ÚŘAD PRO OCHRANU
OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
(10)

ORIGINÁL

Vypraveno dne 30.1.2014

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 555, fax: 234 665 444
e-mail: posta@uoou.cz, www.uoou.cz

Toto rozhodnutí nabylo právní moci dne 8.2.2014
Úřad pro ochranu osobních údajů
dne 10.2.2014

[redacted]

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ 4

Čj. UOOU-00703/14-2

PŘÍKAZ

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, vydává dne 30. ledna 2014 v souladu s § 150 odst. 1 správního řádu tento příkaz:

Je prokázáno, že účastník řízení: společnost ppm factum a.s., se sídlem K Vypichu 1215, 252 19 Rudná, IČO: 278 83 299, jako správce osobních údajů hostesek podle § 4 písm. j) zákona č. 101/2000 Sb.,

I. tím, že v době, minimálně od 18. června 2013 do 10. září 2013 byly po zadání odkazu v internetovém prohlížeči ve formě http://smlouvy.ppmfactum.cz zpřístupněny osobní údaje 100 hostesek v rozsahu ID osoby, jméno, příjmení, rodné číslo, číslo bankovního účtu,

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,

II. dále tím, že prokazatelně od blíže nezjištěné doby, minimálně do 13. září 2013 nepořizoval v souladu s § 13 odst. 4 písm. c) zákona č. 101/2000 Sb. elektronické záznamy, které by umožnily určit, z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány,

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

v bodech I. a II. 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 40.000 Kč
(slovy čtyřicet 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

Podkladem pro vydání tohoto příkazu je kontrolní protokol čj. UOOU-05294/13-22 ze dne 12. listopadu 2013 a spisový materiál shromážděný v průběhu kontroly provedené u účastníka řízení inspektorem Úřadu pro ochranu osobních údajů (dále jen „Úřad") Mgr. Danielem Rovanem ve dnech 28. srpna až 6. listopadu 2013. Kontrola byla zahájena na základě anonymní stížnosti ze dne 12. června 2013, ve které stěžovatel upozorňuje na možnost volného přístupu k osobním údajům hostesek, včetně dohod o provedení práce prostřednictvím webové stránky http://smlouvy.ppmfactum.cz.

Ze spisového materiálu, zejména z podkladů shromážděných v průběhu kontroly, vyplývá, že účastník řízení v databázi označované jako „databáze našich pracovníků", anebo „databáze subjektů údajů", v informačním systému „POHODA SQL" uchovával osobní údaje subjektů údajů hostesek v rozsahu ID osoby, jméno, příjmení, rodné číslo, adresa, číslo bankovního účtu.

Úřadem bylo dne 18. června 2013 zjištěno, že na webové stránce http://smlouvy.ppmfactum.cz. jsou zpřístupněny osobní údaje 100 subjektů údajů v rozsahu ID osoby, jméno, příjmení, rodné číslo, po umožněném rozkliknutí záložky *upravit údaje*, také adresa, číslo bankovního účtu a datum uzavření smlouvy, neboť podle písemného prohlášení účastníka řízení doručeného Úřadu dne 2. října 2013 v období od 15. května 2013 do 11. září 2013 byl povolen port 80 pro prohlížení internet Exploreru a bylo vypnuto SSL zabezpečení, což umožňovalo přístup do databáze účastníka řízení prostřednictvím webových stránek http://smlouvy.ppmfactum.cz.

Účastník řízení v průběhu ústního jednání a místního šetření, konaného dne 11. září 2013, prohlásil, že předmět kontroly, veřejně dostupná databáze hostesek prostřednictvím webové stránky http://smlouvy.ppmfactum.cz, mu není znám a, že bezprostředně po skončení jednání podnikne příslušné kroky k nápravě a přístup do databáze zablokuje. To bylo Úřadem ověřeno dne 12. září 2013, kdy již přístup na webovou stránku http://smlouvy.ppmfactum.cz nebyl z důvodu hlášení systémové chyby „Network Error (dns_unresolved hostname)" umožněn.

Dále ze spisového materiálu vyplývá, že dopisem ze dne 15. října 2013 byl účastník řízení žádán o zaslání elektronických záznamů (logů) z databáze účastníka řízení za období od 1. do 15 září 2013.

Úřadu byl dne 21. října 2013 doručen výpis elektronických záznamů z období 2.9.2013 do 13.9.2013, ze kterého je patrné kdo (kód uživatele), kdy (datum a čas), počet nových záznamů (vyjádřený číslovkou), počet editovaných záznamů (vyjádřený číslovkou) a soubor včetně přílohy. Výpis neobsahuje elektronický záznam (log) ze dne 10.9.2013, kdy do databáze, obsahující osobní údaje zpřístupněné prostřednictvím webové stránky http://smlouvy.ppmfactum.cz, kontrolující nahlížel. Jména uživatelů, uvedených ve výpisu elektronických záznamů, odpovídají uživatelům uvedeným v seznamu oprávněných osob k zpracování osobních údajů, ze dne 17. září 2013 předloženého účastníkem řízení. Výpis dále neumožňuje určit, z jakého důvodu (např. aktualizace, tisk, editace) byly osobní údaje zaznamenány nebo jinak zpracovány.

Účastník řízení je správcem osobních údajů 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. Účastník řízení v souvislosti s předmětem podnikání a za účelem identifikace smluvní strany, hosteskových kampaní, promo aktivit, merchandisingu zpracovává osobní údaje subjektů údajů (hostesek).

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. Jelikož osobní údaje hostesek byly shromažďovány účastníkem řízení a následně uchovávány v databázi účastníka řízení, jedná se o zpracovávání osobních údajů ve smyslu zákona č. 101/2000 Sb.

Správce osobních údajů je povinen dodržovat při zpracování osobních údajů, 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 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 ustanovení § 13 odst. 4 písm. c) zákona č. 101/2000 Sb. je správce v oblasti automatizovaného zpracování osobních údajů v rámci opatření podle odstavce 1 povinen také pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. V případě automatizovaného zpracování je správce povinen způsoby uvedenými v § 13 odst. 4 pod písm. a) až d) zákona č. 101/2000 Sb., ve vztahu k § 13 odst. 1 téhož zákona zajistit, aby nedošlo k jinému neoprávněnému zneužití osobních údajů.

Povinnosti podle § 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).

Skutková podstata správního deliktu podle § 45 odst. 1 písm. h) zákona č. 101/2000 Sb. je naplněna již v situaci, kdy zpracovávaným osobním údajům hrozí (v důsledku nepřijetí či neprovedení dostatečných organizačních a technických opatření) riziko nesprávného či neoprávněného zpracování. V případě, kdy jsou osobní údaje bez jakéhokoli právního titulu již zpřístupněny třetím osobám, nelze o naplnění uvedené skutkové podstaty pochybovat.

Správní orgán tedy konstatuje, že tím, že předmětná interní databáze byla veřejně přístupná prostřednictvím webových stránek http://smlouvy.ppmfactum.cz a tím, že účastník řízení nepořizoval elektronické záznamy, které by umožnily určit, z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, došlo nepochybně k porušení povinnosti stanovené § 13 odst. 1 zákona č. 101/2000 Sb.

Z písemného vyjádření účastníka řízení, *„Závěr ze šetření č.j: 20131109/24 IT"*, doručeného Úřadu dne 2. října 2013 vyplývá, že účastník řízení uznal svá pochybení, neboť jak sám uvedl *„dne 16.5.2013 v 16:23:12 hod došlo k úspěšnému útoku do sítě ppm factum (u záznamu o přihlášení není zapsána IP adresa). Na adrese http://smlouvy.ppmfactum.cz byl povolen port 80 pro prohlížení internet Exploreru. Dále bylo na této adrese vypnuto SSL zabezpečení, které bylo nastaveno na přihlášení uživatele a uvedení hesla. Jednalo se bohužel o úspěšný útok, ale byla*

učiněna opatření, aby k této situaci již nedošlo. Nastavení ochranného firewallu je nyní na vyšším stupni."

Správní orgán považuje ve smyslu § 150 odst. 1 správního řádu skutkové zjištění za dostatečné a na základě výše uvedeného považuje za prokázané, že účastník řízení porušil svým jednáním povinnost stanovenou v § 13 odst. 1 a odst. 4 písm. c) zákona zákona č. 101/2000 Sb.

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 interní databáze účastníka řízení zpřístupněné na webové stránce http://smlouvy.ppmfactum.cz, která obsahovala osobní údaje minimálně 100 hostesek. Přístup k osobním údajům hostesek byl z hlediska uživatelů internetu jednoduše dosažitelný. Dále bylo přihlédnuto jako k přitěžující okolnosti k tomu, že součástí zpřístupněných údajů u každého subjektu údajů bylo rodné číslo, které od 1. dubna 2004 požívá zvýšené právní ochrany.

Jako skutečnost snižující závažnost jednání účastníka řízení lze hodnotit především to, že účastník řízení po nabytí vědomí o zpřístupněné databáze prostřednictvím webové stránky http://smlouvy.ppmfactum.cz provedl opatření, které webovou stránku zablokovalo. Po souhrnném zhodnocení výše uvedených okolností a s přihlédnutím k nápravě předmětných činností uložil správní orgán sankci 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 § 150 odst. 3 správního řádu lze u inspektora Úřadu pro ochranu osobních údajů, který příkaz vydal, podat proti tomuto příkazu ve lhůtě 8 dnů ode dne oznámení příkazu odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz lze oznámit i jeho doručením účastníku řízení. Příkaz je doručen dnem převzetí stejnopisu, nejpozději však desátým dnem od jeho uložení u provozovatele poštovních služeb. V případě doručování do datové schránky je příkaz doručen

okamžikem přihlášení oprávněné osoby do datové schránky, nejpozději však desátý den ode dne dodání příkazu do datové schránky.

Příkaz, proti němuž nebyl podán odpor, se stává pravomocným a vykonatelným rozhodnutím.

Praha, 30. ledna 2014

ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ PRAHA
INSPEKTOR
-12-

[redacted]

Mgr. Daniel Rovan
inspektor Úřadu pro ochranu osobních údajů