Čj. UOOU-07768/16-5

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 13. září 2016 takto:

Je prokázáno, že účastník řízení: Česká republika – Ministerstvo práce a sociálních věcí, se sídlem Na Poříčním právu 1/376, 128 01 Praha 2, IČO: 00551023, v souvislosti se zpracováním osobních údajů přesně nezjištěného počtu žadatelů o sociální dávky a společně posuzovaných osob těchto žadatelů, jako správce jejich osobních údajů podle § 4 písm. j) zákona č. 101/2000 Sb., tím, že při poskytování služeb společností Fujitsu Technology Solutions s.r.o., resp. společností VÍTKOVICE IT SOLUTIONS a.s., nezajistil v období trvání smluvního vztahu, tj. od přistoupení k Prováděcí smlouvě č. 85/2011 dne 15. července 2011 do 31. prosince 2015 průběžnou kontrolu nad nakládáním s produkčními daty, a to osobními údaji minimálně v rozsahu jméno, příjmení, rodné příjmení, datum a místo narození, rodné číslo, adresa bydliště, telefonní číslo, e-mailová adresa, identifikace datové schránky, číslo občanského průkazu, číslo cestovního dokladu, číslo karty sociálního systému, číslo bankovního účtu, a dále citlivými údaji v rozsahu informace o zdravotním stavu žadatelů, které byly zálohovány v externích datových centrech,

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 150.000 Kč
(slovy sto padesát 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 zpracováním osobních údajů žadatelů o sociální dávky a společně posuzovaných osob těchto žadatelů bylo zahájeno oznámením Úřadu pro ochranu osobních údajů (dále jen „Úřad“), které bylo účastníku řízení, České republice – Ministerstvu práce a sociálních věcí, doručeno dne 19. července 2016. Podkladem pro zahájení řízení byl kontrolní protokol čj. UOOU-14181/15-41 ze dne 9. června 2016 a spisový materiál shromážděný v průběhu kontroly provedené u účastníka řízení inspektorkou Úřadu Mgr. et Mgr. Boženou Čajkovou ve dnech 22. prosince 2015 až 9. června 2016.

Součástí oznámení o zahájení správního řízení byla výzva ke sdělení, kolika osob se v době od června 2011 do prosince 2015 týkalo externí zálohování jejich osobních údajů na základě Prováděcí smlouvy č. 85/2011, příp. sdělení přibližného (řádového) počtu. Účastník řízení na tuto žádost správního orgánu nijak nereagoval.

Z kontrolního spisového materiálu vyplývá, že dne 15. července 2011 byla uzavřena mezi účastníkem řízení a společností Fujitsu Technology Solutions s.r.o., IČ: 26115310, Prováděcí smlouva č. 85/2011, kdy předmětem této smlouvy bylo vymezení a poskytnutí licencí a/nebo služeb k produktům Microsoft poskytované společností Fujitsu Solutions s.r.o. účastníku řízení pro jeho informační systém, jehož datová základna byla tvořena centrálním úložištěm, ve kterém se nacházely jednotlivé objekty. Konkrétně se jednalo o úložiště osobních údajů žadatelů o dávky a u některých společně posuzovaných osob těchto žadatelů pro zajištění výplaty nepojistných dávek a dávek státní politiky zaměstnanosti, a to osobní údaje v rozsahu jméno, příjmení, rodné příjmení, datum a místo narození, rodné číslo, adresa bydliště, telefonní číslo, e-mailová adresa, identifikace datové schránky, číslo občanského průkazu, číslo cestovního dokladu, číslo karty sociálního systému, číslo bankovního účtu, a dále i citlivé údaje vypovídající o zdravotním stavu žadatele (tj. zda je zdravotně postižen). Následně bylo uzavřeno k této smlouvě ještě 9 dodatků, kterými byla smlouva rozšířena.

Společnost Fujitsu Solutions s.r.o. plnila předmět dané smlouvy prostřednictvím subdodavatele, a to společnosti VÍTKOVICE IT SOLUTIONS a.s., IČ: 28606582, Prováděcí smlouva včetně dodatků neupravovala postupy při migraci a likvidaci dat při ukončení smluvního vztahu a účastník řízení neměl přístup k záznamům o činnosti se zpracovávanými daty (k tzv. logům). Dále bylo zjištěno, že účastník řízení dodatkem č. 1 uložil společnosti Fujitsu Technology Solutions s.r.o. zřídit datové centrum, což ve skutečnosti realizovala společnost VÍTKOVICE IT SOLUTIONS a.s., která zřídila dvě plnohodnotná a plně zastupitelná geograficky vzdálená datová centra splňující požadavky mezinárodního klasifikačního standardu pro provoz datových center. Dodavatel služby ve smlouvě deklaroval, že datová centra budou po celou dobu užívání koncovým zákazníkem (účastníkem řízení) disponovat opatřeními obsahujícími fyzickou bezpečnost, administraci a správu

informační bezpečnosti systémů, administraci operačního systému, administraci databáze a reporting kvality služeb.

Dále ze spisového materiálu shromážděného v rámci kontroly vyplývá, že účastník řízení prováděl kontroly zpracování a uchovávání dat prostřednictvím odsouhlasení formátů a velikostí dat na předávaných zálohovaných páskách, a to s měsíční pravidelností, přičemž předávaná zálohovaná data neobsahovala tzv. provozní logy umožňující určit kdo, kdy a z jakého důvodu přistupoval ke konkrétním datům. Kontroly logů se prováděly pouze v případě požadavku účastníka řízení na vyhodnocení, přičemž takto se stalo jen jednou, a to za období září až prosinec 2013. V předešlém ani ve zbylém období trvání prováděcí smlouvy účastník řízení o zaslání provozních logů nepožádal. Účastník řízení neměl podle prováděcí smlouvy ani přijatých dodatků přístup k záznamům o činnosti se zpracovávanými daty společností Fujitsu Technology Solutions s.r.o., resp. společností VÍTKOVICE IT SOLUTIONS a.s. v datových centrech, tj. k tzv. logům, tedy účastník řízení neměl průběžnou kontrolu nad nakládáním s produkčními daty zálohovanými v externích datových centrech.

Před ukončením prováděcí smlouvy přijal účastník řízení technicko-organizační opatření, která obsahovala způsob migrace služeb, jenž zajišťovala společnost Fujitsu Technology Solutions s.r.o., do informačního systému účastníka řízení, a současně zabezpečení dat proti jejich zneužití před výmazem a likvidací.

K předmětu řízení lze konstatovat, že údaje zpracovávané v externích datových úložištích účastníka řízení (např. jméno, příjmení, rodné příjmení, datum a místo narození, rodné číslo, adresa bydliště, telefonní číslo, e-mailová adresa, identifikace datové schránky, číslo občanského průkazu, číslo cestovního dokladu, číslo karty sociálního systému, číslo bankovního účtu), jsou údaje vztahující se ke konkrétnímu subjektu údajů a jedná se tak o osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť se týkají určeného resp. určitelného subjektu údajů. Informace o zdravotním stavu je pak citlivým údajem ve smyslu § 4 písm. b) tohoto zákona.

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. Operace, které prováděl správce a na základě smluvního vztahu společnost Fujitsu Technology Solutions s.r.o., resp. společnost VÍTKOVICE IT SOLUTIONS a.s. při zálohování dat v externích datových centrech, lze jednoznačně označit za zpracovávání osobních údajů ve smyslu zákona č. 101/2000 Sb.

Účastník řízení je správcem osobních údajů žadatelů o sociální dávky a společně posuzovaných osob těchto žadatelů 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 datových úložištích bylo plnění úkolů stanovených zvláštními právními předpisy. Současně účastník řízení jako správce

osobních údajů pověřil zpracováním osobních údajů další subjekt, zpracovatele, kterým byla společnost Fujitsu Technology Solutions s.r.o., resp. společnost VÍTKOVICE IT SOLUTIONS a.s. Nicméně i při využití dalších společností pro zpracování osobních údajů účastník řízení odpovídá za dodržování povinností stanovených 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.

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. (ztráta kontroly nad zálohovanými daty 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; z nedostatečné, resp. ze skoro žádné kontroly nad zálohovanými daty po celou dobu trvání smluvního vztahu je zřejmé, že účastník řízení nevynaložil veškeré možné úsilí k tomu, aby měl úplný přehled o tom, kdo, kdy a z jakého důvodu měl přístup k zálohovaným osobním údajům a aby měl i neustálou kontrolu nad těmito zálohovanými osobními údaji v externích úložištích.

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 k délce trvání protiprávního jednání, a dále k tomu, že se jednalo o velký rozsah zpracovávaných osobních včetně citlivých údajů. Další přitěžující okolností, ke které správní orgán přihlédl při stanovení výše sankce, a to bez ohledu na to, že mu účastník řízení nesdělil počet subjektů údajů, jejichž osobní údaje byly zálohovány na externích úložištích, byl počet těchto dotčených subjektů údajů, kdy se dle veřejně známých informací muselo jednat řádově o statisíce osob. Jako k polehčující okolnosti, ke které správní orgán při stanovení výše sankce přihlédl, byla skutečnost, že nedošlo ke zneužití zálohovaných osobních údajů a že likvidace a výmaz veškerých dat po ukončení prováděcí smlouvy proběhl za dostatečných bezpečnostních opatření, které účastník řízení k tomuto účelu přijal.

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.

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 oddělení správních činností proti tomuto rozhodnutí podat ve lhůtě 15 dnů ode dne doručení rozhodnutí rozklad předsedkyni 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, 13. září 2016

otisk
úředního
razítka

Vanda Foldová
vedoucí oddělení správních činností