Čj. UOOU-04741/13-35

ROZHODNUTÍ

Předseda Úřadu pro ochranu osobních údajů, jako příslušný odvolací orgán podle § 2, § 29 a § 32 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a podle § 10 a § 152 odst. 2 zákona č. 500/2004 Sb., správní řád, rozhodl dne 23. září 2014 podle ustanovení § 152 odst. 5 písm. b) správního řádu, takto:

Rozklad účastníka řízení, občanského sdružení SPKFree.Net, se sídlem Dolnostudénská 1293/8, 787 01 Šumperk, IČ: 26989778, proti rozhodnutí Úřadu pro ochranu osobních údajů čj. UOOU-04741/13-30, ze dne 18. srpna 2014, **se zamítá a napadené rozhodnutí se potvrzuje.**

Odůvodnění

Správní řízení pro podezření ze spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., v souvislosti se zpracováváním osobních údajů svých členů, tím, že účastník řízení jako správce osobních údajů nepřijal taková opatření, aby nedošlo k neoprávněnému přístupu k osobním údajům 3.299 členů sdružení v rozsahu jméno, příjmení, adresa bydliště, telefonní číslo a v některých případech také datum narození, emailová adresa, výše měsíčních poplatků a číslo účtu, které byly zpřístupněny prostřednictvím webových stránek občanského sdružení na adrese http://spkfree.freeriderwebhosting.com/index/php, která obsahuje odkaz na databázi členů (http://spkfree.freeriderwebhosting.com/databaze_sql/databaze.htm), čímž měl porušit povinnost stanovenou v § 13 zákona č. 101/2000 Sb., bylo zahájeno oznámením o zahájení správního řízení ze dne 30. května 2013, které bylo účastníkovi řízení doručeno dne 3. června 2013. Součástí oznámení o zahájení správního řízení byla výzva k předložení veškerých dokumentů upravujících podmínky povinností osob při zabezpečení osobních údajů členů občanského sdružení. Pokladem pro zahájení správního řízení byl podnět ze dne 28. května 2013 zaslaný Úřadu.

Účastník řízení se prostřednictvím svého právního zástupce dopisem ze dne 19. června 2013 vyjádřil, že považuje předmětný únik osobních údajů za trestné činy prozatím neznámého pachatele, neboť podobná aktivita byla zaznamenána a šetřena policejním orgánem již v roce 2012 jako neoprávněný přístup k počítačovému systému a nosiči informací podle ustanovení § 230 odst. 1 zákona č. 40/2009 Sb., trestní zákoník. Součástí vyjádření účastníka řízení byla také interní směrnice upravující zacházení s osobními údaji ze dne 9. února 2008.

Vzhledem k tomu, že účastník řízení podal trestní oznámení pro podezření z pokračování v trestném činu podle § 116 zákona č. 40/2009 Sb., přečin dle § 230 odst. 1 zákona č. 40/2009 Sb., požádal účastník řízení dopisem ze dne 20. června 2013 o přerušení

zahájeného řízení do doby ukončení šetření ze strany policejního orgánu, kterému správní orgán prvního stupně usnesením ze dne 21. června 2013 vyhověl.

Dne 3. září 2013 požádal správní orgán prvního stupně o součinnost Krajské ředitelství policie Olomouckého kraje, které Úřadu zaslalo usnesení ze dne 21. února 2014 o odložení trestní věci podezření ze spáchání přečinu neoprávněný přístup k počítačovému systému a nosiči informací podle § 230 odst. 1, 2a zákona č. 40/2009 Sb. Policejní orgán ve svém usnesení uvádí, že došel k závěru, že jednáním popisovaným ve výrokové části usnesení s největší pravděpodobností došlo ke spáchání přečinu neoprávněný přístup k počítačovému systému a nosiči informací, avšak není možné prokázat, jaký konkrétní pachatel a jakým způsobem provedl útok na databázi účastníka řízení.

Dne 27. května 2014 v rámci součinnosti zaslal policejní orgán správnímu orgánu prvního stupně na jeho žádost znalecký posudek vypracovaný Ing. Jiřím Bergerem, znalcem z oboru kybernetika, odvětví výpočetní technika, k výše uvedenému trestnímu řízení.

Správní orgán prvního stupně vydal dne 18. srpna 2014 na základě shromážděných podkladů rozhodnutí doručené účastníkovi řízení dne 18. srpna 2014 prostřednictvím datové schránky. Tímto rozhodnutím byla účastníkovi řízení za spáchání správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb., kterého se měl dopustit tím, že porušil povinnost stanovenou v § 13 odst. 1 zákona č. 101/2000 Sb., uložena pokuta ve výši 30.000 Kč a dále v souladu s ustanovením § 79 odst. 5 správního řádu povinnost nahradit náklady řízení v paušální výši 1.000 Kč.

V odůvodnění svého rozhodnutí správní orgán prvního stupně konstatoval, že účastník řízení jako správce osobních údajů svých členů odpovídá za dodržování povinností stanovených pro jejich zpracování zákonem a jednou z těchto povinností je i povinnost stanovená v § 13 odst. 1 zákona č. 101/2000 Sb., tedy povinnost přijmout opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztráta, neoprávněným přenosům, k jejich neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Skutková podstata podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. je formulována jako odpovědnost objektivní, tedy odpovědnost za následek. Liberační důvod, jehož naplněním se pachatel správního deliktu může této odpovědnosti zprostit, upravuje § 46 odst. 1 zákona č. 101/2000 Sb. Správní orgán prvního stupně dospěl k závěru, že toto ustanovení nelze na daný případ aplikovat, neboť účastník řízení nedostatečně zajistil bezpečnost osobních údajů, neboť nepřijal taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům nebo jejich neoprávněnému zpracování.

Jak uvádí správní orgán prvního stupně, některá nedostatečná opatření k zabezpečení v době útoku plynou přímo ze znaleckého posudku, například možnost vzdáleného přístupu nebo slabá hesla a heslování metodou MD5 bez tzv. soli. Správní orgán prvního stupně rovněž v této souvislosti zmiňuje způsob předání hesla umožňujícího přístup k databázi …, které se uskutečnilo dne 5. ledna 2012 a to prostřednictvím sociální sítě Facebook. Toto heslo pak bylo nadále beze změny užíváno účastníkem řízení a to až do 20. června 2013, kdy bylo teprve změněno.

Správní orgán prvního stupně tedy na základě výše uvedeného považuje za prokázané, že se účastník řízení svým jednáním popsaným ve výroku jeho rozhodnutí dopustil porušení ustanovení § 13 odst. 1 zákona č. 101/2000 Sb.

Proti rozhodnutí správního orgánu prvního stupně podal účastník řízení prostřednictvím

svého právního zástupce k předsedovi Úřadu rozklad doručený Úřadu dne 3. září 2014. V rozkladu účastník řízení uvádí, že se správní orgán zcela a žádným způsobem ani jednotlivě nezabýval zjištěním, zda se jedná o pravdivé, reálné či skutečné členy občanského sdružení, resp. existující osoby a s tím spojené platné adresy, bydliště, telefonní čísla, emailové adresy a čísla účtů, což pokládá za zákonnou povinnost správního orgánu, přičemž nestačí, že se správní orgán opřel o protokol o podaném vysvětlení před policejním orgánem. Správní orgán prvního stupně podle účastníka řízení pouze obecně konstatuje, že zveřejněné údaje členů občanského sdružení jsou nepochybně osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť se vztahují k jednoznačně určenému, resp. určitelnému subjektu údajů. Tento svůj závěr však správní orgán prvního stupně neodůvodňuje žádným provedeným důkazem, což činí tento jeho závěr nepřezkoumatelným.

Dále účastník řízení ve svém rozkladu konstatuje, že se správní orgán prvního stupně žádným způsobem nezabýval ani nevypořádal s materiálním aspektem správního deliktu, který je jedním ze základních atributů správního deliktu a který se musí vždy prokazovat, a nikoli presumovat. Podle účastníka řízení zcela absentuje zjištění intenzity nebezpečí údajného protiprávného jednání pro společnost.

Odvolací orgán posoudil nejprve včasnost podaného rozkladu a dále pak napadené rozhodnutí, včetně celého spisového materiálu týkajícího se dané věci a dospěl k následujícím závěrům.

Odvolací orgán konstatuje, že dle ustanovení § 50 správního řádu mohou být podkladem pro rozhodnutí správního orgánu mezi jinými podklady od jiných orgánů veřejné moci. Pojem orgán veřejné moci Ústava ČR užívá v čl. 87 odst. 1 písm. d), ovšem závazně ho nedefinuje, proto je jeho definice tvořena pomocí soudního výkladu a doktríny. Subjekt, o jehož právech a povinnostech je takto rozhodováno, není s orgánem veřejné moci v rovnoprávném postavení a obsah rozhodnutí nezávisí na jeho vůli. Podle rozhodnutí Nejvyššího soudu ČR čj. 15 Tdo 574/2006, ze dne 28. června 2006 je Policie ČR orgánem veřejné moci. Z výše uvedeného zcela jednoznačně vyplývá, že správní orgán prvního stupně byl zcela oprávněn užít podkladů policejního orgánu jako podkladu pro vydání svého rozhodnutí. Součástí spisu je i vyjádření znalce v oboru kybernetika, které je v tomto směru dostatečně průkazné.

Účastník řízení ve svém rozkladu zpochybňuje pravost osobních dat svých členů, která byla zveřejněna zpřístupněním databáze osobních údajů, přičemž sám účastník řízení podal trestní oznámení na neznámého pachatele v souvislosti s únikem dat a zpřístupnění osobních údajů o 3.299 členech občanského sdružení SPKFree.Net. V úředním záznamu ze dne 30. května 2013 o podání vysvětlení účastník řízení uvádí, že se s největší pravděpodobností jedná o skutečný seznam členů občanského sdružení. Z uvedeného, a z charakteru a obsahu databáze lze bez pochybností učinit závěr, že jejím předmětem byly skutečně osobní údaje konkrétních fyzických osob, členů účastníka řízení, a že se nejednalo o jakousi vymyšlenou databázi osob, přičemž ani sám účastník řízení alternativně nenabízí vysvětlení toho, o jaké údaje by se mělo jednat, pokud ne o osobní údaje jeho členů.

K materiální stránce správního deliktu odvolací orgán uvádí, že závažnost daného jednání spočívající v míře zásahu do soukromí dotčených osob, kdy u bývalých členů sdružení byly zveřejněny osobní údaje v rozsahu jméno, příjmení, adresa bydliště, telefonní číslo a v některých případech také datum narození, emailová adresa, výše měsíčních poplatků, a to v době od 27. května 2013 nejdéle do 21. června 2013, není v žádném případě zanedbatelná, neboť takto uveřejněné údaje byly na internetu zpřístupněny neomezenému počtu osob. Dále je třeba vzít v úvahu množství osob, jejichž osobní údaje byly neoprávněně uveřejněny. Správní orgán prvního stupně se tak s argumentací účastníka řízení vyrovnal již v napadeném rozhodnutí a jeho závěr tak nelze označit za nepřezkoumatelný.

Odvolací orgán dále uvádí, že dle ustanovení § 46 odst. 1 zákona č. 101/2000 Sb. právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. V daném případě účastník řízení toto maximální úsilí nevynaložil, neboť neučinil dostatečná bezpečnostní opatření, aby zabránil úniku z databáze s osobními údaji svých bývalých členů, což zcela jasně vyplývá ze znaleckého posudku, který je součástí spisu. Soudní znalec v oblasti kybernetika uvádí, že skutek mohl provést kdokoli, kdo měl přístup k databázi členů a dále uvádí, že přístupový bod „SPKFree-KOA51“ je jedinou volbou, jak vzbudit dojem, že útok – získání přístupu k vysílači – pochází ze sítě. Přístup k tomuto bodu byl v době úniku dat zabezpečen protokolem WEP, kde zjištění šifrovacího klíče může být provedeno během několika minut za pomoci notebooku nebo výkonného mobilního telefonu. Soudní znalec konstatuje, že toto zjištění nemusí zanechat na přístupovém bodu žádné stopy. Jako porušení bezpečnostních opatření lze jednoznačně označit předání přístupového hesla … (členem komunikační komise sdružení) panu …, předsedovi sdružení, prostřednictvím sociální sítě Facebook dne 5. ledna 2012, přičemž toto heslo užíval pan … beze změny až do 20. června 2013.

Účastník řízení se tak prokazatelně dopustil správního deliktu nepřijetím opatření k zabezpečení osobních údajů podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb.

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, nelze odvolat.

Praha 23. září 2014

otisk úředního razítka

RNDr. Igor Němec, v. r.
předseda

Za správnost vyhotovení:
Martina Junková