Čj. UOOU-06826/16-3

PŘÍKAZ

Úřad pro ochranu osobních údajů, jako příslušný správní orgán podle § 10 zákona č. 500/2004 Sb., správní řád, a § 2 odst. 2 a § 46 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, vydává dne 20. června 2016 v souladu s § 150 odst. 1 správního řádu tento příkaz:

Je prokázáno, že účastník řízení: …, fyzická osoba podnikající dle živnostenského zákona, se sídlem …, IČ: …, v souvislosti se zpracováním osobních údajů při plnění povinností zaměstnavatele v oblasti mzdové a personální evidence, jako správce osobních údajů svých zaměstnanců podle § 4 písm. j) zákona č. 101/2000 Sb., nezajistil minimálně v období od 19. února 2015 do 1. září 2015 řádnou likvidaci písemností umístěných v e-mailové schránce (…) provozovny …, která obsahovala výplatní pásky, pracovní smlouvy, dohody a výpověď z pracovního poměru s osobními údaji zaměstnanců dané provozovny …, …, …, …, …, …, …, …, …, … a paní …, a dále nezajistil, aby heslo k přihlášení se do e-mailové schránky znal pouze vedoucí provozovny, v důsledku čehož došlo ke zpřístupnění osobních údajů jednotlivých zaměstnanců obsažených ve výše uvedených dokumentech i ostatním zaměstnancům dané provozovny,

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 5.000 Kč
(slovy 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. 19-5825001/0710, variabilní symbol IČO účastníka řízení, konstantní symbol 1148.

Odůvodnění

Podkladem pro vydání příkazu je podnět zaslaný Úřadu pro ochranu osobních údajů (dále jen „Úřad“) a kontrolní protokol čj. UOOU-09858/15-7 ze dne 25. dubna 2016 pořízený podle zákona č. 101/2000 Sb. a zákona č. 255/2012 Sb., o kontrole (kontrolní řád), inspektorem Úřadu MVDr. Františkem Bartošem v rámci kontroly provedené u účastníka řízení ve dnech 4. ledna 2016 až 27. dubna 2016, včetně spisového materiálu shromážděného v průběhu této kontroly.

Z výše uvedeného spisového materiálu vyplývá praxe účetního účastníka řízení …, že personální a mzdové dokumenty včetně výplatních pásek zasílá elektronicky na každou provozovnu prostřednictvím e-mailové zprávy vedoucímu provozovny, v daném případě se jednalo o provozovnu v Jablonci nad Nisou s e-mailovou adresou … . Vedoucí provozovny používá ke komunikaci s účetním služební notebook, který je zaheslován a přístupný pouze danému vedoucímu provozovny. Účastník řízení měl současně přijatou směrnici č. 6 Pravidla pro ochranu osobních údajů, která v bodě 8 uvádí, že přístup do „firemního emailu“ má pouze vedoucí prodejny na základě unikátního osobního hesla. Dále v bodě 12 dané směrnice je stanoveno, že hesla ke vstupu do PC (programů) s personální a mzdovou agendou jsou uložena v zapečetěné obálce u majitele společnosti. Další dokument, který účastník řízení v rámci kontroly předložil, byl dokument týkající se náplně práce vedoucího prodejny (provozovny) a jaké má povinnosti. Bod 15 pracovní náplně se týká zákona o ochraně osobních údajů a stanovuje povinnost vedoucího zabránit přístupu ostatních zaměstnanců do „firemního e-mailu“ a tím zabránit případnému zneužití osobních dat zaměstnanců prodejny, která se na tento e-mail mohou soustřeďovat v souvislosti se zasíláním pracovních smluv, výpovědí a různých potvrzení. Dokumenty obsahující osobní data je povinen vedoucí po vytištění neprodleně smazat.

Ze směrnice, seznamu povinností vedoucího a běžné praxe tedy vyplývá, že měl vedoucí provozovny dokumenty, které mu byly zaslány účetním do elektronické schránky, vytisknout a předat konkrétnímu zaměstnanci, kterému byly adresovány, a okamžitě danou e-mailovou zprávu z e-mailové schránky odstranit. Tuto povinnost ale vedoucí provozovny očividně porušoval. Nejenom že okamžitě e-mailové zprávy neodstraňoval, ale ponechával je v e-mailové schránce i po dobu několika měsíců, což dokládá printscreen obrazovky e-mailové schránky s jednotlivými e-mailovými zprávami, který byl součástí podnětu zaslaného Úřadu. Dále ze shromážděného spisového materiálu vyplývá, že přístup do e-mailové schránky měl v podstatě kterýkoliv ze zaměstnanců, protože vedoucí provozovny neprováděl odhlašování. Dále bylo doloženo, že heslo znal nejenom vedoucí provozovny, ale i zaměstnanci, což je mj. uvedeno ve stížnosti, kterou podali bývalí zaměstnanci (…, …, …, … a vedoucí …) na svého zaměstnavatele k Oblastnímu inspektorátu práce Liberec dne 23. září 2015. To bylo důvodem, že kterýkoli zaměstnanec dané provozovny měl umožněn přístup do e-mailové schránky, která obsahovala výplatní pásky s osobními údaji zaměstnanců …, …, …, …, …, …, …, … a …, a pracovní smlouvy, dohody či výpověď z pracovního poměru …, … a paní … .

K předmětu řízení lze konstatovat, že podle § 4 písm. a) zákona č. 101/2000 Sb. je osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. Osobní údaje obsažené ve výplatních páskách, pracovních smlouvách, dohodách či výpovědích z pracovního poměru jsou tak nepochybně osobními údaji.

Účastník řízení jako správce osobních údajů subjektů údajů, svých zaměstnanců, které shromažďuje při své činnosti, ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. 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. Tato povinnost platí i po ukončení zpracování 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 fyzických osob (zaměstnanců účastníka řízení), které obsahovaly dokumenty v doručené elektronické poště, jsou shromažďovány účastníkem řízení, následně jsou uchovávány a používány účastníkem řízení pro jím vymezené účely (resp. účely vymezené jednotlivými právními předpisy, zvláště předpisy upravující povinnosti zaměstnavatele v oblasti mzdové a personální evidence); 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 v § 45 odst. 1 písm. h) téhož zákona 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 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, při jehož naplnění se právnická osoba může odpovědnosti za správní delikt zprostit. Správní orgán po zhodnocení okolností jednání účastníka řízení dospěl k závěru, že v případě účastníka řízení § 46 odst. 1 zákona č. 101/2000 Sb. nelze aplikovat, a to pro absentující kontrolu jím nastavených pravidel.

Povinností správce je dle § 13 odst. 1 zajistit prostřednictvím vhodných bezpečnostních opatření, aby žádná neoprávněná osoba neměla přístup k osobním údajům, které zpracovává. V daném případě byl zaměstnancům provozovny v Jablonci nad Nisou umožněn přístup do e-mailové schránky, ke které měl znát heslo pouze vedoucí. Účastník řízení měl sice dostatečně upravena pravidla ochrany osobních údajů a k tomu se vztahující povinnosti vedoucího svými interními předpisy,

je ale zřejmé, že dostatečně nezajistil, aby dodržování těchto předpisů bylo pravidelně kontrolováno a vymáháno.
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 zákona č. 101/2000 Sb., tedy povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů, neboť účastník řízení dostatečně nekontroloval dodržování vnitřních předpisů, tj. nezajistil, aby heslo k přihlášení se do e-mailové schránky znal pouze vedoucí a aby vyřízená elektronické pošta s dokumenty obsahujícími osobní údaje zaměstnanců byla okamžitě po vyřízení odstraňována.

Při stanovení výše sankce bylo jako k přitěžující okolnosti přihlédnuto zejména k rozsahu osobních údajů, které byly v doručené elektronické poště obsaženy. Jako polehčující okolnost vyhodnotil správní orgán nízký počet dotčených subjektů a dále skutečnost, že měl účastník řízení dostatečným způsobem upraveny povinnosti interními předpisy, jejichž dodržování však nekontroloval ani nevymáhal. Po posouzení všech shora uvedených skutečností 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 příkazu.

Poučení: V souladu s § 150 odst. 3 správního řádu lze u oddělení správních činností, které příkaz vydalo, proti tomuto příkazu podat ve lhůtě 8 dnů ode dne jeho doručení odpor, kterým se příkaz ruší a řízení pokračuje.

Příkaz je doručen 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 příkazu do datové schránky.

Praha, 20. června 2016

otisk
úředního
razítka

Vanda Foldová
vedoucí oddělení správních činností