Čj. UOOU-04741/13-30

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 18. srpna 2014 takto:

Je prokázáno, že účastník řízení: občanské sdružení SPKFree.Net, se sídlem Dolnostudénská 1293/8, 787 01 Šumperk, IČ: 26989778, v souvislosti se zpracováním osobních údajů svých členů, jako správce jejich osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb., nepřijal taková opatření, aby nedošlo k neoprávněnému přístupu k osobním údajům 3299 členů občanského sdružení ke dni 12. prosince 2012 v rozsahu jméno, příjmení, adresa bydliště, telefonní číslo a v některých případech také datum narození, e-mailová adresa, výše měsíčních poplatků a číslo účtu, které byly v době od 27. května 2013 nejpozději do 21. června 2013 zpřístupněny prostřednictvím internetové adresy http://spkfree. freeriderwebhosting.com/index.php, která obsahovala odkaz na databázi členů (http://spkfree. freeriderwebhosting.com/databaze_sql/databaze.htm),

čímž 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 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. v souvislosti se zpřístupněním databáze členské základny občanského sdružení SPKFree.Net na webových stránkách http://spkfree.freeriderwebhosting.com/index.php bylo zahájeno oznámením Úřadu pro ochranu osobních údajů (dále jen „Úřad“), které bylo účastníku řízení, občanskému sdružení SPKFree.Net, doručeno dne 3. června 2013. Podkladem pro zahájení řízení byl anonymní podnět zaslaný Úřadu, který je součástí spisového materiálu.

Součástí oznámení o zahájení správního řízení byla výzva k předložení veškerých dokumentů upravujících podmínky povinností osob při zabezpečení osobních údajů členů občanského sdružení.

Dne 19. června 2013 byla správnímu orgánu doručena odpověď obsahující kopii interní směrnice upravující zacházení s osobními údaji v občanském sdružení SPKFree.Net ze dne 9. února 2008. Směrnice stanovuje pravidla pro zacházení s osobními údaji v rámci občanského sdružení, vymezuje sbírané údaje a zaměřuje se na účel jejich sběru, způsob sběru, uložení a zpracování. Občanské sdružení dle této směrnice zpracovává osobní údaje svých členů v rozsahu jméno, příjmení, adresa (ulice, dům, město, PSČ), číslo telefonu a číslo na mobil, e-mail. Po ukončení členství má člen možnost data o své osobě zrušit nebo ponechat v databázi. Data slouží k prokázání a doložení členské základny, informování členů o skutečnostech souvisejících s chodem sdružení, nalezení bydliště člena pro provedení členem vyžádaného servisního zásahu. Dále je ve směrnici uvedeno, že osobní údaje jsou zpracovávány elektronicky prostřednictvím webového systému. Fyzicky jsou data uložena na webovém serveru SPKFree.Net, jejich zálohování provádí externí společnost zajišťující servis sítě. Přístup k databázovým souborům a exportům tabulek má webmaster a členové komunikační komise, kteří uzavřeli dohodu s občanským sdružením o mlčenlivosti a mají povinnost veškerá data udržovat v tajnosti. Dále má přístup k datům administrátor a smluvní dodavatel, který je na základě servisní smlouvy povinen uchovávat veškerá data v tajnosti. Webový systém umožňuje oprávněným osobám, kterými jsou správci AP, oblastní správci, pracovnice podpory, členové komunikační komise a radní SPKFree.Net, vyhledávat členy, zobrazovat o nich informace, měnit jejich data a zobrazovat statistické přehledy. Oprávněné osoby jsou též vázány uzavřenou dohodou o mlčenlivosti. K zabezpečení osobních údajů směrnice uvádí, že do styku s nimi přichází radní sdružení, pracovnice podpory, oblastní správci a správci, webmaster webového systému a administrátor sítě. Přístup k osobním údajům je sledován a ukládán do databáze. Tyto oprávněné osoby jsou prokazatelně se směrnicí seznámeny a jsou si vědomy, že mohou využívat svěřené funkce a přístupová práva výhradně v souladu s účelem vymezeným touto směrnicí, postup nesmí ohrozit soukromí člena, nesmí předávat získaná data třetím osobám, nesmí kopie databáze uchovávat na úložišti, kam mají přístup i jiné osoby.

Dne 20. června 2013 byla správnímu orgánu doručena žádost právního zástupce účastníka řízení o přerušení správního řízení vedeného s občanským sdružením SPKFree.Net z důvodu prověřování věci Policií České republiky, Krajským ředitelstvím policie Olomouckého kraje, Územním odborem Šumperk, Oddělením hospodářské kriminality SKPV, pod čj. KRPM-69304-70/TČ-2013-140981. Usnesení o přerušení správního řízení bylo vydáno dne 21. června 2013.

Dne 23. května 2014 bylo správnímu orgánu doručeno usnesení o odložení trestní věci podezření ze spáchání přečinu neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1 a 2 písm. a) zákona č. 40/2009 Sb., trestní zákoník, vydané dle § 159a odst. 5 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), které nabylo právní moci dne 18. března 2014. Správní orgán tak pokračoval v přerušeném správním řízení.

Následně byla Policie České republiky požádána o zaslání kopie znaleckého posudku čj. spr. 4127/2005 vypracovaného znalcem Ing. Jiřím Bergerem, který byl přibrán v rámci prověřování výše zmíněné trestní věci. Kopie tohoto posudku byla správnímu orgánu doručena dne 11. června 2014.

V rámci znaleckého posudku provedl znalec analýzu hesel, která uživatelé, kteří měli k serveru přístup, při přihlašování k aplikaci využívali. Ze závěru analýzy vyplynulo, že skutek mohl provést kdokoli s přístupem k databázi. Hesla zde byla uložena v podobě kontrolního součtu MD5 bez tzv. soli, která rozšiřuje heslo do takové podoby, že na výsledný kontrolní součet nelze aplikovat slovníkový útok ani pro něj běžně neexistují připravené tabulky známých kontrolních součtů. Proto je třeba tato hesla považovat za nedostatečně bezpečná vzhledem k jejich malé délce a jednoduchosti.

K heslům lze dále ze znaleckého posudku uvést, že uživatel používal od 17. prosince 2008 do 31. srpna 2009 heslo „martinek“, do 20. června 2013 heslo „6882Mv“. Následně si heslo změnil, ale to se již nepodařilo zjistit. S tímto heslem souvisí seznam pokusů o přihlášení před předmětným útokem, než bylo zadáno správné heslo „6882Mv“. Útočník zkoušel hesla jako „6882mv“, „admin“ a „6882“. Měl tedy o správné podobě hesla představu, pokud se nejednalo pouze o matení stop. Heslo používané … („6882Mv“) bylo dne 5. ledna 2012 panu …, předsedovi občanského sdružení, sděleno prostřednictvím komunikace na sociální síti Facebook. Uživatel, tj. účastník řízení, toto heslo používal nadále, a to až do 20. června 2013.

Dále ze znaleckého posudku vyplývá skutečnost, že v případě, kdy útočník nechtěl využít nechráněné přístupové body, ale chtěl budit dojem, že útok pochází ze sítě, byl pro něj přístupový bod „SPKFree-KOA51“ jedinou volbou. Přístup k tomuto bodu byl jako jediný zabezpečen protokolem WEP, kde zjištění šifrovacího klíče mohlo být provedeno během několika minut za pomoci notebooku nebo výkonného mobilního telefonu. Navíc toto zjištění klíče nemusí zanechat na přístupovém bodu žádné stopy. Další alternativy, tedy že útočník klíč znal nebo jej zjistil z karty člena, byly také možné.

Dne 11. července 2014 bylo správnímu orgánu doručeno vyjádření právního zástupce účastníka řízení, ve kterém uvedl, že účastník řízení není schopen určit, zda osobní údaje zpřístupněné prostřednictvím webových stránek na internetové adrese http://spkfreenetwebhosting.com/index.php, která odkazovala na databázi,

byly osobními údaji jeho členů. Dále se právní zástupce účastníka řízení vyjádřil k přijatým opatřením pro zajištění bezpečnosti zpracování osobních údajů (jak vyplývá ze spisového materiálu, jedná se o opatření přijatá poté, co došlo ke zveřejnění údajů členů účastníka řízení). Pro zabezpečení svých serverů, resp. databází osobních údajů svých členů používá tato opatření: velmi silné heslo o délce 22 znaků kombinujících malá a velká písmena a číslice, při třetím zadání chybného hesla dojde k zablokování internetové adresy na dobu 12 hodin, přístup k databázi je možný pouze přímo ze serveru, tzn., že žádný vzdálený přístup není umožněn a pokus o prolomení hesla je avizován e-mailovou zprávou správcům.

Pro zabezpečení webové stránky účastníka řízení jsou platná tato opatření: přístup k funkcím webové stránky je možný po přihlášení jménem a heslem, na webové stránce jsou zavedeny úrovně práv (správce, oblastní správce, komunikační komise, radní) a každá tato skupina má přístup jen k minimální nutné množině členů (spravovaný vysílač, spravovaná oblast), na webové stránce nejsou data snadno ke stažení, lze tedy jen vyhledat množinu členů a následně jednotlivě vstoupit do karty jednoho člena, každý nositel práv absolvoval minimálně 1x školení správců, kde byl poučen o funkcích webové stránky a o existenci interní směrnice upravující zacházení s osobními údaji v občanském sdružení SPKFree.Net, každý nositel práv v rámci smluvního vztahu (dohoda o provedení práce) minimálně 1x vzal na vědomí a podepsal respektování směrnice o ochraně osobních údajů.

Dále právní zástupce účastníka řízení uvedl, že jeho klient považoval předmětný únik osobních údajů za trestný čin neznámého pachatele, a proto podal trestní oznámení. Výsledkem prověřování Policie České republiky byl zejména závěr, že jednáním popisovaným ve výrokové části tohoto usnesení s největší pravděpodobností došlo ke spáchání přečinu neoprávněného přístupu k počítačovému systému a nosiči informací, avšak nepodařilo se prokázat jaký konkrétní pachatel a jakým způsobem provedl útok na databázi sdružení SPKFree.Net, a dále, že podstatou spáchání přečinu byl přístup přes logovací heslo …, což je očividně cesta, kterou pachatel při svém jednání použil, ale ani přesto nebylo možné určit konkrétního pachatele, který útok provedl.

K porušení povinnosti mlčenlivosti ze strany … právní zástupce účastníka řízení uvedl, že v rámci policejního prověřování bylo zjištěno, že přístupové údaje, konkrétně logovací heslo …, bylo zveřejněno na webových stránkách umístěných na internetové adrese www.obeckoprivna.eu, u nichž je … administrátorem. V této souvislosti je nutné zmínit, že … byl členem komunikační komise účastníka řízení a současně správcem vysílače, když byl v pracovněprávním vztahu k účastníkovi řízení na základě dohody o provedení práce. Současně podepisoval každoročně prohlášení, v němž se zaměstnanec zavazuje dbát na dodržování směrnice občanského sdružení SPKFree.Net. Z těchto skutečností podle právního zástupce účastníka řízení jednoznačně plyne, že … porušil povinnost mlčenlivosti, kterou mu ukládá mj. ustanovení § 15 zákona č. 101/2000 Sb.

Vzhledem ke shora uvedenému má účastník řízení za prokázané, že za správní delikt, který je předmětem tohoto správního řízení, neodpovídá, protože prokázal, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil.

V závěru svého vyjádření právní zástupce účastníka řízení doplnil, že ačkoli se účastník řízení necítí být jakkoli odpovědný ze spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., učinil bezprostředně po zjištění neoprávněného přístupu taková opatření, která již neumožňují přístup k databázi přes logovací údaje …, i když ani tento další přístupové údaje již neobdržel. Dále byla přijata nová opatření spočívající v zablokování přihlašování na dobu 24 hodin po třech špatně zadaných heslech a v poučení všech nositelů práv o existenci směrnice o ochraně osobních údajů a souvisejících povinnostech na letošním školení, přičemž každý nositel práv potvrdil speciálně poučení o důležitosti zajištění důvěrnosti osobních údajů a o nakládání s heslem.

Dne 15. července 2014 si správní orgán vyžádal spisový materiál od Policie České republiky, která prověřovala danou věc jako podezření ze spáchání přečinu neoprávněného přístupu k počítačovému systému a nosiči informací.

Dne 22. července 2014 byl správnímu orgánu doručen spisový materiál, který mj. obsahoval vysvětlení podané na Policii České republiky ze dne 30. května 2013 …. Podle obsahu tohoto vysvětlení … zjistil, že zveřejněný seznam členů je skutečným seznamem odpovídajícím ke dni 12. prosince 2012, když v seznamu chybí nově, tj. od 13. prosince 2012, přihlášení členové. Z této skutečnosti se dá odvodit, že útok neznámým pachatelem byl proveden nejpozději dne 12. prosince 2012. Dne 27. května 2013 byla databáze zpřístupněna veřejnosti. Až dne 30. května 2013, tj. při prvním úkonu u policejního orgánu, se … dozvěděl o úniku osobních údajů členů občanského sdružení. Znepřístupnění webových stránek odkazujících na databázi členů bylo provedeno nejpozději dne 21. června 2013 na základě žádosti podané Policií České republiky Policejnímu prezidiu, které následně zaslalo požadavek zahraničnímu providerovi.

K předmětu řízení lze konstatovat, že zveřejněné údaje členů občanského sdružení SPKFree.Net v rozsahu jméno, příjmení, adresa bydliště, telefonní číslo a v některých případech také datum narození, e-mailová adresa, výše měsíčních poplatků a číslo účtu jsou nepochybně osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť se vztahují k jednoznačně určenému, resp. určitelnému subjektu údajů.

Účastník řízení je správcem osobních údajů svých členů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb., který stanoví, že správcem osobních údajů je každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj. Účelem zpracování osobních údajů v databázi vymezeným účastníkem řízení je prokázání a doložení členské základny, informování členů o skutečnostech souvisejících s chodem sdružení a nalezení bydliště člena pro provedení členem vyžádaného servisního zásahu. Účastník řízení tedy odpovídá za dodržování povinností stanovených pro jejich zpracování zákonem č. 101/2000 Sb. Jednou z těchto povinností je povinnost stanovená v § 13 odst. 1 tohoto zákona, tj. 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.

Za zpracování osobních údajů je podle § 4 písm. e) zákona č. 101/2000 Sb. považována jakákoliv operace nebo soustava operací, které správce nebo

zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace. Osobní údaje členů občanského sdružení SPKFree.Net jsou shromažďovány účastníkem řízení, zpracovávány elektronicky prostřednictvím webového systému, následně jsou uchovávány v elektronické podobě na webovém serveru SPKFree.Net a používány účastníkem řízení pro jím vymezené účely, jedná se tedy o zpracovávání osobních údajů ve smyslu zákona č. 101/2000 Sb.

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, www.nssoud.cz).

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. Účastník řízení tedy 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 předem jakkoliv zobecnit (při současném respektování limitu vyjádřeného v § 2 odst. 4 správního řádu).

Důkazní břemeno se přitom přenáší 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 tedy na základě shora uvedeného posuzoval jednání účastníka řízení z hlediska ustanovení § 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.).

Správní orgán po zhodnocení výše uvedeného dospěl k závěru, že v případě účastníka řízení § 46 odst. 1 zákona č. 101/2000 Sb. nelze aplikovat. V daném případě je správní orgán názoru, že se ze strany účastníka řízení nejednalo o vynaložení maximálně možného úsilí k ochraně osobních údajů (i z následně přijatých bezpečnostních opatření je zřejmé, že si účastník řízení uvědomil nedostatky v jím provedených opatřeních).

Za nedostatečné zajištění bezpečnosti osobních údajů pak správní orgán považuje především formu předání hesla „6882Mv“ …, které se uskutečnilo dne 5. ledna 2012, a to prostřednictvím sociální sítě Facebook, a dobu, po kterou bylo toto heslo účastníkem řízení nadále používáno, konkrétně až do dne 20. června 2013, kdy bylo teprve změněno.

Účastník řízení ve svém vyjádření vyjmenovává přijatá opatření k zabezpečení systému. Ze shromážděného spisového materiálu (zejm. z obsahu znaleckého posudku) je zřejmé, že opatření jako je povinnost dlouhého hesla obsahujícího malá a velká písmena a číslice, zablokování přístupu po třetím špatně zadaném heslu, znemožnění vzdáleného přístupu, avizování pokusu o prolomení hesla e-mailovou zprávou správcům systému, nemožnost stažení celé databáze najednou, ale pouze nahlížení a stáhnutí karty jednotlivých členů, nebyla zavedena v době útoku, ale až následně jako reakce na něj. Některá nedostatečná opatření k zabezpečení v době útoku plynou i přímo ze znaleckého posudku, např. možnost vzdáleného přístupu nebo slabá hesla, kdy heslování bylo prováděno metodou MD5 bez tzv. soli. Naopak nově zavedená hesla, která se musí skládat minimálně z 22 znaků, lze považovat za nadprůměrně bezpečná.

Právní zástupce ve svých vyjádřeních často odkazuje na …, který měl dle jeho tvrzení, porušit povinnost mlčenlivosti, ač jí byl vázán. K tomu správní orgán uvádí, že i když byl … členem komunikační komise občanského sdružení, a i kdyby porušil povinnost mlčenlivosti (např. zveřejněním hesla na webových stránkách www.obeckoprivna.eu), je odpovědným subjektem z hlediska předmětu řízení účastník řízení. Současně je třeba zdůraznit, že právní zástupce účastníka řízení staví svá tvrzení na pouhé domněnce, že daný skutek (tj. zveřejnění databáze členů účastníka řízení) spáchal …, přestože odpovědnost … nebyla policejním orgánem prokázána. Zároveň je třeba oba skutky odlišovat. V předmětném správním řízení je řešena otázka nepřijetí dostatečných opatření, což vedlo ke zveřejnění osobních údajů, nikoli osobní odpovědnost toho, kdo zveřejnění fakticky provedl.

Správní orgán tedy na základě výše uvedeného považuje za prokázané, že účastník řízení porušil jednáním popsaným ve výroku tohoto rozhodnutí § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům nebo k jejich neoprávněnému zpracování.

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.

Při stanovení výše sankce bylo z hlediska závažnosti jednání přihlédnuto jako k přitěžující okolnosti ke skutečnosti, že protiprávní jednání účastníka řízení se týkalo databáze, která obsahovala osobní údaje vysokého počtu dotčených subjektů údajů, a ke skutečnosti, že osobní údaje členů účastníka řízení byly prostřednictvím internetu přístupné v podstatě neomezenému okruhu osob. Další přitěžující okolností, ke které správní orgán přihlédl, byla skutečnost spočívající v porušení základních bezpečnostních pravidel, a to možnost přístupu k databázi bez dostatečného zabezpečení i vzdáleným přístupem a předání hesla (které bylo dále používáno) prostřednictvím komunikace na sociální síti.

Způsob protiprávního jednání účastníka řízení správní orgán nevyhodnotil ani jako přitěžující nebo polehčující okolnost. Účastník řízení se správního deliktu dopustil jednáním, které je popsáno ve výroku tohoto rozhodnutí, tj. nepřijetím opatření k zabezpečení osobních údajů, což je v zásadě obvyklý způsob, kterým je zákon č. 101/2000 Sb. porušován.

Dobu, po kterou byl možný neoprávněný přístup k databázi obsahující osobní údaje (tj. od 27. května 2013 nejdéle do 21. června 2013), správní orgán též nevyhodnotil ani jako polehčující ani jako přitěžující okolnost, protože tato doba nemohla být závislá na aktivní činnosti účastníka řízení (když databáze s osobními údaji jeho členů byla zpřístupněna prostřednictvím webových stránek, nad kterými neměl žádnou kontrolu). Dobu, po kterou účastník řízení nezměnil přístupové heslo poté, co bylo předáno předsedovi občanského sdružení (tj. od 5. ledna 2012 do 20. června 2013), však správní orgán vyhodnotil jako přitěžující okolnost.

Ve vztahu k okolnostem, za nichž bylo protiprávní jednání spácháno, bylo přihlédnuto k tomu, že se Policii České republiky nepodařilo zjistit pachatele trestného činu. Přestože předmětem řízení jsou nedostatečná bezpečnostní opatření, považuje správní orgán za polehčující okolnost skutečnost, že osoba odlišná od účastníka řízení zřejmě záměrně „stáhla“ databázi s osobními údaji a učinila na ní internetový odkaz, na který i písemně prostřednictvím jí k tomu účelu vytvořených webových stránek upozornila. Přijetí patřičných bezpečnostní opatření ex post, považuje správní orgán při stanovení výše sankce též za polehčující okolnost.

Vzhledem k uvedenému byla stanovena sankce v dolní polovině 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, 18. srpna 2014

otisk
úředního
razítka

Vanda Foldová
ředitelka odboru správních činností