

Č. j. 5060/1956/04-RKP/1664/04-OLP
(týká se č. j. 34/04/SŘ-OSR)

V Praze 28. února 2005
Výtisk č. 1

Hlavní město Praha
Mariánské nám. 2
110 01 PRAHA 1 – Staré Město

R o z h o d n u t í

Předseda Úřadu pro ochranu osobních údajů, jako odvolací orgán věcně a místně příslušný podle § 2, § 28, § 29 a § 32 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, § 5 odst. 1 zákona č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů (dále jen „správní řád“), a podle § 61 odst. 2 a § 59 odst. 2 správního řádu rozhodl

takto:

Rozklad účastníka řízení, Hlavní město Praha, se sídlem Mariánské nám. 2, 110 01 Praha 1, proti rozhodnutí odboru správních činností Úřadu pro ochranu osobních údajů č. j. 34/04/SŘ-OSR ze dne 16. prosince 2004, kterým byla uložena za porušení § 13 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, a tedy za správní delikt podle § 46 odst. 1 zákona o ochraně osobních údajů pokuta ve výši 40 000,- Kč (čtyřicet tisíc korun českých) **se zamítá a napadené rozhodnutí se potvrzuje.**

Odůvodnění:

V listopadu roku 2003 byla zahájena kontrola Hlavního města Prahy zaměřená na dodržování povinností stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (dále jen zákon o ochraně osobních údajů) při zpracování osobních údajů evidence obyvatel podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů, v samostatné i přenesené působnosti Hlavního města Prahy. Kontrola zahrnovala zpracování osobních údajů evidence Hlavním městem Prahou jako uživatelem i zpracovatelem podle zákona č. 133/2000 Sb. Tato kontrola byla ukončena kontrolním protokolem, který Hlavní město Praha převzalo dne 16. dubna 2004, což také stvrdilo svým podpisem na kontrolním protokolu. Výsledkem kontroly bylo konstatování, že Hlavní město Praha porušilo svoji povinnost podle § 13 zákona o ochraně osobních údajů tím, že organizovalo zpracování informačního systému Magistrátu tak, že umožňuje zpracování osobních údajů evidence obyvatel i k jiným, než zvláštními zákony stanoveným účelům a v rozsahu větším než nezbytném pro dosažení účelu, k němuž podle zákona osobní údaje evidence obyvatel zpracovává a také, že nepokrylo v dostatečné míře významné bezpečnostní riziko neoprávněného přístupu vlastních zaměstnanců k osobním údajům evidence obyvatel spočívající v užívání aplikací,

tak jak v kontrolním protokolu bylo zjištěno. Proti kontrolnímu protokolu nebyly vzneseny námitky. Na základě výsledků kontroly zahájil Úřad pro ochranu osobních údajů (odbor správních činností) svým podáním ze dne 13. července 2004 správní řízení, neboť na základě výsledků kontroly byl odůvodněn závěr, kdy došlo ke spáchání správního deliktu podle § 46 odst. 1 zákona o ochraně osobních údajů, a to porušením povinnosti stanovené v § 13 téhož zákona. Podkladem pro zahájení správního řízení byl právě písemný materiál, který byl shromážděn v rámci kontroly inspektorkou Úřadu pro ochranu osobních údajů (dále jen „Úřad“). V průběhu správního řízení vzal správní orgán za prokázané, a to ze shromážděné podkladové dokumentace, že došlo k porušení zákona o ochraně osobních údajů a uložil finanční sankci. Vzal za prokázané a vyplývající ze spisového materiálu, že Hlavní město Praha (dále jen „účastník řízení“) za účelem výkonu práv a povinností uložených mu zákonem č. 133/2000 Sb. a dalšími právními předpisy jako zpracovatel i uživatel osobních údajů evidence obyvatel ve smyslu tohoto zákona systematicky provádí soubor operací naplňující znaky zpracování osobních údajů ve smyslu § 4 písm. e) zákona o ochraně osobních údajů. Tyto operace jsou a byly prováděny v návaznosti na příslušné právní předpisy na pokyny a rozhodnutí věcně příslušných orgánů státní správy, tj. Ministerstva dopravy a Ministerstva vnitra, jakožto správců evidence řidičů a registru motorových a přípojných vozidel, resp. evidence obyvatel a dále podle vlastního rozhodnutí účastníka řízení a jsou založeny na přebírání osobních údajů z evidence obyvatel do jiných informačních systémů. Osobní údaje z evidence obyvatel jsou účastníkem řízení zpracovávány v informačním systému správních a dopravně správních evidencí Ministerstva vnitra ČR a v dalších aplikacích, z nichž nejpodstatnější aplikací, do které jsou údaje získávány z informačního systému obyvatel, je tzv. okresní registr obyvatel. Správní orgán vzal za prokázané a za kontrolou a podklady z ní dostatečně doložené, že v rámci jednotlivých zpracování byly v různých typech evidencí, resp. z nich čerpány a využívány údaje, jejichž účel a oprávněnost takového čerpání nebyla v průběhu kontroly doložena, když toto se týkalo zejména tzv. registru dopravně správních agend a také, že je nezpochybnitelným způsobem prokázáno, že další specializovaný subsystém, tzv. okresní registr obyvatel, v němž se vyskytují a do něhož jsou z evidence obyvatel přenášeny všechny údaje o obyvatelích hlavního města Prahy, nemá takovou charakteristiku bezpečnosti, která by vzhledem ke svému rozsahu a možnosti „všeobecného využívání“ zaměstnanci účastníka řízení nastavovala takové bezpečnostní parametry, aby na základě nich bylo možno posoudit, zda tento registr je využíván v souladu se zákony, resp. aby bylo jisté, že nemůže dojít k neoprávněným nebo nahodilým přístupům k osobním údajům v tomto registru uvedených, případně k jejich zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Po zvážení všech podkladů došel správní orgán k závěru, že k porušení zákona o ochraně osobních údajů došlo a uložil sankci na samé spodní hranici zákonné sazby. Ve své úvaze o výši sankce se řídil tím, že je zřejmé, že zpracování osobních údajů účastníkem řízení v předmětných agendách je do značné míry prováděno v návaznosti na postupy jiných správců evidence, zejména Ministerstva vnitra nebo podle jeho metodických pokynů, které účastníka řízení při výkonu jeho působnosti limitují, avšak ani tato skutečnost nemůže účastníka řízení zbavit odpovědnosti za toto zpracování. V odůvodnění dále správní orgán uvádí, že dotčené postupy při zpracování osobních údajů při výkonu státní správy jsou ne zcela dostatečně právně upraveny, současně však bylo zhodnoceno množství a rozsah osobních údajů, které účastník řízení v souvislosti s organizováním a provozováním informačního systému evidence obyvatel zpracovává a které jsou tedy potenciálně ohroženy.

Toto rozhodnutí o uložení sankce bylo účastníku řízení doručeno 20. 12. 2004. Proti rozhodnutí o uložení sankce podal účastník řízení v zákonné lhůtě rozklad, který byl Úřadu doručen dne 30. 12. 2004. Ve svém rozkladu účastník řízení odmítá tvrzení, že nepřijal 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 tak, jak je uvedeno ve výroku napadeného rozhodnutí a vyjadřuje přesvědčení, že i v případě kontroly a

následného rozhodování správního orgánu jde především o subjektivní výklad, ať kontrolujících či rozhodujících osob. Uvádí, že odůvodnění napadeného rozhodnutí se otázce vlastního porušení povinností věnuje pouze okrajově a z větší části se věnuje otázkám právní subjektivity účastníka řízení či shrnuje jednotlivé procesní úkony. Dále s odvoláním na odůvodnění rozhodnutí orgánu prvního stupně uvádí skutečnosti, resp. namítá, že v průběhu správního řízení již nebyly prováděny žádné specializované kontroly a dále uvádí, že po nahlédnutí do spisu se žádný takový důkaz ve spise nenachází a trvá na tom, že kontrola práce s osobními údaji je v úrovni Magistrátu hlavního města Prahy prováděna, což je podle něj dostatečně dokladováno. Cituje ustanovení zvláštních zákonů, tedy zejména zákon č. 133/2000 Sb., o evidenci obyvatel a jeho ustanovení § 8 odst. 2, které stanoví povinnost subjektů, které získávají osobní údaje z informačního systému evidence obyvatel, uvádí, že povinnost zachovávat mlčenlivost je dodržována a že jsou respektována všechna ustanovení zvláštních právních předpisů, tedy i v případě využívání evidencí podle zákona č. 56/2001 Sb. a zákona č. 361/2000 Sb. Dále se v rozkladu speciálně věnuje dokladování přístupů jednoho z pracovníků odboru dopravně správních agend, jehož činnosti spočívající ve využívání evidencí byly speciálně zmíněny v kontrolním protokolu a v přílohách dokládá a na příkladech uvádí, že příslušné přístupy do specializované evidence byl citovaný pracovník oprávněn činit a že pro to měl i právní důvod. Dále namítá formulaci napadeného rozhodnutí „každý zaměstnanec s příslušnými přístupovými právy“ a k této formulaci uvádí, že je v zásadě zjednodušující a zdůrazňuje propojenost přístupových práv s kompetencemi podle právních předpisů, jako je tomu v případě pracovníků odboru dopravně správních agend v souvislosti s povinností mlčenlivosti podle zákoníku práce, dalších právních předpisů, vnitřních norem i náplně činnosti. Uvádí dále, že výše uvedeným přístupovým osobním heslem (právy) je limitován přístup pracovníka do příslušné evidence, což bylo v kontrole a i v rámci správního řízení dokladováno. Svůj rozklad pak uzavírá názorem, že nepovažuje za prokázané spáchání správního deliktu porušením povinnosti stanovené v § 13 zákona o ochraně osobních údajů a uzavírá, že nelze dovodit, že by účastník řízení nepřijal zákonem požadovaná opatření k ochraně osobních údajů. Rozklad pak uzavírá v zásadě námitkou proti výši sankce, i když si je vědom, že je uložena při samé spodní hranici možného rozpětí a že orgán prvního stupně vzal v úvahu při stanovení její výše objem agendy a návaznost na postupy a zpracování, které ne vždy může on sám ovlivnit, když zmiňuje zejména informační systém spravovaný Ministerstvem vnitra. A je přesvědčen, že i kdyby odvolací orgán vzal za prokázané porušení povinností stanovených účastníku řízení při ochraně osobních údajů, je zde přesto důvod, aby zvážil možnost případného snížení sankce, neboť v rámci Magistrátu hlavního města Prahy je této problematice, tedy ochraně osobních údajů při jejich zpracování, věnována značná pozornost. Svůj rozklad pak účastník řízení doplnil ještě přípisem ze dne 28. prosince 2004, který byl Úřadu doručen 7. ledna 2005. V tomto přípisu předkládá vyjádření nadřízených některých pracovníků (kteří jsou zmiňováni v kontrolním protokolu a která se týká práce s osobními údaji v odboru dopravně správních agend), jež mají zjevně dokumentovat, že účastník řízení věnuje ochraně osobních údajů při jejich zpracování velkou pozornost.

Odvolací orgán prozkoumal a posoudil úplný spis správního řízení, a to včetně spisu kontrolního, který je podkladem a důkazním prostředkem pro správní řízení a který obsahuje drtivou většinu dokumentace a zajištěných materiálů, které se k naříkanému případu vztahují. Po posouzení všech důkazů, podkladů a předkládaných tvrzení uvážil k dané věci takto.

Hlavní město Praha – Magistrát jako jeho orgán provádí k plnění úkolů uložených mu zákonem o evidenci obyvatel a v rámci oprávnění svěřených mu tímž zákonem a zákonem o hlavním městě Praze k plnění úkolů uložených mu dalšími zákony s osobními údaji evidence obyvatel svým jménem systematicky soubor operací, naplňující pojmové znaky zpracování podle § 4 písm. e) zákona o ochraně osobních údajů. Tyto operace jsou organizačně uspořádány zčásti podle ustanovení věcně příslušných předpisů, zčásti podle rozhodnutí Ministerstva dopravy a Ministerstva vnitra a ve zbývajícím z vlastního rozhodnutí

kontrolovaného a jsou založeny na vytěžování a přebírání údajů evidence obyvatel z informačního systému, v němž Ministerstvo vnitra vede osobní údaje evidence obyvatel. Tyto operace vytvářejí funkční celky v několika izolovaně provozovaných částech informačního systému Magistrátu. Účastník řízení provádí s osobními údaji evidence obyvatel zejména operace shromažďování, ukládání na nosiče informací, zpřístupňování, úpravu, uchovávání, vyhledávání a používání.

Osobní údaje evidence obyvatel jsou zpracovávány:

a) v IISSDE (Informační systém správních a dopravně správních evidencí Ministerstva vnitra):

- informační systém evidence obyvatel,
- registr motorových a přípojných vozidel
- evidence řidičů a přestupků Praha, (jako součást IISSDE),

b) v aplikacích:

- ORO – okresní registr obyvatel zpřístupňovaný pod aplikačním programem vlastní výroby využívajícím databázi s názvem „Lidi“
- PKO – projekt komunálního odpadu - Správa poplatku za sběr, třídění, využívání a zneškodňování komunálního odpadu,
- EPZ – evidence pohledávek a závazků.

Údaje ORO jsou získávány v agregované podobě z informačního systému evidence obyvatel. Tyto osobní údaje evidence obyvatel se přebírají do aplikací (a databází) PKO a EPZ. Pro ostatní části informačního systému Magistrátu se údaje shromažďují individuálním vyhledáním (výběrem) a opisem, nikoli přímým převzetím.

Informační systém správních a dopravně správních evidencí Ministerstva vnitra IISSDE je souborem aplikací vystavěných na používání některých údajů evidence obyvatel; aplikace užívané Hlavním městem Prahou k plnění jeho úkolů podle jednotlivých věcně příslušných zákonů nakládají s údaji evidence obyvatel automatizovaně, popř. automaticky podle rozhodnutí Ministerstva vnitra a bez možnosti zvolit jiný postup. To platí pro registr silničních vozidel a registr řidičů; jako doklad je možno použít auditní záznamy dotazů v informačním systému správních a dopravně správních evidencí - evidence obyvatel Ministerstva vnitra uskutečněných zaměstnanci Magistrátu.

Vytěžování informačního systému, v němž Ministerstvo vnitra zpracovává osobní údaje evidence obyvatel, je organizováno dvojí formou: část zaměstnanců (některé organizační složky Magistrátu) disponuje osobním přístupovým oprávněním do IISSDE, jiné útvary pracují s individuálními přístupovými oprávněními k osobním údajům ORO – databáze „Lidi“. Další útvary se s požadavky na zjištění osobních údajů z evidence obyvatel (zásadně IISSDE) obracejí na věcně příslušnou organizační složku Magistrátu.

Soubor operací, naplňující pojmové znaky zpracování podle § 4 písm. e) zákona o ochraně osobních údajů, Magistrát provádí systematicky s osobními údaji evidence obyvatel také k plnění úkolů uložených mu zákonem o podmínkách provozu vozidel na pozemních komunikacích a zákonem o provozu na pozemních komunikacích. Ve vztahu k Informačnímu systému správních a dopravně správních evidencí jsou tyto operace operacemi s těmiž osobními údaji.

Rozsah povinností Magistrátu podle zákona o ochraně osobních údajů je jednoznačný a shodný všude tam, kde kontrolovaný tyto údaje zpracovává jako uživatel podle ustanovení § 3a zákona o evidenci obyvatel (aplikace ORO, PKO a EPZ). V aplikaci využívající ORO jsou vedeny (zpracovávány) další popisné údaje subjektu údajů a jiných osob, jimž je v informačních systémech evidence obyvatel přiznáván status tzv. „osoby s vazbou“. Rozsah údajů v obou případech není větší, než jak stanoví zákon o evidenci obyvatel. Jiné popisné údaje evidence obyvatel se v dalších aplikacích nezpracovávají.

Magistrát zpracovává jako správce identifikační a kontaktní osobní údaje evidence

obyvatel, další popisné údaje a údaje transakční. Citlivé údaje Magistrát nezpracovává. U všech popisných údajů zpracovává aktuální a archivní hodnoty.

Transakční údaje k osobním údajům evidence obyvatel jsou generovány automaticky (systémem) k intelektuální činnosti zaměstnanců kontrolovaného pouze v IISSDE. Doplňování transakčních údajů v IISSDE není činností, za níž účastník řízení odpovídá.

Aktualizační dávky ORO jsou získávány měsíčně, se stejnou periodicitou je prováděno zálohování databáze. Zálohy jsou uchovávány v objektu kontrolovaného. Součástí operací s osobními údaji v informačním systému Magistrátu je likvidace osobních údajů evidence obyvatel. Magistrát ji provádí tak, že databázi ORO aktualizuje měsíčními dávkami poskytovanými Ministerstvem vnitra v části „nový registr“; po takto provedené aktualizaci jsou v této části ORO zlikvidovány záznamy s osobními údaji zemřelých nebo odstěhovaných osob. V části „starý registr“ se likvidace neprovádí. Vlastní měsíční aktualizace sestává z aktualizace příznaků o úmrtí a odstěhování v části „starý registr“ i části „nový registr“ a občasné likvidace záznamů v části „nový registr“. Občasná likvidace je prováděna v zásadě 2x ročně.

Obě základní aplikace (IISSDE a ORO) jsou při vytěžování chráněny zvnějšku, a to používáním individuálních přístupových oprávnění vázaných na používání hesla. Individuální autorizaci uživatelů pro zpracování osobních údajů zajišťuje Magistrát pro aplikaci ORO, pro IISSDE ji zajišťuje Ministerstvo vnitra. Magistrát pořizuje záznamy o vytěžování pro aplikaci ORO, pro IISSDE tak činí Ministerstvo vnitra.

Bylo zjištěno, že objem základní databáze osobních údajů evidence obyvatel (ORO) k lednu 2001 činí 1 178 000 záznamů. Měsíčně jsou aktualizovány údaje 10 000 – 20 000 osob. V době od 1. ledna do 30. září 2003 obdržel Magistrát 14 423 žádostí o výdej údajů z informačního systému evidence obyvatel; 14 418 žádostem vyhověl. Objem zpracování osobních údajů vyjadřuje počet auditních záznamů v informačním systému správních a dopravně správních evidencí provozovaném a spravovaném Ministerstvem vnitra.

Absolutní údaje o objemu vytěžování ORO nejsou k dispozici, protože nejsou účastníkem řízení zjišťovány. Lze proto použít pouze údaje nepřímé – zejména počet zaměstnanců, kteří jsou oprávněni ORO vytěžovat, tedy cca 90 zaměstnanců k měsíci lednu 2004 a dále údaje o objemu výdeje údajů z informačního systému evidence obyvatel za celý rok 2003 (17 898 výdejů).

Účastník řízení provádí zpracování osobních údajů popsané výše zčásti jako správce a zčásti jako zpracovatel ze zákona. Hlavní město Praha je veřejnoprávní korporací, hlavním městem České republiky, krajem a obcí (§ 1 zákona o hlavním městě Praze). Jako na orgán územní samosprávy se na něj vztahuje zákon o ochraně osobních údajů. Magistrát je orgánem hlavního města Prahy a jako takový vykonává přenesenou působnost, která je zvláštním zákonem svěřena orgánům obcí, orgánům obcí s pověřeným obecním úřadem a orgánům obcí s rozšířenou působností, není-li zákonem o hlavním městě Praze stanoveno jinak. Při zpracování osobních údajů evidence obyvatel platí, že zákonem, který stanoví něco jiného, je zákon o evidenci obyvatel, a to v ustanoveních § 2 písm. b) a c) a § 3a.

Z ustanovení zákona o evidenci obyvatel, zákona o hlavním městě Praze a statutu města, vydaného v souladu se zákonem o hlavním městě Praze vyplývá, že Hlavní město Praha zastoupené Magistrátem je zpracovatelem a uživatelem osobních údajů evidence obyvatel v informačním systému, jehož správcem a provozovatelem je Ministerstvo vnitra - Informačním systému správních a dopravně správních evidencí (IISSDE).

Pro plnění povinností podle § 13 je ve výše uvedeném postavení reálně pouze v rozsahu bezpečnostních opatření, která lze používat na výstupním rozhraní IISSDE.

Správcem je Hlavní město Praha resp. Magistrát pro osobní údaje evidence obyvatel zpracovávané aplikacemi ORO a PKO bez výjimky, dále při využívání údaje evidence obyvatel (vytěžování IISSDE) pro činnost podle hlavy V. zákona o provozu na pozemních

komunikacích. V rámci svého postavení jako správce je tak účastník řízení povinen dodržovat plnění povinností stanovených § 13 pro celý rozsah uvedených aplikací.

Jak je výše uvedeno, účastník řízení zpracovává osobní údaje ve velmi složitém systému, resp. systémech, což klade nároky na zabezpečení zpracování osobních údajů. Ustanovení § 13 zákona o ochraně osobních údajů stanoví, že správce, resp. zpracovatel je 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. Toto ustanovení je ustanovením obecným, které klade na účastníka řízení poměrně vysoké nároky v tom, že musí sám vyhodnotit bezpečnostní rizika, která při zpracování hrozí, což je v případě účastníka řízení náročné zejména v tom, že zpracovává osobní údaje z evidence obyvatel pro řadu oprávněných agend, ale také velkým množstvím pracovníků pro specifické a rozdílné účely. Je skutečností, že řada opatření byla přijata a aplikována, zejména pokud se týká objektové bezpečnosti a v zásadě dobře stanovených pravidel pro užívání jednotlivých databází či informačních systémů. Jak výše uvedeno, ne ve všech případech může účastník řízení některé typy bezpečnostních opatření sám přímo ovlivnit, protože využívá aplikací a systémů jiných správců a je v některých případech omezen samotnou možností zvolené aplikace. Nicméně jeho informační systémy, zejména ty, u nichž je samostatným správcem, tedy zejména systémy ORO a PKO, jsou takovými systémy, které obsahují osobní údaje všech obyvatel hlavního města Prahy a tomu je třeba přizpůsobit bezpečnostní opatření a velmi pregnantní nastavení pravidel užívání těchto systémů. Bylo nepochybně prokázáno a ze spisové dokumentace to vyplývá, že ne ve všech případech Hlavní město Praha jako správce zajistil dostatečně přesná pravidla s výraznou restriktivní funkcí tak, aby tyto informační systémy mohly být příslušnými pracovníky využívány pouze a výhradně k účelům, pro které jsou tyto systémy a osobní údaje v nich uvedené určeny. Jinak řečeno, u takto složitých systémů si musí být správce osobních údajů jist, kdo z jeho zaměstnanců a pro jaké účely osobní údaje z těchto systémů využívá a musí mít možnost takovéto užívání kontrolovat právě proto, že je ze zákona povinen zajistit, aby osobní údaje byly využívány pouze a toliko k účelům a z důvodů, pro které jsou určeny. Odvolací orgán považuje za prokázané, že transakční údaje informačního systému evidence obyvatel (IISSE) jsou pořizovány pouze k vybraným operacím s osobními údaji. V informačním systému evidence obyvatel nejsou zaznamenávány zjišťovací a ověřovací dotazy pro účely vedení registru řidičů a registru silničních vozidel a pro přebírání osobních údajů evidence obyvatel podle ust. § 4 odst. 8 zákona o podmínkách provozu na pozemních komunikacích. Co však odvolací orgán považuje za klíčové pro hodnocení porušení bezpečnostních pravidel, je skutečnost, že v ORO se transakční údaje nezaznamenávají vůbec, resp. systémem jsou zaznamenávány pouze přístupy do toho systému, ale již není evidováno, a tedy nelze ani zjistit, jaké úkony jednotliví zaměstnanci účastníka řízení v této databázi s osobními údaji provádějí, a tedy nelze ani zjistit a jakkoliv garantovat, že pro tento vstup (zpracování osobních údajů každého ze zájmových subjektů údajů) existoval legální a oprávněný účel a důvod. Tedy sám návrh tohoto informačního systému v sobě obsahuje a přímo zakládá vnitřní bezpečnostní riziko, které, jak je z dokumentace kontroly zřejmé, kontrola odhalila a také na něj upozornila. Za další bezpečnostní riziko je možno považovat v systému IISSE skutečnost, že pro některé odbory, resp. organizační jednotky účastníka řízení, jsou do tohoto systému umožňovány přístupy na základě velmi vágního, v některých případech spíše intuitivního oprávnění, které je pak nutno složitě dohledávat, což koneckonců potvrzují i kontrolním protokolem zdokumentovaná incidenční pochybení v rámci zpracování osobních údajů. Pokud v rámci svého rozkladu účastník řízení a koneckonců i v rámci prvostupňového řízení, dokládal dokumenty, že takováto oprávnění a takové přístupy byly oprávněné, odvolací orgán musí připustit, že zčásti ano, ne však bezvýhradně. Řada dokumentů, jež účastník řízení předkládal jak v rámci prvostupňového řízení, tak v rámci řízení rozkladového, je zcela zjevně vyhotovena až po provedené kontrole, a jsou tedy spíše reakcí na vykonanou kontrolu a na ukládaná opatření. Ta koneckonců směřují právě k tomu, aby zejména v systému ORO byly evidovány přístupy a aby tento systém obecně byl

využíván pouze k legálním a oprávněným účelům, a to oprávněnými pracovníky. Právě vzhledem ke skutečnosti, že jak systém ORO, tak systém PKO obsahuje značné množství osobních údajů, tak i prostá neexistence možnosti ověření oprávněných přístupů do těchto evidencí vlastními pracovníky, představuje výrazné bezpečnostní riziko. Pokud se účastník řízení ve svém rozkladu domáhal možnosti snížení uložené pokuty, a to z důvodů, že ochraně osobních údajů je u účastníka řízení věnována značná pozornost a že kontrola přispěla k dalšímu precizování ochrany osobních údajů, je třeba uvést, že správní orgán musí vždy posoudit výši sankce vzhledem ke všem zjištěným skutečnostem. Je zjevné, že pokud by se jednalo toliko o jednotlivé excesy, např. v rámci systému IISSE, které by byly a které také byly následně dohledatelné, odvolací orgán by tuto možnost skutečně zvažoval. Za zajímavé však považuje, že se účastník řízení ve svém rozkladu vůbec nevěnoval argumentaci pro systém zabezpečení a evidence přístupů svých zaměstnanců do systému ORO a odvolacímu orgánu se jeví, že i v rámci tohoto řízení toto daleko významnější bezpečnostní riziko podceňuje. I když tedy účastník řízení přijal značnou řadu bezpečnostních opatření a bezpochyby neustále zvyšuje kvalitu zabezpečení a ochranu osobních údajů při jejich zpracování, je samu skutečnost, tedy že nebyly sledovány vstupy do souborů osobních údajů v informačních systémech ORO a PKO ve všech případech, nutno považovat za pochybení poměrně zásadního charakteru. Bez tohoto nastavení, tedy evidencí přístupů, se výrazně snižuje efektivita jiných přijatých opatření pro ochranu osobních údajů. Neexistence monitorování vstupů a sledování oprávněnosti přístupu k osobním údajům tak vytváří velké bezpečnostní riziko. Vzhledem k tomu, jak velká populace obyvatel je účastníkem řízení komunikována, vzhledem k počtu zaměstnanců účastníka řízení, je nutno toto pochybení posuzovat jako základní podcenění ochrany zpracování osobních údajů ve využívaných systémech. Odvolací orgán je toho názoru, že je jen shodou okolností, že tato pochybení nevedla k masovému zneužití osobních údajů. Je dokonce možné se domnívat, že v jednotlivých případech k narušení soukromí obyvatel hlavního města mohlo dojít, avšak takto postižení občané si vzniklý stav ani neuvědomili a nepodali proti takovému jednání stížnost. Odvolací orgán se rozhodl potvrdit výši sankce, která je udělena v samé spodní hranici možné sazby právě proto, že další aspekty ochrany osobních údajů jsou účastníkem řízení aplikovány a vzal také v úvahu, že další porušení zákona o ochraně osobních údajů nebylo zjištěno, a tedy že účastník řízení v případě jiných povinností zákon o ochraně osobních údajů neporušil.

Ze všech výše popsanych a uvedených důvodů odvolací orgán rozhodl tak, jak je výše ve výroku tohoto rozhodnutí uvedeno.

Poučení: Proti tomuto rozhodnutí se podle § 61 odst. 2 zákona č. 71/1967 Sb., o správním řízení (správní řád), ve znění pozdějších předpisů, nelze odvolat.

RNDr. Karel Neuwirt
předseda