Zn. SPR-1375/10-55

ROZHODNUTÍ

Předseda Úřadu pro ochranu osobních údajů jako odvolací orgán příslušný podle § 2, § 29 a § 32 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, a podle § 10 a § 152 odst. 2 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, rozhodl podle ustanovení § 152 odst. 5 písm. b) správního řádu takto:

Rozklad účastníka řízení, společnosti banan s.r.o., se sídlem Slavíkova 1744/22, 708 00 Ostrava, IČ: 26867257, proti rozhodnutí Úřadu pro ochranu osobních údajů zn. SPR-1675/10-48 ze dne 24. května 2010, kterým byla účastníku řízení, jako správci osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., v souvislosti s odcizením osobních údajů sedmi klientů účastníka řízení neznámou osobou (hackerem) v lednu 2010, tedy za porušení povinnosti stanovené v § 13 odst. 1 zákona č. 101/2000 Sb., čímž spáchal správní delikt podle § 45 odst. 1 písm. h) tohoto zákona, uložena v souladu s § 45 odst. 3 zákona č. 101/2000 Sb. pokuta ve výši 35.000 Kč a dále povinnost nahradit náklady řízení v částce 1.000 Kč, **se zamítá**.

Odůvodnění

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

Správní orgán prvního stupně ze spisového materiálu dovodil, že v lednu 2010 obdrželi někteří bývalí i stávající klienti účastníka řízení elektronickou poštou zprávu od neznámé osoby (hackera) obsahující jejich osobní údaje, které poskytli účastníku řízení v rámci smluvního vztahu. Tato třetí osoba tak dle správního orgánu prvního stupně prokazatelně získala přístup k osobním údajům sedmi klientů (A. P., V. K., D. R., M. B., Z. M., J. S. a M. P.) v rozsahu ID klienta, jméno, příjmení, e-mail, případně heslo, adresa, telefonní číslo a datum narození.

Správní orgán prvního stupně při hodnocení zjištěného skutkového stavu předně konstatoval, že účastník řízení je ve vztahu k osobním údajům svých bývalých i současných klientů v postavení správce osobních údajů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. a jako takový je povinen dodržovat veškeré povinnosti stanovené tímto zákonem.

K plnění povinnosti správce osobních údajů uložené v § 13 odst. 1 zákona č. 101/2000 Sb. správní orgán prvního stupně uvedl, že skutková podstata správního deliktu odpovídající porušení této povinnosti je formulována jako odpovědnost za následek. S odkazem na judikaturu Nejvyššího správního soudu správní orgán prvního stupně následně konstatoval, že povinnost vyjádřená v § 13 odst. 1 zákona č. 101/2000 Sb. spočívá v tom, že správce osobních údajů musí zajistit vhodná bezpečnostní opatření, tj. je povinen taková opatření nejen přijmout, ale i realizovat v praxi. V případě, kdy zákonem předvídaný následek již nastal (tj. v tomto případě neoprávněná osoba získala v důsledku nedostatečného zabezpečení přístup k osobním údajům klientů účastníka řízení), je dle správního orgánu prvního stupně nepochybné, že došlo ke spáchání správního deliktu a zbývá pouze posoudit, zda je na místě aplikovat liberační důvod dle § 46 odst. 1 zákona č. 101/2000 Sb.

Co se týče uplatnění zmíněné liberace, správní orgán prvního stupně uvedl, že zde přechází povinnost tvrzení a důkazní břemeno na účastníka řízení, který musí navrhovat důkazy k prokázání splnění podmínek pro uplatnění liberace. Účastník řízení však žádné tvrzení či návrh na doplnění dokazování nepředložil. Správní orgán prvního stupně současně konstatoval, že s ohledem na zjištěné okolnosti – tj. zpracování osobních údajů v prostředí internetu – jsou rizika ztráty a zneužití osobních údajů mnohem vyšší a účastník řízení tak byl povinen tato rizika řádně vyhodnotit a minimalizovat je. Správní orgán prvního stupně tak neshledal žádný důvod pro použití § 46 odst. 1 zákona č. 101/2000 Sb.

Při stanovení výše sankce správní orgán prvního stupně hodnotil zejména počet dotčených subjektů údajů (klientů účastníka řízení) a charakter osobních údajů, které získala neznámá třetí osoba. Dle správního orgánu prvního stupně tak došlo k závažnému zásahu do práva na soukromí těchto osob, neboť zde vzniklo značné riziko zneužití odcizených osobních údajů.

Rozhodnutí správního orgánu prvního stupně zn. SPR-1375/10-48 ze dne 24. května 2010 bylo účastníku řízení doručeno 2. června 2010 a dne 17. června 2010 byl Úřadu doručen rozklad proti tomuto rozhodnutí.

V podaném rozkladu účastník řízení nejprve namítá, že správní orgán prvního stupně nesprávně vyhodnotil charakter odpovědnosti za porušení § 13 odst. 1 zákona č. 101/2000 Sb. jako odpovědnost za následek, tj. absolutní odpovědnost bez možnosti liberace. Tuto interpretaci považuje účastník řízení za nezákonnou, resp. v rozporu s ústavními principy pro uplatnění státní moci. Dle názoru účastníka řízení je obsahem citovaného ustanovení povinnost správce osobních údajů vynaložit veškeré možné úsilí na to, aby byla přijata taková opatření, aby nemohlo dojít k neoprávněnému či nahodilému přístupu k osobním údajům. Posouzení plnění této povinnosti pak spočívá ve vyhodnocení, zda správce taková opatření přijal nebo nepřijal, nikoli v tom, zda došlo k neoprávněnému přístupu k osobním údajům. Požadavek, aby správce osobních údajů zajistil bezpečnost osobních údajů za každých okolností, jde dle účastníka řízení nad rámec zákona a je objektivně nesplnitelný. V této souvislosti účastník řízení namítá, že správní orgán prvního stupně se prokazováním přijetí vhodných opatření vůbec nezabýval. Účastník řízení dále uvádí, že k přístupu k osobním údajům došlo v důsledku trestného činu třetí osoby, za který nemůže nést odpovědnost.

Současně účastník řízení namítá, že správní orgán prvního stupně se nezabýval původem zpráv zaslaných klientům účastníka řízení, ani identitou osob, které zaslaly Úřadu své stížnosti. Tento postup je dle účastníka řízení v rozporu s § 3 správního řádu.

Dále účastník řízení zpochybňuje, že by vůbec došlo k neoprávněnému přístupu k osobním údajům jeho klientů. Účastník řízení nevylučuje, že mohlo dojít k přístupu do jeho databází – tyto databáze však neobsahují osobní údaje klientů, ale pouze ID klienta, heslo v zašifrované podobě a název domény klienta. Zprávy zaslané neznámou osobou klientům účastníka řízení přitom obsahují kombinaci informací získaných z různých zdrojů, byly zaslány i na adresy osob, které nejsou a nebyly jeho klienty (což dokládá výtiskem zpráv elektronické pošty zaslaných třemi osobami), a ani svou strukturou neodpovídají databázi účastníka řízení. V této souvislosti účastník řízení odkazuje na vyjádření odborníka, které přiložil k podanému rozkladu.

V předloženém vyjádření (analýze) dochází autor, Ing. M. M., Ph.D., na základě podkladů poskytnutých účastníkem řízení k závěru, že obsah zpráv elektronické pošty zaslaných klientům účastníka řízení neznámou osobou a struktura databází účastníka řízení nejsou totožné, tedy že data ze zpráv elektronické pošty pocházejí z jiného informačního zdroje, než jsou databáze účastníka řízení.

Účastník řízení dále spekuluje o možnosti, že zaslání předmětných zpráv elektronické pošty může být důsledkem koordinované činnosti směřující k poškození účastníka řízení (což dokládá výtiskem části diskuze z prostředí internetu). A dále popisuje, jakým způsobem jsou osobní údaje, které zpracovává, zabezpečeny. Konkrétně uvádí, že informace o klientech uchovává na vyhrazeném serveru, k němuž je přístup uskutečňován prostřednictvím protokolu https a je podmíněn individuálním oprávněním pro každou z aplikací. Server je fyzicky umístěn v uzamčené skříni v datovém centru společnosti Master Internet, s.r.o., s níž má účastník řízení uzavřenou smlouvu o poskytování telekomunikačních služeb, jejíž kopii přiložil k rozkladu. Se zaměstnanci, kteří mají přístup k osobním údajům, byla uzavřena smlouva o zachování mlčenlivosti o důvěrných informacích – kopie těchto smluv také tvoří přílohu rozkladu.

Závěrem svého rozkladu účastník řízení konstatuje, že jeho procesní pasivita (způsobená technickou chybou spočívající ve výpadku zasílání informací o doručení zprávy do datové schránky) nemění nic na povinnosti správního orgánu prvního stupně postupovat tak, aby byl zjištěn stav věci, o kterém nejsou důvodné pochybnosti. Účastník řízení proto navrhuje, aby předseda Úřadu napadené rozhodnutí zrušil.

Na základě podaného rozkladu odvolací orgán přezkoumal napadené rozhodnutí, včetně celého spisového materiálu, jakož i proces, který vydání napadeného rozhodnutí předcházel, a dospěl k následujícím závěrům.

Odvolací orgán předně konstatuje, že východiska správního orgánu prvního stupně, dle kterých jsou informace o klientech účastníka řízení osobními údaji ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. a na účastníka řízení je tak nutno pohlížet jako na správce osobních údajů dle § 4 písm. j) tohoto zákona, který za zpracování osobních

údajů plně odpovídá, považuje za správná a odpovídající zjištěnému skutkovému stavu. Na účastníka řízení se tedy nepochybně vztahuje také povinnost zabezpečit jím zpracovávané osobní údaje mj. proti neoprávněnému či nahodilému přístupu, jak požaduje § 13 odst. 1 zákona č. 101/2000 Sb.

Ze znění § 13 odst. 1 zákona č. 101/2000 Sb. je zřejmé, že obsahem této povinnosti je vyhodnocení rizik spojených se zpracováním osobních údajů (a to jak s ohledem na charakter těchto údajů, tak i s ohledem na veškeré relevantní okolnosti, včetně použitých prostředků zpracování, specifika činnosti správce apod.) a přijetí opatření, která tato rizika v maximální možné míře eliminují. Nedílnou součástí této povinnosti je i provedení všech nezbytných opatření do praxe, tj. nestačí pouze formální přijetí, ale je vyžadována i důsledná realizace, včetně kontroly dodržování zvolených opatření a jejich efektivity. Pokud správce osobních údajů některý z těchto aspektů nezohlední a zpracovává osobní údaje v situaci, kdy hrozí riziko jejich zneužití či ztráty apod., dopouští se správního deliktu spočívajícího v porušení § 13 odst. 1 zákona č. 101/2000 Sb. K naplnění skutkové podstaty správního deliktu dle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. tak postačí již vznik stavu, kdy jsou osobní údaje vystaveny riziku ztráty nebo zneužití, aniž by k jejich ztrátě či zneužití skutečně došlo.

Z uvedeného je zřejmé, že odpovědnost za porušení § 13 odst. 1 zákona č. 101/2000 Sb. je konstruována jako odpovědnost za následek (tj. bez ohledu na zavinění) s možností liberace dle § 46 odst. 1 zákona č. 101/2000 Sb. Toto je výslovně uvedeno i v napadeném rozhodnutí a není tedy pravdou, že by správní orgán prvního stupně pokládal tuto odpovědnost za absolutní bez možnosti liberace, jak uvádí účastník řízení ve svém rozkladu. Správce osobních údajů tedy odpovídá již za to, že osobní údaje jsou zpracovávány pouze za stavu, kdy byla přijata a provedena veškerá možná bezpečnostní opatření, nikoli až v případě, kdy dojde k neoprávněnému přístupu nebo ke ztrátě osobních údajů.

V situaci, kdy k neoprávněnému přístupu, ke ztrátě či ke zneužití dat již došlo, má se v souladu se zněním § 13 odst. 1 a § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. za to, že přijatá a realizovaná opatření nebyla dostatečná, neboť zjevně nezabránila přístupu neoprávněné osoby k osobním datům, příp. jejich zneužití. Vzhledem k tomu, že takto absolutně formulovaná odpovědnost by byla nedůvodně přísná, neboť jsou situace, které nelze předvídat, resp. kterým nelze zcela předcházet (např. lidské selhání či úmyslné jednání v rozporu s pravidly či zákonem anebo *vis maior*), obsahuje zákon č. 101/2000 Sb. ve svém § 46 odst. 1 liberační ustanovení, dle kterého lze správce odpovědnosti za správní delikt zprostit v případě, kdy prokáže, že k porušení zákona č. 101/2000 Sb. došlo právě za okolností, které nemohl předvídat, resp. nemohl zcela eliminovat. Odvolací orgán považuje za podstatné, že dle dikce § 46 odst. 1 zákona č. 101/2000 Sb. správní delikt již nastal, tj. byly naplněny všechny znaky skutkové podstaty, a za splnění zde uvedených podmínek z něj pouze není pro správce vyvozována odpovědnost (tj. sankce).

V této souvislosti je dále nutno zdůraznit, že § 46 odst. 1 zákona č. 101/2000 Sb. jednoznačně přenáší důkazní břemeno na správce, který je povinen prokázat své tvrzení, že okolnosti, které vedly k porušení zákona, nemohl při vynaložení veškerého (tj. objektivně možného) úsilí předvídat či jim zabránit. Citované ustanovení tak zcela jednoznačně neponechává prostor pro vlastní úkony správního

orgánu, čímž pro tento případ zakládá výjimku z obecného pravidla dle § 3 správního řádu (který ostatně s jiným postupem v případě, že tak stanoví zvláštní zákon, výslovně počítá).

Jestliže je tedy naplnění skutkové podstaty správního deliktu prokázáno, což je vzhledem k obsahu povinnosti dle § 13 odst. 1 zákona č. 101/2000 Sb. v případě, kdy již dojde k úniku osobních údajů, zcela nepochybné, je plně na správci osobních údajů, aby tvrdil, že náležitá opatření přijal a provedl, a toto své tvrzení také doložil.

V tomto případě byl účastník řízení až do vydání napadeného rozhodnutí nečinný, ačkoli mu prokazatelně bylo doručeno jak oznámení o zahájení řízení, tak i vyrozumění o možnosti seznámit se s podklady rozhodnutí, přičemž byl současně vždy poučen o svých právech. Správní orgán prvního stupně doručoval v souladu s příslušnými předpisy prostřednictvím informačního systému datových schránek (dále jen „ISDS“) a měl oprávněně za to, že účastník řízení zaslané písemnosti obdržel a rozhodl se svá práva v řízení neuplatnit. V takové situaci nebyl správní orgán prvního stupně povinen, resp. ani oprávněn, jakkoli nahrazovat procesní pasivitu účastníka řízení, předjímat jeho možnou obhajobu a doplňovat v tomto smyslu dokazování, které považoval za dostačující k vydání rozhodnutí. Stejně tak nemohl správní orgán prvního stupně předvídat ani jakkoli zohledňovat, že na straně účastníka řízení mělo dle jeho tvrzení dojít k výpadku zasílání informací o doručení písemnosti prostřednictvím ISDS, neboť písemnost je doručena přihlášením odpovědné osoby do datové schránky anebo uplynutím 10 dní od dodání do datové schránky, nikoli zasláním informace o tomto dodání mimo ISDS. Je povinností účastníka řízení zajistit, aby oprávněné osoby obsah datové schránky pravidelně sledovaly, v opačném případě musí nést důsledky takového opomenutí v podobě doručování na základě uvedené fikce.

Odvolací orgán dále konstatuje, že i v posuzovaném případě lze teoreticky uvažovat o aplikaci ustanovení § 46 odst. 1 zákona č. 101/2000 Sb., a to např. v případě, kdy by útok hackera proběhl doposud neznámým způsobem, nebo způsobem, proti kterému nebylo možné se s ohledem na neustálý vývoj technologií účinně bránit, anebo v případě, kdy by i přes veškerá organizační a technická opatření došlo k úniku dat např. v důsledku nezákonného jednání zaměstnance účastníka řízení či jiné osoby oprávněné s údaji nakládat. Výrok správního orgánu prvního stupně, že v případě informačních systémů (databází) napojených na internet je nutno požadovat absolutní zajištění ochrany dat, proto nelze dle odvolacího orgánu považovat za odmítnutí možnosti posupovat v této oblasti podle § 46 odst. 1 zákona č. 101/2000 Sb. Odvolací orgán je však toho názoru, že při zpracování osobních údajů pomocí výpočetní techniky, obzvláště pokud jde o systémy dostupné prostřednictvím internetu, je nutno v souladu s § 13 odst. 1 zákona č. 101/2000 Sb. požadovat maximální úroveň bezpečnostních opatření, zohledňující mj. aktuální, známé možnosti útoků. Tam, kde to lze, je potom na místě v rámci bezpečnostních opatření trvat na úplném oddělení databází obsahujících osobní údaje od veřejných sítí, právě s odkazem na fakt, že vždy hrozí riziko ztráty (a případného zneužití) těchto dat. V případě zákazníků či klientů je přitom zjevné, že uchovávání databáze s jejich osobními údaji mimo prostředí internetu není nepřiměřený či nerealizovatelný požadavek, přičemž míra ochrany osobních údajů se v důsledku oddělení takové databáze od *a priori* rizikového prostředí internetu výrazně zvyšuje.

Odvolací orgán se dále zabýval tím, zda v daném případě bylo prokázáno v míře požadované v § 3 správního řádu, že ke ztrátě osobních údajů došlo, a to na straně účastníka řízení. V tomto směru považuje odvolací orgán za podstatné, že součástí spisového materiálu je mimo jiné zpráva ze dne 10. února 2010 zaslaná elektronickou poštou jednomu ze stěžovatelů (M. B.), ve které účastník řízení jednoznačně potvrzuje, že dne 19. ledna 2010 došlo k útoku hackera na jeho databázi, po které měnil přístupová hesla. Současně účastník řízení sděluje, že během útoku došlo k úniku dat klientů z jeho databáze. Ve spise tohoto řízení je dále založeno sdělení účastníka řízení zaslané klientům, kteří byli osloveni hackerem, v níž účastník řízení informuje, že klienti mohou obdržet nevyžádané obtěžující e-maily s tím, že se stále jedná o důsledky incidentu (útoku hackera) ze dne 19. ledna 2010. Obdobně i ve své tiskové zprávě ze dne 22. ledna 2010 (umístěné na adrese http://owebu.bloger.cz/_/vyjadreni-spolecnosti-banan-s-r-o-k-utoku-hackera-tiskova-zprava) účastník řízení informuje o tom, že dne 19. ledna 2010 došlo k útoku hackera.

Pro posouzení skutkového stavu věci je dále podstatné, že Úřad obdržel 7 podnětů, v nichž stěžovatelé shodně prohlašují, že jim ze strany neznámé třetí osoby byly zaslány osobní údaje, které poskytli účastníku řízení v souvislosti se smluvním vztahem, který s ním uzavřeli. Obsahem zpráv, které stěžovatelé od hackera obdrželi, je přitom i ID klienta a heslo přidělené účastníkem řízení – přinejmenším tyto informace, jejichž pravost ostatně nepopřel ani účastník řízení, přitom nepochybně nelze dohledat ve veřejně dostupných zdrojích. V kombinaci s dalšími osobními údaji stěžovatelů je potom zjevné, že zdrojem rozeslaných osobních údajů musí být databáze účastníka řízení. Tento fakt potvrzuje i výše uvedené sdělení účastníka řízení, že v návaznosti na útok hackera byl nucen změnit přístupová hesla jednotlivých klientů.

Odvolací orgán tak na základě uvedených skutečností dospěl k totožnému závěru, jako správní orgán prvního stupně, tedy že osobní údaje zpracovávané účastníkem řízení byly odcizeny neznámou osobou, neboť obsah spisového materiálu představuje ve vzájemných souvislostech dostatečný podklad pro tento závěr. S ohledem na výše uvedené je potom nutno konstatovat, že účastník řízení tyto osobní údaje v rozporu s § 13 odst. 1 zákona č. 101/2000 Sb. řádně nezabezpečil, přičemž neprokázal, že by ke ztrátě dat došlo v důsledku jednání či události, kterým nemohl i přes vynaložení veškerého úsilí předejít.

K argumentům účastníka řízení uvedeným v rozkladu lze dále dodat, že osobním údajem ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. se nerozumí pouze identifikační údaje (jméno, příjmení, datum narození apod.), ale jakákoli informace týkající se konkrétní fyzické osoby, tedy včetně ID klientů, hesla a názvu domény. Tyto údaje navíc účastník řízení zpracovává společně s dalšími identifikačními daty, přičemž z hlediska zákona č. 101/2000 Sb. je nepodstatné, zda se tak děje v rámci téže či jiné databáze (resp. „navazující tabulky z databáze“ jak je uvedeno v analýze předložené účastníkem řízení). Ve vztahu ke všem těmto informacím je přitom účastník řízení povinen zajistit bezpečnost dle § 13 odst. 1 zákona č. 101/2000 Sb. Odvolací orgán dále konstatuje, že závažnost posuzovaného deliktu nelze bagatelizovat tím, že měla být odcizena pouze zašifrovaná hesla spolu s ID klienta a označením domény (byť dle skutkových zjištění byly odcizeny i další údaje). Je třeba si uvědomit, že tato data umožňují přístup k produktům, které jsou předmětem

obchodu, a že odcizení hesel je s ohledem na možné dopady (včetně možného získání a zneužití dalších osobních dat) nutno považovat za velmi závažné, a to i přesto, že hesla byla v zašifrované podobě, neboť lze důvodně předpokládat, že tuto šifru je možné prolomit.

Dále lze uvést, že odpovědnost za správní delikt správce osobních údajů nelze zaměňovat s odpovědností fyzické osoby za trestný čin. Skutečnost, že k odcizení osobních údajů došlo v důsledku trestného činu neznámého pachatele, nezprošťuje účastníka řízení odpovědnosti za porušení povinnosti stanovené v § 13 odst. 1 zákona č. 101/2000 Sb. Účastník řízení nese odpovědnost za to, že řádným způsobem nezabezpečil osobní údaje mj. právě proti případnému útoku pachatele trestného činu, nikoli za tento (cizí) trestný čin.

Co se týče analýzy, kterou účastník řízení předložil současně s rozkladem, odvolací orgán konstatuje, že z tohoto dokumentu vyplývá pouze to, že účastníkem řízení zvolená osoba určitým způsobem posoudila dokumenty, které jí byly předloženy účastníkem řízení. Přitom nelze zjistit, zda byla k posouzení předložena struktura databáze účastníka řízení v podobě před útokem hackera, ani zda byly předloženy veškeré relevantní podklady. Předmětnou analýzu proto nelze považovat za důkaz, který by jakkoli zpochybňoval obsah podkladů, které vedly k vydání napadeného rozhodnutí, anebo vyvracel závěry správního orgánu prvního stupně. Z obsahu analýzy dle odvolacího orgánu naopak vyplývá, že struktura databáze účastníka řízení je téměř totožná se strukturou dat ve zprávách zaslaných stěžovatelům neznámou osobou. Jestliže z bodu 2. 2. této analýzy jednoznačně vyplývá, že základní data ve struktuře databáze účastníka řízení spolu s daty v navazující tabulce ve významné míře odpovídají struktuře zpráv popsané v bodu 2. 1. analýzy, je závěr, ke kterému autor analýzy došel (tedy, že oba podklady vykazují značné rozpory) zcela nelogický. Odvolací orgán proto považuje tuto analýzu za čistě účelovou a z hlediska dokazování v tomto řízení irelevantní.

K námitce účastníka řízení, že Úřad nijak nezjišťoval identitu stěžovatelů, odvolací orgán konstatuje, že Úřad je na základě § 29 odst. 1 písm. c) zákona č. 101/2000 Sb. povinen přijímat a vyřizovat i anonymní podání, resp. podání stěžovatelů, jejichž identita není zcela zjevná, pokud z těchto podnětů vyplývá dostatek informací k závěru, že v daném případě mohl být porušen zákon č. 101/2000 Sb. V tomto případě stěžovatelé, jejichž podněty byly zahrnuty do tohoto správního řízení, s Úřadem dále komunikovali a poskytovali doplňující podklady a informace ke svému podnětu (včetně zpráv elektronické pošty, které obdrželi od účastníka řízení na svou elektronickou adresu, shodnou s tou, kterou použili pro komunikaci s Úřadem). Skutečnost, že určitá osoba komunikuje prostřednictvím elektronické pošty, sama o sobě nemůže vést k závěru, že tato osoba neexistuje, resp. že její tvrzení jsou *a priori* nepravdivá. Stejně tak považuje odvolací orgán za nepodložené spekulace účastníka řízení, že by se jednalo o koordinovaný útok na účastníka řízení, ostatně ani tento fakt by účastníka řízení nezbavoval povinnosti dle § 13 odst. 1 zákona č. 101/2000 Sb., resp. důkazního břemene dle § 46 odst. 1 tohoto zákona.

Dále k tvrzení účastníka řízení, že zprávu elektronické pošty obdržely i osoby, které nejsou a nikdy nebyly jeho klienty, odvolací orgán konstatuje, že předmětem tohoto řízení je nezabezpečení osobních údajů 7 konkrétních osob, které se obrátily na Úřad se svou stížností a tvrdí, že byly nebo jsou klienty účastníka řízení, což ani

účastník řízení nepopírá. To, zda bylo obdobné sdělení zasláno i jiným osobám, a zda tyto osoby byly nebo nebyly klienty účastníka řízení, není pro toto řízení podstatné. V této souvislosti je však dle odvolacího orgánu nutno poznamenat, že uvedené tvrzení účastníka řízení (které dokládá výtiskem zpráv elektronické pošty od 3 osob, které reagují na sdělení účastníka neznámého obsahu a zjevně odmítají, že by byly s účastníkem řízení ve smluvním vztahu), může naopak indikovat porušení další z povinností stanovených zákonem č. 101/2000 Sb., konkrétně povinnosti zpracovávat pouze přesné osobní údaje podle § 5 odst. 1 písm. c) tohoto zákona. Jestliže byly databáze účastníka řízení předmětem útoku hackera, je dle odvolacího orgánu velmi pravděpodobné, že došlo ke ztrátě všech osobních údajů zde uchovávaných, nikoli pouze několika klientů. Fakt, že sdělení tohoto hackera následně obdržely i osoby, které nikdy v kontaktu s účastníkem řízení být neměly, naznačuje, že účastník řízení mohl ve svých databázích spolu s osobními údaji skutečných klientů zpracovávat nepřesný (nesprávný) údaj o kontaktní adrese elektronické pošty. V takovém případě by v důsledku nezabezpečení databáze a odcizení dat došlo ke zpřístupnění osobních údajů nejen pachateli útoku, ale i dalším osobám, čímž by se závažnost deliktu účastníka řízení nepochybně zvyšovala.

K plnění dalších povinností dle zákona č. 101/2000 Sb. je dále nutno uvést, že dle tvrzení některých stěžovatelů se jednalo nikoli o stávající, ale o bývalé klienty, jejichž smluvní vztah s účastníkem řízení již skončil. V souladu s § 5 odst. 1 písm. e) zákona č. 101/2000 Sb. je přitom povinností správce osobní údaje, které již nejsou nezbytné, dále nezpracovávat (neuchovávat). Po skončení smluvního vztahu je v souladu s citovaným ustanovením možné zpracovávat osobní údaje ještě po krátkou dobu nezbytnou pro vypořádání veškerých závazků, následně je však nutno údaje zlikvidovat. Uchovávání osobních údajů bývalých klientů i poté, co byl smluvní vztah ukončen, a žádné závazky nepřetrvávají, by bylo v rozporu s povinností stanovenou v § 5 odst. 1 písm. e) zákona č. 101/2000 Sb.

Závěrem lze uvést, že k popisu zabezpečení osobních údajů podanému v rozkladu, resp. k přiloženým podkladům, odvolací orgán nemůže s odkazem na § 82 odst. 4 správního řádu přihlížet, neboť se nepochybně nejedná o skutečnosti a důkazy, které by účastník řízení nemohl uplatnit dříve než v rámci odvolacího řízení. Tvrzení účastníka řízení o tom, že se o doručení písemností v řízení před správním orgánem prvního stupně nedozvěděl, nemá na aplikaci uvedené zásady koncentrace řízení žádný vliv.

Odvolací orgán nicméně považuje za vhodné uvést, že účastníkem řízení předložené důkazy jsou ve vztahu k předmětu tohoto řízení, kterým je absence dostatečných bezpečnostních opatření ve vztahu k odcizení dat neznámou osobou, irelevantní. Ze smlouvy se společností Master Internet, s.r.o. vyplývá, že tato společnost poskytuje účastníku řízení pronájem serveru umístěného v jejích prostorách. Předložená smlouva však nijak nedokládá, jaká bezpečnostní opatření (technická či organizační) společnost Master Internet, s.r.o., pro účastníka řízení zajišťuje. Tvrzení účastníka řízení o používání protokolu https nebo o individuálním oprávnění jednotlivých osob, příp. o organizačních opatřeních přijatých společností Master Internet, s.r.o. (umístění serveru v uzamčené místnosti, omezený přístup osob) smlouva s touto společností tedy nijak nepotvrzuje. Co se týče smluv se zaměstnanci účastníka řízení, je namístě opět zopakovat, že k odcizení osobních údajů došlo útokem

zvenčí, nikoli v důsledku jednání některého ze zaměstnanců při plnění jeho pracovní činnosti. Smlouvy se zaměstnanci tak opět nijak nedokládají, že v době útoku přijal účastník řízení veškerá opatření, aby odcizení dat touto cestou předešel. Současně je nutno poznamenat, že povinnost mlčenlivosti o osobních údajích a o přijatých bezpečnostních opatřeních vzniká zaměstnancům každého správce osobních údajů přímo na základě § 15 zákona č. 101/2000 Sb., a není proto nezbytné ji smluvně upravovat. Poslední z příloh rozkladu, z hlediska tématu i zdroje blíže neurčitelný, výtažek z internetové diskuze či blogu, nedokládá dle odvolacího orgánu vůbec nic, než že se blíže neurčená osoba vyjadřuje k zájmu účastníka řízení o jednu konkrétní doménu a blog.

Odvolací orgán tedy konstatuje, že předložené podklady nijak nedokazují tvrzení účastníka řízení o tom, že vždy řádně plnil svou povinnost vyjádřenou v § 13 odst. 1 zákona č. 101/2000 Sb., naopak obsahem se jedná o zčásti irelevantní a zčásti účelové materiály.

Na základě všech výše uvedených skutečností rozhodl odvolací orgán tak, jak je uvedeno ve výroku tohoto rozhodnutí.

Poučení: Proti tomuto rozhodnutí se podle ustanovení § 91 odst. 1 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů, nelze odvolat.

Praha 10. srpna 2010

otisk úředního razítka

RNDr. Igor Němec
předseda