Čj. UOOU-11264/15-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 10 zákona č. 500/2004 Sb., správní řád, a § 2 odst. 2 a § 46 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, vydává dne 2. listopadu 2015 v souladu s § 150 odst. 1 správního řádu tento příkaz:

Je prokázáno, že účastník řízení: společnost CreditPortal, a.s., se sídlem Argentinská 286/38, 170 00 Praha 7, IČ: 03240207, v souvislosti se zpracováním osobních údajů svých klientů při poskytování nebo zprostředkování spotřebitelského úvěru, jako správce osobních údajů klientů podle § 4 písm. j) zákona č. 101/2000 Sb., tím, že odeslal dne 13. ledna 2015 ve 3:09 hodin z e-mailové adresy kontakt@creditportal.cz e-mailovou zprávu, která měla v záhlaví uveden předmět „Návrh splátkového kalendáře“ a obsahovala osobní údaje jeho klientů …, … a … v rozsahu jméno, příjmení, adresa trvalého pobytu (PSČ, obec/město, ulice, číslo popisné), rodné číslo, číslo občanského průkazu, e-mailová adresa, číslo telefonu, bankovní účet, hlavní zdroj příjmu, jméno zaměstnavatele, výše příjmu, přeplatek, datum vytvoření registrace, počet půjček, výše dluhu a aktuální dlužná částka, a to celkem 87 neoprávněným adresátům,

porušil povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů,

a tím spáchal správní delikt podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., neboť nepřijal nebo neprovedl opatření pro zajištění bezpečnosti zpracování osobních údajů, za což se mu v souladu s § 45 odst. 3 zákona č. 101/2000 Sb. ukládá

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

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 IČ účastníka řízení, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání tohoto příkazu je spisový materiál shromážděný v rámci kontroly provedené u společnosti CreditPortal, a.s., inspektorem Úřadu pro ochranu osobních údajů (dále jen „Úřad“) MVDr. Františkem Bartošem ve dnech 9. března až 23. dubna 2015, a to včetně kontrolního protokolu čj. UOOU-00548/15-7 ze dne 22. července 2015 a vyřízení námitek předsedou Úřadu čj. UOOU-00548/15-10 ze dne 31. srpna 2015.

Ze spisového materiálu vyplývá, že účastník řízení odeslal dne 13. ledna 2015 ve 3:09 hodin z e-mailové adresy kontakt@creditportal.cz e-mailovou zprávu, která měla v záhlaví uveden předmět „Návrh splátkového kalendáře“ a obsahovala osobní údaje jeho klientů …, … a … v rozsahu jméno, příjmení, adresa trvalého pobytu (PSČ, obec/město, ulice, číslo popisné), rodné číslo, číslo občanského průkazu, e-mailová adresa, číslo telefonu, bankovní účet, hlavní zdroj příjmu, jméno zaměstnavatele, výše příjmu, přeplatek, datum vytvoření registrace, počet půjček, výše dluhu a aktuální dlužná částka, a to celkem 87 neoprávněným adresátům používajícím e-mailové schránky na internetových doménách atlas.cz, centrum.cz, email.cz, gmail.com, jstrading.cz, post.cz, seznam.cz, sms.cz a volny.cz.

Dále ze spisového materiálu vyplývá, že účastník řízení zejména v oblasti vývoje, testování a implementace aplikačního programového vybavení do svého rutinního provozu, nepřijal a nedokumentoval technickoorganizační opatření (např. interní dokumenty) k zajištění ochrany osobních údajů. V průběhu kontroly bylo zjištěno, že pouze zapracoval základní povinnosti zaměstnanců v oblasti ochrany osobních údajů do pracovních smluv, a dále demonstroval způsob uzavírání smluv, způsob ověřování informací a způsob vkládání a zpracování osobních údajů klientů v elektronické databázi klientů.

Současně ze spisového materiálu vyplývá, že o chybném rozeslání byl účastník řízení informován jednotlivými adresáty, kteří zásilku obdrželi, a že se účastník řízení e-mailovou zprávou odeslanou dne 15. ledna 2015 v 0:23 hod. omluvil za technické pochybení při odesílání e-mailů, kdy došlo nedopatřením k odeslání údajů týkajících se stavu půjček jeho několika klientů neoprávněným adresátům.

K chybnému rozeslání e-mailových zpráv došlo podle vyjádření účastníka řízení chybou programátora při zapracování nové funkcionality do softwaru pro automatizované rozesílání e-mailů. Bezprostředně poté účastník řízení podle svého vyjádření přijal opatření, aby nedošlo k opakování chybného rozesílání zpráv. V současné době provádí v týdenních cyklech namátkové kontroly správnosti vložených dat s cílem zabránit zneužití systému vlastními zaměstnanci, např. zjišťování duplicity vložených dat, porovnáváním dat vkládaných jedním zaměstnancem s předcházejícími záznamy (duplicita dat). Přístupy zaměstnanců do databáze jsou logovány, rovněž tyto přístupy jsou namátkově kontrolovány.

K předmětu tohoto řízení lze konstatovat, že jméno, příjmení, adresa trvalého pobytu (PSČ, obec/město, ulice, číslo popisné), rodné číslo, číslo občanského průkazu, e-mailová adresa, číslo telefonu, bankovní účet, hlavní zdroj příjmu, jméno zaměstnavatele, výše příjmu, přeplatek, datum vytvoření registrace, počet půjček, výše dluhu a aktuální dlužná částka jsou ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. nepochybně osobní údaje, neboť se vztahují k jednoznačně určeným subjektům údajů.

Dále je třeba konstatovat, že odesílání předmětných e-mailových zpráv klientům je výsledkem řady automatizovaných i manuálních operací účastníka řízení, během kterých dochází k vyhledávání, shromažďování, ukládání na nosiče informací do databáze v jeho informačním systému, uchovávání, třídění, kombinování apod. osobních údajů klientů; jedná se tedy o zpracování osobních údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb.

K předmětu řízení pak správní orgán uvádí, že účastník řízení je správcem osobních údajů svých klientů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., a jako takový je povinen dodržovat při zpracování osobních údajů povinnosti stanovené zákonem č. 101/2000 Sb., včetně povinností vyjádřených v § 13 odst. 1 a 2 tohoto zákona. Podle těchto ustanovení je správce osobních údajů povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, resp. k jejich neoprávněnému zpracování, a dále je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů.

Povinnost dle § 13 odst. 1 zákona č. 101/2000 Sb. a této povinnosti odpovídající skutková podstata správního deliktu je formulovaná jako odpovědnost za následek. Dojde-li tedy k následku předvídanému v § 13 odst. 1 zákona č. 101/2000 Sb. (neoprávněnému přístupu k osobním údajům apod.), což je v této věci nepochybné, znamená to, že se správce osobních údajů dopustil také správního deliktu.

Správní orgán v této souvislosti odkazuje na argumentaci Nejvyššího správního soudu k problematice objektivní odpovědnosti za správní delikt v rozsudku čj. 9 As 36/2007-59 (byť v jiné oblasti veřejného práva a bez výslovného zakotvení liberačního ustanovení). Dle názoru správního orgánu je pojem „přijmout taková opatření“ v normě ukládající primární povinnosti (tj. v § 13 odst. 1 zákona č. 101/2000 Sb.) nutno považovat za synonymum pojmu zajistit. Oba tyto pojmy je poté třeba dle názoru správního orgánu interpretovat jako garanci správce osobních údajů za bezpečnost zpracování osobních údajů, tedy za to, že se s osobními údaji např. neseznámí žádná nepovolaná osoba. Jedině tento výklad je schopen zajistit efektivní fungování právní normy a naplnění jejího elementárního smyslu a účelu, kterým je naplnění práva každého na ochranu před neoprávněným zasahováním do soukromí (viz opět rozsudek Nejvyššího správního soudu čj. 9 As 36/2007-59).

Skutková podstata správního deliktu dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. poté hovoří o nepřijetí nebo neprovedení opatření pro zajištění bezpečnosti zpracování. S ohledem na shora uvedený výklad § 13 odst. 1 zákona č. 101/2000 Sb. je správní orgán toho názoru, že použití pojmů „nepřijme nebo neprovede“ nic nemění na charakteru odpovědnosti správce za nesplnění povinnosti dle § 13 zákona č. 101/2000 Sb.; uvedení bezpečnostních opatření v život, tak aby plnila svůj smysl a účel, nelze jiným způsobem, než jejich přijetím a provedením,

přičemž tyto dva pojmy dle názoru správního orgánu současně plně pokrývají a vystihují všechny možné způsoby naplnění účelu bezpečnostních opatření; jinými slovy, s bezpečnostními opatřeními nelze dělat nic jiného, než je přijmout a provést. Správní orgán je proto toho názoru, že dikce § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. nedává ani účastníkovi řízení prostor k tomu, aby prokazováním svého preventivního jednání popřel, že k naplnění skutkové podstaty deliktu došlo, byl-li přístup neoprávněných osob k osobním údajům nepochybně prokázán.

Ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. je pak formulováno tak, že právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. Posuzování naplnění liberačního ustanovení je přitom závislé vždy na konkrétních okolnostech daného případu a nelze jej dle názoru správního orgánu jakkoliv předem zobecnit (při současném respektování limitu vyjádřeného v § 2 odst. 4 správního řádu).

Správní orgán přitom považuje za nezbytné konstatovat, že v případě § 46 odst. 1 zákona č. 101/2000 Sb. (a ostatně všech liberačních ustanovení) se přenáší důkazní břemeno na účastníka řízení a je to on, kdo musí k prokázání liberace navrhovat důkazy (srov. Mates P. a kolektiv: Základy správního práva trestního, 3. vydání, Praha: C.H. Beck, 2002, str. 12; dále také § 52 správního řádu).

Správní orgán proto na základě shora uvedeného posoudil jednání účastníka řízení z hlediska § 46 odst. 1 zákona č. 101/2000 Sb. Správní orgán v této souvislosti uvádí, že vynaložení veškerého úsilí, které bylo možno požadovat, neznamená jakékoliv úsilí, které správce vynaloží, ale musí se ve vztahu ke každému, konkrétně posuzovanému případu, jednat o úsilí maximálně možné, které je správce objektivně schopen vynaložit (zákon používá kritérium veškeré úsilí, které bylo možno požadovat, a nikoliv např. spravedlivě požadovat, požadovat s ohledem na poměry atp.). V případě účastníka řízení sice došlo k zapracování základních povinností zaměstnanců v oblasti ochrany osobních údajů do pracovních smluv, to ovšem nemění nic na skutečnosti, že přesto došlo k rozeslání předmětných e-mailových zpráv s osobními údaji neoprávněným osobám. Správní orgán má proto za prokázané, že účastník řízení nevynaložil veškeré úsilí, které bylo možné požadovat, když v oblasti vývoje, testování a implementace aplikačního programového vybavení do svého rutinního provozu nepřijal žádná specifická technicko-organizační opatření k zajištění ochrany osobních údajů svých klientů (resp. je přijal až po nastalém incidentu).

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutková zjištění za dostatečná a na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním povinnosti stanovené v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Podle § 46 odst. 2 zákona č. 101/2000 Sb. se při rozhodování o výši pokuty přihlíží k závažnosti, způsobu, době trvání, následkům protiprávního jednání a k okolnostem, za nichž bylo protiprávní jednání spácháno. Správní orgán v souladu s tímto ustanovením při stanovení výše pokuty vycházel z následujících skutečností.

Z hlediska závažnosti správní orgán hodnotí jako přitěžující kritérium zásah do zákonem chráněných práv, který vyplývá především z velmi širokého rozsahu neoprávněně zpřístupněných osobních údajů, a to včetně rodného čísla, jako obecného identifikátoru občana. Tato okolnost současně vyjadřuje následek protiprávního jednání účastníka řízení ve smyslu § 46 odst. 2 zákona č. 101/2000 Sb. Za přitěžující okolnost je pak nutno považovat též velký počet neoprávněných adresátů e-mailových zpráv. Jako polehčující okolnost pak posoudil správní orgán okolnost, že k protiprávnímu jednání došlo zejména v důsledku softwarové chyby při zapracování nové funkcionality softwaru.

Po zhodnocení všech těchto okolností byla uložena sankce při spodní hranici zákonem stanovené sazby.

Při rozhodnutí o uložení povinnosti uhradit náklady řízení správní orgán vycházel z ustanovení § 79 odst. 5 správního řádu, který správnímu orgánu ukládá povinnost uložit paušální částkou náhradu nákladů řízení účastníkovi, který řízení vyvolal porušením své právní povinnosti, 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, kterou se stanoví paušální částka nákladů správního řízení ve výši 1.000 Kč.

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

Poučení: V souladu s § 150 odst. 3 správního řádu lze u oddělení správních činností 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, 2. listopadu 2015

otisk
úředního
razítka

Vanda Foldová
vedoucí oddělení správních činností