



Čj. UOOU-05973/16-3

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 4. srpna 2016 v souladu s § 150 odst. 1 správního řádu tento příkaz:

Je prokázáno, že účastník řízení: společnost UNIQA pojišťovna, a.s., se sídlem Evropská 136/810, 160 12 Praha 6, IČO: 49240480 jako správce osobních údajů svých klientů podle § 4 písm. j) zákona č. 101/2000 Sb., v souvislosti s nasazením aktualizované verze klientské internetové aplikace „myUNIQA“, umožnil, že v době od 18. do 19. ledna 2016 mohlo mít přibližně 25 400 klientů využívajících internetovou aplikaci „myUNIQA“ přístup k osobním údajům přibližně 8 900 dalších klientů obsažených v interní databázi pojistných smluv, a to v rozsahu jméno, příjmení, datum narození, rodné číslo, adresa, telefonní číslo, e-mailová adresa a další informace vztahující se k pojistné smlouvě (např. číslo pojistné smlouvy, datum vzniku škodné události, výše škody, pojistné apod.),

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 135.000 Kč
(slovy sto třicet 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 tohoto příkazu je protokol o kontrole čj. UOOU-00745/16-12 ze dne 15. dubna 2016, pořízený podle zákona č. 101/2000 Sb. a zákona č. 255/2012 Sb. o kontrole (kontrolní řád), inspektorem Úřadu pro ochranu osobních údajů (dále jen „Úřad“) Mgr. Danielem Rovanem v rámci kontroly provedené u účastníka řízení ve dnech 9. února 2016 až 15. dubna 2016 a spisový materiál shromážděný v rámci této kontroly.

Ze spisového materiálu vyplývá, že důvodem pro zahájení kontroly účastníka řízení byl podnět ze dne 19. ledna 2016, který je součástí spisového materiálu a dle kterého bylo prostřednictvím klientské aplikace myUNIQA možné nahlížet do náhodných smluv a škodných událostí jiných klientů obsahující jejich osobní údaje, např. rodné číslo. Přílohou daného podnětu byly snímky obrazovky (screenshot), které dokládají, že uvedené osobní údaje bylo možné prohlížet.

Ze spisového materiálu vyplývá, že předmětem podnikání účastníka řízení je mimo jiné pojišťovací činnost ve smyslu § 3 odst. 1 písm. f) zákona č. 277/2009 Sb. o pojišťovnictví.

Ze spisového materiálu je zřejmé, že klientům společnosti UNIQA pojišťovna, a.s., byla dostupná prostřednictvím internetové aplikace myUNIQA v době od 18. ledna 2016 do 19. ledna 2016 interní databáze pojistných smluv klientů účastníka řízení obsahující osobní údaje klientů účastníka řízení. Ze spisového materiálu dále vyplývá, že účastník řízení měl v přímém vztahu k předmětu řízení uzavřeny smlouvy se společností InsData, spol. s r.o., se sídlem Palárikova 3, 949 01 Nitra, IČO: 34145311. S touto společností měl účastník řízení uzavřeny 3 smlouvy, a to: Rámcovou smlouvu o zpracování osobních údajů ze dne 24. března 2011, která obsahuje konkrétní ujednání o organizačním zajištění spolupráce a záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů, Rámcovou smlouvu o důvěrnosti informací a povinnosti mlčenlivosti ze dne 9. listopadu 2010 a Rámcovou smlouvu o bezpečnostním zajištění smluvní spolupráce ze dne 14. května 2013. V oblasti zajištění bezpečnosti informací v rámci UNIQA pojišťovna, a.s., má účastník řízení přijaty 3 interní dokumenty a to: Řád č. 019/2011/EU Bezpečnostní politika, který je závazný pro všechny zaměstnance účastníka řízení, včetně externích zaměstnanců a pracovníků externích služeb, Směrnici č. 213/20111/EU Bezpečnostní provozní směrnice, která definuje základní rámec pro řízení a zajištění bezpečnosti informací, a Směrnici č. 212/2011/EU k řízení přístupu, definující pravidla pro řízení logického přístupu k prostředkům pro zpracování informací.

Dne 17. února 2016 v průběhu ústního jednání a místního šetření předložil účastník řízení dokument označený jako „Mechanismus vzniku problému“, který obsahuje přesný výčet událostí ze dne 18. až 27. ledna 2016, kdy byla aplikace opět uvedena do provozu, který mimo jiné uvádí: dne 18. ledna 2016 – žádost o nasazení aplikace

myUNIQA verze 2.4.8 na produkční prostředí pro klienty, ve 20:15 provedená kontrola dat s výsledkem OK. Dne 19. ledna 2016 cca od 9:00 probíhalo rozesílání e-mailů s informací, že potvrzení za rok 2015 je dostupné klientům v aplikaci myUNIQA. V 11:41 odeslán společností InsData, spol. s r.o., e-mail s upozorněním na očekávaný zvýšení provoz aplikace. Ve 12:05 hlášení od operátorů z CC Liberec, že je kontaktoval klient s tím, že vidí v aplikaci myUNIQA cizí škody, operátoři následně postupovali podle manuálu k aplikaci myUNIQA. Ve 12:10 ověření pravdivosti hlášení a otestování na soukromém účtu správce myUNIQA s pozitivním nálezem, kontaktován zástupce společnosti InsData, spol. s r.o., s požadavkem na okamžité zastavení aplikace a sdělení předběžných nálezů. Ve 12:40 zpětný kontakt od společnosti InsData, spol. s r.o., s tím, že vracejí předchozí verzi aplikace, následně úspěšně otestováno a znovu spuštěno. Společnost InsData, spol. s r.o., informovala, že v aplikaci myUNIQA bylo 10krát více klientů, než je běžné, ve vztahu k velikosti logu byl nárůst dokonce 1400 %, administrátorské prostředí fungovalo korektně. V 15:30 po vyčištění disku nasazena na produkční prostředí opět verze 2.4.8 a otestována společností InsData, spol. s r.o., s výsledkem OK. V 18:20 otestováno produkční prostředí správcem aplikace s výsledkem OK. V 19:30 přijato na adresu myuniqa@uniqa.cz hlášení od klienta, že vidí cizí škody, následně ověřeno správcem aplikace s pozitivním nálezem, okamžité informování společnosti InsData, spol. s r.o., a vypnutí aplikace. Dne 20. ledna 2016 je aplikace stále vypnuta, podařilo se reprodukovat chybu na administrátorském prostředí. Dne 21. ledna 2016 chyba byla reprodukována i na produkčním prostředí (to bylo pro uživatele blokováno, přístup měli pouze testeři aplikace). Dne 22. ledna 2016 byla připravena oprava programového kódu. Dne 25. ledna 2016 dokončeny testy a kontrola programového kódu. Dne 26. ledna 2016 opravená verze 2.4.8p1 aplikace myUNIQA připravena k nasazení, proběhlo akceptační testování. Dne 27. ledna 2016 v 7:00 byla aplikace opět uvedena do provozu pro klienty.

Z písemného vyjádření účastníka řízení ze dne 22. února 2016 vyplývá, že aplikace my UNIQA byla uvedena do provozu dne 5. června 2013. Aktualizovaná verze aplikace 2.4.8 se závadou, která umožňovala přístup k datům klientů účastníka řízení, byla nasazena dne 18. ledna 2016. Po zjištění závady byla aplikace dne 19. února 2016 večer zablokována a to až do odstranění chyby. Účastník řízení dále uvedl, že postup k získání přístupu k datům jiných klientů byl složitý a byl tedy možný pouze po provedení na sebe navazujících kroků. Jak dále uvádí, nejprve se musel přihlásit klient se škodou (A), po něm klient bez škody (B). Klient A musel nechat zobrazit svůj seznam škod, krátce po něm musel klient B nechat zobrazit seznam škod. Pouze v tomto případě získal klient B pohled na škodu klienta A. Poté musel zadat prohlížení smlouvy vázané k této škodě. Dne 19. února 2016 bylo v databázi 34 356 klientů, z nichž 8 915 mělo evidovanou škodní událost. Tento přístup byl teoreticky umožněn všem klientům, kteří mají přístup a neměli škodu. Teoreticky by tak k tomuto dni byl umožněn přístup 25 441 klientům.

V předmětném vyjádření účastník řízení dále uvedl, že dne 18. ledna 2016 bylo do prohlížení škod přihlášeno celkem 83 klientů, z toho 36 klientů mělo evidovanou škodní událost. Dne 19. ledna 2016 bylo do prohlížení škod přihlášeno 234 klientů, z nich 18 mělo evidovanou škodní událost. Teoreticky tak mohlo dojít ke kompromitaci dat u 54 klientů, přičemž ke dni písemného vyjádření jsou účastníkovi řízení známy 3 případy, kdy k tomu došlo. Účastník řízení dále popsal opatření, která přijal pro napravení vzniklé situace s cílem zajištění maximální bezpečnosti dat, a to ve spolupráci s dodavatelem aplikace společností InsData,

spol. s r.o. Jednalo se o následující opatření: dne 19. ledna 2016 cca v 19:40 bylo na adresu myuniqua@uniqua.cz přijato hlášení od klienta (...), že vidí cizí škody – ověřeno správcem aplikace s pozitivním nálezem – okamžité informování dodavatele – společnost Ins Data, spol. s r.o., telefonicky a vypnutí aplikace přes Administrátorské prostředí. Na webové stránce účastníka řízení bylo umístěno hlášení „aplikace je z technických důvodů mimo provoz“. Dne 20. ledna 2016 byla aplikace stále vypnuta, podařilo se reprodukovat chybu na administrátorském prostředí UNIQA. Dne 21. ledna 2016 byla chyba reprodukována i na produkčním prostředí (to bylo pro uživatele blokováno, přístup měli pouze testeři z koncernové společnosti InsData, spol. s r.o.). Dne 22. ledna 2016 byla připravena oprava kódu. Dne 25. ledna 2016 byly dokončeny testy a kontrola programového kódu Bezpečnostním oddělením koncernu UNIQA. Dne 27. ledna 2016 v 7:00 byla aplikace opět zpřístupněna pro klienty.

K předmětu řízení lze konstatovat, že údaje klientů v rozsahu jméno, příjmení, datum narození, rodné číslo, pohlaví, e-mailová adresa, telefonní číslo a další informace vztahující se k pojistné smlouvě klienta (např. číslo pojistné smlouvy, datum vzniku škodné události, výše škody, pojistné apod.) jsou nepochybně osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb., neboť se vztahují k jednoznačně určenému, resp. určitému subjektu údajů.

Účastník řízení je správcem osobních údajů svých klientů ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. Tyto údaje, včetně údajů uživatelů aplikace myUNIQA, zpracovává v souvislosti s předmětem své činnosti, kterým je mimo jiné pojišťovací činnost ve smyslu § 3 odst. 1 písm. f) zákona č. 277/2009 Sb., o pojišťovnictví. Účastník řízení tedy, jako správce osobních údajů, odpovídá za dodržování povinností stanovených pro jejich zpracování zákonem č. 101/2000 Sb.

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 klientů jsou shromažďovány účastníkem řízení a následně uchovávány v databázi vedeném účastníkem řízení, jedná se o zpracování 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.

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).

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, což je v dané věci nepochybné, nelze o naplnění uvedené skutkové podstaty pochybovat.

Z vyjádření účastníka řízení ze dne 22. února 2016 je zřejmé, že minimálně 3 klienti účastníka řízení vstoupili do databáze s osobními údaji klientů, kdy bylo možné si dané údaje prohlédnout, teoreticky pak dále uložit, popř. vytisknout prostřednictvím tiskárny. Dále je pak zřejmé, že potenciální riziko neoprávněného přístupu do interní databáze účastníka řízení s osobními údaji klientů hrozilo i v případě dalších klientů společnosti UNIQA pojišťovna, a.s., kteří využívají internetovou aplikaci myUNIQA, přičemž se mohlo jednat teoreticky o 25 441 klientů a ohroženy byly osobní údaje 8 915 klientů (viz vyjádření účastníka řízení ze dne 22. února 2016).

Správní orgán se neztotožňuje s tvrzením účastníka řízení obsaženým ve vyjádření ze dne 22. února 2016, že kompromitace klientských údajů (resp. přístup k osobním údajům prostřednictvím aplikace myUNIQA obsažených v databázi účastníka řízení) byla složitá, a to i vzhledem k počtu klientů (tedy 3), kteří v poměrně krátké době (tj. za dobu 2 dnů) vstoupili do dané databáze, jak vyplývá z vyjádření účastníka řízení. Je sice pravdou, že se jednalo o do určité míry nestandardní kroky, nicméně jejich sousled nepostrádal určitou logičnost. Už pouze tím, že klienti měli přístup k předmětným osobním údajům, mohlo dojít k jejich následnému zneužití, popř. jinému neoprávněnému zpracování.

Správní orgán tedy konstatuje, že tím, že osobní údaje klientů byly způsobem, který je popsán výše, přístupné i jiným klientům účastníka řízení, došlo nepochybně k porušení povinnosti stanovené § 13 odst. 1 zákona č. 101/2000 Sb.

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.

Správní orgán se zabýval možností uplatnění liberace a tedy ustanovení § 46 odst. 1 zákona č. 101/2000 Sb., které je formulováno tak, že právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila. Posuzování naplnění liberačního ustanovení je přitom závislé vždy na konkrétních okolnostech daného případu a nelze jej dle názoru správního orgánu jakkoliv předem 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 navrhnout důkazy (srov. Mates P. a kolektiv: Základy správního práva trestního, 3. vydání, Praha: C.H. Beck, 2002, str. 12; dále také § 52 správního řádu).

Vzhledem k výše uvedenému a po zhodnocení všech zjištěných skutečností došel tedy správní orgán k závěru, že účastník řízení v daném případě nevynaložil veškeré úsilí, aby porušení své právní povinnosti spočívající v zabezpečení zpracovávaných údajů (§ 13 odst. 1 zákona č. 101/2000 Sb.) zabránil. Konkrétní podobu takového zabezpečení sice zákonodárce ponechal na správci, stanovil však, před čím vším je třeba osobní údaje chránit. Povinnost vyplývající z tohoto ustanovení klade na správce vysoké nároky spočívající ve vyhodnocování všech možných rizik, která jsou s jeho činností spojena, což v sobě zahrnuje i přehodnocování opatření přijatých k ochraně osobních údajů, neboť rozvoj technologií a vývoj okolností má stoupající tendenci. I přes účastníkem řízení přijatou bezpečnostní dokumentaci k zajištění bezpečnosti zpracovávaných dat a testování aplikace došlo k závažnému ohrožení, co se týká rozsahu a počtu dotčených subjektů. Skutečnost, že primárním původcem chyby v aplikaci nebyl účastník řízení, ale třetí osoba, musí být předmětem řešení v rámci soukromoprávního vztahu mezi těmito společnostmi, nikoli správního řízení vedeného Úřadem.

Z vyjádření účastníka řízení ze dne 22. února 2016 vyplývá, že v rámci svých stanovených procesů přijal okamžitě po zjištění problému odpovídající nápravná opatření, která zamezila dalšímu možnému neoprávněnému přístupu k osobním údajům. Ve vztahu k přijatým opatřením učiněným účastníkem řízení po zjištění možnosti neoprávněného přístupu do interní databáze lze konstatovat, že byly včasné a dostatečné, jak vyplývá z dokumentu označeného jako „Mechanismus vzniku problému“ předložené účastníkem řízení dne 17. února 2016 v průběhu ústního jednání a místního šetření. Následné zajištění bezpečnosti ohrožených osobních údajů však nelze považovat za naplnění liberačního ustanovení, které je popsáno výše. K přijetí opatření k zamezení dalšímu možnému úniku dat však přihlédl správní orgán při stanovení výše sankce (viz níže).

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 § 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 interní databáze, která obsahovala osobní údaje vysokého počtu dotčených subjektů údajů (ohroženy byly osobní údaje více než 25 000 osob), a počtu osob, které se s osobními údaji zájemců potenciálně mohly seznámit. Dále bylo přihlédnuto jako k přitěžující okolnosti k rozsahu osobních údajů, které byly protiprávním jednáním účastníka řízení ohroženy, a k tomu, že součástí těchto údajů byla také rodná čísla jako obecný identifikátor občanů.

Následek protiprávního jednání účastníka řízení spočívající v ohrožení osobních údajů potencionálně 54 zájemců o penzijní produkty a v neoprávněném přístupu tří osob do interní databáze účastníka řízení obsahující jejich osobní údaje správní orgán posoudil jako přitěžující okolnost.

Způsob protiprávního jednání účastníka řízení správní orgán nevyhodnotil 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.

Ve vztahu k okolnostem, za nichž bylo protiprávní jednání spácháno, bylo přihlédnuto, jako k polehčující okolnosti, k tomu, že před zahájením používání dané aplikace byla testována, ačkoliv nedošlo k odhalení dané chyby. Dobu, po kterou byl možný neoprávněný přístup k osobním údajům (tj. doba několik hodin v průběhu dvou dnů), správní orgán vyhodnotil také jako polehčující okolnost. Dále posoudil správní orgán jako polehčující okolnost rychlost reakce účastník řízení po zjištění chyby a přijetí opatření k zajištění okamžité nápravy závadného stavu. Dále pak správní orgán posoudil jako polehčující okolnost i to, že přístup k osobním údajům jiných klientů účastníka řízení nebyl z hlediska posloupnosti kroků potřebných k získání přístupu zcela obvyklý.

Vzhledem k uvedenému byla stanovena 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, 4. srpna 2016

otisk
úředního
razítka

Vanda Foldová v. r.
vedoucí oddělení správních činností

Za správnost vyhotovení:
Klára Truhlářová