy zřejmé, že obviněná neměla zaveden jakýkoliv způsob ověření při přiřazování e-mailových adres (nebo jiných kontaktních údajů) k zákazníkům, jejichž údaje předávala k vymožení dluhu. Právě z tohoto důvodu došlo k automatickému přiřazení dvou e-mailových adres k údajům zákazníka pouze

na základě shodného telefonního čísla, aniž by příslušný zaměstnanec ověřil, zda e-mailové adresy, které z databáze zjistil, patří skutečně [redacted], nebo jiným zákazníkům. V důsledku nedostatečného technického či organizačního nastavení interních procesů následně došlo ke zpřístupnění osobních údajů stěžovatele třetím osobám.

[9] Vzhledem k tomu, že obviněná nedostála své povinnosti přijmout dostatečná technická a organizační bezpečnostní opatření, považuje správní orgán za prokázané, že obviněná porušila svým jednáním čl. 32 odst. 1 nařízení (EU) 2016/679, a tím spáchala přestupek podle § 62 odst. 1 písm. a) zákona č. 110/2019 Sb.

[10] 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 § 62 odst. 1 písm. a) zákona č. 110/2019 Sb. správce nebo zpracovatel se dopustí přestupku tím, že poruší některou z povinností podle čl. 8, 11, 25 až 39, 42 až 49 nařízení (EU) 2016/679.

[11] Podle čl. 83 odst. 1 nařízení (EU) 2016/679 dozorový úřad zajistí, aby ukládání správních pokut v souladu s tímto článkem ohledně porušení tohoto nařízení podle odstavců 4, 5 a 6 bylo v každém jednotlivém případě účinné, přiměřené a odrazující; podle čl. 83 odst. 2 nařízení (EU) 2016/679 při rozhodování o výši správní pokuty v jednotlivých případech řádně zohlední tyto okolnosti:

a) povaha, závažnost a délka trvání porušení s přihlédnutím k povaze, rozsahu či účelu dotčeného zpracování, jakož i k počtu dotčených subjektů údajů a míře škody, jež jim byla způsobena;

b) zda k porušení došlo úmyslně nebo z nedbalosti;

c) kroky podniknuté správcem či zpracovatelem ke zmírnění škod způsobených subjektům údajů;

d) míra odpovědnosti správce či zpracovatele s přihlédnutím k technickým a organizačním opatřením jimi zavedeným podle článků 25 a 32;

e) veškerá relevantní předchozí porušení správcem či zpracovatelem;

f) míra spolupráce s dozorovým úřadem za účelem nápravy daného porušení a zmírnění jeho možných nežádoucích účinků;

g) kategorie osobních údajů dotčené daným porušením;

h) způsob, jakým se dozorový úřad dozvěděl o porušení, zejména zda správce či zpracovatel porušení oznámil, a pokud ano, v jaké míře;

i) v případě, že vůči danému správci nebo zpracovateli byla v souvislosti s týmž předmětem dříve nařízena opatření uvedená v čl. 58 odst. 2, splnění těchto opatření;

j) dodržování schválených kodexů chování podle článku 40 nebo schváleného mechanismu pro vydávání osvědčení podle článku 42 a

k) jakoukoliv jinou přitěžující nebo polehčující okolnost vztahující se na okolnosti daného případu, jako jsou získaný finanční prospěch či zamezení ztrátám, přímo či nepřímo vyplývající z porušení.

[12] Za porušení povinnosti správce podle článků 8, 11, 25 až 39, 42 a 43 nařízení (EU) 2016/679 lze podle čl. 83 odst. 4 nařízení (EU) 2016/679 uložit správní pokutu až do výše 10.000.000 EUR, jedná-li se o podnik, až do výše 2 % z celkového ročního obratu celosvětově

za předchozí finanční rok, podle toho, která hodnota je vyšší. Dle obchodního rejstříku měla obviněná v roce 2022 čistý obrat ve výši [redacted] Kč. Částka odpovídající 2 % z čistého obratu činí [redacted] Kč, tedy při kursu EUR a CZK ve výši 24,74 celkem (ke dni 26. ledna 2024) [redacted] EUR (> 10.000.000 EUR). Pro stanovení pokuty bylo proto nutné vycházet z maximální možné výše představované částkou [redacted] Kč.

[13] Při stanovení druhu správního trestu Úřad přihlédl předně k povaze a závažnosti přestupku dané významem zákonem chráněného zájmu, který byl přestupkem porušen či ohrožen, podle § 38 písm. a) zákona 250/2016 Sb. Zákonem chráněný zájem v této souvislosti je v širším smyslu právo na soukromí zaručené mimo jiné v čl. 7 odst. 1 či v čl. 10 odst. 3 Listiny základních práv a svobod. S ohledem na tuto skutečnost nebylo možné uvažovat o jiném druhu správního trestu než o pokutě.

[14] Při výpočtu pokuty vycházel Úřad z dokumentu Pokyny o výpočtu správních pokut podle obecného nařízení o ochraně osobních údajů vydaného Evropským sborem pro ochranu údajů (dále jen „Pokyny“).

[15] Pokud jde o zhodnocení závažnosti přestupku uvedeného ve výroku I. tohoto příkazu, pro účely stanovení základu pro výpočet pokuty, tento přestupek při zohlednění jeho individuální závažnosti včetně konkrétních okolností, za nichž byl spáchán, Úřad hodnotí jako méně závažný. Podle Pokynů se tak základ pro výpočet pokuty bude pohybovat mezi 0 až 10 % maximální možné výše představované částkou [redacted] Kč. Z důvodu nižší závažnosti, kdy se jednalo pouze o jeden subjekt údajů, byl zpracováván spíše malý rozsah osobních údajů a součástí osobních údajů nebyly žádné údaje patřící do zvláštní kategorie osobních údajů podle čl. 9 odst. 1 nařízení (EU) 2016/679. Úřad stanovil základ pro výpočet pokuty v dolní polovině výše uvedeného rozpětí, konkrétně ve výši [redacted] Kč, která představuje [redacted] % z maximální výše pokuty, tedy z [redacted] Kč. Tuto částku lze dále snížit podle toho, jaký má obviněná čistý roční obrat. Vzhledem k tomu, že čistý obrat obviněné činil v posledním zúčtovacím období [redacted] Kč, jedná se dle Pokynů o společnost poslední kategorie s obratem větším než 500.000.000 EUR, u které lze dále nekrátit základ pro výpočet pokuty, nicméně vzhledem k nízké závažnosti Úřad přistoupil k dalšímu krácení, a to na 50 % a určil tedy základ pro výpočet pokuty ve výši [redacted] Kč.

[16] Při rozhodování o výši pokuty dále Úřad hodnotil skutečnost, že obviněná s Úřadem spolupracovala, přijala opatření, která mají podobným incidentům v budoucnu zabránit, a v daném případě nedošlo ke vzniku škody. K těmto skutečnostem Úřad přihlédl jako k polehčujícím okolnostem ve smyslu § 39 zákona č. 250/2016 Sb., což promítl do výše pokuty tak, že výchozí částku pro výpočet pokuty snížil o 50 %, tedy na 21.152 Kč.

[17] S ohledem na výše uvedené vyhodnocení závažnosti přestupku byla stanovena Úřadem obviněné pokuta ve výši 21.152 Kč, přičemž výsledná částka byla zaokrouhlena na celé tisíce dolů, tj. na 21.000 Kč, a v této výši Úřad pokutu ukládá.

Poučení

V souladu s § 150 odst. 3 zákona č. 500/2004 Sb. 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, 9. února 2024

Mgr. Josef Mička
ředitel odboru dozoru
(podepsáno elektronicky)