



Zn. SPR-1375/10-48

ROZHODNUTÍ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 10 zákona č. 500/2004 Sb., správní řád, § 2 odst. 2 a § 46 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, rozhodl dne 24. května 2010 takto:

Je prokázáno, že účastník řízení: společnost banan s.r.o., se sídlem Slavíkova 1744/22, 708 00 Ostrava, IČO: 26867257, tím, že nezajistil, aby se na přelomu roku 2009 a 2010 neznámá neoprávněná osoba neseznámila a neodcizila osobní údaje klientů, a to A. P. v rozsahu id klienta, jméno a příjmení a e-mail, V. K. v rozsahu id klienta, heslo, jméno a příjmení, e-mail, adresa, telefonní číslo a datum narození, D. R. v rozsahu id klienta, heslo, jména a příjmení, e-mail, adresa a datum narození, M. B. v rozsahu id klienta, heslo, jméno a příjmení, adresa, datum narození a e-mail, Z. M. v rozsahu id klienta, heslo, e-mail a datum narození, J. S. v rozsahu id klienta, heslo, jméno a příjmení, e-mail, adresa, telefonní číslo a datum narození, a M. P. v rozsahu id klienta, heslo, jméno a příjmení, e-mail, adresa, telefonní číslo a datum narození,

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 35.000 Kč
(slovy třicet pět 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. 3754-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Správní řízení pro podezření ze spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. bylo zahájeno oznámením Úřadu pro ochranu osobních údajů, které bylo účastníku řízení, společnosti banan s.r.o., doručeno dne 8. dubna 2010. Podkladem pro zahájení řízení byly stížnosti doručené Úřadu pro ochranu osobních údajů.

Ze spisového materiálu (obsahu stížností a jejich příloh) je zřejmé, že v měsíci lednu 2010 obdrželi klienti (bývalí i současní) účastníka řízení zprávu od neznámé osoby (hackera), která obsahovala jejich osobní údaje, které sdělily účastníkovi řízení v souvislosti se vzájemným smluvním vztahem. Tímto způsobem získala třetí osoba prokazatelně osobní údaje A. P. v rozsahu id klienta, jméno a příjmení a e-mail, V. K. v rozsahu id klienta, heslo, jméno a příjmení, e-mail, adresa, telefonní číslo a datum narození, D. R. v rozsahu id klienta, heslo, jména a příjmení, e-mail, adresa a datum narození, M. B. v rozsahu id klienta, heslo, jméno a příjmení, adresa, datum narození a e-mail, Z. M. v rozsahu id klienta, heslo, e-mail a datum narození, J. S. v rozsahu id klienta, heslo, jméno a příjmení, e-mail, adresa, telefonní číslo a datum narození, a M. P. v rozsahu id klienta, heslo, jméno a příjmení, e-mail, adresa, telefonní číslo a datum narození. K tomuto neoprávněnému přístupu přitom došlo ze strany neznámé osoby opakovaně.

Účastník řízení je ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. správcem osobních údajů svých současných i bývalých klientů a jako takový je povinen dodržovat veškeré povinnosti stanovené zákonem č. 101/2000 Sb., včetně povinnosti vyjádřené v § 13 odst. 1 tohoto zákona. Podle tohoto ustanovení je správce osobních údajů povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, resp. k jejich neoprávněnému zpracování.

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.

Odpovědnost za správní delikt je přitom postavena na objektivní odpovědnosti (tedy bez ohledu na zavinění), přičemž zákon č. 101/2000 Sb. upravuje v § 46 odst. 1 liberační důvod, jehož naplněním se pachatel správního deliktu může odpovědnosti zprostit.

Za případnou poté považuje správní orgán 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). Správní orgán proto považuje za vhodné se v souvislosti s citovaným rozsudkem podrobněji vyjádřit k naplnění skutkové podstaty správního deliktu dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. 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, www.nssoud.cz).

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 poté 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 účastníkovi řízení prostor k tomu, aby prokazováním svého preventivního jednání popřel, že k naplnění skutkové podstaty deliktu došlo, byl-li přístup neoprávněné osoby k osobním údajům nepochybně prokázán.

Ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. je formulováno tak, že účastník řízení za správní delikt neodpovídá, jestliže prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil. 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 ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. (a ostatně všech liberačních ustanovení) se

přenáší břemeno tvrzení a důkazní břemeno na účastníka řízení a je to on, kdo musí k prokázání liberace navrhnout důkazy (srov. Mates P. a kolektiv: Základy správního práva trestního, 3. vydání, Praha: C.H. Beck, 2002, str. 12; dále také § 52 správního řádu).

V daném případě účastník řízení žádné naplnění liberačního ustanovení netvrdil ani žádné důkazy v tomto smyslu nenavrhnul (byť je to dáno tím, že v průběhu správního řízení je mu doručováno do datové schránky na základě tzv. fikce doručení; je ovšem povinností účastníka řízení zajistit si řádné přebírání pošty i prostřednictvím datové schránky jako jednoho, a v jeho případě i jediného a povinného, komunikačního kanálu státního správy s ním). Současně lze konstatovat, že v případě osobních údajů v databázích či jiných informačních systémech napojených a dostupných prostřednictvím sítě internet, je třeba požadovat absolutní zajištění ochrany údajů, a v daném případě nepostačí k prokázání liberace ani použití dostupných a standardních bezpečnostních opatření a programů sloužících k zabránění neoprávněnému přístupu do systému, neboť riziko neoprávněného přístupu přes internet je z povahy této sítě mnohem vyšší a každý správce osobních údajů s ním musí počítat a minimalizovat ho (např. umístěním údajů v počítačovém systému, který na síť internet není napojen).

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb.

Při stanovení výše sankce bylo přihlédnuto jako k přitěžující okolnosti zejména ke skutečnosti, že k neoprávněnému přístupu k osobním údajům došlo prokazatelně u 7 osob, současně správní orgán přihlédl k charakteru a rozsahu odcizených osobních údajů a také ke skutečnosti, že k tomuto došlo opakovaně. Správní orgán také zohlednil, že krádež osobních údajů na internetu je závažným zásahem do práva na soukromí dotčených osob, neboť je spojena se značným rizikem jejich zneužití. Po zhodnocení všech těchto kritérií rozhodl správní orgán o uložení sankce při dolní hranici zákonné 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 rozhodnutí.

Poučení: V souladu s § 152 odst. 1 správního řádu lze u odboru správních činností proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedovi 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, 24. května 2010

otisk
úředního
razítka

Daniel Pospíšil
ředitel odboru správních činností