úřad
pro ochranu
osobních
údajů

VÝROČNÍ ZPRÁVA 2008

Rok 2008 z pohledu předsedy Úřadu

Při ohlédnutí za rokem 2008 nemám pocit, že by se mnoho změnilo v trendu upřednostňování kolektivní bezpečnosti na úkor práva na ochranu soukromí, který jsem konstatoval na sklonku roku 2007. Úřad pro ochranu osobních údajů však nemůže ani nechce zaujímat pasivní úlohu pozorovatele uvedeného trendu. Předkládaná výroční zpráva je toho dokladem. Je však nejenom podrobnou bilancí práce, která byla za loňský rok vykonána; podává také obraz o úsilí Úřadu o zlepšení péče o soukromí občanů už ve stadiu přípravy právních norem, které jejich základní právo na ochranu soukromého života ovlivňují.

Jsem rád, že mohu jako příklad uvést jisté zlepšení v ochraně osobních údajů v katastru nemovitostí. Nejde sice o stav ideální, ale oproti původnímu nekontrolovatelnému využívání této databáze, dotýkající se podstatně života tisíců občanů, bylo dosaženo toho, že lze okamžitě reagovat na podezřelé využívání údajů, a pokud se potvrdí jeho neoprávněnost, také je následně postihnout.

V nemenší míře s uspokojením konstatuji, že se Úřad vydal na jistě ne snadnou cestu hledání pravidel pro zodpovědné nakládání s údaji genetickými. Stav, který jsme zjistili, nás nenaplňuje bezstarostným optimismem, ale je nám jasné, že zpracování údajů v databázích DNA se musíme věnovat velmi soustředěně. Vždyť jde o údaje nejcitlivější, jejichž zneužití může mít fatální důsledky i pro příští generace.

K mnoha důležitým poznatkům jsme se také dobrali při využívání kamerových systémů. Lituji ovšem, že z nich plynoucí návrhy legislativě, která by mohla zlepšit stav využívání kamerových systémů Policií ČR, se zatím zadrhly v procesu vyjednávání.

Absurdní využívání tohoto vůči soukromí velmi invazivního prostředku jsme začlenili letos do výroční zprávy i v podobě obrazové přílohy. Bohužel, občas úsměv, který vyvolává, tuhne na rtech a, jak se říká, nechává rozum stát…

Je třeba také říci, že letošní výroční zpráva více než kdy jindy nejen bilancuje, ale přináší i mnoho konkrétních poznatků jak pro veřejnost, tak pro zákonodárce i moc výkonnou. Soustředili jsme se v části o kontrolní činnosti na několik oblastí – na informační systémy veřejné správy, zdravotnictví, informační systémy v oblasti justice a státního zastupitelství, zpracování osobních údajů a problematiku DNA, na informační systémy EU, technologii RFID, zejména ve vztahu k čipovým kartám v dopravě – a shromáždili tak mnoho podnětného materiálu. Detailní popis jednotlivých kauz, postupu správního řízení i řízení druhostupňového a soudního přezkumu poskytuje dosti hluboký pohled jak na proces kontroly samé, tak na problémy, které jsou kontrolou obnaženy; de facto tedy jde o modelové příklady, jež mohou v rozhodování o zpracování osobních údajů orientovat také správce osobních údajů, ale i správní instituce. Nabízíme tak i sumu poznatků o ochraně osobních údajů jako stále naléhavější součásti lidských práv.

Obdobným přínosem by se měla stát i rozsáhlá kapitola výroční zprávy soustřeďující se na dozorovou činnost a agendy, které jsou součástí této složky Úřadu.

Jednoznačně s potěšením se mohu ohlédnout za výsledky mezinárodních aktivit Úřadu. Je možné říci, že Úřad je zahraničím vnímán jako seriózní a přínosný partner. Opodstatňuje to mé přesvědčení, že se úspěšně zhostí i všech těch úkolů, které ho čekají v době předsednictví ČR v Radě Evropské unie. A těch není málo.

O kvalitě informačního úsilí ve vztahu k občanům jistě svědčí i fakt, že webové stránky Úřadu byly vybrány a zařazeny mezi ty elektronické informační zdroje, které jsou pro budoucnost uchovávány jako národní dědictví.

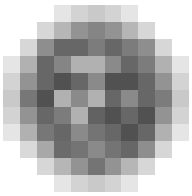
Jestliže celosvětová konference komisařů osobních údajů, která se konala v říjnu 2008 ve Štrasburku, věnovala velkou pozornost problematice mládeže a novým technologiím a položila důraz na potřebu šíření poznatků o ochraně osobních údajů mezi mladou generací, je třeba říci, že český Úřad už po dva roky soustředěně s mládeží a s pedagogy pracuje. Projekt akreditovaný MŠMT ČR vstupuje do třetího roku dalšího vzdělávání pedagogických pracovníků a těší se z jejich strany skutečnému zájmu i dobrým hodnocením. Radostné je pro nás každoroční setkání s mladými lidmi u příležitosti pořádání soutěže Moje soukromí! Nekoukat, nešťourat!

Úřad tedy předkládá svou výroční zprávu s pocitem, že tak uzavírá rok intenzivní práce. Obdobně intenzivní bude nepochybně i příští půlrok českého předsednictví EU a pro Úřad nastupuje i období příprav celoevropské konference ochránců osobních údajů, na kterou je třeba naše partnery pozvat už na jaře roku 2009.

Věřím však okruhu lidí, s nimiž spolupracuji, a nemám proto pochybností, že jak ony velké jednorázové úkoly, které už jsou pro nás jisté v době blízké i vzdálenější, tak každodenní práce budou naplňovat poslání Úřadu: chránit osobní údaje a sloužit uchování základního lidského práva na soukromý a rodinný život.

Igor Němec

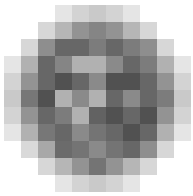
Obsah



Úřad v číslech 2008

Dotazy a konzultace	dotazy ČR	1 813
	zahraničí	130
	osobní konzultace celkem	115
	státní správě	35
	samosprávě	17
	právnickým osobám	46
	fyzickým osobám podnikajícím	10
	fyzickým osobám	7
Podání a stížnosti	přijaté podněty dle zákona o ochraně osobních údajů	697
	stížnosti předané ke kontrole	202
Nevyžádaná obchodní sdělení (kompetence podle zákona 480/2004 Sb.)	podnětů celkem	1 458
	vyřešených podnětů	1311
	zahájených kontrol	155
	ukončených kontrol	91
	správních rozhodnutí o pokutě	81
Kontroly (vyjma kontrol týkajících se zákona č. 480/2004 Sb.)	zahájeno	112
	ukončeno	112
	předáno jiným státním úřadům	45
	napadeno námitkami	35
	námitkám vyhověno	12
	nevyhověno	14
	převážně vyhověno	1
	převážně nevyhověno	3
Správní trestání	správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb.	87
	přestupková řízení podle zákona č. 101/2000 Sb.	8
	přestupková řízení o porušení zákona č. 159/2006 Sb., o střetu zájmů	0
	rozklady napadená rozhodnutí o porušení zákona	33
	zamítnutých rozkladů	16
	zrušeno a vráceno k novému projednání	1

	zrušených rozhodnutí a zastavená řízení	2
	změna rozhodnutí	2
Soudní přezkum	podaných žalob k soudu	13
	zamítnutých žalob soudem	1
	zrušených rozhodnutí soudem	0
	ukončených / neukončených soudních řízení	1/12
Registrace	přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.)	3 327
	zaregistrovaná zpracování	2 841
	zaregistrovaných správců	1 914
	zrušené registrace	90
	oznámení o změně zpracování	1 141
	Řízení podle § 17	99
	zastaveno (nedochází k porušení zákona)	78
	zastaveno z procesních důvodů (např. oznámení vzato zpět)	9
	nepovoleno	12
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	23
	rozhodnutí o povolení předávání	33
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	6
Stížnosti podle § 175 správního řádu	přijatých stížností	33
	stížností vyřízených jako důvodné	6
	stížností vyřízených jako částečně důvodné	5
	stížností vyřízených jako bezdůvodné	24
Stížnosti a jiné podněty na postup Úřadu, které nebyly řešeny podle § 175 správního řádu	došlých podnětů	1
	vyřízených jako důvodné	1
	vyřízených jako bezdůvodné	0
Žádosti podle zákona č. 106/1999 Sb.	přijatých žádostí	6
	vyřízených žádostí	6
	odmítnutých žádostí	0
Publikované materiály	Věstník Úřadu (počet částek)	3
	Bulletin Úřadu (počet čísel)	3
Tiskové konference	pravidelné tiskové konference	4
	mimořádné	1
Připomínkované legislativní návrhy	zákony	69
	prováděcí předpisy	48
	ostatní	80



Kontrolní činnost

Obecná problematika kontrolní činnosti

V roce 2008 bylo **na základě podnětů a stížností** vedeno téměř 90% kontrol; zbývající kontroly byly vedeny **na základě plánu** kontrol.

Stížnosti na porušení zákona č. 480/2004 Sb., o některých službách informační společnosti, týkající se zasílání nevyžádaných obchodních sdělení, byly převážně podávány prostřednictvím webového formuláře Úřadu.

Podněty, které inspektoři řeší, lze rozdělit do dvou základních skupin – stížnost na jednorázové porušení zákona a stížnosti vykazující podezření na systémové porušení zákona.

U jednorázových kontrol byla příslušná věc často řešena a vyřešena již v rámci tzv. předběžného šetření. V takových případech je zjednána náprava bez formální kontroly.

Tento procesní institut není výslovně uveden v zákoně, lze jej však zahrnout pod kompetenci Úřadu dle § 29 odst. 1 a) zákona o ochraně osobních údajů a vyplývá z povinnosti Úřadu provádět dozor nad dodržováním povinností stanovených zákonem. Tento přístup nelze uplatnit vždy a u každého správce. Pokud však již tato forma byla zvolena, ukazuje se, že převážná většina zástupců těchto subjektů s inspekčními pracovníky spolupracuje. Svědčí to například i o zvyšující se autoritě Úřadu. Pozitivně se může uplatňovat i konzultační povinnost Úřadu. Řešeny jsou tak případy, kdy pochybení nevzniklo na základě úmyslu. Jde tedy o formu dozoru, která zaručuje časově efektivní ukončení případu.

Obdobný postup je realizován i při řešení ojedinělých stížností na porušování zákona o některých službách informační společnosti, kdy by Úřad prokazováním autorství jedné e-mailové zprávy nepostupoval hospodárně.

Převážná většina podnětů je však stále inspektory řešena v rámci výkonu řádné státní kontroly. V průběhu kontrol velkých subjektů – lhostejno, zda státních orgánů nebo velkých soukromých společností – se kontrolní pracovníci obvykle setkávají s odborně připravenými a fundovanými zástupci, kteří znají a uplatňují svá práva kontrolovaného a ve většině případů jsou dobře právně připraveni. U menších, převážně soukromých subjektů se naopak lze v průběhu kontrolních jednání v některých případech nadále setkat i s minimálním právním povědomím o povinnostech v oblasti ochrany osobních údajů, zakrývaných občas i arogancí vůči kontrolujícím. Častěji je pak nutno sáhnout i k zákonem daným donucovacím prostředkům, jejichž prostřednictvím lze dosáhnout kontrolního cíle.

Ve větším měřítku než v předchozích letech se v průběhu prováděných kontrol ukazuje, že někteří stěžovatelé využívají kompetence Úřadu pro ochranu osobních údajů s vědomím, že mu zákon ukládá šetřit každý podnět. V průběhu kontrol se však nakonec často prokáže, že podnět zaslala osoba, která byla například zachycena kamerou a na základě pořízeného záznamu byla usvědčena z deliktního jednání. Zarážející je, že často taková podání za tyto osoby přicházejí od advokátů. Stále častěji je Úřad zneužíván k řešení sporů mezi různými subjekty, kdy ve sporu je jako „vedlejší produkt“ zneužita skutečnost, že zpracování osobních údajů se promítá téměř do všech činností. Podněty a stížnosti podávané s vědomím male fi-

de jsou pro kontrolní činnost zatěžující a odčerpávají čas potřebný na opodstatněné případy, které kontrolu skutečně vyžadují.

Rok 2008 lze v oblasti kontrolní činnosti Úřadu charakterizovat rovněž tím, že se vzrůstající kvalifikací kontrolovaných osob jsou ve větší míře využívány proti kontrolním protokolům opravné prostředky. Přesto lze konstatovat, že se podíl kontrolních zjištění, která byla druhostupňovým orgánem Úřadu zrušena, oproti předchozím létům nezvýšil.

Kontrolní činnost podle plánu kontrol

Jak již bylo řečeno výše, **výkon kontrolních činností** Úřadu není závislý jen na tom, do které oblasti právě směřují podané stížnosti či podněty; Úřad řadu svých, zejména kontrolních, aktivit vykonává na základně plánu kontrolní činnosti, který každoročně schvaluje a vyhodnocuje předseda Úřadu společně s inspektory. V roce 2008 se kontrolní aktivity podle plánu kontrolní činnosti soustředily do následujících oblastí:

Informační systémy veřejné správy

Jednou z priorit kontrolní činnosti Úřadu i v kontrolním plánu na rok 2008 bylo sledování podmínek, které musí respektovat každý správce nebo jiný provozovatel informačního systému veřejné správy.

Kontrola v této oblasti se zaměřila na diagnostický ústav, dětský domov se školou, dětský domov, středisko výchovné péče, základní školu a školní jídelnu. Kontrola dosud nebyla ukončena.

Informační systémy v oblasti justice a státního zastupitelství

V návaznosti na zkušenost, kterou Úřad získal z kontrolní činnosti prováděné v této oblasti v předchozím roce, pokračoval i v roce 2008 ve výkonu své pravomoci v této oblasti.

Nadnárodní informační systémy

Z jednání společných dozorových orgánů pro Schengenský informační systém a pro Celní informační systém, stejně jako z jednání koordinační skupiny pro EURODAC, vyplynulo, že tyto orgány i v roce 2008 budou iniciovat další koordinované inspekce uvedených systémů. I vzhledem ke vstupu České republiky do Schengenského prostoru považoval Úřad za nezbytné tyto kontroly provést.

Kontroly probíhaly v období 15. 4. 2008 – 9. 6. 2008, 19. 8. 2008 – 29. 10. 2008. Kontrola Policie ČR v oblasti schengenského informačního systému byla zahájena 22. 10. 2008 a dosud nebyla ukončena.

Zpracování osobních údajů při nasazení sledovacích systémů

Úřad po zkušenostech z předchozích let a v návaznosti na nárůst nasazování monitorovacích systémů, který zaregistroval i v počtu registrací a došlých podnětů, v roce 2008 uplatnil své kontrolní aktivity i v této oblasti. Úřad se zaměřuje především na oblast zdravotnictví a na poskytování sociálních služeb.

Kontroly dosud nejsou v úplnosti ukončeny, lze však předložit parciální poznatky.

Ochrana spotřebitele

V návaznosti na rostoucí zájem dodavatelů i uživatelů technologií umožňujících rychlou a bezpečnou identifikaci subjektu údajů, Úřad registruje celospolečenský zájem o vytvoření pravidel, která by omezila zásah do soukromí fyzické osoby v souvislosti s používáním čipových karet a karet vybavených RFID technologiemi.

Kontrolní činnost podle pokynů předsedy Úřadu

Kromě zásadních směrů kontroly Úřadu, vymezovaných každoročně plánem kontrolních činností, řeší Úřad některé společensky významné kontrolní aktivity prostřednictvím pokynu předsedy Úřadu jednotlivým inspektorům, kteří pak na jeho základě vykonávají své kontrolní pravomoci.

Na základě pokynu předsedy provedl inspektor Úřadu v období 6. 2. 2008 – 22. 4. 2008 kontrolu společnosti Evropský investiční holding, a.s., která mj. provozuje i Hotel Savoy v Praze. Podle veřejně publikovaných informací došlo k úniku záznamu z kamerového systému, který byl v tomto hotelu provozován. Proto dal předseda Úřadu pokyn k provedení kontroly zpracování osobních údajů tímto kamerovým systémem. Kontrolou bylo konstatováno porušení ustanovení § 5 odst. 1 písm. d), § 5 odst. 2, § 11 odst. 1 a § 16 zákona o ochraně osobních údajů a § 316 odst. 2 zákona č. 262/2006 Sb., zákoníku práce.

Poznatky z provedených kontrol

INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

Osobní údaje a veřejná správa

Trvalou pozornost Úřad věnuje zpracováním osobních údajů prováděným orgány veřejné správy. Tato oblast je nejen značně rozsáhlá co do počtu trvale prováděných zpracování, ale také dopadá na absolutně největší počet lidí. Navíc vykazovala v roce 2008 poměrně velkou dynamiku.

Podání, která byla vyhodnocena jako důvodná a na jejichž základě Úřad konal, se týkala zveřejňování osobních údajů získaných orgánem veřejné správy v rámci výkonu veřejné správy, provozování zón placeného parkování a používání informačního systému evidence obyvatel. Správní řízení byla vedena jak na základě zjištění z kontrol, tak přímo na základě vybraných podání. Všechny kontroly s takovým tematickým zaměřením, které byly pravomocně ukončeny, byly zahájeny na základě podnětu doručeného Úřadu podle ustanovení § 29 odst. 1 písm. c) zákona o ochraně osobních údajů.

Úřad v roce 2008 obdržel podnět, aby prošetřil podezření z porušení zákona o ochraně osobních údajů, ve kterém pisatelka uvedla, že na elektronické úřední desce města X byla zveřejněna usnesení stavebního úřadu, která obsahovala osobní údaje pisatelky a jejího manžela (jméno, příjmení, adresu bydliště, data narození, číslo parcely pozemku). Na základě tohoto podnětu proběhla v měsíci únoru až dubnu v MěÚ kontrola. V kontrolovaném případě není správci údajů dána jiná (zákonná) možnost zpracování osobních údajů než ta, která vyplývá z práv a povinností správce podle zvláštních právních předpisů.

MěÚ v uvedené věci plní povinnosti správce osobních údajů (orgánu veřejné správy), které vyplývají ze zákona o územním plánování a stavebním řádu (dále jen „stavební zákon“) a ze správního řádu. Zaměstnankyně MěÚ odeslala předmětná usnesení k doručení na uvedené adresy a současně je naskenovala a postoupila tajemníkovi MěÚ ke zveřejnění.

Zákonná možnost doručení veřejnou vyhláškou, nebo zveřejnění usnesení stavebního úřadu MěÚ nebyla zjištěna. V daném případě nebyl důvod k propojení stavebního a územního řízení podle stavebního zákona a ani nebyl zjištěn jiný právní titul umožňující náhradní doručení, protože obě usnesení byla stěžovatelům řádně doručena. Když MěÚ zveřejnil dálkovým přístupem usnesení, šlo o nesprávný postup správního orgánu, neboť tak bylo učiněno bez nezbytného oprávnění dle zvlášt-

ního právního předpisu. Tím MěÚ porušil povinnost podle ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů při zpracování osobních údajů účastníků stavebního řízení, uvedených v usneseních, která byla zveřejněna dálkovým přístupem. Na základě kontroly bylo se správcem vedeno správní řízení o uložení pokuty za výše uvedený správní delikt.

Na základě podání dotčeného subjektu údajů byl vydán příkaz, kterým byla statutárnímu městu uložena pokuta ve výši 500 Kč, a to za porušení povinnosti stanovené v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, ke kterému došlo tím, že město v odůvodnění rozhodnutí uvedlo rodné číslo stěžovatelky.

Podle zákona o evidenci obyvatel a rodných číslech lze rodné číslo využívat, jen jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, o činnost vyplývající z jejich zákonem stanovené působnosti, nebo o činnost notářů pro potřebu vedení Centrální evidence závětí. Současně je ale nutno konstatovat, že ačkoliv správní orgány mají zmocnění k využívání rodných čísel, nelze to vykládat tak, že by mohly s rodným číslem neomezeně nakládat. Při jeho používání musejí respektovat § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, podle něhož je správce povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny.

Podle správního řádu obsahuje odůvodnění rozhodnutí důvody výroku nebo výroků rozhodnutí, podklady pro jeho vydání, úvahy, kterými se správní orgán řídil při jejich hodnocení a při výkladu právních předpisů, a informace o tom, jak se správní orgán vypořádal s návrhy a námitkami účastníků a s jejich vyjádřením k podkladům rozhodnutí. Z uvedeného je zřejmé, že odůvodnění rozhodnutí již nemá obsahovat jednoznačnou identifikaci účastníka řízení, kterou je naopak potřeba provést ve výroku rozhodnutí. Ve výroku rozhodnutí byla stěžovatelka identifikována pouze pomocí jména, příjmení, data narození a adresy pobytu, tedy v souladu se správním řádem.

Kontroly zaměřené na evidenci obyvatel odpovídají postavení tohoto úředního zdroje osobních údajů všech obyvatel České republiky a skutečnosti, že tento zdroj je využíván řadou orgánů veřejné správy, a to jak na základě zákona o evidenci obyvatel, tak na základě několika desítek zvláštních zákonů.

Stěžovatelka M. P. podala Ministerstvu vnitra (dále jen „MV“) žádost o poskytnutí osobních údajů z informačního systému evidence obyvatel. V podání adresovaném Úřadu uvedla, že jí byl zaslán výpis, který obsahoval údaje nepatřící její osobě. Při osobní návštěvě MV na tuto skutečnost upozornila a posléze obdržela opravené dokumenty, které jsou neúplné. MV uvedlo ve výpisu, který byl stěžovatelce M. P. doručen jako první, údaje, které byly vedeny v informačním systému evidence obyvatel. Údaje, které stěžovatelka napadla u Úřadu, se vztahují zčásti k době před zřízením informačního systému evidence obyvatel (dále též jen „ISEO“) podle zákona č. 135/1982 Sb., o hlášení a evidenci pobytu občanů. Historické údaje o trvalém pobytu stěžovatelky M. P., vedené k 23. lednu 2008 v ISEO, se shodují s údaji uvedenými ve výpisu, který jí poskytlo MV. Na výzvu inspektorky své výhrady stěžovatelka M. P. upřesnila tak, že označila za nepravdivé údaje o bydlišti v době od 20. 11. 1959 do 12. 10. 1992. Její vyžádané dodatečné vyjádření dále změnilo posouzení podnětu podle zákona o ochraně osobních údajů: Původně tvrzená záměna osobních údajů se nepotvrdila.

Nesprávnost údajů o trvalém bydlišti stěžovatelky M. P. v letech 1959 – 1992 není problémem správy ISEO, za který by neslo odpovědnost MV, neboť záznam o trvalém pobytu nezakládá konflikt s jinými údaji ISEO a neobsahuje nepřípustné nebo obecně nepravdivé či jinak nepřesné údaje: Na jedné z chybně vykazovaných adres měla později stěžovatelka trvalý pobyt, na druhé měl trvalý pobyt její bývalý manžel. MV na základě žádosti stěžovatelky M. P. a ve spolupráci s příslušnými městskými úřady a jinými zdrojovými místy prověřilo archivní údaje z přihlašovacích lístků pro

trvalý pobyt stěžovatelky a osoby jí blízké. Vysvětlení, které bylo stěžovatelce M. P. poskytnuto písemně, navázalo na závěry z osobního jednání na MV, při němž bylo stěžovatelce ústně podáno vysvětlení, a byl s ní dohodnut další postup; to stěžovatelka nikdy nezpochybnila. Postup MV vůči stěžovatelce byl tedy v souladu se zákonem o ochraně osobních údajů i se zákonem o evidenci obyvatel. Do zahájení kontroly Úřadu však MV nezajistilo ani blokování údajů o trvalém pobytu stěžovatelky M. P., ani doplnění chybějících a odstranění nesprávných údajů v souladu s ustanovením § 8a odst. 2 zákona o evidenci obyvatel.

V rámci téže kontroly byly dále prověřeny skutečnosti ze dvou jiných podání, která napadala postup MV v souvislosti se změnou rodného čísla J. T. a při využívání osobních údajů stěžovatelů T. T. a E. Z. K 23. lednu 2008 byl v informačním systému evidence obyvatel u stěžovatele E. Z. zaznamenán rodinný stav ženatý a u stěžovatelky T. T. rodinný stav vdova s účinností ode dne 2.10.2007, což je datum úmrtí stěžovatele E. Z. Tento stav vyplývá z problému správy informačního systému evidence obyvatel, neboť obě fyzické osoby, které uzavřely manželství, byly ke dni uzavření manželství osobami, jejichž údaje byly vedeny v informačním systému evidence obyvatel podle § 3 odst. 3 zákona o evidenci obyvatel. Skutečnost, že je možné zavést mezi takovými osobami jednostrannou partnerskou vazbu, aniž by systém reagoval signalizací problému, zakládá stav, kdy je přípustné v ISEO uchovávat, popř. do něho i zavádět nepřesné osobní údaje. Takový stav trval i ve dnech, kdy bylo prováděno vyhledávání v ISEO pro potřeby kontroly. U zemřelého partnera zůstává v ISEO po záznamu údaje o úmrtí zachována hodnota rodinného stavu a je vedena nadále jako odpovídající aktuálnímu stavu, zatímco u druhého partnera je hodnota změněna.

Na základě zjištěné incidence věcných chyb bylo systematicky zjišťováno, jak MV plní povinnost stanovenou v § 5 odst. 1 písm. c) zákona o ochraně osobních údajů, tedy zpracovat pouze přesné osobní údaje, které získalo v souladu s tímto zákonem, je-li to nezbytné, osobní údaje aktualizovat a při zjištění, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provést bez zbytečného odkladu přiměřená opatření, jimiž jsou i podle zákona o evidenci obyvatel blokování a oprava osobního údaje.

MV evidovalo k 11. září 2007 v Informačním systému evidence obyvatel u stěžovatelky T. T., rodinný stav provdaná a jako její manžel byl evidován stěžovatel E. Z., u něhož byl uveden rodinný stav rozvedený. K 23. lednu 2008 evidovalo u stěžovatele E. Z. rodinný stav ženatý a u stěžovatelky T. T. rodinný stav vdova s účinností od data úmrtí stěžovatele E. Z. Tyto údaje navíc nebyly označeny tak, že by byla signalizována jakákoli pochybnost o jejich přesnosti.

V náhodně vytvořeném vzorku údajů uchovávaných v Informačním systému evidence obyvatel – žijících nositelů příjmení K_k a K_á – bylo k 24. lednu 2008 uvedeno 42 osob, jejichž rodné číslo mělo „nulovou“ koncovku (tj. 000 nebo 0000), dvě dvojice osob se shodným jménem, příjmením a dnem narození, z nichž vždy jedna měla nulovou a jedna nenulovou koncovku. Žádný ze zobrazených záznamů s nulovou koncovkou rodného čísla nebyl označen tak, aby bylo patrné, že je prověřována správnost rodného čísla. Dále bylo v ISEO nalezeno 2 912 403 osob, které byly evidovány buď bez rodného čísla, nebo s nulovými koncovkami, z toho 1 390 se záznamem podle § 3 odst. 3 nebo 4 zákona o evidenci obyvatel.

S ohledem na rozdíl v počtu žijících stoletých a starších obyvatel zapsaných v evidenci obyvatel a v evidenci České správy sociálního zabezpečení 2208 : 726 bylo vedeno další zjišťování. Při něm bylo shledáno, že osobní údaje některých osob narozených v letech 1898 – 1908, vedené v ISEO, neodpovídaly skutečnosti a současně u žádného z těchto subjektů údajů nebylo označení, které by signalizovalo pochybnosti o platnosti kteréhoko-

liv osobního údaje, tzn. že nebylo provedeno blokování způsobem stanoveným v § 8a odst. 2 zákona 133/2000 Sb., o evidenci obyvatel a rodných číslech. Na tomto základě bylo konstatováno, že MV porušilo povinnost stanovenou v § 5 odst. 1 písm. c) zákona o ochraně osobních údajů.

K nápravě zjištěného stavu bylo uloženo sedm opatření k nápravě, zahrnujících zejména rutinní provedení nebo zajištění revize záznamů všech osob, které jsou v ISEO zapsány s rodným číslem s koncovkou 000 nebo 0000 a osob, které jsou v ISEO zapsány jako žijící a narozené před 1. březnem 1928 a blokování příslušných údajů. Správní řízení nebylo, s ohledem na uplatnění řádných opravných prostředků účastníkem řízení, dosud pravomocně ukončeno.

Přímo na základě podání postoupeného Úřadu státním zastupitelstvím bylo zahájeno správní řízení, jehož výsledkem bylo konstatování, že statutární město při poskytnutí informace podle zákona č. 106/1999 Sb., zpřístupnilo žadateli osobní údaje o existenci pobytu manželů O. v roce 2002, které získalo z evidence bytové kanceláře, a to aniž disponovalo jejich souhlasem s tímto postupem, čímž porušilo povinnost stanovenou v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tedy povinnost zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, za což mu byla uložena pokuta ve výši 5 000 Kč.

K předmětu tohoto řízení lze uvést, že zákon o svobodném přístupu k informacím v § 8a stanoví, že informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobních údajů poskytne povinný subjekt jen v souladu s právními předpisy, upravujícími jejich ochranu. I když byla v odpovědi na žádost podanou podle uvedeného zákona uvedena pouze informace o existenci pobytu v roce 2002 bez uvedení jmen osob, kterých se týká, byl zde uveden také odkaz na žádost, kde byly jejich jména a adresa trvalého pobytu jasně specifikovány. Je proto nepochybné, že údaj o pobytu se vztahuje k identifikovatelné osobě a jde proto o osobní údaj ve smyslu § 4 písm. a) zákona o ochraně osobních údajů.

Statutární město v souvislosti se zpracováním osobních údajů osob vedených v evidenci bytové kanceláře vystupuje jako správce osobních údajů, přičemž je podle § 5 odst. 1 písm. f) zákona o ochraně osobních údajů povinno nakládat s osobními údaji pouze v souladu s účelem, pro který byly shromážděny. Tím, že byly údaje o pobytu manželů O. zpřístupněny žadateli bez jejich souhlasu, je nutno dojít k závěru, že stanovený účel zpracování (vedení evidence bytové kanceláře provozované pro účely činnosti města) byl zjevně překročen.

V návaznosti na **zprovoznění zón placeného parkování v hlavním městě Praze** byla Úřadu doručena podání čtyř stěžovatelů. Na počátku roku 2008 bylo ukončeno pět kontrol. Na základě zjištění z kontroly byla vedena čtyři správní řízení.

V jednom řízení bylo konstatováno, že městská část v souvislosti s vydáváním parkovacích karet do zón placeného stání neinformovala žadatele v řízení o vydání parkovacích karet o jejich právech vztahujících se k jím prováděnému zpracování, zejména pak o tom, jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny. Neinformovala rovněž o právu přístupu k osobním údajům a právu na opravu osobních údajů, a dále nepředložila dokument o tom, že přijala technicko-organizační opatření k zajištění ochrany osobních údajů žadatelů, čímž porušila povinnost informovat subjekty údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny. Nesplnila též povinnost informovat jej o právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 uvedeného zákona a dále je poučit o tom, zda je poskytnutí osobního údaje povinné či dobrovolné. Dále porušila povinnost zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů subjektů údajů v souladu se zákonem a s jinými právními předpisy. Za tato porušení povinností jí byla uložena pokuta ve výši 12 000 Kč.

V rámci provedené kontroly bylo dále zjištěno, že dokumentované bezpečnostní opatření bylo provedeno a je průběžně, resp. trvale užíváno. Technicko-organizační opatření tvořící součást systému, však nebylo možné vyhodnotit a zejména nebylo možno ověřit, zda byly pořizovány elektronické záznamy, které umožňují určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány v rozsahu stanoveném v § 13 odst. 4 zákona o ochraně osobních údajů.

Pro porušení povinnosti stanovené v § 11 odst. 1 a 2 stejným způsobem a ve shodném rozsahu byla vedena další tři řízení, z toho jedno pouze pro porušení této povinnosti.

Jedno řízení bylo vedeno proto, že účastník řízení kopíroval jako správce osobních údajů při řízení k vydání parkovacích karet do zóny placeného stání občanské průkazy žadatelů a občanské průkazy osob jednajících jejich jménem, přičemž u žádného subjektu údajů neprokázal jeho souhlas k pořízení kopie občanského průkazu pro zpracování jeho osobních údajů.

Jedno řízení bylo vedeno také proto, že jeden účastník řízení nestanovil pro vydávání parkovacích karet prostředky a způsob zpracování osobních údajů obyvatel – žadatelů. Jím vydaný předpis a Metodika pro vydávání parkovacích karet do zóny placeného stání neobsahují žádné ustanovení, které lze považovat za určující způsob nebo prostředky zpracování osobních údajů. Závazný pokyn pro vydávání parkovacích karet do zóny placeného stání, vydaný účastníkem řízení, určuje způsob a prostředky zpracování pro vybrané doklady, které jsou požadovány po žadateli v případě, že žadatel nedoloží originál nebo ověřenou kopii výpisu z obchodního rejstříku a katastru nemovitostí. Základní formou určení prostředků a způsobů zpracování osobních údajů je tak rozhodnutí účastníka řízení o pořízení a používání systému, v němž jsou zpracovávány osobní údaje držitelů parkovacích karet. Na ně navazují dílčí rozhodnutí, která je třeba dovozovat ze zjištěné funkčnosti používaných prostředků automatizovaného zpracování a z postupů v jakékoli míře popsaných v dokumentech zjištěných v městských částech. V části listinné lze považovat za stanovené pouze takové prostředky a způsoby, které jsou v nějaké formě zachyceny v zápisech (záznamech) z jednání vedených mezi účastníkem řízení a starosty městských částí.

Uvedený postup nelze považovat za řádné stanovení prostředků a způsobů zpracování osobních údajů ve smyslu ustanovení § 5 odst. 1 písm. b) zákona o ochraně osobních údajů.

Týž účastník dále nezahrnul požadavky na bezpečnostní opatření do smluv se zhotovitelem aplikačního softwaru, v němž jsou zpracovávány osobní údaje žadatelů o vydání parkovacích karet, nevypracoval ani nezadal vypracování dokumentace ve smyslu ustanovení § 13 odst. 3 a 4 zákona o ochraně osobních údajů a nezabýval se ani návazností na opatření přijatá městskými částmi X. Neprokázal žádným dokladem, že by vydal k zabezpečení osobních údajů subjektů údajů opatření ve smyslu ustanovení § 13 odst. 1 a 2 tohoto zákona tak, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k jejich osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití těchto osobních údajů. V rámci automatizovaného zpracování účastník řízení nezajistil, ve smyslu ustanovení § 13 odst. 4 zákona o ochraně osobních údajů, pořizování elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. V tomto řízení byla uložena pokuta 70 000 Kč, v řízeních zbývajících pokuta ve výši 20 000 a 10 000 Kč.

Zpracování osobních údajů ve veřejné správě bylo častým předmětem dotazů a žádostí o konzultace. Tazateli jsou zpravidla zaměstnanci jednotlivých orgánů veřejné správy, výjimkou však nejsou ani zastupitelé. Několik orgánů veřejné správy se obrátilo na Úřad s žádostí o stanovisko ke zpracování osobních údajů, na které dopadá současně více právních předpisů. Předmětem zájmu bylo na-

př. využívání informačního systému evidence obyvatel pro zahajování správního řízení. Úřad v této souvislosti vyjádřil názor, že údaje potřebné k náležité identifikaci fyzické či právnické osoby pro účely zahájení správního řízení je nutno získat především v rámci výkonu kontrolních pravomocí; absence takového zjištění sama o sobě nemůže být důvodem pro vyhledávání v informačních systémech vedených jinými orgány.

Některé problémy při zpracování osobních údajů obecními a městskými úřady ve vedených evidencích souvisejí se vztahy odborného aparátu a zastupitelů. Zatímco prvně jmenovaní většinou znají a dodržují právní předpisy, zastupitelé někdy mají odlišné požadavky a domnívají se, že z titulu své funkce mají právo vědět téměř o všem, co se na „jejich" úřadu děje. V roce 2008 byl opakovaně řešen výše uvedený problém s dlouholetou pracovnicí jednoho z městských úřadů Jihočeského kraje.

Zásadu, že **veřejná správa může činit jen to, co jí zákon ukládá, případně umožňuje, nemůže prolomit ani případný souhlas subjektu údajů**, jak se o to v zájmu jistě dobré věci snažila jedna z pražských nemocnic s cílem napravit legislativní nedůslednost při poskytování rodných čísel novorozenců v řetězci Ministerstvo vnitra – matrika – porodnice – zdravotní pojišťovna. Navrhovaný model, kdy by **matrika získávala souhlas zákonných zástupců novorozenců s předáním jejich rodného čísla porodnici, tak nemohl Úřad doporučit. Zjednání nápravy je v kompetenci Ministerstva vnitra**, které bylo o problému informováno v únoru 2008.

Poměrně značná **neujasněnost** se dlouhodoběji objevuje **při poskytování osobních údajů podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím**. Opakovaně je Úřadem vysvětlován § 8a citovaného zákona odkazující na postup podle zákona o ochraně osobních údajů. Povinné subjekty se dopouštějí chyby i v tom, že souběžně se zveřejněním své odpovědi zveřejní i osobní údaje tazatele, což je bez jeho souhlasu nepřípustné. Objevuje se i různě motivovaná **tendence požadované informace záměrně neposkytnout s evidentně neadekvátním odkazem na povinnosti podle zákona o ochraně osobních údajů, jak tomu bylo např. při žádosti o výši ceny obecního bytu prodávaného do osobního vlastnictví určeného soudním znalcem**. Osobní údaje stávajícího nájemníka jsou zde irelevantní a nemohou být v této souvislosti bez jeho souhlasu poskytnuty, na soudní odhad však má potenciální zájemce o koupi bytu nepochybně právní nárok.

Opakovaně byly podávány dotazy na podmínky **zpřístupňování osobních údajů z evidencí obecní nebo městské policii**. V jednom případě městská policie vyžadovala osobní údaje majitele psa, aby mohla provádět kontroly dodržování vyhlášek o místních poplatcích ze psů, případně provádět další šetření týkající se napadení osob psem neznámého majitele. K tomu považovala za žádoucí přístup městské policie do evidence MěÚ i v mimoúřední hodiny. Úřad zaujal právní názor, že je to ve veřejném zájmu možné, nicméně evidence nemůže obsahovat údaje nad rámec rozsahu stanoveného právními předpisy, který je formalizován v ohlašovací kartě. V opačném případě by šlo o porušení povinnosti shromažďovat osobní údaje jen v rozsahu nezbytném pro naplnění stanoveného účelu, kterým je vybírání místních poplatků. Současně obecní policie může obdržet údaje jen v rozsahu nezbytně nutném pro své další šetření. Dálkový přístup do evidencí obcí obecní policii umožňuje až novela zákona o obecní policii platná od 1. ledna 2009. Technicky však musí být vyřešeno, aby obecní policie měla přístup jen k základním identifikačním údajům držitele psa, tj. jméno, příjmení, datum narození, bydliště a faktu, zda byl či nebyl poplatek zaplacen. Tento právní názor byl prezentován i na jednání svolaném Ministerstvem financí. Za účasti Ministerstva vnitra bylo 26. listopadu 2008 konstatováno, že obě ministerstva připraví odborné stanovisko, které bude zasláno Úřadu k vyjádření a následně distribuováno různými informač-

ními kanály obecním úřadům, s cílem sjednotit přístup na zcela transparentních právních východiscích.

Předmětem dotazů jsou i **problémy vyplývající z nově účinných zákonů**. Příkladem toho je žádost o stanovisko **k součinnosti Archivu Ministerstva zahraničních věcí České republiky** (dále jen „AMZV") **s Úřadem pro studium totalitních režimů** (dále jen „ÚSTR") podle § 5 odst. 2 zákona č. 181/2007 Sb., o Ústavu pro studium totalitních režimů a o Archivu bezpečnostních složek a o změně některých zákonů, který nabyl účinnosti k 1. 8. 2007. Úřad mj. konstatoval, že tento zákon nezbavuje subjekty, na které se vztahuje povinnost součinnosti dle § 5 odst. 2 tohoto zákona, povinnosti dostát požadavkům zákona o ochraně osobních údajů a zákona č. 499/2004 Sb., o archivnictví a spisové službě. Citované právní předpisy neupravují odlišný režim pro zpracování osobních údajů při činnostech ÚSTR. Zpřístupnění archivních materiálů AMZV obecně umožňuje ustanovení § 5 odst. 2 písm. a) zákona o ochraně osobních údajů, které obsahuje oprávnění správce osobních údajů zpracovávat data i bez souhlasu subjektu údajů v případě, kdy je to nezbytné pro dodržení právní povinnosti správce. Úřad dále upozornil na zvláštní ochranu citlivých údajů ve smyslu § 4 písm. b) zákona o ochraně osobních údajů, poskytovanou v případě žijících fyzických osob nejen v tomto zákoně, ale také v § 37 odst. 2 zákona o archivnictví a spisové službě; uvedl, že jsou-li součástí archivních materiálů citlivé údaje žijících osob, není AZMV povinen ÚSTR tyto údaje poskytnout bez souhlasu dotčených osob. Úřad připomněl, že uvedené znamená oprávnění odepřít pouze určité informace, nikoli veškeré dokumenty.

K otázce charakteru informace o členství v KSČ s ohledem na účel zřízení ÚSTR a předmět jeho bádání Úřad konstatoval, že je možné se přiklonit k závěru, že členství v KSČ před rokem 1990 není nutno považovat za citlivý údaj ve smyslu citovaného ustanovení.

Finanční úřady, finanční ředitelství a Ministerstvo financí

Provedené kontroly narazily na několik závažných problémů:

Předně se ukazuje, že daňová správa je natolik propojena, že nelze kontrolovat jednotlivé stupně nezávisle. Byla provedena kontrola dvou finančních úřadů a příslušných finančních ředitelství a nakonec probíhá i kontrola Ministerstva financí; dále byla na finančních úřadech ukončena jedna incidenční kontrola a druhá je přerušena vzhledem k níže uvedeným problémům.

První problém, na který kontrola narazila, byl výklad ustanovení § 3 odst. 6 písm. f) zákona o ochraně osobních údajů: *Ustanovení § 5 odst. 1 a § 11 a 12 se nepoužijí pro zpracování osobních údajů nezbytných pro plnění povinností správce stanovených zvláštními zákony pro zajištění významného finančního zájmu České republiky nebo Evropské unie, kterým je zejména stabilita finančního trhu a měny, fungování peněžního oběhu a platebního styku, jakož i rozpočtová a daňová opatření,* přičemž pod čarou jsou jako příklad uváděny zákon č. 218/2000 Sb., o rozpočtových pravidlech a o změně některých souvisejících zákonů (rozpočtová pravidla), ve znění pozdějších předpisů, zákon č. 250/2000 Sb., o rozpočtových pravidlech územních rozpočtů, ve znění pozdějších předpisů, zákon č. 6/1993 Sb., o České národní bance, ve znění pozdějších předpisů, a zákon č. 212/1992 Sb., o soustavě daní, ve znění zákona č. 302/1993 Sb., ale ne zákon č. 337/1992 Sb., o správě daní a poplatků (dále jen „zákon o správě daní").

Dle názoru Úřadu vyplývajícího z výše uvedeného ustanovení zákona o ochraně osobních údajů běžná daňová správa nespadá pod zákonem stanovenou výjimku, neboť se nejedná o *významný finanční zájem České republiky nebo Evropské unie*. Při posuzování ochrany osobních údajů v daňové sféře je třeba mít na zřeteli, že aplikací zákona o správě daní dochází k omezení práva na nedotknutelnost

soukromí osoby (čl. 7 Listiny) a že při používání ustanovení o mezích základních práv a svobod musí být ušetřena jejich podstata a smysl. To znamená, že správce daně musí činit opatření potřebná ke správnému a úplnému zjištění, stanovení a splnění daňových povinností s důrazem na šetření podstaty a smyslu práva na nedotknutelnost soukromí osoby (čl. 4 Listiny). Rozsáhlé pravomoci při zjišťování skutečností rozhodných pro řádné vyměření daně a právo na ochranu soukromí jen potvrzují legitimnost působnosti Úřadu v souvislostí dozorovou činností při správě daní a poplatků.

Dalším problémem je mlčenlivost vůči kontrolujícím. Kontrolující se dovolávali ustanovení § 2 odst. 5 zákona o správě daní: *Jakékoliv osoby, které byly jakkoliv zúčastněny na daňovém řízení, jsou povinny zachovávat mlčenlivost o všem, co se v řízení nebo v souvislosti s ním dozvěděly; tato povinnost však nezprošťuje správce daně povinnosti poskytnout údaje* ***osobě, která prokáže, že je oprávněna tyto údaje získat podle zvláštního právního předpisu*** (kterým je právě zákon o ochraně osobních údajů). Ustanovení § 24 odst. 3 písm. b) zákona o správě daní říká, že: *„Pracovníci správce daně mohou poskytovat informace… orgánům oprávněným ze zvláštního zákona ke* ***kontrolní*** *či dohlídkové činnosti u správce daně při výkonu správy daní* ***v rozsahu jejich zákonného oprávnění.“*** Dle názoru Úřadu toto ustanovení potvrzuje práva jeho kontrolu provádějících pracovníků. (Rozsah oprávnění kontrolujících vymezuje § 37 zákona o ochraně osobních údajů.) Tudíž pracovníci daňové správy se vůči nim nemohou odvolávat na povinnosti mlčenlivosti.

Stalo se tak v případě, kdy stěžovatel tvrdil, že jeho osobní údaje byly vloženy do spisu firmy, jejímž je jednatelem, přičemž uváděl, že nijak nesouvisejí s daňovou povinností dané firmy. V tomto případě bylo aplikovatelné ustanovení § 21 odst.1 a 3 zákona o ochraně osobních údajů, neboť stěžovatel poukazoval, *„že správce provádí zpracování jeho osobních údajů, které je v rozporu se zákonem“*, a obrátil se na Úřad, aby zjednal nápravu. Aby kontrolující pracovníci Úřadu mohli ověřit, zda jsou či nejsou stěžovatelovy osobní údaje zpracovávány v souladu se zákonem, musí mít možnost zjistit, zda se v daňovém spisu firmy opravdu nalézají osobní údaje stěžovatele, které nijak nesouvisejí s daňovou povinností firmy, či ne. Tomu se příslušný finanční úřad brání. Kontrolující se naopak pokoušejí vymoci si své pravomoci udělením pořádkové pokuty.

Je třeba si uvědomit, že na rozdíl od správních nebo trestních spisů, které po ukončení kauzy končí v archivu, může být daňový spis, pokud se daňový poplatník nebude stěhovat, jeden pro celý život. A i když se přestěhuje, jeho elektronická podoba bude stále živá po celé republice a po celý jeho život. Tudíž se lze ptát, zda jsou informace o dávno propadlých a zaplacených daňových povinnostech likvidovány. Daňová správa má velké pravomoce při zpracovávání osobních údajů poplatníků, může získávat údaje, týkající se možných činností, které by mohly být zdroji financí, prakticky od kohokoliv (pod pokutou až dva miliony korun), a tudíž je ochrana osobních údajů v daňové sféře nezbytná.

Další zásadní rozpor se týká ustanovení § 12 zákona o ochraně osobních údajů, podle kterého má každý subjekt údajů právo vědět, jaké osobní údaje jsou o něm zpracovávány; navíc domnívá-li se, že jde *o zpracovávání v rozporu s ochranou soukromého a osobního života subjektů údajů, nebo v rozporu se zákonem o ochraně osobních údajů, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování* může požádat o vysvětlení, případně požadovat odstranění takového stavu zpracování (§ 21 zákona o ochraně osobních údajů). Smyslem právě zmíněných ustanovení je ochrana před neoprávněným shromažďováním, zpřístupňováním nebo jiným zneužíváním osobních údajů (čl. 10 Listiny). Rozsah osobních údajů, které jsou o poplatníkovi shromážděny a zpracovávány, musí být nezbytný pro daňovou správu.

Finanční úřady se brání odkazem na ustanovení § 23 zákona o správě daní, resp. jeho chybným výkladem, kdy argumentují, že daňový subjekt nemá právo nahlížet do neveřejné části. Zde je třeba upozornit, že záleží často na konkrétním finančním úřadu a jeho pravidlech, nebo dokonce na konkrétním pracovníkovi daňové správy, které dokumenty vloží do veřejné a které do neveřejné části.

Dle výkladu obsaženém v rozsudku Nejvyššího správního soudu 1Afs 94/2006 – 60 je limitem nahlížení do neveřejné části ochrana informací, které se týkají jiných subjektů: *Cílem vyjmenovaných omezení je zcela evidentní ochrana informací, týkajících se ostatních subjektů, jež má správce daně k dispozici a ze kterých pro jejich vhodnost může vycházet při stanovení daně za užití pomůcek. Jestliže však správce daně při stanovení daňové povinnosti vycházel pouze z údajů, které se týkaly žalobce samotného, nebyl zde žádný důvod žalobci odepřít seznámení se s pomůckou, na základě které správce daně dospěl k výši daně.*

Při kontrole Úřad dále upozornil na větší ochranu zpracování citlivých údajů, což je např. odsouzení za trestný čin nebo zdravotní stav.

Celá daňová správa pracuje na jednotném Automatizovaném daňovém informačním systému územních finančních orgánů České republiky (ADIS). Speciálně při kontrole možného zneužití osobních údajů daňové správy, se kontrolující pracovníci Úřadu zaměřili na splnění nového ustanovení zákona o ochraně osobních údajů § 13 zákona, odst. 4. písm. c): *V oblasti automatizovaného zpracování osobních údajů je správce povinen pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány.* Z toho důvodu byla posléze zahájena kontrola Ministerstva financí.

Na Úřad byly v průběhu uvedených kontrol podány dvě stížnosti: jedna se týkala podezření ze zneužití osobních údajů získaných z daňové správy k soukromým účelům, druhá stížnost se týkala zpracování osobních údajů, které nijak nesouvisely s daňovou správou, v daňovém spise.

Kazuistika – další případy

Výzkum osudů osob pobývajících do zletilosti v zařízeních pro ústavní nebo ochrannou výchovu

Usnesením vlády ČR bylo Republikovému výboru pro prevenci kriminality uloženo provést výzkum dalších osudů všech osob, jež do nabytí zletilosti pobývaly ve školských zařízeních pro výkon ústavní výchovy nebo ochranné výchovy (dále jen „zařízení“) a v letech 1995 až 2004 z nich odešly do běžného života (dále jen „dotčené osoby“). Zejména byla zjišťována míra jejich konfliktů se zákony a možná vazba mezi institucionální péčí o ně a jejich obtížným začleňováním do běžného života, případně kriminální kariérou.

Sbírání dat probíhalo od března 2005, přičemž prostřednictvím vzorového dotazníku zpracovaného odborem a rozeslaného elektronickou poštou bylo ohledně každé ze 17 454 dotčených osob shromažďováno mimo rodného čísla ještě dvanáct dalších údajů: pohlaví, věk při umístění do ústavní péče, typ nařízeného opatření, typ ústavu, do kterého byla dotčená osoba umístěna, délka pobytu v zařízení včetně smluvního pobytu, věk při odchodu, důvod odchodu, prostředí, do kterého dotčená osoba odešla, počet krátkodobých útěků, počet dlouhodobých útěků, počet dní na krátkodobém útěku, počet dní na dlouhodobém útěku a také číselné označení diagnostického ústavu, jehož pracovníkem byla shromažďovaná data sebrána. Shromažďovaná rodná čísla sloužila k identifikaci dotčených osob. Při transferu sbíraných údajů z jednotlivých zařízení do diagnostických ústavů nebyla používána elektronická pošta. Kontrolu údajů, sebraných v jejich spádové oblasti, prováděly diagnostické ústavy.

Data byla posléze spojena z celého území České republiky. Cílem spojení bylo vytvořit soubor dat, s nímž se ve výzkumu dále pracovalo. Bylo možné od něj oddělit soubor rodných čísel za účelem jejich předání příslušnému orgánu k doplnění údajů o trestné činnosti dotčených osob. Kontrolou bylo zjištěno, že při provádění výzkumu nebyl opatřován souhlas se zpracováním osobních údajů od osob, jejichž osobní údaje byly zpracovávány.

Ze zákona o výkonu ústavní výchovy nebo ochranné výchovy ve školských zařízeních a o preventivně výchovné péči ve školských zařízeních, je určeno, že zařízení mohou informace o dětech na žádost poskytovat pouze diagnostickému ústavu, v jehož územním obvodu se nacházejí, zákonným zástupcům a orgánům sociálněprávní ochrany dětí.

Orgán veřejné správy zpracovával osobní údaje k jinému účelu, než ke kterému byly shromážděny, aniž k tomu daly subjekty údajů předem souhlas.

Kontrolovaný subjekt nerespektoval povinnost vyplývající ze zákona o ochraně osobních údajů nesdružovat osobní údaje, které byly získány k rozdílným účelům. **Orgán veřejné správy jako správce při zpracování osobních údajů dotčených osob (nezletilých) postupoval v rozporu se zákonem o ochraně osobních údajů**, protože neuchovával osobní údaje pouze po dobu, která byla nezbytná k účelu jejich zpracování, nezpracovával osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, přičemž k tomu nedaly subjekty údajů předem souhlas, sdružoval osobní údaje, které byly získány k rozdílným účelům, nezpracovával citlivé údaje jen v mezích oprávnění stanovených v zákoně o ochraně osobních údajů a neprovedl likvidaci osobních údajů, jakmile pominul účel, pro který byly osobní údaje zpracovány.

Kontrolou bylo prokázáno, že uvedeným jednáním orgánu veřejné správy došlo k porušení zákona o ochraně osobních údajů **v některých jeho ustanoveních, a proto mu byla uložena opatření k nápravě.**

Kontrola zpracování osobních údajů hostů státní instituce

I.

V roce 2007 vstoupili kontrolující na jedno z ministerstev a byli nuceni odevzdat občanské průkazy (přestože předložili služební průkazy), z nichž byly okopírovány osobní údaje.

Na tomto ministerstvu byla v roce 2008 provedena kontrola. Bylo však zjištěno, že není vedena žádná evidence návštěv: Pokud někdo chce navštívit některého zaměstnance ministerstva, pak se mu na vrátnici ohlásí prostřednictvím vnitřního telefonu a příslušný zaměstnanec, nebo jeho podřízený, návštěvu osobně doprovodí do kanceláře na jednání a posléze ji opět odvede k vrátnici. Vrátný pouze kontroluje, zda je návštěva stále pod dozorem zaměstnance ministerstva.

Z hlediska ochrany osobních údajů je tato praxe správná.

Je třeba si uvědomit, že občan není povinen nosit s sebou občanský průkaz. Výše uvedený systém doprovodu návštěv činí zodpovědným hostitele, tj. doprovázejícího zaměstnance ministerstva. *(Poznámka: Obdobná kontrola evidence hostů byla se stejně pozitivním závěrem provedena v soukromé firmě.)*

Takový způsob nakládání s osobními údaji Úřad vítá.

II.

Paní XY požádala ministerstvo o dvě různá rozhodnutí a ke své žádosti přiložila ověřené kopie, na jejichž základě mělo být rozhodnuto. Ministerstvo nejenže nereagovalo, ale dokonce na její urgenci přijetí žádosti popřelo. Zareagovalo teprve na

další stížnost, a aniž rozhodlo v jedné žádosti, postoupilo druhou žádost pro nepříslušnost jiné instituci, přičemž této jiné instituci poslalo neověřené kopie dokumentů a původní si ponechalo, i když muselo být jasné, že další instituce nemůže na základě neověřených kopií rozhodnout. Na dopis stěžovatelky o zpětvzetí žádosti a o vrácení všech dokumentů ministerstvo opět nereagovalo a teprve po zahájení kontroly zpracování osobních údajů Úřadem byly ověřené kopie žadatelce vráceny.

Kontrolou bylo zjištěno, že běžná praxe ministerstva je taková, že v případě postoupení pro nepříslušnost je spis okopírován a teprve poté odeslán. Kontrola Úřadu dospěla k závěru, že jde o porušování zákona o ochraně osobních údajů, neboť v případě postoupení věci pro nepříslušnost neexistuje právní titul pro zpracovávání osobních údajů (kromě těch, které jsou obsaženy v Rozhodnutí o postoupení).

Uchovávání kopií příloh podání, která jsou pro nepříslušnost postupována jinému orgánu, je obecně nedůvodné. Ustanovení § 12 správního řádu, ani jiné ustanovení tohoto zákona, neupravuje, jakým způsobem má být naloženo s kopiemi, které správní orgán před postoupením daného podnětu pořídil. Úpravu této otázky však zcela jistě obsahuje právě zákon o ochraně osobních údajů, a to především v ustanovení § 5 odst. 1 písm. d) a e) a § 5 odst. 2. Z uvedeného vyplývá, že správní orgán, kterému bylo doručeno podání, k jehož vyřízení není příslušný, má povinnost toto podání postoupit věcně příslušnému orgánu (je-li takový), přičemž jako doklad o tomto svém postupu si může, na základě citovaných ustanovení zákona o ochraně osobních údajů uchovat kopii předmětného podání, avšak již nikoli kopie všech jeho příloh (a tedy i všech zde uvedených osobních údajů), které s ohledem na fakt, že věc nevyřizuje, nejsou pro jeho činnost nezbytné. Automatickým pořizováním kopií veškerých podkladů podání by docházelo k vytváření zcela neopodstatněných, duplicitních souborů osobních údajů. Uchování kopií určitých příloh postoupeného podání musí být daný správce osobních údajů schopen vždy odůvodnit s ohledem na nezbytnost zpracování těchto osobních údajů pro účely, jejichž dosažení je v souladu s některým ustanovením podle § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů.

Správní řízení

V návaznosti na provedenou kontrolu byl dne 9. prosince 2008 vydán příkaz, ve kterém správní orgán konstatoval, že je prokázáno, že v souvislosti se žádostí o uznání zahraničního vysokoškolského vzdělání a se žádostí o uznání odborné způsobilosti a kvalifikace pro účely výkonu povolání učitele střední školy, uchovávalo Ministerstvo školství od 23. července 2007 (tj. od zpětvzetí žádosti) do ledna 2008 bez zákonného důvodu osobní údaje stěžovatelky, obsažené v přílohách žádostí, tj. notářsky ověřených kopiích diplomů a vysvědčení, čímž porušilo povinnost stanovenou v § 5 odst. 1 písm. e) zákona, tedy povinnost uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Popsaným jednáním tak ministerstvo spáchalo správní delikt, za který mu byla uložena pokuta ve výši 5 000 Kč. Vydaný příkaz nabyl právní moci dne 19. prosince 2008.

ZDRAVOTNICTVÍ

Zdravotnictví je předmětem stálého zájmu Úřadu pro ochranu osobních údajů mj. také proto, že zde dochází ke každodennímu zpracování citlivých údajů v masovém rozsahu. Riziko jejich zneužití je poměrně vysoké a závažné bývají zpravidla i důsledky pro subjekty údajů.

Zvláštní právní předpis (zákon č. 20/1966 Sb., o péči o zdraví lidu) stanoví velmi přesné (a současně i přísné) podmínky nakládání se zdravotnickými dokumentacemi. V souvislosti s tím jsou stanoveny i přesné podmínky pro zpracování citlivých údajů vypovídajících o zdravotním stavu. Přesto jsou poměrně časté případy, kdy zdravotnická zařízení (zahrnující ve smyslu zákona o péči o zdraví lidu i lékaře vykonávající soukromou praxi) zákonná pravidla nerespektují a dostávají se do střetu s povinnostmi stanovenými zákonem o ochraně osobních údajů. Citlivé údaje o zdravotním stavu mohou být zpracovávány podle ustanovení § 9 písm. c) a b) uvedeného zákona; pokud jsou zpracovávány na základě zvláštního právního předpisu (zákona o péči o zdraví lidu), mohou být zpracovány bez souhlasu subjektu údajů /viz § 5 odst. 2 písm. a) a c) zákona o ochraně osobních údajů/, je však třeba přihlédnout k ustanovení § 5 odst. 3 zákona o ochraně osobních údajů a velmi důsledně dbát práva na ochranu soukromého a osobního života subjektu údajů a ustanovení § 10 uvedeného zákona, tj. dbát, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti; je třeba také respektovat ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

Plně se na taková zpracování vztahují povinnosti osobní údaje náležitě zabezpečit, jak stanoví § 13 zákona o ochraně osobních údajů.

Úřad se ve své dozorové činnosti opírá o řadu evropských dokumentů, jako například:

- *Návrh směrnice Evropského Parlamentu a Rady o uplatňování práv pacientů v přeshraniční zdravotní péči (dokument č. KOM(2008)0414 v konečném znění vydala Evropská komise 2. 7. 2008),*
- *Pracovní dokument o zpracování osobních údajů týkajících se zdraví v elektronických zdravotních záznamech (EHR) (dokument č. WP 131 vydaný Pracovní skupinou pro ochranu dat podle článku 29 (WP 29) dne 15. 2. 2007),*
- *Evropská směrnice pro zdravotnické pracovníky týkající se zacházení s důvěrnými informacemi a práva na soukromí pacientů ve zdravotní péči (vydala společnost EuroSOCAP v květnu 2006),*
- *Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: e-Zdraví – vytváření lepší zdravotní péče pro evropské občany: Akční plán pro evropskou oblast e-Zdraví (dokument č. KOM(2004)0356) v konečném znění vydala Evropská komise dne 30. 4. 2004).*

Mezi zajímavými zkušenostmi aplikovatelnými i v podmínkách ČR je třeba zvláště upozornit na názory pracovní skupiny WP29 Evropské komise ve výše uvedeném pracovním dokumentu, který poskytuje určité vodítko k výkladu právního rámce ochrany osobních údajů EU aplikovatelného pro systémy EHR (Electronic Health Records – elektronických zdravotních záznamů). Dokument rovněž formuluje požadavky na vnitrostátní ochranná opatření při budování celostátních systémů EHR, která by se v různých členských státech EU měla používat jednotně. Pracovní skupina připomíná, že základním východiskem je obecný zákaz zpracování citlivých dat typu zdravotních údajů mimo zákonem stanovené výjimky, což se týká i odchylek v souvislosti se systémem EHR, přičemž zdůrazňuje nutnost úzkého výkladu těchto odchylek.

Dále zde Pracovní skupina vydává doporučení k 11 oblastem (např. identifikace a autentizace pacientů a zdravotníků, oprávnění pro přístup k EHR pro čtení a zápis, mezinárodní předávání lékařských záznamů nebo zabezpečení údajů, kontrolní mechanismy), v nichž jsou zvláštní ochranná opatření v rámci systému EHR zvláště potřebná, aby byla pacientům a dalším osobám zaručena práva na ochranu údajů. Kromě toho Pracovní skupina zdůrazňuje, že je nutné, aby systémy EHR byly zakládány a provozovány uvnitř solidního legislativního rámce ochranných opatření určených k ochraně osobních údajů, a to bez ohledu na specifický právní základ těchto systémů.

Úřad poskytl v roce 2008 pro oblast zdravotnictví konzultaci, jíž zaujal negativní stanovisko k povinnosti soukromých lékařů, uložené Ministerstvem zdravotnictví, uvádět v používaném razítku i osobní údaje nesouvisející s poskytováním zdravotní péče jako bydliště a soukromé telefonní číslo. Po upozornění Úřadu byla ministerstvem zjednána náprava.

Odmítavý právní názor zaujal Úřad i k otázce zveřejňování osobních údajů členů lékařských komisí, když oponoval mínění Ministerstva zdravotnictví, že tak lze činit jen se souhlasem lékařů. Závěr Úřadu, že pacient by měl, obdobně jako je tomu např. u soudních znalců, vědět, kdo o něm rozhodoval, podpořili na společném jednání v červenci 2008 i pracovníci Kanceláře veřejného ochránce práv.

K předávání rodných čísel novorozenců v řetězci Ministerstvo vnitra – příslušná matrika – porodnice – zdravotní pojišťovna, bylo konstatováno, že současný stav není legislativně dořešen a porodnice je skutečně odkázána až na sdělení zákonného zástupce novorozence. S ohledem na uvedené dospěl v daném případě Úřad k závěru, že stávající právní předpisy nezakládají (kromě souhlasu zákonného zástupce novorozeného dítěte s poskytnutím rodného čísla dítěte) právní titul pro poskytování rodných čísel novorozených dětí zdravotní pojišťovnou příslušnému zdravotnickému zařízení. Na tuto situaci, tj. legislativní mezery v ustanoveních upravujících vztahy zainteresovaných subjektů při přidělování rodného čísla a jeho následného využívání při poskytování zdravotní péče, tedy v řetězci Ministerstvo vnitra – matriční úřad – zdravotnické zařízení – zdravotní pojišťovna, Úřad dlouhodobě upozorňuje, zatím však se svými návrhy a připomínkami řešení problému, které musejí být systémové, neuspěl. Ministerstvo vnitra bylo o situaci, kdy matrika nemůže porodnici přidělené rodné číslo sdělit, čímž by odpadla řada praktických problémů, informováno.

Ačkoliv je většina zpracování v oblasti zdravotnictví upravena speciálním zákonem (zákon o péči o zdraví lidu) a nepodléhá oznamovací povinnosti dle zákona o ochraně osobních údajů, byla Úřadu oznámena i zpracování oznamovací povinnosti podléhající.

Jednak v případě vedení lékových karet u tří subjektů, které je zřídily jako službu pro pacienty za účelem sledování jejich preskripce. Pacient vyplněním formuláře dává výslovný souhlas s vedením této karty. Tato služba funguje, aby usnadnila a zkvalitnila péči o pacienta ve spolupráci s lékaři. Důvodem je kontrola interakcí léčiv v návaznosti na poskytnuté údaje o diagnózách. Jde o údaje výšky a váhy, o zdravotním stavu a výsledcích laboratorních vyšetření, o záznam onemocnění, genetických údajů, zdravotní diagnózy a potíží a o předepsaných a užívaných lécích a potravinových doplňcích. Údaje jsou uchovávány až dva roky. V lékové kartě se zatím vyskytují pouze údaje z dané lékárny, což znamená, že pokud si pacient vyzvedne léky jinde, nebude o tom v lékové kartě záznam. Časem by mohlo dojít na napojení systému celostátní evidence preskripce pacientů.

Údaj věku, pohlaví a druhu postižení zpracovávaly dva subjekty. Důvody jsou různé – žádosti o dotace, dotazníkové šetření, pojištění akcí, nákup vstupenek a dále nutnost vyplývající z charakteru sdružení a aktivit (jde o asociaci rodičů a přátel zdravotně postižených dětí).

Účelem zpracování a vedení lékařské karty jiného subjektu byla výdělečná činnost: subjekt nabízí garantovaný systém zdraví fungující jako program na 4 měsíce. Součástí tohoto programu je vstupní prohlídka, prohlídka po 2 měsících a prohlídka po ukončení programu. V případě, že nedojde ke zlepšení zdravotního stavu po absolvování celého programu, jsou peníze klientovi vráceny. Z důvodu vyhodnocení dopadu léčby jsou všechny výsledky prohlídek uchovávány.

V roce 2008 byla registrována i 4 oznámení týkají se lékařských výzkumů.

První oznámení žádá o registraci kamerového systému na pokoji pacientů trpících epileptickými záchvaty. Jelikož není možné být s pacientem na pokoji 24 hodin denně, kamerový systém pomáhá ošetřujícímu personálu s péčí o nemocného. Sestra může včas rozpoznat epileptický záchvat a poskytnout nemocnému pomoc. Zároveň pak díky záznamu může být zjištěna i příčina vzniku (to vede k rozvoji lékařského výzkumu v této oblasti).

Druhá registrace se vztahuje na genetiku dospělých lidí, kdy klient kontaktuje danou společnost, je mu proveden stěr ze sliznice na vnitřní části dásní a následně proveden kompletní genetický rozbor. Díky tomu se dá zjistit, jestli klient má či nemá vrozené dispozice k přibližně 20 chorobám (jaké je riziko, že klient může danou nemocí onemocnět). Na základě výsledků je mu pak doporučena prevence.

Třetí a čtvrté oznámení je spojené s vědeckovýzkumným bádáním v oblastech medicíny a genealogie za účelem zjištění četnosti určitého znaku v populaci. Klient může na základě svého zařazení do české DNA databáze zjistit, odkud pocházejí jeho předci, nalézt ztracené příbuzné, určit pravděpodobnost příbuznosti s jinou osobou, zjistit predispozice lidských vlastností a určit biologické vztahy s jinými osobami.

V oblasti zdravotnictví došlo Úřadu množství stížností; z nich 20 bylo odloženo jako nedůvodných, přičemž Úřad pokračoval v nadstandardní praxi: Nad rámec povinností ukládaných správním řádem poskytoval stěžovatelům vysvětlení, proč nedošlo k porušení povinností konkrétním správcem nebo zpracovatelem osobních údajů a současně jim bylo vždy doporučeno, jak v jejich věci dále postupovat.

Obsah stížností poukazoval na poskytování osobních údajů zaměstnanců jejich zaměstnavateli „závodním“ lékařům, v čemž stěžovatelé nesprávně spatřovali porušení zákona o ochraně osobních údajů.

Přetrvávajícím nešvarem bylo předávání osobních údajů novorozenců, respektive jejich zákonných zástupců, pojišťovacím zprostředkovatelům, kteří jim následně neetickým způsobem vnucovali produkty finančních institucí. Protože však zdroje těchto informací nebyly doloženy, nemohl Úřad uplatnit své dozorové kompetence.

Další okruh stížností se týkal zasílání nabídek obchodu a služeb listinnou poštou, kdy bylo konstatováno, že se tak děje v souladu s ustanovením § 5 odst. 5 zákona o ochraně osobních údajů. Stěžovatelům bylo doporučováno vyjádřit správcům nebo zpracovatelům písemně svůj nesouhlas s dalším zasíláním obdobných nabídek.

Poslední vlna stížností byla zaznamenána v listopadu 2008 v souvislosti s TV Nova medializovanými webovými stránkami www.znamylekar.cz. Jejich autor zpracoval s využitím údajů z veřejného obchodního rejstříku databázi řádově tisíců lékařů se soukromou praxí, v níž přispěvatelé hodnotí svého lékaře. Některá vyjádření hraničí s trestnou činností (např. pomluva) a jsou zřejmě v rozporu s občanským zákoníkem, nelze je však kvalifikovat jako porušení zákona o ochraně osobních údajů, neboť přispěvatelé nemají postavení správce ani zpracovatele osobních údajů. Autor webových stránek se zatím pouze v jednom případě dopustil shromažďování osobních údajů neuvedených v obchodním rejstříku ani v jiném veřejném seznamu (soukromého mobilního telefonního čísla lékařky) bez souhlasu subjektu údajů.

V rámci provedených kontrol byla v roce 2008 zjištěna řada porušení zákona o ochraně osobních údajů:

U nemocničních informačních systémů (NIS) bylo konstatováno, že zpracovávat údaje ve zdravotnické dokumentaci je nemocnice povinna dle ustanovení § 67a zákona o péči o zdraví lidu, tudíž se na ni vztahuje výjimka podle ustanovení § 9 písm. c) zákona o ochraně osobních údajů pro zpracování citlivých údajů, jimiž údaje o zdravotním stavu jsou. Přesto se na nemocnici, jako správce osobních údajů, vztahují povinnosti vyplývající ze zákona o ochraně osobních údajů, zvláště při zabezpečení před neoprávněným nebo nahodilým přístupem k osobním údajům. Informace uložené v NIS slouží lékařům jako podklad pro jejich další práci s pacientem. Do zdravotnické dokumentace konkrétního pacienta má mít možnost nahlížet pouze ten lékař, který pacienta opravdu léčí.

Aby byly splněny oba tyto požadavky, tj. nebyla příliš ztížena možnost oprávněných lékařů nahlížet do zdravotnické dokumentace pacientů na straně jedné, a zabránit neoprávněnému přístupu k citlivým údajům ostatních pacientů na straně druhé, existuje systém logování, kdy je každý přístup k osobním údajům konkrétního pacienta zaznamenán a v případě pochybností je možno zjistit důvody přístupu k datům. Jelikož ovšem kontrola pomocí logů je prováděna pouze namátkově a většinou až ve chvíli, kdy k úniku (nebo podezření) došlo, je třeba i ztížit přístup k osobním údajům jednotlivých pacientů tím, že nebude možno nalézt seznam všech (současných či bývalých) pacientů a vstoupit do zdravotnické dokumentace jednotlivce, je však třeba pro první přístup ke konkrétnímu pacientovi zadat pojišťovací číslo (rodné číslo); nahlížet do seznamu všech pacientů s jejich rodnými čísly lze jen ve výjimečných případech (např. je-li pacient v bezvědomí) – a to opět pouze po dalším logování. Používat seznam všech bývalých a současných pacientů jako zdroj informací o jejich rodném čísle a bydlišti, popř. příbuzných, je vyloučeno.

Přístup jednotlivých zaměstnanců nemocnice musí být určen podle jejich postavení: pouze konsiliární lékaři mají přístup ke zdravotnické dokumentaci všech pacientů, sestry pouze k dokumentaci pacientů z příslušného oddělení, laboranti pracují pouze s napsanými žádankami. Lze také požadovat, aby do zdravotnické dokumentace měli přístup pouze lékaři a zdravotní pracovníci oddělení, na kterém je pacient právě ošetřován, popř. toto zpřísnění požadovat pouze pro vybraná oddělení, např. onkologické, gynekologické, psychiatrické, kožní, genetické a jiné, kde je citlivost údajů a možnost jejich zneužití (psychické choroby, potraty) ještě větší než u běžných onemocnění.

Poslední možnost ochrany je ponechána na vůli pacienta: ten má mít možnost požadovat, aby do jeho zdravotnické dokumentace měl přístup pouze jeho ošetřující lékař.

Zabezpečení NIS lze shrnout do tří podmínek:

- Bez znalosti pojišťovacího (rodného) čísla nelze nalézt žádnou informaci o pacientovi daného jména ani žádné bližší informace o jeho zdravotním stavu.
- Jednotliví zdravotní pracovníci mají různá oprávnění k nahlížení do zdravotnické dokumentace.
- Lze zjistit, kdo vstupoval do zdravotnické dokumentace daného pacienta, kdo ji četl, měnil, připisoval do ní či z ní vypisoval, eventuálně v ní cokoli rušil.

Kazuistika

I.

Ve zdravotnickém zařízení v Praze 1 došlo k tomu, že při ukončení pracovního poměru byly lékaři odneseny (odcizeny) listinné zdravotní dokumentace pacientů tohoto zdravotnického zařízení.

Při šetření vyšlo najevo, že v uvedeném zdravotnickém zařízení nelze přesně zjistit, kdy je který lékař jeho zaměstnancem a kdy zde vykonává svou soukromou praxi. Uvedené zdravotnické zařízení nevedlo písemnou evidenci o předávání zdravot-

nické dokumentace svých pacientů novým lékařům, a to bez ohledu na to, zda šlo o vlastní zaměstnance nebo smluvní lékaře. Tato skutečnost je ještě předmětem dalšího šetření. Původní podezření na neoprávněné nakládání se zdravotnickou dokumentací lékaři, kteří zde již praxi nevykonávají, se neprokázalo.

II.
Praktické lékařce byla odebrána registrace k výkonu nestátního zdravotnického zařízení v oboru praktického lékaře. Přes několik výzev odmítla předat zdravotnickou dokumentaci svých pacientů. Svou pracovní neschopnost vydávala za důvod, proč zdravotní dokumentaci nevydá. Ve spolupráci s příslušným Odborem sociální a zdravotní péče kraje a Policie ČR se podařilo zdravotní dokumentaci zajistit a předat příslušnému státnímu orgánu. Kontrolou bylo zjištěno, že lékařka měla zdravotní dokumentaci uloženou v rozporu s § 13 zákona o ochraně osobních údajů (v nevyhovujících pronajatých prostorách, ke kterým mělo přístup více neoprávněných osob). Navíc byla zdravotní dokumentace uložena v prostorách, kde hrozilo její poškození a zničení.

V druhostupňovém řízení předseda Úřadu nevyhověl námitkám uvedené lékařky, u níž bylo kontrolou zjištěno, že po zrušení zdravotnického zařízení, které provozovala, nepředala, ani přes několikeré výzvy, příslušnému krajskému úřadu zdravotnickou dokumentaci svých bývalých pacientů, jak k tomu byla povinna podle zákona č. 201/966 Sb., o péči o zdraví lidu. V průběhu kontroly provedené Úřadem bylo zjištěno, že zdravotnická dokumentace (597 pacientů) je uložena v budově, ve které sídlí lékárna, v zadní místnosti za touto lékárnou. Dokumentace byla uložena z velké části volně (na stole i na zemi), přičemž klíč od této místnosti byl k dispozici v prostorách lékárny. Tento stav byl posouzen jako porušení povinnosti správce osobních údajů podle § 13 odst. 1 zákona o ochraně osobvních údajů, tedy povinnosti 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, přičemž tato povinnost platí i po ukončení činnosti, při níž docházelo ke zpracování osobních údajů, tedy v daném případě po zrušení registrace nestátního zdravotnického zařízení. Nalezená dokumentace byla zajištěna ve spolupráci s Policií České republiky a pracovníky příslušného krajského úřadu. Předseda Úřadu v této souvislosti dále uvedl, že v daném případě se jednalo o nakládání s údaji, které naplňují definici citlivého údaje dle § 4 písm. b) zákona, jejichž zpracování podléhá přísnějšímu režimu. Tomuto charakteru údajů musí proto odpovídat i přístup k posouzení možných rizik a přijetí vhodných opatření ve smyslu § 13 odst. 1 citovaného zákona. Kontrolou zjištěný stav však zcela zjevně vypovídal o tom, že lékařka svoji povinnost dle tohoto ustanovení buď zcela opominula, nebo výrazně podcenila, přičemž důsledkem byl stav, kdy citlivé údaje pacientů byly po delší dobu vystaveny zvýšenému riziku ztráty či zneužití.

III.
Podnět proti NCO-NZO (Národní centrum ošetřovatelství a nelékařských zdravotnických oborů) zaslal ošetřovatel, který se zúčastňuje povinného doškolování nelékařských pracovníků ve zdravotnictví i nepovinných přednášek a školení, které NCO-NZO organizuje. Stížnost směřovala proti zpracování nadbytečného rozsahu osobních údajů, zejména rodného čísla frekventantů nepovinných přednášek. V rámci šetření bylo zjištěno, že rozsah zpracovávaných osobních údajů u povinného celoživotního vzdělávání vyplývá z příslušných právních předpisů. Porušení zákona však bylo konstatováno v souvislosti s plněním informační povinnosti, jak ji vyžaduje § 11 zákona o ochraně osobních údajů. V průběhu šetření byla praxe změně-

na. Po ukončení šetření byla Úřadem zajištěna přednáška o ochraně osobních údajů pro zaměstnance NCO-NZO.

IV.

Dle podnětu praktická lékařka v době své hospitalizace uzavřela dohodu o činnosti se svou dcerou, studentkou pátého ročníku UK – obor všeobecné lékařství. Ta v době nepřítomnosti matky po dobu jednoho týdne prováděla lékařská vyšetření a údajně neoprávněně nahlížela a zapisovala údaje do zdravotní dokumentace pacientů a vypisovala recepty a doporučení na odborná lékařská vyšetření. Stejnou věc šetřilo MZ ČR, VZP ČR, krajský Odbor zdravotnictví ČLK.

Praktická lékařka byla po celou dobu své nepřítomnosti v neustálém „elektronickém" kontaktu s dcerou, a to prostřednictvím mobilního telefonu a prostřednictvím online napojení na svůj PC, který byl umístěn v ordinaci. Tedy její dcera vykonávala činnost zprostředkovatele mezi pacientem a nepřítomnou lékařkou, tj. sama nevykonávala práci lékaře nebo zdravotní sestry, ale ošetřovatele. Jako studentka 5 ročníku medicíny měla kvalifikaci pro výkon práce zdravotnického pracovníka – ošetřovatel.

V rámci šetření byly využity závěry VZP a ČLK. Ze závěrů ČLK vyplývá, že praktická lékařka se dopustila disciplinárního provinění a její jednání bylo v rozporu s § 9 odst. 2 písm. a) zákona č. 220/1991 Sb., zákon o České lékařské komoře, České stomatologické komoře a České lékárnické komoře. ČLK nezjistila, že by dcera praktické lékařky nahlížela, či zaznamenávala informace, do zdravotnické dokumentace. Kontrola Úřadu konstatovala, že kontrolovaná praktická lékařka neporušila zákon o ochraně osobních údajů, neboť její dcera měla jako ošetřovatel možnost nakládat se zdravotní dokumentací s tím, že nebylo zjištěno, že by konkrétně nahlížela do zdravotnické dokumentace pacientů nebo s ní jinak nakládala.

V.

Syn zemřelé pacientky si stěžoval na to, že při přebírání osobních věcí po své zemřelé matce si zaměstnanec nemocnice zapisoval jeho osobní údaje v rozsahu jméno, příjmení, adresa a číslo občanského průkazu. Kontrolou bylo zjištěno, že žádný zdravotnický předpis toto neupravuje. Proto byla věc hodnocena podle občanského zákoníku a zákona o ochraně osobních údajů. Bylo konstatováno, že nemocnice je oprávněna zpracovávat osobní údaje osob, kterým předává věci po osobách zemřelých, a to z důvodu právní jistoty a ochrany a povinnosti, kterou jim jako osobám, která dočasně nakládají s cizí věcí, ukládá občanský zákoník. Kontrolou bylo konstatováno, že nemocnice porušila § 11 odst. 1 zákona o ochraně osobních údajů, tj. nesplnila informační povinnost vůči subjektu údajů.

VI.

Na základě pravidelné lékařské prohlídky zaměstnanců, vyplnil praktický lékař poukazy (doporučení na odborná vyšetření, rehabilitace apod.) a nejméně ve třech případech tyto poukazy předal nadřízenému vyšetřovaných pracovníků (mistrovi). Důvodem bylo, aby pracovníkům ušetřil čas a nemuseli si pro tyto poukazy dojít v pracovní době sami. Došlo tak ale k porušení § 13 odst. 1 zákona o ochraně osobních údajů, tedy nepřijetí dostatečných opatření pro zabezpečení zpracovávaných osobních údajů, došlo tedy k neoprávněnému přístupu k osobním, navíc citlivých údajům.

VII.

Dva podněty se týkaly zdravotních pojišťoven. V obou případech vzniklo podezření, že zdravotní pojišťovna předala seznam svých pojištěnců komerční pojišťovně. Šetřením bylo zjištěno, že na základě smlouvy komerční pojišťovny vytiskly dopisy

s nabídkou svých pojistných komerčních zdravotnických služeb na svém hlavičkovém papíru, kde oslovovaly adresáty jménem zdravotní pojišťovny. Tyto dopisy a obálky předaly zdravotním pojišťovnám. Ty si na rozeslání dopisů najaly v souladu s § 6 zákona o ochraně osobních údajů zpracovatelskou společnost. Zdravotní pojišťovna nepředala jiné, komerční pojišťovně osobní údaje svých pojištěnců. Zdravotní pojišťovny postupovaly v souladu se zákonem o ochraně osobních údajů.

VIII.

V oblasti správního trestání je zdravotnictví přetrvávající problémovou oblastí, a to při zpracování osobních údajů obsažených ve zdravotnické dokumentaci, zejména pak při dodržování povinností týkajících se zabezpečení těchto údajů.

Jako příklad lze uvést lékaře, který po hádce s pacientem týkající se placení regulačních poplatků, předal tomuto pacientovi nejen jeho vlastní dokumentaci, ale i dokumentaci rodinných příslušníků „problémového" pacienta, které měl ve své péči, a to bez jejich vědomí a souhlasu. Zákon č. 20/1966 Sb., o péči o zdraví lidu, přitom stanovuje jak pravidla pro případ změny ošetřujícího lékaře (§ 67b odst. 13), tak pravidla pro určení osoby, která může být informována o zdravotním stavu pacienta (§ 67b odst. 12), přičemž v daném případě nebylo splněno ani jedno z nich. Tudíž byl opět porušen § 13 zákona o ochraně osobních údajů, neboť došlo k neoprávněnému přístupu k osobním, dokonce citlivým údajům.

Za nepřijatelný lze považovat též přístup vycházející ze zavedené praxe, která zjevně nepřináší dostatečné zabezpečení citlivých údajů obsažených ve zdravotnické dokumentaci, avšak byla a je dlouhodobě používána lékaři v daném zařízení. Jde o postup, kdy zásilky, včetně těch, které obsahují citlivé údaje vypovídající o zdravotním stavu, jsou umísťovány v prostorách polikliniky, které jsou během dne volně přístupné a kde zásilky přebírá smluvní přepravní společnost. Argumentace tím, že „to tak dělají všichni" a „nikdy se nic nestalo" zjevně neobstojí, neboť v takovém případě je jen otázkou času, kdy se „něco stane" a údaje natolik citlivé jako jsou údaje vypovídající o zdravotním stavu, budou vystaveny neoprávněnému zpracování třetími osobami.

IX.

Ne vždy jde v oblasti poskytování zdravotní péče o chyby, které se týkají zpracování citlivých údajů vypovídajících o zdravotním stavu. Tak tomu bylo i v případě lékaře, který vyvěsil na dveřích zdravotního střediska seznam svých 86 pacientů, kteří se přeregistrovali k jinému lékaři, s jejich osobními údaji v rozsahu jméno, příjmení a adresa trvalého pobytu. Dle svého vyjádření to učinil jako upozornění s žádostí, aby mu své rozhodnutí potvrdili, neboť jim chtěl dát možnost obrany před přeregistrací bez jejich vědomí. Dále přitom uvedl, že teoreticky mohl tyto pacienty osobně kontaktovat, ale při počtu cca 200 osob a při pracovním a časovém vytížení to bylo nereálné, a kdyby vyvěsil jenom výzvu o potvrzení přeregistrace bez seznamů, nemohli by reagovat ti, kteří o své přeregistraci nemuseli vědět. K vyvěšení seznamu pacientů, kde bylo pouze jméno a adresa, přistoupil až k jako poslednímu řešení, když jeho předchozí úřední postupy (např. stížnost u krajského úřadu) zůstaly bez výsledku. K tomu lze konstatovat, že zdravotnické zařízení zpracovává osobní údaje pacientů za účelem vedení zdravotnické dokumentace a poskytování zdravotnické péče. Zveřejnění osobních údajů o části pacientů uvedeným způsobem v souladu s tímto účelem nepochybně není.

X.

Práva a povinnosti při zpracování osobních údajů souvisejícím se zajišťováním zdravotní péče se řídí dle § 67b odst. 9 zákona č. 20/1966 Sb. zvláštním zákonem, kterým je zákon o ochraně osobních údajů. Zákon č. 20/1966 Sb., o péči o zdraví

lidu v § 67b odst. 13 také výslovně stanovuje, že v případě změny ošetřujícího lékaře je dosavadní lékař povinen předat nově zvolenému lékaři všechny informace potřebné pro zajištění návaznosti poskytování zdravotní péče. Účastník řízení je povinen přihlédnout k charakteru osobních údajů a zvolit odpovídající relevantní opatření pro zajištění bezpečnosti při jejich předávání, čemuž způsob zaslání zdravotnické dokumentace, resp. její uložení na místě, kde měla být vyzvednuta k doručení, neodpovídá; když jí účastník řízení nepředal smluvní přepravní společnosti prokazatelným způsobem, neměl jistotu, že nemůže být zcizena třetí osobou z místnosti, kam je volný přístup, a nevěděl ani následně, zda vůbec a komu byla doručena *(Pozn.: Rozhodnutí správního orgánu prvního stupně obsahující uvedený právní závěr bylo potvrzeno, na základě podaného rozkladu, i rozhodnutím předsedy Úřadu).*

Soudní přezkum

Bylo ukončeno soudní řízení s poliklinikou. Jednalo se o žalobu z roku 2007 proti rozhodnutí Úřadu, kterým byla poliklinice uložena pokuta ve výši 1 750 000 Kč za porušení povinnosti podle § 13 odst. 1 zákona o ochraně osobních údajů, a to v souvislosti s nálezem zdravotnické dokumentace (zdravotních karet) přibližně 2 000 pacientů, ke kterému došlo na konci roku 2005 ve sběrném dvoře. Tato dokumentace byla identifikována jako pocházející z budovy zdravotnického zařízení – polikliniky. Městský soud v Praze řízení o žalobě podané poliklinikou zastavil v září 2007 usnesením z důvodu neuhrazení soudního poplatku a Nejvyšší správní soud následně (v březnu 2008) zamítl kasační stížnost polikliniky proti tomuto usnesení.

INFORMAČNÍ SYSTÉMY V OBLASTI JUSTICE A STÁTNÍHO ZASTUPITELSTVÍ

Osobní údaje a činnost exekutorů

Se zpracováním osobních údajů v souvislosti s činností exekutorů se Úřad v roce 2008 setkal jednak při konzultacích a dále v oblasti kontrolního řízení, správního trestání a také (následně) v rámci soudního přezkumu rozhodnutí Úřadu. Jako problematický se jeví zejména způsob identifikace povinných v exekučním řízení a zveřejňování popř. zpřístupňování osobních údajů povinných exekutory.

V oblasti správního trestání nelze činnost exekutorů při zpracování osobních údajů považovat za marginální problém. Vedle zmiňovaného zpřístupnění osobních údajů povinných v exekučním řízení neoprávněným osobám, jde především o konkrétní postupy exekutora, případně jeho zaměstnanců, při plnění zákonem stanovených povinností.

Ke zpřístupňování osobních údajů účastníků exekučního řízení exekutorem

Kontrolou bylo zjišťováno, zda a jak exekutor, který je správcem osobních údajů, realizuje povinnosti stanovené mu zákonem – tj. zda zpracovává údaje pouze v souladu s účelem, k němuž byly shromážděny.

Shledáno bylo pochybení v práci exekutora, který předal kopie písemností spisu obsahující osobní údaje povinné osoby a tím zpřístupnil údaje neoprávněné osobě. Bylo také zjištěno, že k takovému postupu nezískal souhlas povinné osoby, jak by vyžadoval zákon o ochraně osobních údajů. Kontrolou bylo prokázáno, že uvedeným jednáním soudního exekutora došlo k porušení zákona v jeho ustanoveních § 5 odst. 1 písm. f) a § 5 odst. 2.

Za uvedený správní delikt byla exekutorovi ve správním řízení uložena pokuta.

K informační povinnosti exekutora vůči povinnému při zpracování osobních údajů

Kontrolou bylo zjištěno, že soudní exekutor, když povinný nahlížel do spisu, pořídil a do uvedeného spisu zařadil kopii jedné strany občanského průkazu povinného, obsahující mimo jiné jeho podobiznu, kvůli současné i budoucí identifikaci povinného. Zároveň mu sdělil, že tak činí za účelem jeho identifikace a že pořízená kopie bude založena do spisu vedeného ohledně exekuce na jeho majetek. Jiné informace v této souvislosti povinnému neposkytl.

Exekutor sice získal konkludentní souhlas povinného, ale neposkytl mu jakožto subjektu údajů informace v rozsahu požadovaném zákonem o ochraně osobních údajů v případě jejich shromažďování.

Kontrolou bylo prokázáno, že uvedeným jednáním soudního exekutora došlo k porušení zákona o ochraně osobních údajů v jeho ustanoveních § 5 odst. 4 a § 11 odst. 1 a 2. Ve správním řízení mu byla uložena pokuta.

Neoprávněné zpřístupnění osobních údajů povinných z exekučního spisu jiným osobám

Na základě podání se Úřad zabýval případem, kdy při nahlížení do spisu se stěžovatel seznámil s obsahem písemností, v nichž byly uvedeny osobní údaje jiných osob (identifikační, včetně rodných čísel) a další informace.

Při nahlížení do spisu byly povinnému zpřístupněny i osobní údaje jiných osob. Při zařazení do spisu měly zůstat přístupné jen osobní údaje související s exekucí. Soudní exekutor tak porušil jednak svou povinnost mlčenlivosti, jednak zpřístupnil neoprávněným osobám osobní údaje, s nimiž se seznámil při exekuční činnosti.

Soudní exekutor tedy jako správce nepřijal taková opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, čímž nesplnil povinnost vyplývající z ustanovení § 13 odst. 1 zákona o ochraně osobních údajů, za což mu byla ve správním řízení uložena pokuta.

Ke zpřístupnění osobních údajů povinného z registru evidence obyvatel

Soudní exekutor, který byl pověřen provedením exekuce, poskytl oprávněné straně kopii výpisu z centrální evidence obyvatel povinného.

Zákon o evidenci obyvatel stanoví, že subjekty, které získávají osobní údaje z informačního systému (informačního systému evidence obyvatel) podle zvláštního právního předpisu (v daném případě jde o zákon o soudních exekutorech a exekuční činnosti – exekuční řád), nejsou oprávněny k jejich shromažďování, předávání a využívání mimo působnost stanovenou v tomto předpisu. Ochrana osobních údajů při činnosti exekutora je zabezpečena v exekučním řádu také povinností exekutora zachovávat mlčenlivost o všech skutečnostech, o nichž se dozvěděl při provádění exekuční nebo další činnosti. V předmětné věci je meritorním způsobem určena manipulace s osobními údaji také ustanovením exekučního řádu, jež taxativně určuje, že identifikace fyzické osoby v návrhu na nařízení exekuce musí být provedena jejich osobními údaji, a to v rozsahu jméno, příjmení a bydliště.

Kontrolou bylo také zjištěno, že na webových stránkách Exekutorského úřadu byla umístěna instrukce k identifikaci povinných v návrzích na nařízení exekuce prostřednictvím jejich rodných čísel. Těmito skutky je prokázáno, že soudní exekutor nepřijal taková opatření, aby nemohlo dojít jednak k neoprávněnému přenosu osobních údajů a dále k jejich jinému neoprávněnému zpracování, tedy že nerespektoval povinnosti, uložené mu jako správci osobních údajů.

Kontrolou bylo prokázáno, že uvedeným jednáním soudního exekutora došlo k porušení ustanovení zákona o ochraně osobních údajů v jeho §§ 5 odst. 1 písm. f), 5 odst. 2 a 13 odst. 1. Za uvedené jednání byla soudnímu exekutorovi uložena pokuta.

Z rozhodovací činnosti

Ke zpřístupňování osobních údajů povinných exekutorem

Účastník řízení má v daném případě stanoven jako účel řádné provedení exekuce a vymožení dlužné částky. Tento proces zpracování osobních údajů se přitom skládá z řady jednotlivých úkonů (operací), při kterých je různým způsobem (shromáždění, uchování, použití, někdy i zveřejnění) zpracováván rozdílný rozsah osobních údajů.

Jedním z výše uvedených úkonů je tzv. výzva k dobrovolnému splnění povinnosti a její doručení povinnému. V daném případě je třeba konstatovat, že výzva k dobrovolnému splnění povinnosti je jedním z úkonů exekučního řízení (sice méně formalizovaným), stejně jako exekuční příkaz, usnesení exekutora apod., který je zachycen v písemné podobě v určité listině. Je zřejmé, že tato listina musí být povinnému řádně doručena, tak aby mohla vyvolat zamýšlený účinek. Jelikož exekuční řád až na výjimky neupravuje postup pro doručování, použijí se v souladu s ním přiměřeně ustanovení občanského soudního řádu. Byla-li písemnost uložena, je třeba v místě doručování zanechat adresátovi výzvu, jejíž náležitosti občanský soudní řád taxativně upravuje. V daném případě ze spisového materiálu vyplývá, že rozsah údajů uvedených na vylepené výzvě neodpovídal ustanovení občanského soudního řádu. Účastník řízení ve svém vyjádření dle správního orgánu ztotožňuje výzvu k dobrovolnému plnění s výzvou k vyzvednutí doručované písemnosti; obě tato ustanovení ovšem spolu nijak nesouvisejí a upravují hmotněprávně i procesně rozdílné instituty. Správný postup by podle správního orgánu byl takový, kdy by účastník řízení v domě vylepil výzvu o možnosti vyzvednout si doručované písemnosti, kterou by byla výzva k dobrovolnému splnění povinnosti, tzn. že by na výzvě uvedl pouze adresáta, své označení a dále u koho, kde a v který den byla písemnost (výzva k dobrovolnému splnění povinnosti) uložena a do kdy si ji může adresát vyzvednout. Pokud v dané věci účastník řízení postupoval tak, že vyvěsil v domě i další osobní údaje uvedené ve výzvě k dobrovolnému splnění povinnosti, zpřístupnil tím tyto údaje dalším osobám, které v tomto domě bydlí, resp. které do něj vstoupily, a tím použil tyto osobní údaje k jinému účelu, než ke kterému byl ze zákona o ochraně osobních údajů oprávněn.

V druhostupňovém řízení bylo předsedou potvrzeno rozhodnutí o uložení (v podstatě symbolické) sankce za výše uvedené porušení zákona o ochraně osobních údajů. Se závěry první instance, včetně výše uložené sankce, se plně ztotožnil.

Ve svém rozhodnutí předseda Úřadu zdůraznil, že zákon o ochraně osobních údajů se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby, a dále se vztahuje na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky. Exekutor jako orgán pověřený soudem působí v pozici orgánu veřejné moci, a proto může v rámci výkonu této své činnosti konat pouze to, co je mu zákonem povoleno.

Ohledně příslušnosti Úřadu k posuzování způsobu doručování listin předseda Úřadu konstatoval, že v daném případě ze strany Úřadu nejde o výklad uvedeného zákona, ale o aplikační přístup ve vztahu k zákonu o ochraně osobních údajů.

Uvedené názory vycházejí rovněž ze skutečnosti, že exekuční řízení není řízením veřejným, a není proto důvod, aby exekutor zveřejňoval osobní údaje povinného tak, jak se v daném případě prostřednictvím způsobu doručení výzvy vykonavatelem exekutora stalo.

Rozhodnutí Úřadu bylo napadeno správní žalobou, o které nebylo (Městským soudem v Praze) dosud rozhodnuto.

Ke zpracování rodného čísla exekutorem

Podle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů je správce osobních údajů povinen zpracovávat pouze přesné osobní údaje. Ze spisového materiálu však vyplývá, že exekutor zpracovával při jím prováděné exekuci nesprávné rodné číslo povinného, tedy nepochybně zpracovával nepřesný osobní údaj. Vzhledem k míře zásahu do soukromí povinného je přitom podle Úřadu jakožto správního orgánu nezbytné, aby měl účastník řízení (a obecně každý exekutor) ještě před provedením prvního úkonu jistotu v identifikaci povinného. Ze spisového materiálu přitom vyplývá, že účastník řízení na základě provedené lustrace v evidenci obyvatel a registru rodných čísel vybral jednu ze dvou možných fyzických osob a tuto dále považoval za povinného, aniž si správnost svého závěru dále ověřil. Ze spisového materiálu rovněž vyplývá, že ačkoliv byl účastník řízení upozorněn na použití nesprávného rodného čísla, v důsledku čehož své exekuční příkazy zrušil, přesto nadále zpracovával nepřesné rodné číslo a vydal exekuční příkaz opět proti subjektu, který nebyl v dané věci povinným.

Exekutor přitom má ze zákona široký rozsah oprávnění k provedení exekuce, a v případě, kdy je mu známo alespoň identifikační číslo povinného a místo podnikání, měl si v souladu s ustanoveními exekučního řádu, které ho opravňují k výkonu, vyžádat potřebné údaje, jimiž by ověřil správnost subjektu, proti němuž vydal exekuční příkaz. Úřad tedy spatřuje porušení povinnosti podle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů i ve skutečnosti, že účastník řízení již od počátku zpracovával nepřesný osobní údaj, kdy nesprávně provedl přiřazení dalších osobních údajů k údajům uvedeným k identifikaci povinného v návrhu na nařízení exekuce, resp. v usnesení soudu o pověření soudního exekutora provedením exekuce. Proti správnímu rozhodnutí o uložení pokuty byl podán rozklad.

Druhostupňové řízení

Předseda Úřadu, jako odvolací orgán, na základě podaného rozkladu potvrdil závěry prvního stupně, tedy to, že v daném případě došlo k porušení povinnosti podle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů (tj. povinnosti zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny). V této souvislosti uvedl, že ačkoli má rodné číslo svou zvláštní právní úpravu, jde rovněž o osobní údaj, jehož zpracování, pokud je systematické, podléhá rovněž právní úpravě zákona o ochraně osobních údajů.

V daném případě, kdy šlo o přiřazení rodného čísla k nesprávné osobě, které bylo navíc opakované, je zjevné, že exekutor nevyužil při zjišťování povinné osoby všech možností, které měl k dispozici, k identifikaci povinného. Na základě upozornění nesprávně označené osoby exekutor sice vydané exekuční příkazy zrušil a s nesprávně označenou osobou se vyrovnal, avšak současně nepřijal taková opatření, aby k obdobné chybě již nemohlo dojít. O tom, že přijatá opatření byla nedostatečná, a tedy o porušení ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů, svědčí skutečnost, že i další vydaný exekuční příkaz byl namířen proti nesprávně označené osobě. Exekutor tento příkaz zrušil teprve poté, co se tato osoba opět ohradila.

Předseda Úřadu se v této souvislosti vyjádřil i k otázce plnění povinnosti podle § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, pro který bylo původně správní řízení rovněž zahájeno, když uvedl, že účastník řízení měl právo rodné číslo využívat, a to i bez souhlasu subjektu údajů, neboť v daném případě vystupoval jako osoba pověřená výkonem soudního rozhodnutí, tedy bezpochyby jako subjekt, kterému svědčilo oprávnění zpracovávat osobní údaje fyzických osob z titulu výkonu exekuční činnosti, kdy na něj byla přenesena působnost soudu. Úřad vyjádřil v této souvislosti názor, že ačkoliv zákon o evidenci obyvatel a rodném čísle neumožňuje

soudnímu exekutorovi využívat rodná čísla při jakékoliv jeho činnosti, lze v daném případě rodné číslo v exekučním řízení použít, neboť bylo třeba rozlišit dvě osoby stejného jména, příjmení i data narození, a tudíž rodné číslo, které bylo získáno v souladu se zákonem, mělo identifikovat povinnou osobu. V obdobném případě tedy lze považovat rodné číslo za identifikátor nezbytný pro identifikaci povinného.

Obecně je však nutno trvat na tom, že občanský soudní řád povinnost identifikovat účastníky exekučního řízení (fyzické osoby) rodným číslem nestanoví. Teprve v případě, kdy je nezbytné a nutné odlišit od sebe jednotlivé osoby, lze kromě základních identifikačních údajů (jméno, příjmení, bydliště) použít i údaje další, a to především datum narození. Použití těchto čtyř osobních údajů je v naprosté většině případů dostačující pro jednoznačnou identifikaci subjektů údajů. V daném případě proto nejde o postup v rozporu s § 5 odst. 1 písm. f) zákona o ochraně osobních údajů.

Rozhodnutí Úřadu bylo napadeno správní žalobou, o které nebylo (Městským soudem v Praze) dosud rozhodnuto.

Soudní přezkum

V případě zpracování osobních údajů, konkrétně rodných čísel, exekutory se Úřad v roce 2008 dočkal potvrzení svých závěrů ze strany Nejvyššího správního soudu.

Šlo o rozhodnutí Úřadu z roku 2006, kterým byla uložena pokuta exekutorovi, jenž v rámci exekučního řízení vydal usnesení o ceně nemovitosti, ve kterém povinného označil také rodným číslem. Toto usnesení následně umístil na internetu. Úřad v tomto případě, v prvé i ve druhé instanci, konstatoval porušení povinnosti podle § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tj. povinnosti zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny.

Rozhodnutí Úřadu bylo napadeno správní žalobou k Městskému soudu v Praze (dále jen „Městský soud“), který v závěru roku 2007 rozhodl, že napadené rozhodnutí Úřadu se zrušuje a věc se vrací k dalšímu řízení. Městský soud se ve svém rozsudku (sp. zn. 11 Ca 53/2007) ztotožnil s názorem Úřadu, že pro označení účastníků exekučního řízení není nezbytné uvádět jejich rodná čísla a že oprávnění exekutora k přístupu do informačního systému evidence obyvatel a registru rodných čísel nezakládá automaticky oprávnění využívat rodná čísla v rámci veškeré činnosti exekutora. Je-li to v konkrétním případě nezbytné pro odlišení osob, lze (v souladu s požadavky § 79 a § 157 zákona č. 99/1963 Sb., občanský soudní řád) účastníka řízení určit dalšími údaji, zejména datem narození. Městský soud však dále konstatoval, že porušení zákona o ochraně osobních údajů bylo konstatováno podle ustanovení § 45 odst. 1 písm. c) tohoto zákona, z něhož však není zcela zřejmé, v jakém jednání tento správní delikt spočívá a jaký objekt by měl být tímto deliktem zasažen (tj. podle Městského soudu není formulace „zpracovává údaje způsobem, který neodpovídá stanovenému účelu“ dostatečně určitá, pokud tento účel není stanoven a ani příslušné zpracování není definováno vyčerpávajícím způsobem). Takto formulovanou skutkovou podstatu považoval Městský soud za natolik neurčitou, že (s ohledem na nezbytnost restriktivního výkladu v oblasti správního trestání) ji nelze na daný případ aplikovat. Městský soud tak dospěl k závěru, že ačkoli popsané jednání exekutora nebylo v souladu se zákonem o ochraně osobních údajů, pokutu za toto jednání uložit nelze.

Na základě kasační stížnosti podané Úřadem proti tomuto rozsudku Městského soudu se případem zabýval Nejvyšší správní soud, který svým rozsudkem z července 2008 (sp. zn. 1 As 36/2008) citovaný rozsudek Městského soudu zrušil a věc vrátil tomuto soudu k dalšímu řízení. Nejvyšší správní soud ve svém rozsudku uvedl, že nesdílí názor Městského soudu, že skutková podstata správního deliktu podle § 45 odst. 1 písm. c) zákona o ochraně osobních údajů je formulována příliš obecně, neboť účel zpracování (k němuž mohou být údaje zpracovány) má pod-

le § 5 odst. 1 písm. a) citovaného zákona stanovit sám správce, popř. jej jako v tomto případě stanoví zákon, a každý subjekt, který údaje zpracovává, si tedy účelu zpracování musí být vědom. Obdobně i pojem zpracování je v § 4 písm. e) zákona o ochraně osobních údajů podle Nejvyššího správního soudu definován dostatečně určitě. Postup Městského soudu, který pouze na základě úvahy, že vyjádření skutkové podstaty správního deliktu není dostatečně určité, dospěl k závěru, že toto ustanovení nelze vůbec aplikovat (tj. nikoli že nelze aplikovat na daný případ s ohledem na jeho okolnosti), považuje Nejvyšší správní soud za jednoznačné porušení vázanosti soudu právem a principu iura novit curia (lat., „právo zná soud“).

Z konzultační činnosti

Ke zpřístupňování osobních údajů exekutorům (povinnost součinnosti)

V souvislosti s činností exekutorů (popř. insolvenčních správců) se často vyskytuje otázka zpřístupnění informací o manželovi povinného, proti němuž směřuje exekuce, na žádost exekutora. Jde zejména o informace z evidencí či registrů vedených v rámci státní správy, a to jak soudy, orgány státní správy a samosprávy nebo obcemi, tak i právnickými či fyzickými osobami, pokud tyto rozhodují o právech a povinnostech.

Názor Úřadu je takový, že exekuční řád jasně stanoví povinnost třetím osobám poskytnout exekutorovi požadovanou součinnost, a to v poměrně širokém rozsahu, když dožádaný subjekt je povinen poskytnout veškeré údaje potřebné k provedení exekuce. Z uvedeného ustanovení současně vyplývá, že v odpovědi na písemnou žádost exekutora se nelze odvolat na povinnost mlčenlivosti podle zvláštního právního předpisu, tedy ani podle zákona o ochraně osobních údajů. Exekuční řád ukládá povinným orgánům, na základě písemné žádosti exekutora, povinnost sdělit údaje nejen o majetku povinného, ale také další informace, které jsou jim známy z jejich úřední činnosti.

Z hlediska ochrany osobních údajů jde v daném případě (tj. předávání osobních údajů exekutorovi) bezpochyby o zpracování osobních údajů, k němuž správce osobních údajů nepotřebuje souhlas subjektů údajů.

V případě, že exekutor, resp. insolvenční správce, požaduje údaje o jiných osobách než o povinném (např. o manželce), jejichž předání je, jak bylo uvedeno, nutno považovat za zpracování osobních údajů, je podle názoru Úřadu přinejmenším vhodné, aby svoji žádost řádně odůvodnil tak, aby dožádaný subjekt měl jistotu, že postupuje v souladu se zákonem o ochraně osobních údajů. Podle Úřadu má dožádaný subjekt, jako správce osobních údajů, který za zpracování údajů odpovídá, právo požadovat, aby písemná žádost exekutora byla odůvodněna, a to jak ve vztahu ke všem osobám, jejichž údaje jsou požadovány, tak i ve vztahu k vyžádanému rozsahu údajů. O předání údajů týkajících se manžela povinného tak lze uvažovat např. na základě sdělení exekutora, že dotčená osoba je manžel/ka povinného, který/á se na základě konkrétního zákonného ustanovení, případně úkonu exekutora, stal/a účastníkem řízení.

Obdobná situace nastává v případě insolvenčních správců postupujících podle insolvenčního zákona.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ A PROBLEMATIKA DNA

S problematikou nakládání s DNA a souvisejícím zpracováním osobních, respektive citlivých údajů, se Úřad v roce 2008 setkal jak v soukromé, tak i ve veřejné sféře. Toto zpracování osobních údajů se stává běžným, a protože jde o zpracování citlivých údajů, které může velmi vážně narušit soukromí, je třeba mu věnovat soustředěnou pozornost.

V oblasti problematiky DNA bylo možno se opírat o řadu významných dokumentů, jako například:

– *„Prováděcí pravidla Prümské úmluvy by měla zajistit přesnost ve výměně dat DNA a otisků prstů“ (vydal Evropský inspektor pro ochranu údajů (EDPS) dne 19. 12. 2007),*
– *„Pracovní dokument o genetických údajích“ (dokument č. WP 91 vydaný Pracovní skupinou pro ochranu dat podle článku 29 (WP 29) dne 17. 3. 2004),*
– *„Mezinárodní deklarace o lidských genetických datech“ (dokument č. SHS/EST/03/CIB–10/3 vydalo UNESCO dne 16. 10. 2003),*
– *„Zpráva Mezinárodní bioetické komise (IBC) o možnosti vypracování univerzálního nástroje pro bioetiku“ (dokument č. SHS/EST/02/CIB-9/5 (Rev. 3) vydalo UNESCO dne 13. 6. 2003).*

Jedním z nejvýznamnějších je právě druhý výše jmenovaný dokument.

Jeho účelem je určení problémové oblasti související se zpracováním genetických dat z hlediska ochrany osobních údajů a zjednodušení postupů v národních opatřeních přijatých v této oblasti na základě směrnice 95/46/ES.

V dokumentu se zdůrazňuje, že jakékoliv použití genetických údajů pro jiné účely, než je přímá ochrana zdraví subjektu údajů nebo provádění vědeckého výzkumu, musí vycházet z vnitrostátních právních předpisů, které by měly být v souladu se zásadami ochrany osobních údajů stanovenými ve výše zmíněné směrnici, zejména v souladu se zásadou účelu a proporcionality. S ohledem na tyto zásady je tedy plošné genetické testování protiprávní.

Národní databáze DNA

Na základě kontrolního plánu Úřadu byla provedena v letech 2006 – 2008 **kontrola Kriminalistického ústavu Policie ČR**, který zpracovává osobní a citlivé údaje **v Národní databázi DNA** (dále ND DNA).

Vznik databáze je podložen poznatkem, že ze stop, které se nacházejí na místě činu, lze zjistit profil možného pachatele, a srovnat jej s profily potencionálních zločinců, speciálně osob už dříve odsouzených.

Z hlediska ochrany osobních údajů je bukální stěr – výtěr části sliznice ústní dutiny pro zpracování příslušné DNA – nosičem osobních údajů a samotný profil je citlivým údajem. Policie České republiky (dále jen „Policie“) jako státní orgán může ovšem konat pouze to, co jí dovoluje zákon. Při zpracování osobních údajů má sice výjimky z některých povinností správce, citlivé údaje však Policie smí zpracovávat pouze tehdy, jde-li o zpracování *podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách* /§ 9 písm. i) zákona o ochraně osobních údajů/.

Zvláštní zákon, kterým byl v době kontroly platný zákon č. 283/1991 Sb., o Policii České republiky (dále jen „zákon o policii“), dával policistovi, *který při plnění úkolů policie nemůže získat osobní údaje, umožňující budoucí identifikaci, jiným způsobem, oprávnění u osob obviněných ze spáchání trestného činu, u osob ve výkonu trestu odnětí svobody za spáchání úmyslného trestného činu… odebírat bio-*

logické vzorky umožňující získání informací o genetickém vybavení. Dále zákon o policii umožňoval sdružovat osobní údaje a vytvářet databáze, ale zpracování citlivých údajů bylo možné pouze podle ustanovení § 42g zákona o policii, kde odst. 3 říká, že Policie *při zpracování osobních údajů je oprávněna zpracovávat citlivé údaje, je-li to s ohledem na povahu trestného činu nezbytné pro plnění úkolů Policie v souvislosti s trestním řízením.*

Tudíž český zákon o policii nepovoloval vytvářet databázi, která obsahuje profily všech odsouzených, ale pouze s ohledem na povahu trestného činu, který spáchali, neboť pouze s ohledem na trestný čin lze usuzovat, zda je obviněný a odsouzený dále nebezpečný pro společnost.

Proto bylo konstatováno, že při vytváření Národní databáze DNA je porušeno ustanovení § 9 zákona o ochraně osobních údajů, neboť citlivé údaje byly shromažďovány, dále zpracovávány a uchovávány v rozsahu, který přesahoval zákonné oprávnění. V takových případech by tedy bylo třeba aplikovat zákonem o ochraně osobních údajů vyžadované získání souhlasu subjektu údajů.

V roce 2008 schválený zákon č. 273/2008 Sb., o policii, sice už neobsahuje § 42 g v původním znění, přesto nelze jednoznačně říci, že umožňuje zpracování profilů všech odsouzených za úmyslný trestný čin, nemluvě o tom, že evropské instituce požadují, aby členské státy měly zpracování biometrických údajů speciálně upraveno zákonem.

V *Doporučení č. R(92) 1 Výboru ministrů členských států o využívání analýzy deoxyribonukleové kyseliny (DNA) v rámci systému trestní justice* je uvedeno:

Vytvoření a provozování jakéhokoli registru DNA pro účely vyšetřování a stíhání trestných činů by mělo být právně upraveno. Závazný pokyn policejního prezidenta takovou právní úpravou není. Jde o interní ustanovení, které dostatečně nesplňuje požadavek podřídit zpracování citlivých údajů zpřísněnému režimu, jak je vyjádřeno v zákoně o ochraně osobních údajů i v zákoně o policii.

Úprava provedená zákonem o policii je však značně nespecifická a problematická, takže vytváření ND DNA s ohledem na všechny zjištěné skutečnosti vyžaduje samostatnou právní úpravu, která bude formou zákona řešit všechny problémy, které existují při vytváření ND DNA: Měla by například taxativně vymezit okruhy osob, jimž lze biologické vzorky odebírat a ukládat je v ND DNA, upravit postup likvidace a vyřazení údajů z ND DNA, stanovit přesná pravidla pro dobu uchovávání záznamů v ND DNA a měla by také řešit otázky její kontroly.

Dále výše uvedené Doporučení podporuje výklad přístupu kontrolujících k odběrům DNA: *Výsledky analýzy DNA a informace z nich odvozené však mohou být uchovány, jestliže byl dotčený jednotlivec odsouzen pro závažné trestné činy ohrožující život, zdraví nebo bezpečnost osob. … Tam, kde vnitrostátní právní předpisy připouštějí odběr vzorků bez souhlasu podezřelého, měl by být vzorek odebrán, pouze pokud okolnosti případu takový úkon opodstatňují.*

Podle projednávaného *Ujednání mezi Ministerstvem vnitra ČR a Protiteroristickým prověřovacím centrem USA za účelem výměny prověřovacích informací týkajících se teroristů a osob podezřelých z terorismu* a podle Prümských či obdobných dohod, budou mít do české ND DNA přístup nejen čeští policisté, ale bezpečnostní složky zemí Evropské unie a Spojených států amerických. Vzhledem k tomu je třeba dodržet všechna doporučení Evropské unie a oprávněnost uložení profilů do ND DNA přísně kontrolovat.

Proti kontrolnímu protokolu podal Kriminalistický ústav námitky, kterým však předseda Úřadu, jako vedoucí kontrolního orgánu, v převážné většině nevyhověl a potvrdil závěry kontroly, včetně nápravného opatření, kterým je likvidace osobních údajů zpracovávaných v rozporu se zákonem o ochraně osobních údajů.

Úřad nezpochybňuje důležitost úkolů Policie, včetně předcházení trestné činnosti, nicméně s ohledem na charakter údajů, které při své činnosti Policie využívá a zejména s ohledem na dopad, který zpracování těchto dat pro dotčené osoby má: Kromě skutečnosti, že jde o citlivé údaje, je nutno vzít v úvahu i veškeré souvislosti zpracování – tj. možné spojení subjektu údajů s trestnou činností. Požadavek přijetí jednoznačných norem se jeví Úřadu jako nezbytný. Úpravu podzákonným předpisem je nutno považovat za pouhé provizorium.

Soukromá společnost provádějící genetické testování

Úřad v roce 2007 až 2008 provedl i **kontrolu soukromé společnosti**, která se od svého vzniku **zaměřuje na genetické testování** pro potřeby určování otcovství, identifikace a příbuznosti a analýzu deoxyribonukleové kyseliny (dále jen „DNA“) pro výzkum a testování geneticky podmíněných druhů onemocnění a pro předpovídání účinnosti jejich léčby.

Společnost po předání výsledků testů otcovství a genografických testů zadavatelům nelikvidovala veškerou dokumentaci, kterou na základě ustanovení zákona o ochraně osobních údajů může uchovávat pouze po dobu, která je nezbytná k naplnění účelu jejich zpracování; společnost nelikvidovala ani biologické vzorky s nimi související.

Porušení ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů se společnost dopustila také tím, že při uchovávání osobních údajů z klinických testů identifikovala pacienty jejich jmény, příjmeními a rodnými čísly, přestože v informovaných souhlasech s těmito testy souvisejícími uvedla, že informace o dotčených osobách budou v záznamech pro účely výzkumu uloženy pouze pod iniciálami jména a číslem, které bude dotčené osobě přiděleno na začátku studie. Výše uvedené ustanovení zákona ukládá při použití osobních údajů pro vědecké účely dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné. V daném případě se tak ovšem nestalo.

Na dobu před zahájením kontroly společnost neprokázala, že tiskopisy předkládané zadavatelům služby obsahovaly výslovný souhlas zadavatele se zpracováním osobních údajů. Bylo zjištěno, že tyto dokumenty neobsahovaly ani zákonem požadované informování subjektů údajů.

Společnost v době před kontrolou prováděla testy otcovství a původu, aniž by uvedený fakt sdělila Úřadu, a zpracovávala jako správce osobní údaje, přičemž tuto skutečnost písemně neoznámila Úřadu před zpracováváním osobních údajů. Tím porušila ustanovení § 16 odst. 1 zákona o ochraně osobních údajů.

Společnost jako správce při zpracování osobních údajů jejích klientů postupovala v rozporu se zákonem o ochraně osobních údajů, protože neuchovávala osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Dále při použití pro vědecké účely osobní údaje neanonymizovala, jakmile to bylo možné, nezpracovávala citlivé údaje, jen pokud subjekt údajů dal ke zpracování výslovný souhlas a byl při udělení souhlasu příslušně informován. Rovněž neinformovala a nepoučila subjekt údajů podle § 11 odst. 1 a odst. 2 a jako správce zpracovávající osobní údaje tuto skutečnost písemně neoznámila Úřadu před zpracováváním osobních údajů. Kontrolou bylo prokázáno, že uvedeným jednáním společnosti došlo k porušení zákona o ochraně osobních údajů. Proti kontrolnímu protokolu byly podány námitky k předsedovi Úřadu.

Druhostupňové řízení

Předseda Úřadu, jako vedoucí kontrolního orgánu, většině námitek podaných proti kontrolnímu protokolu nevyhověl a tím potvrdil závěry, které vyplynuly z kontroly, včetně požadavku na likvidaci osobních údajů zpracovávaných v rozporu se zákonem o ochraně osobních údajů.

Na základě námitky podané proti uložené likvidaci osobních údajů včetně genetických vzorků se předseda Úřadu (v samostatném rozhodnutí o likvidaci) důkladně zabýval i otázkou, zda se uložení likvidace má vztahovat jen na osobní údaje získané prostřednictvím dokumentace a v rámci výsledků provedených testů, nebo také na údaje obsažené v genetických vzorcích, tedy zda i v případě uchování odebraných vzorků lze hovořit o zpracování osobních údajů. K této otázce je nutno uvést, že ani odebrané vzorky, ani v nich obsaženou DNA nelze označit přímo za osobní nebo citlivý údaj (obdobně jako není údajem list papíru nebo média typu CD-ROM či USB-disku), avšak jde o nosiče těchto údajů, přičemž v daném případě jsou dle názoru odvolacího orgánu, tj. předsedy Úřadu, osobní údaje s těmito svými nosiči neoddělitelně spjaty. Osobními, resp. citlivými údaji, jsou v daném případě až údaje získané analýzou DNA a zpracované obvykle v podobě tzv. DNA profilu (obdobné stanovisko je zastáváno i na evropské úrovni, konkrétně Pracovní skupinou pro ochranu osobních údajů zřízenou na základě čl. 29 směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů – viz stanovisko této Pracovní skupiny WP136). Jestliže jsou však nosič údaje a údaj spjaty natolik neoddělitelně, jako je tomu v daném případě, je podle Úřadu zcela zjevné, že nápravné opatření, které má směřovat k ukončení nezákonného zpracování (uchování) osobních údajů, musí zahrnovat i nosič, na kterém jsou předmětné údaje zaznamenány (likvidace pouze údajů ve výsledcích testů a dalších dokumentech, avšak nikoli ve vzorcích, z nichž lze DNA profily kdykoli opět vytvořit).

Popsaným jednáním se tak společnost dopustila správních deliktů spočívajících v porušení těchto povinností, za což jí byla uložena pokuta ve výši 90 000 Kč. Vydaný příkaz již nabyl právní moci.

NADNÁRODNÍ INFORMAČNÍ SYSTÉMY

Osobní údaje ve společných informačních systémech EU

S členstvím České republiky v Evropské unii souvisejí také závazky při dozoru nad zpracováním osobních údajů ve společných informačních systémech, které vznikly buď na základě zvláštní smlouvy, k níž Česká republika přistoupila, nebo na základě sekundární legislativy, zakotvující povinnost přispívat do takového systému. Na nadnárodní úrovni pak určený národní dozorový orgán jednak provádí dozor na území státu nad věcně odpovídajícím zpracováním podle vnitrostátního předpisu, jednak se podílí na kontrolách centrální části. Dohled nad zpracováním osobních údajů v centrálních datových souborech Evropské unie přísluší buď společnému dozorovému orgánu (JSB, JSA), nebo spolupracujícím národním orgánům a evropskému inspektoru ochrany údajů (EDPS). Působení na této úrovni vyžaduje, aby Úřad byl patřičně obeznámen se zpracováním prováděným v České republice a jménem České republiky. V zájmu toho byly do plánu kontrolní činnosti na rok 2008 zařazeny kontrolní akce Zpracování osobních údajů v Celním informačním systému, Zpracování osobních údajů EURODAC a Zpracování osobních údajů v Schengenském informačním systému. Celní informační systém a Schengenský informační sytém vznikly shodně na základě zvláštní mezinárodní smlouvy, EURODAC je provozován na základě několika nařízení.

Kontrola zaměřená na národní část Celního informačního systému, určenou pro potřeby orgánů činných v trestním řízení, byla provedena ve dnech 15. dubna – 3. června 2008 na Generálním ředitelství cel. Při zpracování osobních údajů v Celním informačním systému, včetně plnění povinností stanovených Úmluvou vypracovanou na základě článku K.3 Smlouvy o Evropské unii o používání informační technologie pro celní účely, na jejímž základě systém vznikl a je provozován smluvními stranami, nebylo zjištěno porušení povinností stanovených zákonem o ochraně osobních údajů za použití ustanovení Úmluvy o celním informačním systému. Byl zjištěn postup neodpovídající ve svých důsledcích požadavkům na ochranu osobních údajů zakotveným v Úmluvě o celním informačním systému. Kontrolujícím nebylo jasné, jak může Celní správa České republiky a Generální ředitelství cel naplňovat účel, k němuž je systém provozován, pokud systém nepoužívá, ačkoli to je základním záměrem příslušné úmluvy. Z hlediska ochrany osobních údajů znamená takový postup a přístup ohrožení kvality zpracovávaných osobních údajů, a to i s přihlédnutím k ustanovení článku 13 odst. 3 Úmluvy o Celním informačním systému, podle něhož je systém v každém členském státě považován za vnitrostátní datový soubor upravený vnitrostátními ustanoveními uvedenými v této úmluvě a specifickými ustanoveními této úmluvy. Celní informační systém jako takový soubor tedy obsahuje osobní údaje, na které se vztahuje požadavek zajistit úroveň ochrany podle Úmluvy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat. Nepoužívání postupů stanovených Úmluvou o Celním informačním systému neodpovídá zásadám kvality údajů podle článku 5 Úmluvy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, jmenovitě zásadě podle písm. a). Neodpovídá rovněž zásadě článku 5 téže Úmluvy č. 108 podle písm. d), neboť nijak nesměřuje k udržování aktuálního stavu zpracovávaných osobních údajů, ačkoli je to nepochybně potřebné.

Při kontrole byly zjištěny vágně formulované informace o době uchování osobních údajů v Celním informačním systému. Odpovědnost za formulaci ustanovení článku 12 Úmluvy o celním informačním systému, která je zdrojem této informace, však Generální ředitelství cen jako kontrolovaný nenese.

Kontrola byla provedena s využitím poznatků získaných z práce společného dozorového orgánu pro Celní informační systém (JSA Customs).

K naplnění záměrů kontrolního plánu na rok 2008 pro Zpracování osobních údajů EURODAC bylo třeba vykonat kontroly dvě: 19. srpna 2008 byla zahájena kontrola na Ministerstvu vnitra, jejímž předmětem bylo zpracování osobních údajů v elektronické databázi otisků prstů využívaných v rámci Dublinského systému (EURODAC) a při zpracování údajů o otiscích prstů azylantů a žadatelů o udělení mezinárodní ochrany obecně. Jako právní rámec plnění povinností podle zákona o ochraně osobních údajů byla použita příslušná ustanovení řady právních předpisů, zejména zákona č. 325/1999 Sb., o azylu a o změně zákona č. 283/1991 Sb., o Policii České republiky, zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky zákona č. 221/2003 Sb., o dočasné ochraně cizinců, sdělení Ministerstva zahraničních věcí č. 115/2001 Sb. m. s., o Úmluvě č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, sdělení Ministerstva zahraničních věcí č. 28/2005 Sb. m. s. k Úmluvě č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, nařízení Rady (ES) č. 2725/2000 ze dne 11. prosince 2000, o zřízení systému „EURODAC“ pro porovnávání otisků prstů za účelem účinného uplatňování Dublinské úmluvy, nařízení Rady (ES) č. 343/2003 ze dne 18. února 2003, kterým se stanoví kritéria a postupy pro určení členského státu příslušného k posuzování žádosti o azyl podané státním příslušníkem třetí země v některém z členských států (dále jen „nařízení rady (ES) č. 343/2003“) a nařízení Komise (ES) č. 1560/2003 ze dne 2. září 2003, kterým se stanoví kritéria a postupy pro určení státu příslušného k posuzování žádosti

o azyl podané státním příslušníkem třetí země v některém z členských států. Bylo také přihlédnuto k vybraným ustanovením směrnice Evropského parlamentu a Rady Evropské unie 95/46/ES ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů (dále jen „směrnice 95/46/ES").

Pro zjištění, zda došlo k porušení zákona o ochraně osobních údajů, byla jako rozhodující vzata ustanovení § 5 odst. 1 písm. d), § 5 odst. 3, §§ 9, 11, 13 a 18 odst. 2 zákona o ochraně osobních údajů. Dále bylo použito ostatních ustanovení § 5 odst. 1 a odst. 2. Pro použití jiných ustanovení tohoto zákona nenastaly podmínky. Ministerstvo vnitra (dále jen „MV") je podle § 8 zákona o azylu příslušné k řízení o udělení mezinárodní ochrany a k řízení o odnětí azylu nebo doplňkové ochrany. Podle § 71 vede MV evidence s osobními údaji cizinců, kteří jsou podrobeni daktyloskopování a jejichž údaje jsou využívány v Dublinském systému. V míře vymezené zákonem o azylu a dalšími věcně příslušnými předpisy, především v návaznosti na nařízení Rady, MV určuje prostředky zpracování osobních údajů. Za zpracování osobních údajů v rozsahu vymezeném správními spisy MV, odpovídajícími částmi informačního systému MV odpovídá. Jelikož operace s osobními údaji vykonává MV systematicky a je státním orgánem, vztahuje se na toto zpracování zákon o ochraně osobních údajů. Ve smyslu tohoto zákona je MV správcem osobních údajů. V rámci toho odpovídá rovněž za zpracování osobních údajů z Dublinského systému, která mu byla poskytnuta sekundárně, tedy jako příjemci; i v této části zpracování je MV v postavení správce.

U kontrolovaného byla konstatována povinnost podle ustanovení § 18 odst. 2 zákona o ochraně osobních údajů, totiž povinnost zajistit, aby informace o účelu zpracování, kategoriích osobních údajů, kategoriích subjektů údajů, kategoriích příjemců a o době uchování byly jako explicitně formulované zpřístupněny přímo subjektu údajů, a to v okamžiku započetí samotného zpracování osobních údajů. Zveřejnění takových údajů nebo zpřístupnění jinou formou jiným osobám, než jsou žadatelé o mezinárodní ochranu, zjištěno nebylo. V tom bylo shledáno porušení zákona o ochraně osobních údajů. Naproti tomu formulace o době uchování osobních údajů, určená každému jednotlivému subjektu údajů, navozující nejistotu, po jak dlouhou dobu budou nebo mohou být osobní údaje uchovávány, nebyla inspektorkou považována za vadu v plnění povinnosti podle ustanovení § 18 odst. 2 zákona o ochraně osobních údajů, mající za následek porušení povinnosti, neboť účelu, který toto ustanovení zákona o ochraně osobních údajů sleduje, je dosaženo – příjemce získává informaci o době uchování.

Samostatným posouzením vnitrostátní právní úpravy a zjištěného stavu s relevantními ustanoveními tří relevantních nařízení (ES) bylo shledáno, že rozsah údajů, které jsou v České republice shromažďovány podle zákona o azylu, je větší, než jak stanoví nařízení *Komise (ES) č. 1560/2003 ze dne 2. září 2003, kterým se stanoví kritéria a postupy pro určení státu příslušného k posuzování žádosti o azyl podané státním příslušníkem třetí země v některém z členských států*, což není v rozporu se zákonem o ochraně osobních údajů.

Posouzena byla rovněž odpovídající ustanovení Úmluvy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat – vzhledem k jejich přímé aplikovatelnosti v situaci, kdy by postup kontrolovaného byl napaden stížností subjektu údajů podanou podle zákona o ochraně osobních údajů. Jako základní byla vzata ustanovení článku 5 a 8 Úmluvy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat; za použití sdělení Ministerstva zahraničních věcí č. 28/2005 Sb. m. s., k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat, jímž byla působnost Úmluvy vztažena rovněž na sou-

bory osobních údajů, které se nezpracovávají automatizovaně. Postup Ministerstva popsaný a doložený v kontrolním protokolu odpovídá požadavkům zakotveným v ustanovení článku 5. Nebylo zjištěno porušení žádného z práv, které Úmluva č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat přiznává subjektu údajů. Dodatečné záruky pro subjekt údajů, garantované smluvními stranami Úmluvy č. 108 o ochraně osob se zřetelem na automatizované zpracování osobních dat, jsou pro kontrolované zpracování k dispozici. Kontrola byla ukončena 24. října 2008.

Na základě zjištění, že na zpracování osobních údajů, které bylo předmětem této kontroly, se podílejí další subjekty, rozhodla inspektorka o provedení kontroly v Policii České republiky.

Výsledky obou kontrol byly bezprostředně využity pro koordinační schůzky národních orgánů s evropským inspektorem ochrany údajů.

Kontrola zpracování osobních údajů v národní části Schengenského informačního systému byla zahájena 5. listopadu 2008 s předpokladem dokončení počátkem roku 2009 – tak, aby poznatky z kontroly bylo možno plně využít při plnění úkolů vyplývajících pro Úřad z českého předsednictví EU, kdy bude zapotřebí při plnění svěřených úkolů v této oblasti vycházet také z vlastních zkušeností ohledně fungování tohoto systému.

Výstupy ze zmíněné kontroly budou dále využity i v rámci koordinované kontroly sjednané na půdě společného dozorového orgánu pro Schengenský informační systém (JSA Schengen), který v průběhu několika předešlých let postupně prověřil (na centrální úrovni a prostřednictvím národních úřadů i na národní úrovni) jednotlivé oblasti zpracování osobních údajů v tomto informačním systému a v současné době se zaměřuje na kontrolu postupů podle čl. 97 a 98 tzv. Schengenské prováděcí úmluvy.

Členem kontrolního týmu byl u všech uskutečněných akcí v této oblasti vždy rovněž jeden zaměstnanec Úřadu zařazený v útvaru odpovědném za mezinárodní spolupráci v dané problematice. Program kontroly umožnil získat podklady pro poskytování údajů pro účely sledování a harmonizace ochrany osobních údajů na úrovni EU. Některé požadavky však nebylo možné vyřídit v rámci kontroly. Tak tomu bylo v případech, kdy předmětem dotazu byly činnost nebo operace s osobními údaji, které nejsou v působnosti Úřadu.

V přímé reakci na požadavky na součinnost při provádění dozoru nad zpracováním osobních údajů podle Úmluvy o Evropské unii o zřízení Evropského policejního úřadu (Úmluva o Europolu), založené na článku K.3 Smlouvy (dále jen „Úmluva o Europolu“), byla za použití podkladů Společného kontrolního orgánu Europolu ve dnech 12. – 23. května 2008 provedena kontrola v Policii České republiky. Byly při ní prověřeny případy zjištěné v informačním systému Europolu. Vzhledem k tomu, že dosáhnout požadovaného cíle nebylo možné kontrolou plnění povinností stanovených Policii České republiky zákonem o ochraně osobních údajů, byla kontrola provedena na základě ustanovení § 2 a § 29 odst. 1 písm. c), e) a g) zákona o ochraně osobních údajů a podle Úmluvy o Europolu a za použití ustanovení § 29 odst. 2 a dále § 37 až 43 tohoto zákona. Zákon o ochraně osobních údajů a Úmluva o Europolu byly pro daný případ považovány za zdroj platných vnitrostátních postupů podle článku 23 Úmluvy o Europolu.

Bylo zjištěno, že Policie ČR nepostupovala při zpracování osobních údajů uložených v informačním systému Europolu v plném souladu s ustanoveními Úmluvy o Europolu. V jednom případě bylo zjištěno pochybení při posuzování přípustnosti zpracování osobních údajů na základě příslušnosti Europolu pro určitou formu trestné činnosti nebo její zvláštní projevy. Pro zpracování osobních údajů nebyly při vložení záznamu do informačního systému Europolu naplněny všechny podmínky,

které jsou pro takovou operaci stanoveny v článku 2, přičemž tyto znaky nebyly naplněny ani později. Postup neodpovídající ustanovení článku 21 odst. 3 Úmluvy o Europolu zjištěn nebyl. S ohledem na skutečnost, že záznam s osobními údaji, u nichž nebyly naplněny současně všechny podmínky pro vložení do informačního systému Europolu vedeného podle článku 7 a 8 Úmluvy o Europolu, byl vymazán a osobní údaje tam obsažené byly zlikvidovány v době trvání kontroly prováděné Úřadem, nebyly dány důvody pro uložení opatření k nápravě.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PŘI NASAZENÍ SLEDOVACÍCH SYSTÉMŮ

Kamerové systémy a zpracování osobních údajů

Úřad se v roce 2008 opětovně velkou měrou zabýval problematikou zpracování osobních údajů prostřednictvím kamerových systémů.

Obecně lze shrnout, že nejčastější využívání kamerových systémů je zdůvodňováno ochranou osob, ochranou majetku, ochranou veřejného pořádku, odhalováním, prevencí a stíháním trestné činnosti, získáváním důkazů a bojem proti terorismu. Jde tedy o legitimní důvody, které pomáhají přímo či nepřímo k ochraně jednotlivce, jeho soukromí je však stále se zvyšujícím monitorováním vážně ohroženo.

Uvedenými problémy i dalšími otázkami ochrany soukromí při využívání monitorovacích kamerových systémů pro různé účely se zabývá řada evropských dokumentů. Důraz je bezvýhradně kladen na zásadu proporcionality.

Rezoluce Parlamentního shromáždění Rady Evropy (Resolution 1604/2008 CoE) se zabývá problémem stále širšího použití moderních kamerových systémů pro prevenci kriminality a s tím souvisejícím fenoménem „Velkého bratra“, ze kterého vyplývá nutnost vytvořit právní předpisy proti zneužití této techniky k zásahům do soukromí a sledování soukromých záležitostí jednotlivců. Stanovisko Evropského hospodářského a sociálního výboru k Prevenci terorismu a násilné radikalizace (200/334/JHA) varuje před nepřiměřeným nasazením bezpečnostních opatření včetně kamer, které vyvolává negativní ohlasy veřejnosti. Dokument pracovní skupiny WP29 Evropské komise (Working Document 1/2008 on the protection of Children's Personal Data. WP29, 2008) se zabývá ochranou dětí, včetně použití kamer ve školách. Zde je konstatováno, že k využití kamerového sledování dětí by mělo být přistupováno pouze, je-li to nezbytné pro dosažení účelu a neexistuje-li jiný prostředek zasahující méně do soukromí dětí a zaměstnanců školy. Dokument rovněž doporučuje, aby před rozhodnutím o instalaci kamer ve školách předcházela diskuse za účasti zaměstnanců, pedagogů, dětí a jejich rodičů, která by se zaměřila na řešení otázky nezbytnosti přijetí takového opatření. Řada dokumentů v rámci EU se zabývá monitorováním zaměstnanců na pracovišti. Je v nich zdůrazňován oprávněný zájem zaměstnavatele na straně jedné a právo zaměstnanců na soukromí na straně druhé. Mnoho dokumentů vzniká i na národních úrovních. Pro český Úřad jsou tyto dokumenty důležitou inspirací, poskytují mu však také možnost porovnávat řešení, která v rámci svých kompetencí aplikuje v domácím prostředí.

Na provozovatele kamerového systému se zákon o ochraně osobních údajů vztahuje za předpokladu, že systematicky zpracovává získávané informace ve smyslu § 4 písm. e) tohoto zákona. Je tomu tak vždy, když je kamerový systém (zaměřený na monitorování fyzických osob) vybaven záznamovým zařízením, neboť v takovém případě dochází k systematickému shromažďování snímků osob nacházejících se v určitém časovém úseku v monitorovaném prostoru. V uvedených souvislostech lze nadto vyslovit i jistou presumpci dalšího využívání těchto záběrů; v opačném případě (pokud by záběry neměly být nijak využívány) by záznamové zařízení postrádalo jakýkoli smysl.

Při zpracování osobních údajů, které je nezbytné pro ochranu práv a právem chráněných zájmů správce, nesmí dojít k rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Při posuzování tohoto hlediska zpracování osobních údajů je třeba posuzovat umístění kamer a směřování jejich záběru spolu s charakterem sledovaných prostor a provozními okolnostmi tak, aby neměly za následek zpracování, které by nepřiměřeným způsobem zasahovalo do soukromého a osobního života subjektů údajů.

Správce současně v případě zahájení zpracování plně odpovídá za to, že bude osobní údaje zpracovávat v souladu s povinnostmi uloženými mu zákonem o ochraně osobních údajů; je proto kromě jiného povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, a v žádném případě je nemůže využívat k jinému účelu.

Registrační oznámení o provozování kamerových systémů

V roce 2008 došlo opětovně k výraznému nárůstu počtu registračních oznámení týkající se provozování kamerových systémů. Úřad se v souvislosti s registračním procesem kamerových systémů snaží vydat cestou osvěty a prevence. Přesto se, byť v menší míře než roku 2007, v registračních oznámeních objevila zpracování, která jsou v rozporu s povinnostmi správce ukládanými zákonem o ochraně osobních údajů (např. nelegitimní účely, nedostatečné plnění informační povinnosti, nepřiměřené délka uchování záznamu, zjevné porušení práva na ochranu soukromí apod.).

Nejzávažnějšími nedostatky, které se v oznámeních o registraci vyskytují, je zejména nesprávné posouzení poměru mezi hodnotami, které mají být kamerovým systémem chráněny, a hodnotami, do kterých kamerový systém zasahuje. Podstatným problémem zůstává nedostatečné využití jiných prostředků, které mohou efektivněji dosáhnout účelu, jenž správce sleduje, a nesprávná, ve většině případů příliš úzká, interpretace pojmu soukromí, což vede k nedostatečnému zohlednění spojitosti mezi umístěním kamery a zásahem do soukromí.

V rámci posuzování legálnosti použití kamerového systému jsou ze strany Úřadu rozhodující hlediska:

- Zda kamerový systém nezasahuje nepřiměřeným způsobem do práva subjektů na ochranu jejich soukromého života.
- Zda je využívání kamerového systému skutečně nezbytně nutné a zda je s ohledem na okolnosti opravdu jedinou a poslední legální možností jak dosáhnout vytýčeného účelu.
- Zda záznam z kamerového systému je schopen naplnit deklarovaný účel.

Kritéria vycházejí z Rozhodnutí Ústavního soudu PI. US 4/94 řešící kolizi základních práv a svobod (tedy např. právo na soukromí versus právo na ochranu majetku). Z ústavního pořádku a z tohoto rozhodnutí vyplývá, že i když to ústavní úprava nepředpokládá, může v případě kolize základních práv a svobod dojít k jejich omezení. Při posuzování možnosti omezení základního práva či svobody ve prospěch jiného základního práva resp. svobody lze stanovit následující podmínky, při jejichž splnění má prioritu základní právo nebo svoboda: a) vzájemné poměřování, b) šetření jejich podstaty a smyslu (čl. 4 odst. 4 Listiny) a určit tato kritéria:

- Kritérium vhodnosti tj. zda institut omezující určité základní právo, umožňuje dosáhnout sledovaný cíl (ochranu jiného základního práva).
- Kritérium potřebnosti spočívající v porovnávání legislativního prostředku, omezujícího právo resp. svobodu a jiných opatření umožňujících dosáhnout stejného cíle, a nedotýkají se přitom základních práv a svobod.
- Kritérium porovnání závažnosti obou v kolizi stojících základních práv nebo svobod.

Z mnohých registračních rozhodnutí vyplývá, že provozovatel a správce kamerového systému se rozhoduje o instalaci na základě „vrchnostenského“ přístupu, který přiznává práva pouze sobě a právy jiných opovrhuje. Úřad individuálně posuzuje, zda dočasné nasazení kamerového systému k odhalování drobné kriminality a opakujícímu se vandalismu je v daném místě a čase oprávněné nebo zda jde pouze o jedno z bezvýchodných a nouzových opatření.

Kamerový systém na veřejném prostranství

V rámci registračních oznámení se v roce 2008 stále častěji na Úřad obracely menší obce hodlající provozovat kamerový systém na veřejném prostranství (náměstí, ulice, parky). Důvodem monitorování má být zajištění veřejného pořádku a předcházení a odhalování trestné činnosti. Žadatelem je tedy obec, která nemá obecní policii a má zájem provozovat kamerový systém na veřejných prostranstvích, za veřejnoprávním účelem. K této problematice Úřad vydal stanovisko zveřejněné ve Věstníku č. 49/2008, v jehož rámci byl učiněn závěr, že zpracování osobních údajů prostřednictvím kamerového systému se záznamem provozovaného obcí, která nemá obecní policii, na veřejných prostranstvích (náměstí, ulice), a to za účelem prevence a postihu kriminality, by bylo v rozporu s platnými právními předpisy ČR. Provozování kamerového systému na veřejných prostranstvích za veřejnoprávním účelem je možné jen prostřednictvím Policie ČR nebo obecní policie.

Podání občanů směřovala k provozování kamerových systémů na veřejně přístupných místech, předmětem kritiky byly zejména tzv. městské a dopravně bezpečnostní kamerové systémy monitorující situaci na náměstích, v ulicích a na komunikacích. Ke správnímu řízení byl předán podnět upozorňující na kamery na náměstí v Trutnově, Janských Lázních a Žacléři, provozované městskými úřady bez registrace. Pozornost vzbudil medializovaný záměr provozovat kamerový systému v Dubí a Chomutově, respektive tendence využívat jej k monitorování návštěvníků veřejných domů. Zástupce chomutovského magistrátu akceptovali připomínky Úřadu tak, aby realizací legitimního cíle, kterým je vytlačit prostituci z ulic města, nedocházelo k neoprávněnému provozování kamerového systému.

Kamerový systém v bytových domech

Úřad na základě zvyšujícího se počtu přijatých stížností vydal stanovisko č. 1/2008, „Umístění kamerových systémů v bytových domech“, řešící problematiku provozu kamerových systémů v bytových domech. Na základě zveřejnění informací o této problematice, se výrazně zvýšil i počet přijatých registračních oznámení vlastníky bytových domů. A to bez ohledu na to, zda šlo o bytové domy ve vlastnictví obcí, soukromém, družstevním apod. Nechtěným, ale očekávaným výsledkem bylo i zvýšení počtu přijatých podnětů ke kontrole Po zveřejnění Stanoviska Úřadu č. 1/2008 deklarujícího možnost používání kamerových systémů se záznamovým zařízením v bytových domech jen se souhlasem nájemníků, byl zaznamenán nárůst stížností tohoto typu. Celkem 13 z nich bylo postoupeno k další analýze před zahájením kontroly. V příštím roce Úřad shromáždí názory veřejnosti na uvedené stanovisko v zájmu skutečně efektivní aplikace zákona.

Kamerový systém v hotelích a restauracích

Zejména v první polovině roku, pod dojmem úniku záznamů pořízených kamerovým systémem v Hotelu Savoy do masmédií, se pozornost veřejnosti soustředila na kamerové systémy provozované v obdobných zařízeních. Ve spolupráci s Asociací hotelů a restaurací proběhl 12. listopadu 2008 seminář pro pozvaný management hotelů z celé ČR. Lze učinit závěr, že provedené prezentace výrazně přispěly k po-

chopení celé problematiky a perspektivně i ke zvýšení ochrany zpracovávaných osobních údajů prostřednictvím kamerových systémů se záznamovým zařízením. Asociace hotelů a restaurací projevila zájem o pokračující spolupráci s Úřadem.

Kamerové systémy na pracovištích

Časté dotazy a stížnosti docházejí na přetrvávající problém spočívající ve sledování zaměstnanců prostřednictvím kamer na pracovišti, a to jak u velkých institucí a továren, tak i u drobných soukromých provozoven. Bývají to i anonymní podněty a rovněž se množí žádosti o nezveřejnění jména stěžovatele. Stížnosti na provoz kamerových systémů, kterými jsou monitorováni pouze zaměstnanci, tedy ze kterých vyplývá podezření z porušování § 316 odst. 2 zákoníku práce, jsou předávány věcně příslušnému úřadu, kterým je Státní úřad inspekce práce.

Značný počet stížností upozorňujících na provozování kamerových systémů se záznamovým zařízením fyzickými nepodnikajícími osobami v drtivé většině případů pro účel ochrany vlastního majetku byl odkládán jako nedůvodný. Stěžovatelům bylo vysvětlováno, že zákon o ochraně osobních údajů nelze podle § 3 odst. 3 aplikovat na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu. Protože některé případy signalizovaly možné porušení § 12 zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, bylo stěžovatelům doporučováno řešit věc podáním občanskoprávní žaloby. I když je Úřad povinen zabývat se všemi podáními, jsou obecná upozornění anonymních stěžovatelů na skutečnost, že je v určité instituci nebo konkrétní osobou provozován kamerový systém, aniž bylo sděleno, v čem spočívá podezření z porušení zákona o ochraně osobních údajů a zda byl stěžovatel provozem tohoto kamerového systému poškozen, odkládána jako nedůvodná.

Kazuistika

V roce 2008 provedli inspektoři Úřadu řadu šetření a přes 40 kontrol, které se zabývaly výhradně využíváním kamerových systémů provozovaných v různých prostředích. Šlo o kontroly ve státních nebo obecních institucích, školách, výrobních prostorách, nemocnicích nebo bytových domech.

Pro ilustraci jsou dále uváděny typově rozdílné provedené kontroly.

I.

Stěžovatel napadl v březnu 2008 vyvěšení fotografie jemu podobného muže s nápisem „chytli jsme zloděje“ na vstupních dveřích prodejny drogerie; fotografie měla být pořízena kamerovým systémem. Prodejnu provozuje jako fyzická osoba P. V den zahájení kontroly byla na vstupních dveřích do prodejny umístěna fotografie tak, aby byla vidět zvenčí; zobrazovala muže, který buď vkládá nějaký předmět do svého vnějšího oděvu, nebo jej vyjímá. Snímek byl opatřen informativním řádkem s údaji o času pořízení, v těsném okolí fotografie byl dále umístěn ručně psaný text *KAMERY ZAZNAMENALY ZLODĚJE V NAŠÍ PRODEJNĚ*. Těsně pod fotografií byl umístěn další papír s textem reklamní povahy. Kontrolou bylo zjištěno porušení povinností uložených P. v ustanoveních § 5 odst. 1 písm. b), § 10 a § 15 zákona o ochraně osobních údajů. Zveřejnění formou vývěsky na vstupních dveřích prodejny drogerie a nepřihlédl k ustanovením § 11 a 12 občanského zákoníku.

K nápravě zjištěného stavu bylo uloženo, aby byl neprodleně změněn způsob a případně i některé prostředky zpracování osobních údajů, tak, že bude vyloučeno zveřejňování jiných osobních údajů, než údajů anonymních.

II.
Anonymní stěžovatel vyjádřil podáním doručeným Úřadu 17. dubna 2008 jménem zaměstnanců A. obavu z nepřetržitého sledování zaměstnanců kamerovým systémem v prostorách sedmi prodejen A. v obchodním centru v O. Při kontrole bylo mj. konstatováno, že A. stanovila účel zpracování osobních údajů podle zákona o ochraně osobních údajů; jí stanovený účel je dostatečně specifický a nepřekračuje rámec stanovený v ustanovení § 44 odst. 2 písm. a) zákona o ochraně osobních údajů. Požadavku zákonnosti A. nevyhověla v tom, že podmínky pro pohyb zaměstnanců nepřizpůsobila ustanovením § 316 odst. 2 zákoníku práce. V daném případě nesmí zaměstnavatel bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování. Proto je postup A. porušením povinnosti podle ustanovení § 5 odst. 1 písm. b) zákona o ochraně osobních údajů vůči zaměstnancům, kteří mají zázemí v prostorách podrobených záznamu z kamerového systému. Současně tím byla porušena povinnost podle § 10 zákona o ochraně osobních údajů. Rozsah, v němž jsou v souvislosti s provozováním kamerového systému zpracovávány osobní údaje osob, pohybujících se v prostoru prodejny, v zásadě nezasahuje do jejich práva na ochranu soukromého a osobního života. Je však z podstaty spojen se zasahováním do práva upraveného v ustanovení § 11 a 12 občanského zákoníku. Pořízení obrazového záznamu kteréhokoli zákazníka a zaměstnance kontrolované firmy a jeho použití způsobem popsaným v předchozích částech tohoto kontrolního protokolu není s ustanoveními § 12 občanského zákoníku v souladu. Jako neoprávněný zásah do osobnostního práva je proto spjat s porušením povinnosti kontrolované firmy podle ustanovení § 10 zákona o ochraně osobních údajů. A. bylo proto uloženo do deseti dnů ode dne převzetí kontrolního protokolu vhodnými organizačními postupy nebo technickými opatřeními omezit (snížit) rozsah sledování pohybu zaměstnanců, jejichž zázemí v rozsahu šatny a prostor určených k odkládání osobních věcí je nedílnou součástí prostorů monitorovaných kamerovým systémem, který byl předmětem kontroly.

III.
Kontrola byla provedena v galerii. Sbírky jsou chráněny rovněž prostřednictvím kamerového systému se záznamem. Při posuzování rozsahu zpracování, tj. rozmístění kamer, je třeba zvážit, kde přesně jsou nebo mají být umístěny a zda v daném případě není v rozporu ochrana práv a právem chráněných zájmů správce s právy subjektů údajů na ochranu jejich soukromého života. Není pochyb o tom, že kamery umístěné na střechách a pláštích budov galerie, které nezabírají žádné procházející osoby, kamery umístěné přímo v místnostech výstav a namířené na vzácné exponáty, stejně tak jako kamery snímající vnitřní prostory depozitářů, které jsou pro běžné návštěvníky zapovězeny a i zaměstnanci tam vstupují pouze zřídka, uvedeným kritériím vyhovují. Naproti tomu kamery umístěné v průchodech a na ulicích v okolí galerie zabírají často osoby, které nemají s návštěvou galerie nic společného a ani netuší, že by mohl být jejich pohyb zdokumentován a uchováván, neslouží k ochraně majetku. Podobné námitky lze uvést i v případě kamer, které jsou umístěny na vstupu do budov a zabírají všechny vstupující návštěvníky galerie. Na tomto místě lze připustit umístění kamer pro online kontrolu plynulosti provozu, uchovávání záznamů z těchto kamer však není pro stanovený účel nezbytné.

Důležitým prvkem nemožnosti zneužití záznamů z kamer je jejich ochrana před neoprávněným přístupem (§ 13 zákona o ochraně osobních údajů). K záznamům, které jsou pořizovány za účelem ochrany majetku, by měla mít přístup v případě inci-

dentu pouze policie, popř. bezpečnostní technik, avšak pouze se souhlasem ředitele instituce. Tyto zásady by měly být upraveny v technicko-organizačních opatřeních k zajištění ochrany osobních údajů (§ 13 odst. 2 zákona o ochraně osobních údajů).

IV.

Dvě kontroly se týkaly kamerového systému se záznamem v garážovém stání pod nově zřízenými bytovými domy. Garážová stání jednotlivých domů jsou vzájemně průjezdná a průchozí. O instalaci kamer rozhodla již developerská společnost v průběhu výstavby domů. Kromě instalace jednotlivých kamer uzavřela smlouvu s bezpečnostní agenturou, mezi jejíž povinnosti patří i využívání kamerového systému. Noví majitelé bytů, resp. nově vzniklá společenství vlastníků bytů při koupi nemovitosti získala kromě společných nebytových prostor i vybavení kamerami. Současně nová společenství vstoupila místo developerské společnosti do již uzavřené smlouvy s bezpečnostní agenturou. Z hlediska zákona o ochraně osobních údajů se tak dostala do pozice správců osobních údajů a bezpečnostní agentura do pozice zpracovatele.

Kamery byly instalovány tak, že neplnily svůj účel. Ze záběrů nebylo možné identifikovat osoby sedící v přijíždějících a odjíždějících autech, nebyla sledována zaparkovaná auta, ale příjezdové cesty a vstup z jednotlivých domů do podzemního garážového stání. Záznam byl pořizován bez souhlasu vlastníků bytů a jejich rodinných příslušníků a rovněž bez souhlasu dalších dotčených osob. Kontrola konstatovala, že obě společenství vlastníků porušují zákon o ochraně osobních údajů, protože záběry kamer neplní stanovený účel, tedy ochranu majetku, konkrétně zaparkovaných aut. Kontrolním protokolem byla uložena nápravná opatření spočívající v odstranění nedostatků, se zaměřením na správné a účelné nastavení zorného úhlu kamer.

V.

Kontrola v organizační složce zahraniční společnosti, která se zabývá mediální činností, byla provedena na základě podnětu, který podali novináři z jiných sdělovacích prostředků. Šlo o kontrolu zcela atypickou, kde byl zvolen nestandardní, avšak zákonný postup, zohledňující bezpečnostní rizika.

Kontrolním šetřením bylo zjištěno, že tato organizační složka pořizuje kamerové záznamy bez souhlasu monitorovaných osob v souladu se zákonem. Byla zjištěna pochybení spíše formálního rázu, jako např. ne zcela dostatečné splnění informační povinnosti nebo nedostatečné náležitosti vyžadované zákonem ve smlouvě se zpracovatelem, v tomto případě bezpečnostní službou, která se podílí na ochraně této společnosti. Při kontrole nebylo zjištěno, a nebyly předloženy žádné jiné důkazy, k tvrzení novináře, že by onen údajně existující záznam z kamery dokumentující souložící dvojici v parku v sousedství sídla organizační složky, pocházel z kontrolovaného kamerového systému. Proti kontrolnímu protokolu nebyly podány námitky. Bylo dosaženo příznivého výsledku při odstraňování zjištěných nedostatků během realizace uložených nápravných opatření, při kterých organizační složka spolupracuje s kontrolujícím inspektorem.

VI.

Kontrola týkající se kamerových systémů byla provedena ve společnosti, která se zabývá převážně směnárenskou činností. V rámci kontroly bylo posuzováno oprávnění zpracovávat osobní údaje prostřednictvím kamerových systémů se záznamem bez souhlasu dotčených osob. Bylo shledáno, že stanovený účel je legitimní a vychází z oprávněním společnosti chránit své právem chráněné zájmy s tím, že zásah do soukromí klientů není intenzivní. Pokud se týká zaměstnanců, bylo společnosti doporučeno změnit nastavení kamer, resp. zorný úhel tak, aby zaměstnanci

nebyli zabírání mimo prostor, kde dochází k finančním transakcím, nebo v malých prostorách tak, aby nebyla zabírána celá postava, ale byla zaznamenávána a dokumentována výměna, včetně možnosti identifikace. V rámci závěrů kontrolního šetření byl vzat v úvahu rovněž zákon o praní špinavých peněz, který ukládá identifikovat a uchovávat údaje o osobách, které provádějí obdobné finanční transakce (na pobočkách docházelo k výměnám nejen v běžném turistickém rozsahu, ale i k větším, obchodním transakcím, které dosahovaly obratu 300 – 500 tisíc Kč). Společnost dokumentovala, že v jednom případě bylo prostřednictvím záznamu doloženo, že došlo k chybě při výměně „balíčku" bankovek, a to, že místo 2 000 Kč bankovek byly zákazníkovi předány i bankovky v hodnotě 5 000 Kč. Došlo tedy k poškození společnosti o 300 tisíc Kč.

VII.

Kromě mediálně sledované kauzy úniku záznamů z Hotelu Savoy, byly provedeny další tři kontroly, kamerových systémů se záznamem využívaných v hotelových provozech. V průběhu kontrolního šetření byly zjištěny obdobné podmínky. Kamerové systémy byly provozovány dlouhodobě, a to bez registrace u Úřadu. Provoz kamer byl zdůvodňován ochranou zdraví hostů a zaměstnanců hotelu a zejména ochranou majetku jak hotelu, tak i ubytovaných hostů. Kamery byly instalovány tak, že sledovaly všechny vstupy do prostoru, včetně přilehlých komunikací, dále byla sledována parkoviště a garážová stání a zejména vstupní prostor do hotelu, tedy recepce, hala, příchod ke schodištím a výtahům, ale i kavárenskou část v hotelové hale (lobby bar). Kamery byly instalovány dále v zázemí, za účelem ochrany skladů, zboží apod. Ani v jednom případě nebyly kamery umístěny v ubytovací části.

Kontrola v Hotelu Savoy byla zahájena bezprostředně po zveřejnění záznamů, pořízených prostřednictvím kamerového systému z hotelu, ve sdělovacích prostředcích. Bylo zdokumentováno, že sledování společných prostor není nezbytné, protože ty jsou soustavně sledovány přímo zaměstnanci hotelu. Bylo zjištěno, že nastavení a instalace kamer je nevhodná k naplnění stanoveného účelu a že lze přijmout jiná opatření, u kterých nedochází k zaznamenávání soukromého chování. Použití kamerového systému v Hotelu Savoy vykazovalo obecný přístup vedení hotelových společností k právu třetích osob na soukromí. Je zcela legitimní chránit majetek hostů i hotelu, je zcela legitimní zajistit ochranu zdraví osob, které jsou v hotelu ubytovány. Využití záznamů k objasnění relativně marginálních krádeží nebo poškození majetku nebylo přiměřené zásahu do soukromí. Z uvedeného je zřejmé, že k naplnění legitimního cíle bylo použito nepřiměřeného prostředku. V části kontroly, která se zaměřila na únik části záznamu do médií, bylo nepochybně prokázáno, že zveřejněný záznam byl pořízen prostřednictvím kamerového systému instalovaného v hotelu, dále bylo ve spolupráci s Inspekcí ministra vnitra potvrzeno, že zmíněný záznam byl pracovníkem hotelu předán v souladu s příslušným ustanovením trestního řádu příslušníkovi Policie ČR. Ze strany hotelu nedošlo k porušení příslušných ustanovení zákona o ochraně osobních údajů upravujících zabezpečení pořízených záznamů.

Kontroly provedené v dalších hotelích zjistily v podstatě shodná porušení zákona, jako v předchozím případě. V jednom případě argumentovali majitelé hotelu tím, že povinnost využívat kamerový systém jim ukládá zákon na ochranu proti alkoholismu a toxikománii – aby nedocházelo k nezákonnému podávání alkoholu nezletilým a podnapilým; argumentovali i tím, že záznam je pořizován z důvodu povinnosti, kterou jim ukládá zákon na ochranu spotřebitele, aby nedocházelo k diskriminace spotřebitele a dodržování stanovené kalibrace podávaných nápojů a jídel. Tedy odůvodnění, které je nejen právně nesprávné, ale zejména z hlediska ochrany soukromí zcela nesmyslná, ba svědčí o naprostém pohrdání právem na soukromí jiných osob.

Další kontrolovaný hotel měl instalován kamerový systém pouze vně hotelu, nesledoval žádný vnitřní prostor, pouze parkoviště, venkovní terasu a plášť hlavní budovy. Kamerový systém je spouštěn ve 22.00 hodin, tedy po uzavření restaurace, a vypínán v 06.00 hodin ráno, po příchodu zaměstnanců do hotelu. V noční době je přítomen pouze jeden zaměstnanec – recepční. Deklarovaným účelem pro využívání kamerového systému je ochrana majetku. Kontrolovaný dokumentoval předchozí krádeže a poškozování venkovního vybavení a zařízení, včetně pláště budovy (sprejerství). V rámci kontroly bylo zjištěno, že kamery jsou nastaveny tak, aby snímaly chráněný prostor. Rovněž bylo zjištěno, že provozem kamerového systému se záznamem dochází k občasnému zachycení náhodných chodců, kteří využívají vnitřních komunikací hotelu k průchodu. Záznamy byly uchovávány po dobu 24 hodin. V závěrečné zprávě bylo zhodnoceno, že provoz kamerového systému je v souladu se zákonem, neboť zásah do soukromí osob, které jsou zachyceny při průchodu je, podle zásady přiměřenosti, nižší než oprávněný zájem majitele hotelu chránit svůj majetek.

VIII.

Kontrola byla provedena na základě podnětu zaměstnanců velínu velké teplárny v okresním městě. Provoz teplárny byl zajišťován v nepřetržitém provozu. Vedení teplárny uvedlo, že účelem instalace kamer je dokumentovat mimořádné události, ke kterým by v rámci chodu teplárny mohlo dojít. Toto rozhodnutí se opíralo o řadu právních norem, které upravují chod v obdobných provozech z hlediska nebezpečí obecného ohrožení, ohrožení životního prostředí, ale i z hlediska zabezpečení proti případnému teroristickému útoku atd.

V rámci kontroly bylo vyžádáno stanovisko Státního úřadu inspekce práce, zda provoz teplárny lze podřadit pod výjimku „zvláštní činnost zaměstnavatele“, dle § 316 odst. 2 zákoníku práce. Z obdrženého stanoviska bylo zřejmé, že provoz teplárny lze pod tuto výjimku zařadit. Na základě této skutečnosti bylo posouzeno, že zaměstnavatel je oprávněn zasahovat do soukromého a osobního života svých zaměstnanců ve velínu, a to i bez jejich souhlasu.

IX.

Byly provedeny dvě kontroly nemocnic. Rozhodnutí o instalaci kamer bylo v obou případech učiněno vedením nemocnic. V jedné nemocnici bylo instalováno zhruba 30 kamer, ve druhé nemocnici bylo instalováno přes 80 kamer. V obou případech šlo o rozhodnutí pořizovat záznamy dle vlastního přesvědčení, že k provozování kamerového systému mají právní nárok a právní povinnost. Ani v jednom případě nebyla vzata v úvahu práva sledovaných osob.

Při prověřování pořízených záznamů bylo zjištěno, že prostřednictvím kamer jsou zaznamenáváni prakticky všichni zaměstnanci nemocnice, dále všichni návštěvníci a hospitalizovaní, kteří chodí nebo jsou odváženi na odborná vyšetření.

I přes skutečnost, že v rámci nemocničního provozu nelze de facto zajistit soukromí ani hospitalizovaných osob, ani příchozích k ambulantnímu vyšetření, a v nemocničním provozu ani zaměstnancům, je nutno ve zvýšené míře dbát na to, aby zásah do soukromí i do osobní integrity byl co nejmenší.

Nemoc je vždy individuální, ryze osobní záležitost, a proto zaznamenávat chování postižené osoby je nejen v rozporu s právem na soukromí, ale je také hluboce nemorální. Dále se kontrola zaměřila na nezbytnost zpracování osobních údajů prostřednictvím kamerových systémů. Bylo konstatováno, že kromě zpětné identifikace osoby, která by se dopustila nežádoucího deliktního jednání, by bylo možné využít kamerového systému v režimu online, tedy bez pořizování záznamů. Bylo také konstatováno, že při dodržování základních organizačních opatření, jakým je například kontrola osob vstupujících na uzavřená oddělení, zamykání místnostní

apod., lze zajistit ochranu majetku jiným, méně invazivním způsobem. U obou kontrolovaných nemocnic bylo konstatováno porušení zákona o ochraně osobních údajů, konkrétně porušení jeho ustanovení v § 5 odst. 2 a § 5 odst. 1 písm. d).

V souvislosti s kontrolou těchto nemocnic bylo nutno řešit i otázku, zda lze prostřednictvím kamerového systému chránit hospitalizované, bezmocné pacienty, před okradením. I přes skutečnost, že takové osoby nemají možnost se bránit samy, je nutno právě s ohledem na jejich stav, ve zvýšené míře dbát na jejich soukromí a bezpečnost zajistit jiným způsobem – bez ohledu na organizační a finanční náročnost. Úřad projednal a přijal registraci jedné velké nemocnice, která rozhodla o provozování kamerového systému (provoz dvou kamer), které nepřetržitě sledují epileptické pacienty za účelem včasné indikace epileptického záchvatu a monitoringu příčin jeho vzniku. Nemocnice přijala nadstandardní opatření k zabránění zneužití pořízených záznamů.

X.

Byly provedeny kontroly ve třech školách. Ve dvou případech se v průběhu kontrolního šetření zjistilo, že instalované kamery nejsou vybaveny záznamovým zařízením a byly instalovány tak, aby umožnily jako „intercom" mít online přehled o osobách, které vstupují do budovy a které se pohybují v prostorách šaten. Nešlo tedy o zpracování osobních údajů.

Provoz kamerového systému se záznamem byl nastaven v základní škole a v mateřské škole. Motivován byl snahou zajistit ochranu majetku školy, zajištění bezpečnosti a zdraví žáků a zaměstnanců i možností sledovat a dokumentovat nevhodné chování žáků tak, aby mohlo být potrestáno.

Kontrolou bylo zjištěno, že záznamy z kamerových systémů byly využívány k objasnění drobných incidentů a krádeží, ale nebyly předávány kompetentním orgánům. Ke zpracování osobních údajů prostřednictvím kamerového systému se záznamem nebyl udělen souhlas žádným z pedagogů, ostatních zaměstnanců školy, ani zákonnými zástupci žáků.

V rámci kontroly bylo zhodnoceno právo školy na zpracování osobních údajů bez souhlasu ve vztahu k právem dotčených osob na soukromí a dále nezbytnost využívat zpracování osobních údajů. Bylo konstatováno, že použití kamerového systému se záznamem je nepoměrně závažnějším zásahem do soukromého a osobního života pedagogů i žáků školy než odhalování drobnějších incidentů. Škola má nepochybně řadu jiných možností, jak zamezit drobným krádežím a zejména, jak vyřešit dozor na chodbách, šatnách apod., aby se zabránilo různým konfliktům, ke kterým mezi žáky dochází. Rovněž nebyl akceptován názor, že prostřednictvím kamerového systému a stálého sledování lze potlačit šikanu mezi žáky: Instalované kamery pouze vytlačí šikanu do jiných míst. Nehledě na skutečnost, že škola žádný případ šikany, i mimo dosah kamery, nedokumentovala. V tomto případě došlo tedy ke zpětné „výrobě" odůvodnění instalace kamer, včetně zneužití klišé o šikaně. Na základě výsledků kontrolního protokolu a uložených nápravných opatření, ukončila škola provoz kamerového zařízení v době školního vyučování a zařízení bylo využíváno v době, kdy ve škole není provoz. Došlo tedy k nápravě a místo sledování osob je zařízení využíváno ke sledování prostor, případně majetku a zařízení školy.

XI.

Na základě anonymní stížnosti byla provedena kontrola na detašovaném pracovišti dozorové státní instituce. Kamerový systém byl instalován v přízemí budovy a kamerou je sledován vchod do budovy, jsou tedy zaznamenávány všechny osoby, které do budovy vcházejí a z ní odcházejí. Kamerovým systémem byl dále sledován prostor chodby kontrolované instituce. Tím se monitoruje pohyb osob, které při-

cházejí do a odcházejí z podlaží a současně i vstupy do jednotlivých kanceláří, skladů a toalet. Na chodbě přímo pod kamerou byla umístěna centrální tiskárna, která byla využívána všemi zaměstnanci.

Deklarovaným účelem pro instalaci a provoz kamerového systému byla ochrana majetku, s důrazem na ochranu státního majetku a zejména ochrana zdraví zaměstnanců, s odůvodněním, že jde o dozorový státní orgán.

Vedením pracoviště nebyl dokumentován žádný závažný případ krádeže či poškození svěřeného majetku a ani žádné fyzické napadení zaměstnance instituce. Pořízený záznam přispěl pouze v jednom případě k odhalení krádeže kancelářských potřeb. Jinak nebyl záznam nikdy využit, ani předán příslušným orgánům. Instituce pořizovala záznamy bez souhlasu dotčených osob.

Bylo konstatováno, že zaznamenávání běžného chování nejen zaměstnanců, ale i návštěvníků v pracovní době, kdy jsou zaměstnanci přítomni, za účelem ochrany majetku, je zjevně nepřiměřeným zásahem do soukromí monitorovaných osob.

Kontrolním protokolem bylo uloženo nápravné opatření: Ukončit zpracování osobních údajů prostřednictvím pořizování záznamů z kamerového systému a zlikvidovat pořízené záznamy s doporučením, aby kamerový systém byl využíván pouze v mimopracovní době.

XII.

Byla provedena řada kontrol kamerových systémů, jejichž společným znakem bylo obecné podání, bez konkrétního podezření na porušení zákona. Často bylo zjištěno, že instalované kamery jsou pouhými maketami. Kontrolovány tak byly například dvě základní školy, kde byl kamerový systém využíván pouze k online sledování a několik bytových domů, kde majitel využíval systém rovněž k přímému sledování činnosti v domě. Byly provedeny kontroly ve čtyřech restauracích, ve dvou obchodech a v jednom hostelu.

V případech, kdy se takové online sledování týkalo zaměstnanců kontrolovaných subjektů, byla věc postoupena Státnímu úřadu inspekce práce s podezřením na porušení § 316 odst. 2 zákoníku práce. V jednom kontrolovaném případě bylo již v průběhu předběžného šetření zjištěno, že podnět byl podán pouze na základě rozhovoru zveřejněném ve sdělovacích prostředcích, kde autor určitého projektu vyslovil i možný úmysl využívat pro svou činnost kamerový systém. Tento projekt však zůstal pouze v oblasti záměru a nikdy nebyl realizován. V několika případech bylo až v průběhu kontroly zjištěno, že stěžovatel souběžně vede nějaký jiný spor s provozovatelem kamerového systému a jeho cílem bylo „znepříjemnit mu život“.

XIII.

V souvislosti s kontrolami kamerových systémů, které provozuje městská policie je třeba upozornit na skutečnost, že města, jež zřídila městské policie, jsou, pokud jde o zpracování osobních údajů – a to i těch, které jsou shromažďovány kamerovým systémem a dále zpracovány či zpracovávány – v postavení správce ve smyslu ustanovení § 4 písm. e) zákona o ochraně osobních údajů, neboť ony určují účel a prostředky zpracování osobních údajů, provádějí zpracování a odpovídají za ně. Městské policie jsou orgány obcí, resp. měst. V tomto směru v praxi v některých případech dochází k nesprávnému právnímu výkladu, kdy za správce je považována městská policie, anebo městská policie je pokládána za zpracovatele ve smyslu ustanovení § 4 písm. k) zákona o ochraně osobních údajů. Subjektem údajů ve smyslu ustanovení zákona o ochraně osobních údajů je v daném případě fyzická osoba, jež je snímána kamerovým systémem města, jakožto správce, a jejíž osobní údaje shromažďované tímto kamerovým systémem se k ní vztahují.

XIV.

Kontrola záznamů o překročení povolené rychlosti ve Zlíně (shromažďovány jsou na základě zákona č. 361/2000 Sb., o provozu na pozemních komunikacích) prokázala, že jsou shromažďovány bez souhlasu subjektu údajů a mohou být použity v rámci přestupkového řízení. Systém úsekového měření rychlosti v té formě, jak je provozován, je však zasahováním do soukromého a osobního života subjektu údajů a je v rozporu s požadavky § 10 zákona. Uchovávání informací o všech projíždějících vozidlech městským informačním systémem nemá oporu v zákoně. Byla uložena nápravná opatření, např. aby používaná aplikace „zájmová vozidla" byla využívána pouze Policií ČR, a to na základě řádně vedených šetření, neboť město Zlín, ani Městská policie Zlín, toto oprávnění nemá.

Obrazová dokumentace provozování kamerových systémů

Ve všech případech se jedná o provozování kamerového systému se záznamem, přičemž záznam je pořizován bez souhlasu dotčených osob.

Přiložené snímky jsou extrahovány ze záznamů, které byly zajištěny v rámci kontrolní činnosti, snímek č. 6 byl převzat z internetového deníku.

U snímků č. 1., 2., 3., 5., 7., 8 byly obličeje z důvodu anonymizace osob dodatečně rozostřeny. Rovněž byla rozostřena SPZ u vozidla na snímku č. 4.

Obr. 1
Kamera na schodišti činžovního domu.
Účel sledování - pořizování důkazů pro vedení majetkových sporů.

(zachycena pachatelka lámající keřík)

Obr. 2
Kamera na městském úřadu, přepážka odboru dopravních agend.
Účel sledování - ochrana majetku města a zajištění bezpečí osob.

(když víme, co má klient v peněžence, budeme se všichni cítit bezpečněji...)

Obr. 3
Kamera sleduje vstup do činžovního domu garážemi.
Účel sledování - ochrana garážovaných vozidel před poškozením.

(A kde jsou ta vozidla...?)

Obr. 4
Kamera v podzemních garážích činžovního domu.
Účel sledování - ochrana garážovaných vozidel před krádeží.

(také jste toho řidiče-zloděje poznali...?)

Obr. 5
Městská ubytovna pro občany v nouzi – chodba před okénkem ostrahy.
Účel sledování - ochrana osob a majetku.

(je přece třeba mít zdokumentované, co návštěva přinesla...)

Obr. 6
Hotel Savoy - kamera v lobby baru.
Účel sledování - zabezpečení majetku a bezpečí ubytovaných osob.

(my přece máme právo dokumentovat, která ze známých osobností si k nám chodí posedět...)

Obr. 7
Krajská nemocnice, 31 kamer na chodbách.
Účel sledování - prevence proti vstupu bezdomovců a proti kapesním krádežím.

(nejsem bezdomovec, tak bych se pod kamerou měla cítit bezpečně...)

Obr. 8
Krajská nemocnice, 31 kamer na chodbách.
Účel sledování - prevence proti vstupu bezdomovců a proti kapesním krádežím.

(tu ruku na dívčím zadečku je přece třeba zdokumentovat...!)

Obr. 9
Městská nemocnice, kamera v kanceláři.
Účel sledování - ochrana majetku nemocnice.

(rozlišovací schopnost záznamu jistě přispěje k odhalení pachatele neoprávněného kopírování...)

Obr. 10
Obchodní dům.
Účel sledování - ochrana majetku.

(bez komentáře...)

Správní řízení

V případech, kdy bylo kontrolou konstatováno porušení zákona o ochraně osobních údajů, bylo dle zákonné povinnosti vedeno s příslušnými subjekty řízení ve věci spáchání správního deliktu, související se zpracováním osobních údajů prostřednictvím kamerového systému.

Pokuta ve výši 200 000 Kč byla uložena státnímu podniku, který prostřednictvím vnitřního kamerového systému v jednom ze svých výrobních závodů zpracovával osobní údaje svých zaměstnanců za účelem zjištění porušení zásad bezpečnostní ochrany výroby a kontroly plnění výkonových norem, potvrzení poruch a prostojů, bez jejich souhlasu. Při zpracování za těmito účely, a dále za účelem zjištění porušení předpisů o bezpečnosti a ochraně zdraví při práci a protipožárních předpisů a za účelem odhalení spáchání trestné činnosti nestanovil dobu uchovávání pořízených záznamů, které fakticky uchovával po dobu v řádu několika měsíců. V souvislosti s provozováním vnitřního i vnějšího kamerového systému ve výrobním závodě neposkytl subjektům údajů informace o zpracování osobních údajů. Dále dotyčný uchovával osobní údaje uvedené ve „Vyhodnocení kamerového záznamu ze dne 5. 3. 2005“ v plastovém pořadači v místnosti mistrů, kde byly ostatním zaměstnancům přístupné i po dobu nepřítomnosti mistrů. Pro účely personální evidence ve výrobním závodě rovněž zpracovával jako nadbytečný osobní údaj získaný prostřednictvím fotografie zaměstnanců vlepené do osobního dotazníku a evidenčního lístku. A konečně, jako správce osobních údajů, nesplnil ve vztahu k uvedenému zpracování osobních údajů kamerovým systémem oznamovací povinnost vůči Úřadu. Uvedeným jednáním došlo k porušení povinností stanovených v § 5 odst. 2, § 5 odst. 1 písm. e), § 11 odst. 1, § 13 odst. 1, § 5 odst. 1 písm. d) a § 16 zákona o ochraně osobních údajů. Proti rozhodnutí o pokutě podal účastník řízení rozklad, který však předseda Úřadu zamítl a napadené rozhodnutí tak nabylo právní moci. Proti rozhodnutí Úřadu byla následně podána správní žaloba, o které dosud příslušný soud nerozhodl.

Pokuta ve výši 60 000 Kč byla uložena městu, které svým jednáním v souvislosti s provozováním kamerového systému porušilo povinnosti stanovené v § 5 odst. 1 písm. d) a e), § 5 odst. 2 a § 11 odst. 1 zákona o ochraně osobních údajů. Město shromažďovalo osobní údaje všech osob pohybujících se v prostorách městského úřadu bez jejich souhlasu a také v rozporu se stanoveným účelem a nad rozsah nezbytný k naplnění účelu, kterým je ochrana majetku města, zamezení korupce a ochrana osob. Dále uchovávalo osobní údaje po dobu 5 dnů, která není nezbytná k účelu jejich zpracování, a nesplnilo rovněž informační povinnost v rozsahu stanoveném v § 11 zákona o ochraně osobních údajů. I toto rozhodnutí správního orgánu prvního stupně bylo napadeno rozkladem, který byl předsedou Úřadu zamítnut.

Počet řízení podle § 17 zákona o ochraně osobních údajů a jejich výsledky jsou předmětem samostatné tabulky vypovídající o činnosti Úřadu. Nicméně v rámci této činnosti a v souvislosti s problematikou zpracování osobních údajů prostřednictvím záznamu z kamerového systému provozovaného na veřejných prostranstvích (jako jsou například náměstí, ulice) obcí, které nemají vlastní obecní policii, a to za účelem předcházení a odhalování pouliční kriminality, vandalismu a za účelem zajišťování bezpečnosti občanů a návštěvníků obce, došel Úřad k závěru, že jakékoliv zpracování osobních údajů (obrazových záznamů) pořízených prostřednictvím kamerového systému z míst veřejně přístupných prováděné subjektem, který k tomu není ze zákona zmocněn (takovým zmocněným subjektem je Policie České republiky a v omezené míře i obecní policie), a to za účelem předcházení a odhalování pouliční kriminality, zajištění bezpečnosti občanů apod., představuje zásah do soukromého a osobního života subjektů údajů, tedy osob, které se ve sledovaném prostoru pohybují a „žijí své běžné denní životy“. V rovině ústavněprávní

lze poté dovodit porušení práva na ochranu před neoprávněným shromažďováním osobních údajů vyjádřeným v čl. 10 odst. 3 Listiny základních práv a svobod. Na základě uvedeného nezbývá než konstatovat, že na oznámené zpracování osobních údajů nelze aplikovat ani výjimku uvedenou v § 5 odst. 2 písm. e) zákona o ochraně osobních údajů.

Druhostupňové řízení

S posuzováním kamerových systémů se Úřad v rámci druhostupňových řízení setkává ve třech rovinách.

1. Námitky podané proti kontrolnímu protokolu v souvislosti s kontrolami subjektů, které tyto systémy provozují.
2. Druhostupňové odvolací řízení proti rozhodnutí Úřadu o nepovolení registrace zpracování dat prostřednictvím kamerového systému (viz § 16 a 17 zákona o ochraně osobních údajů).
3. Případy, kdy je za zpracování osobních údajů tímto způsobem ukládána pokuta a toto rozhodnutí je opět napadeno rozkladem, o němž je třeba rozhodnout.

V roce 2008 bylo v souvislosti s provozem kamerového systému ve druhém stupni projednáno 5 případů námitek proti kontrolnímu protokolu, 5 případů rozkladů proti rozhodnutí o nepovolení registrace podle § 17 odst. 2 zákona o ochraně osobních údajů a 5 případů rozkladu proti uložení pokuty v souvislosti se zpracováním osobních údajů kamerovým systémem.

V rámci rozhodování o námitkách, které dle zákona přísluší předsedovi Úřadu, byly posuzovány námitky podané proti závěrům z kontrol kamerových systémů umístěných v hotelech, v budově úřadu, v prostorách galerie a také systému využívaného městskou policií. Ve všech případech byly hlavní závěry učiněné inspektory Úřadu potvrzeny.

K monitorování hotelových prostorů předseda Úřadu konstatoval, že kamerový systém není z hlediska zákona o ochraně osobních údajů nepřípustným opatřením k ochraně majetku, že jeho parametry se však musejí setkat s požadavky stanovenými zákonem o ochraně osobních údajů, zejména co se týče přiměřenosti tohoto prostředku sledovanému účelu, tj. nezbytnosti zpracovávat osobní údaje s využitím kamerového záznamu. V souladu s výkladovou praxí Úřadu, která odráží i evropské standardy, je podle odvolacího orgánu (předsedy Úřadu) zapotřebí přistupovat k provozování kamerových systémů se záznamem jako k významnému zásahu do soukromí dotčených osob, neboť tak dochází k průběžnému sledování jejich chování. V této souvislosti byl také posuzován způsob plnění informační povinnosti podle § 11 zákona o ochraně osobních údajů prostřednictvím informačních štítků – kdy podle názoru předsedy Úřadu jde o minimální rozsah informací, které by měly být tímto způsobem sděleny osobám vstupujícím do monitorovaného prostoru – informaci, že prostor je sledován, kdo je správcem kamerového systému, a kde lze získat další informace v rozsahu dle § 11 zákona o ochraně osobních údajů. Samozřejmostí je umístění informačních štítků takovým způsobem, aby byly zcela zřetelně viditelné již při vstupu do sledovaných prostor. Absence informací o prováděném zpracování představuje totiž zásadní překážku v posouzení daného zpracování jako legitimního, neboť v důsledku nedostatku informací o prováděném zpracování je dotčeným osobám výrazně ztížena, popř. zcela upřena možnost uplatnit svá práva dle § 12 a 21 zákona o ochraně osobních údajů a tím se aktivně podílet na ochraně svých osobních údajů.

V případě kamer v budovách úřadu či jiných veřejně přístupných institucí (konkrétně galerií) dospěl předseda Úřadu k názoru, že je třeba důsledně oddělit monitorování vnějších prostor, kde jsou sledovány i osoby, které pouze procházejí

monitorovanou oblastí a nemají s činností správce kamerového systému nic společného, od využití kamer k dohledu nad instalovaným cenným zařízením či exponáty. V obou případech je však nutno brát zřetel také na zaměstnance, kteří se v těchto prostorách pohybují, a kteří mají i na základě zákona č. 262/2006 Sb., právo na ochranu svého soukromí na pracovišti.

Ke kamerovému systému využívanému městskou policií, který byl Úřadem posuzován v souvislosti se sledováním soukromých prostor a zpřístupňováním záběrů na webových stránkách města, bylo v rámci druhostupňového řízení uvedeno, že je zcela nezbytné odlišovat účel zpracování osobních údajů získaných tímto způsobem v rámci činnosti městské policie, na kterou se obvykle vztahuje výjimka podle § 3 odst. 6 písm. c) zákona o ochraně osobních údajů a účel zpracování sledovaný zpřístupňováním záběrů určitých záběrů veřejnosti, na který se citovaná (ani jiná) výjimka nevztahuje.

Obecně bylo konstatováno, že pokud dochází pomocí kamer městského kamerového systému ke sledování podezřelých osob či situací v prostoru veřejnosti nepřístupném strážníky městské policie, jde o nezákonné narušení (ústavně zaručené) nedotknutelnosti obydlí. Takové skryté sledování osob v jejich soukromí (přičemž není rozhodné, zda záznamové zařízení je umístěno uvnitř či vně sledovaného objektu) lze provádět pouze za podmínek stanovených trestním řádem a orgány k tomu příslušnými, mezi které však městská policie, resp. strážníci či jiné orgány měst a obcí nepatří. Výjimkou by mohl být pouze případ, kdy by strážníci dokumentovali vstup do obydlí např. z důvodů krajní nouze. Postup, kdy strážníci městské policie sledují prostřednictvím kamerového systému soukromé prostory, je tedy s ohledem na uvedené a zejména s ohledem na fakt, že takový postup je natolik závažným zásahem do práv sledovaných osob, že je striktně upraven právními předpisy pro oblast trestního práva a je vyhrazen pouze určitým orgánům, nutno považovat za zcela nezákonný a případně i trestný podle § 158 odst. 1 písm. a) nebo § 178 odst. 2 zákona č. 140/1961 Sb., trestní zákon.

V rámci odvolacích řízení, kterými bylo rozhodováno o nepovolení zpracování osobních údajů prostřednictvím kamerového systému se záznamem, byly v rámci přezkumu rozhodnutí první instance posuzovány kamerové systémy instalované v obytných domech, v hotelu, v prodejnách obchodního řetězce a v prostředcích hromadné dopravy (tramvajích).

Obecně lze konstatovat, že v souladu se závěry správního orgánu I. stupně je i v odvolací instanci nejpřísněji přistupováno ke kamerovým systémům instalovaným v obytných domech. V obou posuzovaných případech se předseda Úřadu věcně ztotožnil s rozhodnutím, že takové zpracování osobních údajů může být v rozporu především s § 5 odst. 2 a § 10 zákona o ochraně osobních údajů (byť v jednom případě byla věc vrácena s odkazem na nedostatečnost odůvodnění a řízení bylo následně ukončeno z důvodu zpětvzetí podaného oznámení).

Co se týče posuzovaného kamerového systému v hotelu, v této souvislosti předseda Úřadu mj. konstatoval, že zákon o ochraně osobních údajů se nevztahuje pouze na obrazové záznamy kombinované se zvukovými, které je samozřejmě obvykle důvodné považovat za zvýšený zásah do osobnostních práv sledovaných osob, ale i na obrazové záznamy bez zvuku, neboť je zcela zjevné, že určitou skupinu osob bude možné z takového záznamu jednoznačně identifikovat (např. zaměstnance či hosty hotelu, případně osoby veřejně známé) a získat o nich určité informace. Současně je nutno vycházet z faktu, že předmětný záznam je pořizován právě za účelem identifikace osob, a proto je zcela opodstatněný závěr ohledně aplikace § 4 písm. a) a e) zákona o ochraně osobních údajů, a tedy i veškerých povinností, které z tohoto zákona vyplývají.

Vyjádřil se také k výkladu pojmu „doba, která je nezbytná k účelu zpracování“. V dané situaci poskytuje doba 3 dnů dostatečný prostor pro zjištění sledované

události i pro rozhodnutí o tom, jakým způsobem bude vyřešena. Zmíněnou dobu nepovažuje Úřad za absolutní hodnotu, ale za standardní horní hranici, jejíž překročení je, v souladu se stanoviskem Úřadu č. 1/2006 (Provozování kamerového systému z hlediska zákona o ochraně osobních údajů) možné, nicméně na základě jednoznačných důvodů (např. odlehlost sledovaného místa neumožňující častou osobní kontrolu) a obvykle nikoli paušálně ve vztahu k celému kamerovému systému, ale částečně, k jednotlivým kamerám, resp. prostorám.

Úřad uznává kamerový systém jako legální a legitimní prostředek k ochraně majetku a zdraví či života osob, avšak s ohledem na působnost svěřenou mu zákonem o ochraně osobních údajů, musí zpracování osobních údajů, ke kterému pořizováním záznamu z kamer dochází, posuzovat z hlediska principů dle citovaného zákona, aby zásah do osobnostních práv subjektů údajů, k němuž v souvislosti se zpracováním osobních údajů vždy dochází, byl úměrný sledovanému účelu. Přiměřenost je nutno, na základě § 5 odst. 1 písm. a) a b) zákona o ochraně osobních údajů, posuzovat jednak podle deklarovaného účelu (cíle či záměru, kterého má být dosaženo právě prostřednictvím zpracování osobních údajů), jednak podle zvolených prostředků. V případě zpracování osobních údajů prostřednictvím záznamu z kamerového systému je přitom nepochybné, že s ohledem na charakter tohoto prostředku, dochází k neselektivnímu shromáždění informací o velké skupině osob, z nichž jen u některých (resp. spíše jen u zcela malého procenta, tj. těch, kteří se dopouštějí určitého nedovoleného či nežádoucího jednání) je splněn sledovaný účel zpracování. Současně je zde však velká skupina osob, které nejsou primárním objektem sledování, ale jsou z hlediska správce systému snadno identifikovatelné – v daném případě jde především o hosty a zaměstnance hotelu, ale také o zástupce obchodních partnerů, nejrůznější dodavatele a o další osoby s určitým, obvykle pracovním, vztahem k hotelu, případně obecně známé osoby. Ve vztahu k těmto určitelným osobám je pak nutno veškeré informace zaznamenané prostřednictvím kamerového systému považovat za osobní údaje podléhající režimu zákona o ochraně osobních údajů (jde např. o údaj, kdy se daný host v hotelu ubytoval, kým byl doprovázen, kdy a v jakém čase přicházel či odcházel, obdobně v případě zaměstnanců hotelu či spolupracujících společností lze ze záznamu zjistit čas jejich příchodu a odchodu, včetně doby strávené v prostorách hotelu). Nejde tedy pouze o informace týkající se obsahu verbální či neverbální komunikace, ale o komplex informací týkajících se chování sledovaných osob, které by v případě zneužití zcela jistě mohly mít výrazný dopad na práva a zájmy těchto osob, z nichž – a to je nutno opět zdůraznit – v naprosté většině případů nejde o osoby, které mají být, s ohledem na deklarovaný účel, objektem monitorování.

Odmítnuto (tj. nepovoleno) s odkazem na § 5 odst. 2 a § 10 zákona o ochraně osobních údajů bylo také zpracování osobních údajů prostřednictvím kamerového systému v obchodním řetězci, kterým měl být sledován prostor každé pokladny. Uvedený závěr byl přijat zejména s ohledem na § 316 odst. 2 zákoníku práce.

Předseda Úřadu se v tomto případě dále vyjádřil také obecně k pojmu soukromí, neboť tento pojem je často vykládán v příliš úzkém smyslu zahrnujícím pouze ryze soukromé aktivity a interpersonální kontakty, ačkoli z praxe Evropského soudu pro lidská práva (tj. z judikatury k Evropské úmluvě o ochraně lidských práv a základních svobod, např. rozhodnutí ve věci Niemietz v. Německo z roku 1992) i z praxe Úřadu je zřejmé, že tento pojem je naopak nutno chápat a vykládat extenzivně. Ochrana poskytovaná zaměstnancům prostřednictvím zákona o ochraně osobních údajů, a v této souvislosti také prostřednictvím § 316 odst. 2 zákoníku práce, směřuje k naplnění ústavně garantovaných práv na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů, které je základním lidským právem, úzce souvisejícím s právem na lidskou důstojnost, osobní

čest a ochranu soukromého a rodinného života. Z uvedeného je tedy zřejmé, že pojem soukromí na pracovišti nelze omezit na úzkou skupinu důvěrné sféry osobního života zaměstnance, ale zahrnuje celou škálu situací, kdy zaměstnanec oprávněně očekává zvýšenou míru zachování své důstojnosti a osobní integrity. Podrobením zaměstnance soustavnému monitoringu jeho chování, což je jednoznačný důsledek instalace kamer směřujících na každou jednotlivou pokladnu, a to na pracovišti, kde zaměstnanec tráví podstatnou část pracovního dne, dochází dle odvolacího orgánu jednoznačně k zásahu do práv zaměstnance na ochranu jeho soukromí.

Ve zvýšené míře byla v roce 2008 projednávána odvolání subjektů, kterým byla uložena pokuta. Projednávání v rámci rozkladové komise se ukázalo jako velice přínosné pro celkový postoj Úřadu k řešení této problematiky. Došlo ke sblížení výkladu mezi prvo- a druhostupňovým orgánem.

Soudní přezkum

V roce 2008 byly proti pravomocným rozhodnutím Úřadu podány dvě žaloby, kterými se dotčené subjekty prostřednictvím mimořádného opravného prostředku domáhají změny. Byla podána žaloba v případu uložení pokuty ve výši 200 000 Kč státnímu podniku, který prostřednictvím vnitřního kamerového systému v jednom ze svých výrobních závodů, zpracovával osobní údaje svých zaměstnanců za účelem zjištění porušení zásad bezpečnostní ochrany výroby a kontroly plnění výkonových norem, potvrzení poruch a prostojů. Tato žaloba dosud nebyla projednána.

Dále bylo žalobou ke správnímu soudu napadeno rozhodnutí ve věci pokuty (90 000 Kč) základní umělecké škole, která instalovala kamerový systém a jeho pomocí dokumentovala chování zaměstnanců, žáků a jejich doprovodu, zaměstnanců pronajatých provozoven a uživatelů bytu umístěného v budově školy a rovněž dalších osob, které náhodně docházejí do budovy školy. Ani tato žaloba nebyla zatím projednána.

V závěru roku bylo žalobou ke správnímu soudu napadeno také rozhodnutí předsedy Úřadu potvrzující pokutu ve výši 60 000 Kč uloženou městu, které monitorovalo prostory městského úřadu. Tato žaloba bude příslušným soudem projednávána nejdříve v průběhu roku 2009.

Problematikou zpracování osobních údajů prostřednictvím kamerových systémů se záznamem, se bude Úřad zabývat v nezmenšené míře i nadále. Budou využívány nejen zkušenosti z vlastní dozorové činnosti, ale i z činnosti ostatních obdobných úřadů v Evropě, a to zejména ve smyslu závěrů jednání Mezinárodní konference komisařů pro ochranu dat a soukromí, která se konala v září 2007 a která deklarovala, že ten, kdo chce zpracovávat osobní údaje prostřednictvím kamerového systému, musí prokázat, že instalace takového systému je:

– prokazatelně nutná pro řešení konkrétního problému,
– prokazatelně vhodná k vyřešení daného problému,
– proporcionální vůči bezpečnostnímu přínosu,
– zasahuje do soukromí prokazatelně méně než alternativní možnosti.

OCHRANA SPOTŘEBITELE

Technologie RFID – čipové karty

Úřad prováděl v roce 2008 kontrolu tří subjektů, které využívají technologie RFID čipů. Ve všech případech jde o společností zabývající se zajišťováním veřejné osobní dopravy.

– RFID (Radio Frequency Identification) znamená použití elektromagnetických rádiových vln pro komunikaci k/z čipu modulovanými a kódovacími schématy pro unikátní přečtení identity RFID čipu nebo dalších dat, která jsou na něm uložena. Vzhledem k jejich stále masivnějšímu rozšíření, obtížné kontrolovatelnosti, zmenšující se velikosti, klesající ceně a zvětšování kapacity čipů dochází také k masivnějším dopadům na soukromí občanů a zvyšování rizik zneužívání zaznamenaných údajů zejména ve spojení s osobními údaji, a to jak v privátní sféře, tak i úřadů. Nařízení Rady Evropské unie o povinnosti členských států zavést tzv. biometrické pasy, tedy pasy s bezkontaktním čtením údajů, fotografie a otisků prstů, se již uskutečňuje a není daleko doba, kdy budeme mít povinně občanské průkazy se svými identifikačními údaji na RFID čipu.

– Jednou z prvních masivních aplikací RFID, bylo jejich nasazení v supermarketech jako náhrada tzv. barkódů (čárových kódů) pro zjednodušení a urychlení evidence výrobků, prevence proti krádežím a urychlení obsluhy zákazníků u pokladen. Protože však nebyla ochota provozovatelů informovat o rizicích, která byla s touto technologií spojena a docházelo ke zneužívání údajů z čipů, začaly se množit stížnosti od společností na ochranu zákazníků.

– V reakci na stížnosti zákazníků supermarketů a v důsledku širokého nasazování aplikací a technologií RFID vydala WP29 (pracovní skupina vzniklá jako nezávislý poradní orgán Evropské komise podle článku 29 směrnice 95/46/EC) již v roce 2005 stanovisko, kterým reguluje využívání této technologie v právním rámci ochrany dat této směrnice. Stanovila rovněž zásady, které musejí správci údajů dodržovat, aby nedošlo k narušování soukromí a ochránily se osobní údaje jednotlivců.

– Stanovisko WP29 zdůrazňuje, že rámec, který se použije na využívání technologie RFID i jakékoliv jiné technologie, je stanoven v 2. bodě odůvodnění směrnice o ochraně údajů, který říká, že „systémy zpracování údajů slouží lidem; (…) musejí bez ohledu na státní občanství nebo bydliště fyzických osob dodržovat základní svobody a práva těchto osob, zejména právo na soukromí, a přispívat k hospodářskému a sociálnímu pokroku, k rozvoji obchodu, jakož i dobrých životních podmínek jednotlivců“.

Zásady zpracování osobních údajů při použití technologie RFID

– **Zásady související s kvalitou údajů:** Nesmějí se shromažďovat žádné nepodstatné údaje, a jestliže již byly shromážděny, musejí být vymazány.
– **Zásada uchovávání:** Vyžaduje, aby osobní údaje nebyly uchovávány déle, než je nezbytné pro účel, pro který byly údaje shromážděny nebo dále zpracovány.
– **Zákonné důvody zpracování:** Jediným zákonným důvodem pro legitimní shromažďování informací prostřednictvím RFID je souhlas jednotlivých osob (subjektů údajů), pokud by toto zpracování mohlo být legitimní pro zachování životně důležitých zájmů subjektu údajů (například označení předmětů využívaných při operacích).

– **Informační požadavky:** Správci údajů, kteří zpracovávají informace prostřednictvím technologie RFID, musejí poskytnout subjektům údajů následující informace: totožnost správce, účely zpracování a mj. také informace o příjemcích údajů a o existenci práva na přístup k těmto údajům. Např.: maloobchodní prodejna musí poskytnout subjektům údajů alespoň zřetelné oznámení o těchto skutečnostech. Správce údajů musí informovat také o tom, jak deaktivovat nebo odstranit štítky z výrobků a zabránit tak tomu, aby sdělovaly další informace, a jak uplatňovat právo na přístup k informacím. Tyto informace budou nutné v případech, kdy RFID čipy budou součástí zboží. Informace musejí být poskytnuty zřetelně a srozumitelně.
– **Subjekt údajů by měl být schopen pochopit důsledky použití RFID.**

Pozornost Úřadu se zaměřila na využívání čipových karet používaných dopravci v osobní železniční i autobusové dopravě. Čipové karty jsou v tomto případě využívány zejména jako elektronická peněženka a forma předplatní jízdenky. Systém RFID tak nahrazuje stávající systémy úhrady jízdného, vstupného i samotného placení v hotovosti. Podle provozovatelů karet je důvodem pro jejich zavedení vždy zvýšení efektivity a snížení provozních nákladů. Ani v jednom případě nebyl ze strany provozovatele technologie RFID deklarován záměr „sledovat" držitele karet. Ukázalo se, že si provozovatelé ve velké většině nebyli vědomi toho, že tato nová technologie jako „přidružený" produkt obsahuje informace o tom, kde a kdy se držitel karty pohyboval. Tedy, jazykem zákona o ochraně osobních údajů, dochází ke shromažďování osobních údajů držitelů čipových karet, které neodpovídá stanovenému účelu, a to bez vědomí, tedy také bez souhlasu těchto osob.

Všichni vydavatelé čipových karet vybavených technologií RFID shodně vysvětlují, proč shromažďují tyto údaje. Důvodem je pouze zúčtování vzájemných finančních operací, které se prostřednictvím karty uskutečnily. To, že jsou současně zpracovávány osobní údaje, je tedy z jejich hlediska nezbytné.

Úřad je však přesvědčen, že základem pro shromažďování těchto údajů je již výchozí přístup vydavatelů karet při jejich prodeji nebo distribuci, kteří evidují osobní údaje každého držitele čipové karty. V rámci odůvodnění, proč je tak činěno, jsou uváděna různá vysvětlení, která se týkají zejména důvodů spočívajících v zákonném zajišťování dopravních služeb občanům. Úřad se setkal i s tvrzením, že aby mohl přepravce poskytovat slevu, tak musí občan souhlasit s tím, že bude odevzdávat, a to zcela „dobrovolně", své osobní údaje. V rámci provedených kontrol bylo zjištěno, že sice právní předpisy upravují jednotlivé oblasti poskytování veřejné dopravy, ale ani v jednom není nařízena povinnost evidovat cestující. Úřad samozřejmě prověřoval všechny předkládané důvody s ohledem na ochranu osobních údajů, dbal ovšem na to, aby nenarušil kontrolní funkce systémů. Zaznamenal i názory stěžovatelů a některé názory v médiích, že elektronická kontrola cestujících, propojená s evidencí jejich osobních údajů, je důsledkem „vrchnostenského" postoje úředníků, kteří rozhodují o tom, kdo a za jakou částku bude moci využívat dopravních služeb. A k tomu využívají ekonomický nátlak: roční cenový rozdíl za využívání dopravy anonymně nebo s umožněním vlastního sledování činí až několik tisíc korun, což nelze hodnotit jinak než jako vynucení poslušnosti občanů. Cenové otázky jsou ale mimo kompetenci Úřadu a spadají do oblasti, kterou může kontrolovat Česká obchodní inspekce, či jiné kompetentní státní orgány.

Z hlediska zákona o ochraně osobních údajů je však třeba položit otázku, zda nedochází k vynucování souhlasu. Podle dikce zákona o ochraně osobních údajů však získaný souhlas se zpracováním osobních údajů má být **svobodným projevem** vůle subjektu údajů.

Kontrola prováděná u největšího železničního dopravce se zaměřila na zpracování osobních údajů v souvislosti s využíváním elektronických karet, na jejichž základě lze využívat jednotlivé typy slevových jízdenek nebo jsou i formou před-

placeného jízdného. Kontrola se zaměřila na oprávněnost zpracování osobních údajů, na jejich rozsah a na další povinnosti, které správci osobních údajů ukládá zákona o ochraně osobních údajů, zejména na to, zda jde o zpracování osobních údajů na základě zvláštního zákona, nebo na základě souhlasu držitele karty. Ačkoli drážní zákon umožňuje železničnímu přepravci zpracovávat osobní údaje cestujících z mnoha důvodů, nebylo zjištěno, že by opravňoval evidovat každého cestujícího. Takto široce stanovený účel zpracování osobních údajů v zákoně o drahách není zakotven, a přepravce si jej vyložil tak, aby vyhovoval jeho záměrům. Bylo rovněž konstatováno, že o všech účelech a rozsahu zpracovávaných osobních údajů nejsou cestující informováni v souladu se zákonem o ochraně osobních údajů. Kontrola proto byla ukončena uložením nápravného opatření, které spočívá v průběžné anonymizaci a likvidaci všech osobních údajů, které byly o cestujících shromážděny. Dále bylo uloženo fyzické oddělení jednotlivých databází, které jsou v souvislosti s poskytováním dopravních služeb vedeny.

Kontroly prováděné u dopravních společností se zaměřily především na oprávnění a legalitu shromažďovat osobní údaje již při distribuci nebo prodeji čipových karet. Bylo zjištěno, že pro shromažďování a další zpracování osobních údajů při vydávání čipových karet neexistuje zákonná povinnost. Ukazuje se také, že lze vydávat jízdní doklady – karty s čipem RFID tak, že osobní údaje v rozsahu jméno, příjmení a fotografie lze otisknout pouze na kartu a neukládat je v databázi. Často uváděný důvod dopravců, že seznamy osob, kterým byla karta vydána, slouží právě těmto osobám pro případ krádeže nebo ztráty karty, aby karta mohla být snadno a rychle zablokována a aby tím bylo znemožněno její zneužití neoprávněnou osobou, je třeba odmítnout, protože zákon dává přednost takovým prostředkům, které nenarušují soukromí a neohrožují osobní údaje. Je totiž zcela jednoduché vydat každému držiteli při předávání karty potvrzení o předání (zaplacení) karty, které může obsahovat informaci o druhu a čísle karty, případně i jméno a příjmení, jimiž lze prokázat oprávněnost držení karty i zaplacené aplikace. Podle čísla karty uvedeného na takovém dokladu ji lze okamžitě zablokovat. V praxi však vydavatel karty, jako správce osobních údajů, rozhoduje za cestujícího sám, neumožňuje mu projevit svobodnou vůli a navíc paternalisticky zodpovídá za občana. Kontroly zjišťují, že čipová karta, vydávaná jedním velkým přepravcem je na základě smlouvy využívána dalšími dopravci, kteří se v rámci jednoho kraje podílejí na osobní přepravě. Na základě smluv dochází ke vzájemnému vyúčtování na základě informací, které jsou získávány „přečtením“ informací čtečkou, která je umístěna v každém smluvním dopravním prostředku. Z čipu jsou zjišťovány informace o čísle čipu, místu nástupu, místu výstupu, dni a hodině nástupu pro vzájemné finanční zúčtování. Prostřednictvím čísla čipu je ovšem možné velice snadno zjistit držitele karty, tedy konkrétní fyzickou osobu. Následně pak tedy není těžké zjistit, kdy a kde se konkrétní fyzická osoba – cestující pohyboval.

Kazuistika

I.

Na základě plánu byla provedena kontrola Českých drah, a.s. Jejím předmětem bylo zpracování osobních údajů za použití nového systému úhrady jízdného prostřednictvím čipové karty In-karty. Kontrolou bylo zjištěno, že České dráhy zavedly systém prodeje předplatních jízdenek s využitím čipových karet a povinnosti správce osobních údajů porušily tím, že nesplnily informační povinnost dle § 11 zákona o ochraně osobních údajů a neúplně informovaly držitele čipových karet o zpracování jejich osobních údajů. Osobní údaje byly zpracovávány v rozporu se stanoveným účelem a nad rámec stanoveného účelu, tedy v rozporu s ustanovením § 5 odst. 1 písm. d) zákona o ochraně osobních údajů. Kontrolou bylo zjištěno, že při zpracování informací o provozu In-karty dochá

zí ke shromažďování informací o jednotlivých uskutečňovaných jízdách, tedy ke sledování pohybu držitele In-karty. Na základě zjištěných skutečností, nařídil kontrolující inspektor Úřadu Českým drahám nápravné opatření, spočívající ve změně vedení databází, ve kterých byly uchovávány informace o pohybu cestujících. České dráhy k 31. prosinci 2008 oznámily splnění uloženého nápravného opatření.

II.
V roce 2008 prováděl Úřad kontrolu Hlavního města Prahy, a to v souvislosti se zpracováním osobních údajů při vydávání a provozu čipové karty Opencard. Protože v průběhu roku došlo k výraznému rozšíření využívání čipové karty o další aplikace v rámci městské hromadné dopravy a následně předměstské integrované dopravy, nebylo možné tuto kontrolu ukončit do konce roku.

Z průběhu kontrol obou výše uvedených subjektů lze odvodit i poznatek, spočívající v tom, že ani při rozhodování o zavedení nové technologie, ani při zpracování projektů, nejsou zahrnuty povinnosti, vyplývající ze zákona o ochraně osobních údajů. Teprve v průběhu kontroly jsou následně, a často násilně, vymýšleny rozličné důvody, proč jsou osobní údaje klientů zpracovávány a zpětně „šroubovány“ do celého informačního procesu.

Na základě zjištění, že karta je využívána v rozporu s přepravním řádem, lze následně provést její zablokování. Ke zjištění, zda držitel karty je oprávněným, či není oprávněným držitelem karty, tedy není nutné vést databázi všech osob, kterým byla karta vydána.

Poznatky o využívání technologie RFID

Úřad se ve své dozorové praxi setkává s dalším častým využíváním čipových karet, a to zejména při využívání kontroly vstupů, elektronického zamykání a kontroly docházky zaměstnanců. Tak jako u každé technologie jsou vlastnosti čipů RFID využívány ke zkvalitnění určité činnosti. Základním problémem se však stává nekontrolovatelnost shromažďovaných a následně zpracovávaných údajů. Bezkontaktní technologie umožňuje správci instalovat čtečky čipů kdekoliv i skrytě a rovněž mu umožňuje naprogramovat celé zařízení rozličnými funkcemi. V praxi jsou využívány systémy, které nejen umožňují vstup oprávněným držitelům karet do určitého prostoru, ale současně jsou ukládány informace o vstupu, tedy identifikace konkrétního čipu a času vstupu. Stále častěji jsou tyto systémy doplňovány o další čtečky čipů, které jsou umístěny nejen u vchodů, ale i v dalších vnitřních prostorách. Vzhledem k tomu, že vysílače RFID mají dosah kolem 10 metrů, není problémem snímat všechny pohyby čipů v okolí. Základním problémem je tedy skutečnost, že běžný držitel čipové karty nemá možnost ovlivnit, jaká data jsou prostřednictvím RFID shromažďována a uchovávána, a zejména neví, jakým způsobem a proč jsou zpracovávána a vyhodnocována, neboť kromě správce systému nemá nikdo praktickou možnost tento stav zkontrolovat. Zejména v pracovně právních vztazích napomáhá využívání technologie RFID k nerovnému postavení mezi zaměstnanci a zaměstnavatelem.

Technologie RFID na čipových kartách je v posledních dvou letech více využívána i k monitorování vstupů do bytových domů. Je zcela legitimní využití čipových karet pro to, aby byl umožněn vstup do bytového domu pouze oprávněným osobám, ale v praxi se Úřad setkává s tím, že jsou zaznamenávány a uchovávány veškeré příchody a odchody obyvatel domu. Správci těchto zařízení většinou deklarují, že účelem shromažďování těchto údajů je prevence před kriminalitou a zabránění vstupu neoprávněným osobám do domu. Shromažďují informace, ale na jejich základě nelze zabránit vstupu neoprávněné osoby a zdaleka nelze odhalit případný í delikt, kterého se dopustí ten, kdo není držitelem čipové karty. Lze se setkat i s případy, kdy systém bývá doplněn také kamerovým systémem.

Z hlediska zákona o ochraně osobních údajů jde o zpracování osobních údajů, které neodpovídá stanovenému účelu.

Naopak se Úřad ve své dozorové a konzultační praxi v porovnání se zahraničím jen v malé míře setkává s využíváním technologie RFID v obchodní činnosti – v oblasti, pro kterou byla tato technologie primárně vyvíjena – tedy v oblasti logistiky a sledování oběhu zboží, v obchodní činnosti, ke kontrole v čistírnách a prádelnách, v půjčovnách zboží atd. Úřad však i v této oblasti průběžně sleduje vývoj a postupnou aplikaci této technologie.

Úřadem jsou však též zaznamenávány informace o dalším využívání technologie RFID, jako je například sledování bankovek a cenin nebo identifikace zvířat. Zvláštní pozornost je věnována využívání technologie RFID ve zdravotnictví, kde slouží ke kontrole v léčebném procesu. Úřad se doposud nesetkal s módním výstřelkem aplikace čipu pod kůži, který následně slouží jako kreditní karta. S postupným zlevňováním výroby čipů RFID, lze očekávat jejich masivnější využívání v běžném životě, čímž zákonitě dojde k častějšímu zneužívání vlastností RFID. Bezkontaktní výměna informací, kterou téměř nelze kontrolovat, a snaha shromažďovat informace jakéhokoliv druhu k následnému využití, je reálnou hrozbou.

NEVYŽÁDANÁ OBCHODNÍ SDĚLENÍ

Problematika šíření obchodních sdělení je upravena zákonem č. 480/2004 Sb., o některých službách informační společnosti, který je transpozicí příslušných směrnic ES týkajících se podmínek elektronické komunikace při obchodování. A stejně jako příslušné zákony v ostatních členských státech, vyvolává určité výkladové problémy. Lze říci, že Úřad již po zkušenostech, které získal, velmi intenzivně plní roli regulátora této oblasti, i když se neustále potýká se snahou rozesílatelů obchodních sdělení najít v zákoně určité možnosti či využít výkladových problémů, aby mohli rozesílat obchodní sdělení potenciálním zákazníkům bez jejich předchozího souhlasu. Z poctivých podnikatelů se tak mnohdy stávají nelegální rozesílatelé. Obecně lze říci, že počet podávaných stížností na zasílání nevyžádaných obchodních sdělení je na stejné úrovni jako v roce 2007. V roce 2008 se Úřad v rámci kontrolních a správních činností vyplývajících z kompetence postihovat nevyžádaná obchodní sdělení zaměřil především na ty subjekty, které zasílaly obchodní sdělení ve větším rozsahu a na ty, které se dopouštějí porušení výše uvedeného zákona opakovaně.

V roce 2008 obdržel Úřad 1458 podnětů na šíření nevyžádaných obchodních sdělení, z toho bylo vyřešeno 1311. Zahájeno bylo 155 kontrol a v průběhu roku bylo 91 kontrol ukončeno. 255 stížností bylo shledáno neoprávněnými (176 nebylo obchodní sdělení, 79 pocházelo ze zahraničí), v 94 případech se nepodařilo dohledat odesílatele. 320 subjektům bylo uloženo nápravné opatření. S 81 subjekty bylo vedeno správní řízení a byla jim pravomocně uložena pokuta v celkové výši 896 500 Kč.

Poznatky z praxe

1) Důkazní břemeno odmítnutí zasílání obchodních sdělení je na straně adresáta obchodního sdělení (zákazníka, uživatele e-mailové adresy).
Zákon o některých službách informační společnosti umožňuje zasílat obchodní sdělení svým zákazníkům, kteří to předem neodmítli, bez jejich souhlasu a ostatním pouze na základě jejich souhlasu. Zasílat obchodní sdělení lze až do jejich odmítnutí či do odvolání uděleného souhlasu. V případě sporu je pak důkazní břemeno přesunuto na adresáta (tedy na příjemce) obchodních sdělení, který musí prokázat, že další zasílání odmítl. Z tohoto odmítnutí však musí být patrno, že bylo druhé stra-

ně (tedy odesílateli) doručeno. Stává se, že odesílatelé obchodních sdělení k tomu využívají e-mailové adresy, které slouží právě jen pro odeslání zpráv, nikoli však již pro jejich příjem. Pokud by tedy adresát odmítl další zasílání formou odpovědi na zaslané obchodní sdělení, může se stát, že takové odmítnutí zasílateli obchodního sdělení vůbec nepřijde. Je tedy třeba využívat zejména možností, které jsou v zaslaném obchodním sdělení pro jeho další odhlášení stanoveny. Pokud odhlášení probíhá formou kliknutí na odkaz pro odhlášení, kdy se objeví informace o tom, že byla daná e-mailové adresa ze zasílání obchodních sdělení odhlášena či odstraněna, je vhodné si tuto informaci např. v podobě printscreenu obrazovky (tedy uložení jejího obsahu do formátu obrázku) uchovat.

2) Smysl výjimky z definice obchodního sdělení

Negativní definice obchodního sdělení vychází ze směrnice 2000/31/ES, o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu, kde je stanoveno, že údaje umožňující přímý přístup k činnosti podniku, organizace nebo osoby, zejména název domény nebo adresa elektronické pošty jako takové, nepředstavují formu obchodního sdělení.

Smyslem této výjimky je umožnit zaslání informace týkající se např. změny telefonního čísla, adresy, www stránek nebo adresy elektronické pošty, svým zákazníkům či klientům, kteří zasílání obchodních sdělení odmítli, je však třeba jim tyto změny sdělit. Dále se tato výjimka vztahuje i na případy, kdy jsou zasílány ryze soukromé zprávy elektronické pošty (které tedy neslouží k podpoře podnikání), ale jsou zasílány z adresy obsahující doménové jméno nebo je v této zprávě vložen automatický podpis obsahující údaje o společnosti (jako www stránky, adresa elektronické pošty, telefonní číslo apod.).

V právním řádu chybí definice toho, co se považuje za doménové jméno. Názor Úřadu je takový, že se jím rozumí jen registrovaný název domény, nikoli tedy celé URL (tj. internetová adresa) či názvy jednotlivých subdomén, ve kterých je obsaženo nebo z nich lze dovodit činnost fyzické či právnické osoby nebo podniku. Toto tvrzení podporuje též fakt, že z jakéhokoliv textu (jakkoli dlouhého) lze učinit přímý odkaz na jakékoli www stránky. Je tedy nepřípustný výklad, že za doménové jméno může být pokládán jakkoli dlouhý text zapsaný ve formě odkazu na webovou stránku a odeslaný jako samostatná zpráva elektronické pošty. Smyslem této výjimky tedy rozhodně není umožnit takovéto obcházení zákona.

3) Problémy při registraci na webových stránkách – heslo a potvrzující e-maily

V rámci kontrolní činnosti bylo zjištěno, že některé internetové subjekty, které požadují registraci e-mailovou adresou a heslem, si ponechávají heslo v otevřené formě. Mnoho uživatelů používá k takové registraci stejné heslo, jaké má nastaveno na přístup do uvedené e-mailové schránky. Internetové subjekty získávají takto přístup k privátním e-mailovým schránkám. Z hlediska zákona o ochraně osobních údajů je třeba říci, že od klientů jsou osobní údaje získávány s jejich souhlasem, avšak pouze k určitému účelu; přesto získávají tyto internetové subjekty přístup do osobních schránek uživatelů. Úřad není schopen toto počínání postihnout. Je tedy třeba, aby si lidé byli popsaného rizika vědomi a při registraci nepoužívali stejné heslo, jakým zajistili svou osobní e-mailovou schránku.

Zaregistrování na webových stránkách je způsob vyjádření předběžného souhlasu se zasíláním obchodních sdělení, musí však být následně zajištěno, aby uživatel potvrdil, že právě on byl tou osobou, která se zaregistrovala a poskytla svůj souhlas. Pro potřeby zákona o některých službách informační společnosti je takovým postačujícím potvrzením informační e-mail vygenerovaný na základě registrace a souhlasná odpověď na tento e-mail. Registrace by měla být provedena (včetně zasílání obchodních sdělení) až po souhlasné odpovědi na výše uvedený e-mail.

I takto provedená registrace však může být zneužita, a to tím, že po registraci je uživatelem kontaktní e-mailová adresa změněna. S touto „škodolibostí“ je třeba počítat a novou adresu zapsat až po odsouhlasení jejím držitelem.

4) Žádost o souhlas se zasíláním obchodních sdělení zaslaná prostřednictvím e-mailu
Situace, kdy je adresát žádán o souhlas se zasíláním obchodních sdělení pomocí e-mailu není jednoduchá. Souhlas musí být informovaný (ve smyslu: osoba udělující souhlas musí být plně informována, s čím souhlasí), takže už v prvotní žádosti o souhlas je nutno uvést, k čemu je získáván (co bude předmětem nabídek, kdo přesně je bude zasílat atd.). Tímto však už vzniká obchodní sdělení, a to bez předchozího souhlasu posílat e-mailem nelze. Pakliže je taková žádost o souhlas omezena pouze na jméno firmy, adresu či webovou adresu jako takové, tak o obchodní sdělení sice nejde, avšak takto získaný souhlas by nebyl oním výše uvedeným informovaným souhlasem. V každém případě by k odeslání takovéhoto e-mailu na každou jednotlivou e-mailovou adresu mělo dojít pouze jednou, nikoli opakovaně.

Lze tedy konstatovat, že pokud by došlo ke sporu a byla by podána stížnost na rozesílání obchodních sdělení na základě tohoto „neinformovaného“ souhlasu, bude takováto zpráva elektronické pošty považována za obchodní sdělení zaslané bez souhlasu.

Nejlepší způsob je požádat adresáta o souhlas se zasíláním reklamních sdělení přímo na internetových stránkách propagujících danou službu či výrobek. Návštěva stránky je totiž jeho vlastní aktivitou a není zde již problém dostát povinnosti o správném informování, čeho se souhlas týká. Je zde však ještě jeden důležitý moment, který vyplývá ze směrnice 58/2002/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací. Jde o to, že políčko vyjadřující souhlas nesmí být předem zaškrtnuto. Tedy implicitní hodnotou musí být neudělení souhlasu, a souhlas lze udělit až explicitním zásahem uživatele (označením příslušného políčka).

Mezinárodní spolupráce

Úřad je zapojen do Evropské kontaktní sítě orgánů zabývajících se spamem (Contact Network of Spam Authorities – CNSA) a do tzv. Londýnského akčního plánu (London Action Plan – LAP). V rámci těchto mezinárodních organizací lze předávat jednotlivé případy do země původce. Stížnosti na zahraniční nevyžádaná obchodní sdělení však dostává Úřad pouze ojediněle. U žádné z nich však nešlo prokázat porušení mezinárodních kritérií, a to jmenovitě: množství, způsobená škoda či zaviněná újma. Zákon č. 480/2004 Sb., o některých službách informační společnosti, je přísnější než je tomu ve většině evropských zemí, neboť neobsahuje výše uvedená omezující kritéria. Tato kritéria jsou však brána v potaz při rozhodování o výši sankce.

Pokud jde o vymahatelnost zákona přes hranice, tak Úřad postupuje podle nařízení Evropského parlamentu a Rady (ES) č. 2006/2004, o spolupráci v oblasti ochrany spotřebitele. V rámci této spolupráce byl vytvořen i mezinárodní informační systém CPCS (Consumer Protection Cooperation System). Úřad získal během roku 2008 přístup do komunikační sítě TESTA II, která umožňuje výměnu dat v rámci systému CPCS, pro všechny orgány, které v rámci této sítě pracují. Úřad tak může prostřednictvím tohoto systému předávat příslušným zahraničním orgánům případy, kde je přítomen právě onen zahraniční prvek (např. odesílatel nevyžádaných obchodních sdělení je usídlen v některém z evropských států).

Kontrolní proces

V mnoha případech je tento proces zdlouhavý

Při provádění kontroly, jejímž předmětem je dodržování povinností při rozesílání obchodních sdělení prostřednictvím elektronických prostředků, postupuje Úřad podle zákona č. 552/1991 Sb., o státní kontrole. Administrativní vyřizování takové stížnosti v tomto režimu může být velice zdlouhavým procesem. V rámci zahájení kontroly je kontrolovaný dotazován prostřednictvím již standardně pokládaných otázek, vztahujících se na jím zaslaná obchodní sdělení. Jestliže má kontrolující pochybnost ohledně pravdivosti poskytnutých odpovědí, požaduje na kontrolovaném doplnění, nebo provede kontrolu na místě. Délka kontrolního procesu je tak závislá zejména na složitosti případu a spolupráci kontrolovaného. V případě, že kontrolovaný součinnost potřebnou ke kontrole neposkytuje, jsou mu ukládány pořádkové pokuty, jinou možnost kontrolující nemá, a celý kontrolní proces se pak tímto prodlužuje. Kontrolní proces je pak ukončen až uplynutím lhůty k podání námitek vůči kontrolnímu protokolu či vyřízením těchto námitek. Pokud je shledáno porušení zákona, tak na kontrolní řízení navazuje řízení správní – zde má účastník řízení právo využít opravné prostředky, čímž se řízení prodlužuje. Stěžovatel je pak vyrozumíván až o konečném vyřízení jeho stížnosti, tedy často až po ukončení správního řízení, tj. poté, co je rozhodnutí pravomocné.

KAZUISTIKA – RŮZNÉ

Kontrola ve společnosti s ručením omezeným zaměřená na dodržování povinností společnosti při zpracování osobních údajů žáků a studentů škol, účastníků školní soutěže

Z obsahu podnětu vyplývalo, že uvedená společnost při shromažďování (zpracování) osobních údajů požaduje uvedení rodného čísla účastníka soutěže, jako součást registračního formuláře prezentovaného na internetových stránkách společnosti. Před ukončením soutěže si zástupce společnosti uvědomil nadbytečnost zpracování rodného čísla a neprůkaznost souhlasu s jeho zpracováním v průběhu zákaznické soutěže a ihned po zaslání zpracované databáze účastníků tento seznam přihlášených přes příslušná přístupová hesla otevřel a odstranil sloupec s rodnými čísly.

Při zpracování osobních údajů vyplývá pro správce údajů povinnost odst. 1 shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Správcem stanovený účel byl kontakt na výherce soutěže a doručení soutěžní ceny. Za tímto účelem byl správcem stanovený rozsah údajů, uvedený v „Registračním formuláři pro žáky“, který obsahoval jméno, příjmení, e-mail, rodné číslo, ulici, číslo popisné, město, PSČ a uvedení školy, kterou žák navštěvuje. Takto stanovený a následně zpracovávaný rozsah údajů účastníků soutěže nebyl nezbytný pro naplnění stanoveného účelu a tím došlo k porušení povinnosti správce.

V případě zpracování rodného čísla, bylo nezbytné konstatovat, že na jeho zpracování (na užívání, nakládání s rodným číslem) se vztahuje ustanovení zvláštního právního předpisu, a to zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech. Při zpracování rodného čísla účastníků soutěže správce údajů nesplnil povinnost uloženou uvedeným zvláštním právním předpisem, a to tím, že neprokázal kontrolujícím právní titul k tomuto zpracování, tj. souhlas nositele rodného čísla, nebo jeho zákonného zástupce.

Na základě posouzení zjištěných skutečností **bylo konstatováno, že kontrolované povinnosti správce byly v rozporu s plněním povinností správce ukládaných zákonem o ochraně osobních údajů a zákonem o evidenci obyvatel.**

Na základě výše uvedeného se správce dopustil správního deliktu, za což mu byla udělena pokuta ve správním řízení.

Zpracování osobních údajů uchazečů o zaměstnání

Odbor správních činností, na základě podnětu doručeného Úřadu, vedl správní řízení, ve kterém došel k závěru, že zaměstnavatel, který má v úmyslu přijmout nového zaměstnance na základě výběrového řízení, shromažďuje osobní údaje předem neurčeného počtu osob (uchazečů), které projeví zájem stát se jeho zaměstnancem, a to bez jejich souhlasu na základě § 5 odst. 2 písm. b) zákona o ochraně osobních údajů, neboť takové zpracování je nezbytné pro jednání o uzavření (pracovní) smlouvy uskutečněného na návrh subjektu údajů (přihláška do výběrového řízení). Podle správního orgánu je jednání o uzavření smlouvy v případě výběrového řízení na volné pracovní místo ukončeno v okamžiku, kdy je uchazeč vyrozuměn o tom, že nebyl na pracovní místo vybrán, nebo kdy je s ním naopak v případě jeho výběru uzavřena např. pracovní smlouva. Při posuzování této otázky správní orgán zejména vycházel z § 43b odst. 1 písm. c) zákona č. 40/1964 Sb., občanský zákoník, podle kterého návrh na uzavření smlouvy, i když je neodvolatelný, zaniká dojitím projevu o odmítnutí návrhu navrhovateli. Obdobně tedy platí, že v předmětné věci mohl účastník řízení bez souhlasu uchazeče zpracovávat jeho osobní údaje pouze do okamžiku, kdy mu sdělil, že nebyl na pracovní místo vybrán. Pro další zpracování jeho osobních údajů by poté musel mít jeho prokazatelný souhlas, neboť nepřijatý uchazeč oprávněně předpokládal, že jednání o uzavření pracovní smlouvy bylo ukončeno. Rozhodnutí ve věci nabylo právní moci.

Kontrola zpracování osobních údajů ve sběrně kovošrotu

Kontrolou bylo na základě podnětu zjišťováno, zda a jak se podnikatel v uvedené sběrně řídí právní úpravou zpracování osobních údajů, kterou je jeho činnost regulována. Správce je povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu: Při shromažďování osobních údajů je povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům a o právu na opravu osobních údajů, jakož i o dalších právech stanovených zákonem. (V případě, kdy správce zpracovává osobní údaje získané od subjektu údajů, musí subjekt údajů poučit o tom, zda je poskytnutí osobního údaje povinné či dobrovolné. Je-li subjekt údajů povinen podle zvláštního zákona osobní údaje pro zpracování poskytnout, poučí jej správce o této skutečnosti, jakož i o následcích odmítnutí poskytnutí osobních údajů.)

Povinnost podnikatele vést evidenci osob, od kterých vykoupil odpady, a řídit se dalšími právními ustanoveními s tím souvisejícími je stanovena zákonem č. 185/2001 Sb., o odpadech. Provozovatel je povinen při odběru nebo výkupu odpadů vést evidenci osob, od kterých odpady odebral nebo vykoupil; k plnění této povinnosti je oprávněn vyžadovat k nahlédnutí osobní průkazy totožnosti těchto osob. Bez ověření totožnosti tento odpad neodebere ani nevykoupí. Při nakládání s osobními údaji fyzických osob tedy postupuje provozovatel podle uvedeného zvláštního zákona. Prováděcím právním předpisem je vyhláška Ministerstva životního prostředí č. 383/2001 Sb., o podrobnostech nakládání s odpady. Zde je sta-

novena povinnost provozovatele zařízení k výkupu odpadů vést evidenci osob, od nichž byl vykoupen kovový odpad, evidovat druh a množství vykoupeného odpadu, přičemž je zde vymezen i rozsah zpracování osobních údajů. Protože kontrolovaný podnikatel nejednal v souladu s těmito právními ustanoveními, jeho činnost musí být posuzována i podle příslušných ustanovení zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech: Když podnikatel do evidence osob, od nichž vykoupil odpady, zařazoval i rodná čísla těchto osob, nerespektoval ani ustanovení tohoto zákona. A jelikož shromažďoval osobní údaje v rozsahu větším než pro naplnění stanoveného účelu nezbytném, jednal také v rozporu se zákonem o ochraně osobních údajů. Osoby, od kterých vykupoval odpady, při zpracování jejich osobních údajů o ničem neinformoval. Tím rovněž porušil zákon o ochraně osobních údajů.

Kontrolou bylo prokázáno, že uvedeným jednáním podnikatele došlo k porušení zákona o ochraně osobních údajů a že se dopustil také jiného správního deliktu. Ve správním řízení mu byla uložena pokuta.

Nabídka služeb zprostředkovatelskou kanceláří

V srpnu 2008 obdržel Úřad stížnost na jednání zprostředkovatelské kanceláře, která bez jakéhokoliv podnětu oslovila dopisem paní X s nabídkou bezplatné služby při uplatnění nároků na náhradu škody od pojišťovny za účasti specializované kanceláře. Tento dopis byl poslán, přestože paní X nikdy nesdělovala žádné zprostředkovatelské kanceláři své či manželovy osobní údaje a informace týkající se úmrtí jejího manžela a nikdy nedala souhlas s odesláním této nabídky. Úřad uvedené jednání shledal jako možné porušení zákona a proto byla na základě tohoto podnětu zahájena kontrola. Zprostředkování služeb na základě ustanovení živnostenského zákona prováděla zprostředkovatelská kancelář pro samostatnou advokátku, která poskytuje advokátní služby v oblastech občanského, trestního a pojišťovacího práva.

Advokátní kancelář sama potenciální klienty neoslovuje, činí tak jen výjimečně.

Kontrolou bylo zjištěno, že zprostředkovatelka advokátní kanceláře napsala dopis, který odeslala pozůstalým po zemřelém X. V tomto dopise jim nabídla pomoc při uplatnění jejich nároků na náhradu škody vůči pojišťovně za účasti specializované advokátní kanceláře, přičemž v textu dopisu jednak použila adresu dotčených osob a dále v něm uvedla informaci o úmrtí pana X při dopravní nehodě.

Podle zákona o ochraně osobních údajů za účelem nabízení služeb subjektu údajů lze použít pro tento účel jméno, příjmení a adresu subjektu údajů, pokud jsou tyto údaje získány z veřejného seznamu nebo v souvislosti se svou činností jakožto zpracovatele. Zpracovatelka však do zmíněného dopisu s nabídkou pomoci k adrese subjektů údajů přiřadila další osobní údaj, který se jich týká, spočívající v informaci o úmrtí člena jejich rodiny pana X při dopravní nehodě v červnu 2007, což by mohla učinit pouze se souhlasem subjektů údajů. Tedy nerespektovala povinnost stanovenou poslední větou § 5 odst. 5 zákona o ochraně osobních údajů. Zároveň tak jednala v rozporu s ustanovením § 5 odst. 2 tohoto zákona, podle kterého může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat, pokud je splněna některá z podmínek uvedených pod písm. a) až g) tohoto ustanovení. Žádná z těchto podmínek ovšem v předmětném případě splněna nebyla.

Kontrolou bylo prokázáno, že uvedeným jednáním zprostředkovatelky došlo k porušení zákona o ochraně osobních údajů v jeho § 5 odst. 2 a odst. 5.

Na základě výše uvedeného se zpracovatel dopustil jiného správního deliktu, za což mu byla udělena pokuta ve správním řízení.

Shromažďování finančních prostředků pro nadace a nadační fondy

I.

Nadační fond se obrátil na před šesti lety zemřelého otce stěžovatele D. s žádostí o finanční příspěvek. Stejný postup napadla u Nadace stěžovatelka M. P.; oslovenou byla její matka, která zemřela před více než sedmi lety. Stěžovatel O. H. měl opakovaně písemně požádat Nadaci o vymazání své adresy z její databáze, Nadace mu však dále zasílá žádosti o finanční pomoc. Stěžovatelka A. V. požádala Nadaci o sdělení, jakým způsobem zjistila její adresu. Obdržela odpověď, se kterou nebyla spokojená, neboť jí nebyl sdělen zdroj osobních údajů a bylo naznačováno předchozí profilování.

Nadační fond nedostál povinnosti podle ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů tím, že zpracoval osobní údaje osob oslovovaných s žádostí o finanční příspěvek shromážděné a oprávněně zveřejněné pro jiné účely v letech 2001 a 2004, aniž učinil jakýkoli krok k zjištění jejich aktuálnosti. Nadační fond dále porušil povinnost podle ustanovení § 12 odst. 1 a 2 tím, že ve třech případech neposkytl subjektu údajů na jeho písemnou žádost informace o zpracování, nebo poskytl informace neúplné, ačkoliv úplné, přesné a pravdivé informace měl ke dni podání zprávy k dispozici. Ve dvou případech přitom nesprávně posoudil žádost subjektu údajů.

II.

V souvislosti se správním řízením vedeným na základě podnětu doručeného Úřadu, odbor správních činností konstatoval, že ke zpracování osobních údajů v souvislosti se zasíláním žádostí o poskytnutí daru nelze využít právní úpravu obsaženou v § 5 odst. 5 až 10 zákona o ochraně osobních údajů, neboť zjevně nejde o nabízení obchodu nebo služeb, ale o žádost o finanční příspěvek. Pokud zpracovávané údaje byly získány z telefonního seznamu, jde o údaje oprávněně zveřejněné, které lze podle § 5 odst. 2 písm. d) zákona o ochraně osobních údajů zpracovávat bez souhlasu subjektu údajů, přičemž však nesmí být dotčeno právo na ochranu soukromého a osobního života subjektu údajů. Přitom má správní orgán za to, že vyslovením nesouhlasu s dalším zasíláním informačních letáků účastníkem řízení dá osoba, jíž byla taková žádost zaslána, najevo, že tento postup účastníka řízení považuje za zásah do svého soukromého a osobního života. Vyslovením nesouhlasu tedy zaniká právní titul pro zpracování osobních údajů a správce je povinen provést jejich likvidaci. Rozhodnutí ve věci nabylo právní moci.

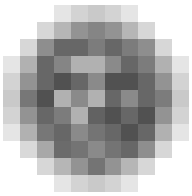
Informování členů sdružení o zpracování osobních údajů

Také v roce 2008 obdržel Úřad důvodné stížnosti na postup právnických osob vzniklých a rozvíjejících činnost podle zákona č. 83/1990 Sb., o sdružování občanů, při zpracování osobních údajů svých členů. Pravomocně byly ukončeny čtyři kontroly; všechny byly zahájeny na základě stížnosti podané dotčeným subjektem údajů. Stížnosti směřovaly proti dvěma samosprávným sdružením sportovních klubů a oddílů, které jsou shodně sdruženy v Českém svazu tělesné výchovy a dvěma subjektům sdruženým v zájmovém svazu, činném v oboru upraveným zvláštním zákonem.

Jeden stěžovatel je rozhodčím sportovního svazu a jeho osobní údaje byly bez souhlasu subjektu údajů zveřejněny v otevřeném internetu na oficiální webové vývěsce svazu; seznam rozhodčích bylo možno číst i tisknout. Podle tvrzení dalšího stěžovatele nebylo přes jeho opakované písemné stížnosti na zpracování osobních údajů, nakládání s jeho osobními údaji uspokojivě vysvětleno. Další stěžovatel napadl používání rodných čísel bez souhlasu subjektu údajů; z podání vyplynulo podezření na porušení dalších povinností.

Kontrolou bylo u jednoho sdružení zjištěno porušení povinnosti získat souhlas subjektu údajů podle § 5 odst. 2 zákona o ochraně osobních údajů, u tří pak porušení povinnosti získat tento souhlas jako informovaný a prokazatelný podle ustanovení § 5 odst. 4. U tří kontrolovaných svazů bylo shledáno porušení povinnosti podle ustanovení § 11 odst. 1 a 2 tohoto zákona. Povinnost byla použita s ohledem na skutečnost, že jedním ze zpracovávaných osobních údajů je rodné číslo, které může být ve všech případech shodně sdružením zpracováno v rozsahu a pro účely popsané v kontrolním protokolu pouze se souhlasem nositele – dotčeného subjektu údajů. Kontrolou nebylo ani v jednom případě zjištěno, že by informace podle ustanovení § 11 odst. 1 věty druhé byly součástí některého z vnitřních předpisů sdružení nebo dokumentu určeného nebo dostupného členům sdružení a zájemcům o členství. Rovněž dokument prokazující poskytování informací o právech podle ustanovení § 21 zákona o ochraně osobních údajů a poučení o dobrovolnosti / obligatornosti poskytnutí osobních údajů nebyl zjištěn.

U jednoho z kontrolovaných bylo konstatováno porušení povinnosti podle § 21 odst. 1 a 2 zákona o ochraně osobních údajů, spočívající v tom, že na dotaz stěžovatele, který je třeba považovat za žádost podle ustanovení § 21 odst. 1 písm. a) tohoto zákona, poskytl jako subjekt odpovědný za zpracování rodných čísel členů svazu subjektu údajů vysvětlení, které je v rozporu s věcně příslušnými předpisy, jež stanoví povinnost zpracovávat rodná čísla pouze se souhlasem nositele rodného čísla nebo jeho zákonného zástupce. U téhož sdružení bylo zjištěno rovněž porušení povinnosti podle § 10 zákona o ochraně osobních údajů.



Dozorová a správní činnost

PŘIJÍMÁNÍ PODNĚTŮ A STÍŽNOSTÍ, POSKYTOVÁNÍ KONZULTACÍ

Telefonické dotazy občanů jsou primárně v obecné rovině vyřizovány zřízeným samostatným pracovištěm odboru pro styk s veřejností, což uvolnilo časový prostor pro pracovníky provádějící právní posuzování obsahu písemných podnětů a stížností na porušování povinností uložených zákonem o ochraně osobních údajů. Teprve ve složitějších případech telefonických dotazů a žádostí následuje odpověď referenta specializovaného na příslušnou oblast, písemná odpověď nebo osobní konzultace.

Z 68 osobních konzultací poskytnutých odborem v letošním roce ústředním orgánům státní správy, veřejné správy i soukromému sektoru lze jen pro ilustraci uvést tyto subjekty: Ministerstva obrany, vnitra, spravedlnosti, průmyslu a obchodu, dopravy, školství, mládeže a tělovýchovy, zdravotnictví, Úřad vlády, Český telekomunikační úřad, Telefónica O2, Český báňský úřad, Pražské teplárny, Letiště Praha, Řízení letového provozu Praha, Škoda auto, ČSAD SVT Praha, Antidopingový výbor ČR. Na základě žádosti o konzultaci zpravidla následovalo posouzení a vyjádření Úřadu k předloženým projektům, z nichž k nejrozsáhlejším patřily: Elektronické zpracování osobních údajů účastníků akcí, které budou v ČR pořádány v souvislosti s jejím předsednictvím v Radě Evropské unie, bezpečnost silničního provozu a hloubková analýza dopravních nehod, souhrnná analýza rizik a potřeb odsouzených osob pro účely podmíněného propuštění, zpracovávání osobních údajů v rámci Středočeské integrované dopravy. Úřad rovněž poskytl konzultaci Antidopingovému výboru ČR, který chce poskytovat informace celosvětové databázi ADAMS.

Přes nárůst počtu obdržených dotazů v odboru (odpovězeno na 1 778 oproti 1 674 v roce 2007) se podařilo udržet průměrnou dobu vyřízení podnětu či žádosti na cca 10 pracovních dnech. Nutno podotknout, že ve sledovaném období se zvyšovala i kvalifikovanost dotazů směřujících často i ke složitějším otázkám, např. předávání osobních údajů do zahraničí, včetně států stojících mimo Evropskou unii.

Podnětů k zahájení řízení z moci úřední bylo vyřízeno celkem 697, což je v porovnání s 574 podněty v roce 2007 nárůst o 21%. Prakticky celý nárůst se promítl do počtu podání odložených jako nedůvodných, přičemž bylo podrobně, často opakovaně, stěžovatelům vysvětlováno a zdůvodňováno, proč Úřad neshledal důvody k uplatnění svých dozorových kompetencí. Celkově tedy bylo odloženo jako nedůvodných 64% podání. Ostatní způsoby řešení věci byly na procentuální úrovni obdobné jako v roce 2007. Úřad se znovu zabýval anonymními podáními, která však i nadále důsledně vyřizuje podle závažnosti jejich obsahu, zejména pokud se došlý anonymní podnět vyhodnotí jako podnět vyvolávající důvodné podezření, že nesprávný postup správce nebo zpracovatele osobních údajů je způsobilý zasáhnout velký počet subjektů údajů a řešení zjištěného závadného stavu je tedy ve významném veřejném zájmu nebo jde o významnou skupinu citlivých osobních údajů. Také tyto podněty jsou předávány k prověření inspektorem Úřadu.

Statistika stížností vyřízených odborem pro styk s veřejností

Celkem..... 697....., z toho:

- předáno ke kontrole 202
- předáno na zahájení řízení 37
- postoupeno příslušným orgánům 12
- odloženo s vyrozuměním 446

Nejfrekventovanějšími problémy, respektive předměty zájmu občanů v postavení subjektů údajů, byly i v roce 2008 kamerové systémy, zpracovávání citlivých osobních údajů ve zdravotnictví, evidence vedené orgány veřejné správy a samosprávy a zavádění různých typů čipových karet zejména v dopravě. Vzhledem k tomuto enormnímu zájmu jsou těmto problematikám věnovány samostatné pasáže výroční zprávy týkající se kontrolní činnosti.

Nejúčinnější metodou je systémové řešení zjištěných nedostatků s příslušnými věcně odpovědnými státními i soukromými subjekty. Úřad se proto důsledně věnoval jednání s ministerstvy spravedlnosti, zdravotnictví, financí a vnitra, Asociací bytových družstev, Asociací hotelů a restaurací ČR, Dopravním podnikem hlavního města Prahy a rovněž s Kanceláří veřejného ochránce práv, který je pro Úřad významným partnerem v oblasti ochrany základních lidských práv. Úřad se aktivně účastnil konference na téma „Komplexní bezpečnost" pořádané společností F. S. C. Bezpečnostní poradenství, a. s., na mezinárodním veletrhu ISET 2008.

I v roce 2008 pokračoval Úřad ve svém úsilí přimět příslušné orgány k přijetí opatření měnících stávající právní stav, kdy povinnost uvádění osobních údajů ve veřejně dostupných seznamech je sice v souladu se zvláštní právní úpravou, ale podle názoru Úřadu již nikoli v souladu s obecnými principy ochrany osobních údajů. Z iniciativy Úřadu byla navázána spolupráce s Ministerstvem spravedlnosti a expertní meziresortní skupina připravující novelu obchodního zákoníku by měla zjednat nápravu současného právního stavu.

K množícím se případům zpracovávání biometrických údajů k identifikaci nebo autentizaci subjektů údajů v pracovněprávních vztazích, zejména v souvislosti s provozem elektronických docházkových systémů, připravuje Úřad nové a poměrně restriktivní stanovisko, které bude v nejbližší době zveřejněno na jeho webových stránkách.

VEDENÍ REGISTRU POVOLENÝCH ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ

Registr je veden na základě ustanovení § 16 a násl. zákona o ochraně osobních údajů. Registr ale kromě jiného poskytuje orientaci, v jaké oblasti společenského zájmu právě probíhá rozvoj zpracování osobních údajů a signalizuje tak, kam bude třeba v budoucnu zaměřit svou dozorovou činnost.

Veřejnost je o registrovaných zpracováních informována veřejně přístupným registrem umístěném na webových stránkách Úřadu a umožňujícím vzdálený přístup.

Mezi veřejností však stále přetrvává mylný výklad registračního procesu, pokud jde o jeho smysl a zařazení v rámci dozorové činnosti Úřadu. Na registrační proces, který je upraven § 16 zákona, a je procesem sui generis, se podle § 16 odst. 5 zákona o ochraně osobních údajů nepoužije zákon č. 500/2004 Sb., správní řád. Registrační řízení je zahájeno doručením registračního podání, které je hodnoceno z hlediska náležitostí stanovených zákonem. Neobsahuje-li oznámení některou z náležitostí, je oznamovateli zaslána podle § 16 odst. 4 zákona o ochraně osobních údajů výzva s upozorněním na nedostatečné, nebo chybějící informace a je stanovena lhůta k doplnění oznámení. Pokud není lhůta oznamovatelem splněna, po-

hlíží se na oznámení, jako by nebylo podáno. Následně dochází k uvážení v intencích, zda z oznámení vzniká důvodná obava z porušení zákona a je tedy na místě zahájit se správcem správní řízení podle § 17 zákona o ochraně osobních údajů, nebo zda tato důvodná obava není a zpracování osobních údajů je možno zaregistrovat.

Výše popsané uvážení se pak zakládá na informacích, které správce v rámci jím dodané dokumentace poskytne. Je tedy na odpovědnosti správce, aby tvrzené odpovídalo skutečnému stavu věcí. Navíc je nutno dodat, že Úřad posuzuje v této fázi taková zpracování, která ve skutečnosti ještě neprobíhají, resp. by ještě neměla probíhat (praxe je ovšem jiná a Úřadu jsou oznamována často i zpracování, která jsou již v běhu a správce se snaží o jejich dodatečnou legalizaci).

Nedílnou součástí činnosti registru je vydávání rozhodnutí o zrušení registrace podle § 17a odst. 2 zákona. V letošním roce bylo takto zrušeno celkem 90 zpracování na žádost správce, nejčastěji z důvodů zániku společnosti, či sloučení společnosti, zrušení podnikatelské činnosti, nebo ukončení zpracování osobních údajů. Informace o zrušených registracích Úřad zveřejňuje ve Věstníku.

Registrační oznámení, které nevykazuje znaky závadnosti, je zapsáno do registru. Správce může zahájit zpracování ve chvíli, kdy je jeho zpracování do registru zapsáno, o čemž se může dozvědět nahlédnutím do veřejného registru, který je dostupný na webových stránkách Úřadu. V případě nečinnosti Úřadu se po uplynutí lhůty 30 dnů od doručení má za to, že zpracování bylo zaregistrováno. Pouze na základě žádosti vydá Úřad správci osvědčení o registraci, které obsahuje datum vyhotovení, číslo jednací, jméno, příjmení a podpis osoby, která osvědčení vydala, otisk úředního razítka, identifikační údaje správce a účel zpracování.

Registrační řízení podle § 16 zákona se v roce 2008 uplatňovalo zejména ve vztahu ke zpracováním, která oznamovala Úřadu úmysl správců zpracovávat osobní údaje prostřednictvím kamerového systému. Na základě upozornění formou dopisu či v rámci ústního jednání, vyvolaného výhradně na žádost správce, že dané zpracování by mohlo být v rozporu se zákonem, došlo v mnoha případech ze strany správců ke korekci původního záměru a oznámené zpracování bylo uvedeno do souladu se zákonem. Registrační řízení je tedy třeba vnímat i jako určitou službu a pomoc správcům, kteří si často dostatečně neuvědomují rizika spojená se zpracováním zejména citlivých údajů, či se zpracováním údajů prostřednictvím kamerových systémů. Správce může být včasnou registrací upozorněn na zásadní problémy spojené se zamýšleným zpracováním a může tak předejít nezákonnému postupu při zpracování osobních údajů i při možné pokutě za přestupek či jiný správní delikt. V roce 2008 proběhlo takových řízení 749, což je cca 23% z celkového počtu přijatých oznámení.

V roce 2008 se opakovaně potvrdila efektivnost podávání oznámení prostřednictvím elektronického formuláře a webových stránek Úřadu.

Mnoho oznamovatelů se staví do role správce, ač jím ve skutečnosti není. Často až v rámci registračního řízení dojde k vyjasnění a konstatování, že v daném případě jde o zpracování osobních údajů zpracovatelem, na kterého se oznamovací povinnost nevztahuje.

Stále také dochází k situacím, kdy jsou na Úřad podávána registrační oznámení, na která se oznamovací povinnost nevztahuje vzhledem ke skutečnosti, že taková zpracování splňují podmínku pro výjimku z oznamovací povinnosti podle § 18 zákona o ochraně osobních údajů (nejčastěji jde o zpracování z oblasti sociální péče, zdravotnictví, zaměstnaneckých údajů, činnosti územně samosprávných celků, občanských sdružení a další). Značnou část těchto oznámení zaslaly v roce 2008 personální agentury, které v souvislosti se zprostředkováním zaměstnání či brigády zpracovávají osobní údaje zájemců o práci. Zvláštním zákonem, který v těchto

případech předpokládá zpracování osobních údajů, je zákon č. 435/2004 Sb., o zaměstnanosti, konkrétně § 17. V této souvislosti byly zaznamenány také případy, kdy činnost personálních agentur byla vykonávána v rozporu s platnou legislativou, jelikož jim ke zprostředkování zaměstnání nebylo v souladu s § 6 odst. 1 písm. k) zákona č. 435/2004 Sb., o zaměstnanosti, uděleno povolení od Ministerstva práce a sociálních věcí České republiky.

Velmi často jsou Úřadu oznamována zpracování za účelem uzavření smluvního vztahu se zákazníkem, plnění povinností vyplývajících z uzavření pracovní smlouvy, ze smluv uzavřených s obchodními partnery, zákazníky, klienty, zprostředkování prodeje nemovitostí, nájmů, pronájmů apod. Taková a jim podobná zpracování mají povětšinou oporu v zákoně č. 40/1964 Sb., občanský zákoník, či zákoně č. 513/1991 Sb., obchodní zákoník, a na taková zpracování je tedy nutno nahlížet jako na zpracování, která jsou vykonávána v rámci zvláštními právními předpisy upravené činnosti, jak předpokládá § 18 odst. 2 písm. b) zákona o ochraně osobních údajů.

V případě, že Úřad dospěje na základě informací poskytnutých správcem v průběhu registračního řízení k závěru, že se na dané zpracování oznamovací povinnost nevztahuje, je o této skutečnosti oznamovatel informován dopisem s upozorněním, že takové zpracování do registru zapsáno nebylo a s odůvodněním tohoto postupu.

Podobně jako v roce 2007 došlo také v průběhu roku 2008 k nárůstu podaných registračních oznámení.

Nejčastějším typem zpracování, která se v roce 2008 objevovala, byla bezkonkurenčně zpracování prostřednictvím kamerového systému, v porovnání s loňským rokem jde o více než dvojnásobný nárůst (podrobněji o kamerovém sledování ve zvláštní kapitole věnované kontrole). Kromě kamerových systémů se registrace nejčastěji prováděla zejména v oblasti marketingu, internetového obchodu a reklamní činnosti. Marketingová a reklamní činnost byla od počátku roku zaznamenána celkem u 139 subjektů. Jde o subjekty, které z různých důvodů vytvářejí rozsáhlé databáze lidí. Mezi nejčastější důvody vytváření těchto databází patří vedení agendy žadatelů o práci (hostesek, utajených zákazníků, promotérů, tazatelů apod.) a reklamní a marketingové důvody (provádění nejrůznějších soutěží a průzkumů).

Rozsah zpracovávaných údajů se liší v závislosti na účelu zpracování. Z oznámení vyplývá, že údaje nejsou dále nikomu poskytovány, a že slouží pouze pro potřeby společnosti. Zpracování se děje vždy se souhlasem subjektu údajů. Úřad zaznamenal i několik zpracování v oblasti zdravotnictví, především zpracování, jejichž účelem bylo vedení lékových a lékařských karet, nebo zpracování spojené s vědeckovýzkumným bádáním v oblastech medicíny (podrobnosti viz kap. o zdravotnictví).

V roce 2008 výrazným způsobem vzrostl počet oznámení o zpracování osobních údajů, jejichž předmětem byla vůle subjektů registrovat se za účelem provozování internetových obchodů. Jelikož některá z podaných oznámení neobsahovala dostatečné informace k posouzení zpracování, bylo nutno zahájit registrační řízení podle § 16 zákona o ochraně osobních údajů, v jehož rámci byly zjištěny podrobnosti fungování internetových obchodů, především způsob nakládání s osobními údaji subjektů. Registrační řízení bylo ve všech případech ukončeno zápisem do registru. V zásadě jde o tři základní koncepce fungování internetového obchodu, resp. zpracování.

Prvý okruh zpracování je charakterizován bezprostředním provozováním obchodu samotným podnikatelem, tj. osobou, která provozuje webovou stránku, resp. obchod. Tato osoba sama obstarává prodávané zboží, poskytuje zákaznický servis a shromažďuje nebo jiným způsobem zpracovává osobní údaje subjektů, které si u ní objednávají nějaké zboží nebo službu, případně osob, které se v rámci tohoto jejího obchodu registrují.

Druhá skupina zpracování je založena na principu „obchodních cestujících“. Síť zainteresovaných osob je napojena na „matku“. K této matce přímo směřují všechny osobní údaje a objednávky, které zákazníci obchodu učiní, tj. veškeré údaje, které zákazníci zadají do registračních formulářů apod. Tato „matka“ rovněž vede databáze zákazníků a jejich osobních údajů. Na „matku“ jsou pak napojeny další osoby, které jí pomáhají obchod za úplatu provozovat. Tyto osoby pracují doma na svém počítači, kam jim „matka“ zasílá osobní údaje subjektů, které učinily objednávku.

Třetí skupina zpracování spojuje fakticky obě předchozí možnosti. V tomto případě jde o napojenou osobu, která do rámce softwaru pro provozování internetového obchodu, který jí je poskytnut „matkou“, zakomponuje software pro provozování vlastního obchodu. Základním problémem spjatým se zpracováním v rámci internetového obchodu, jak vyplynulo z registračních řízení, je řádné plnění povinností uložených § 11 a 13 zákona o ochraně osobních údajů.

Ve třetím čtvrtletí roku 2008 se začala množit oznámení o zpracování osobních údajů a dotazy, jejichž předmětem byl tzv. whistleblowing. Tento anglický novotvar, jež je vytvořen ze slovního spojení whistle blower, což doslovně znamená oznamovatel, informátor nebo udavač, bývá uživateli v českém jazyce překládán jako oznamování, případně jako oznamovací systém. Jen v krátkosti je na místě zmínit, že jde o systém zavedený společnostmi, které buďto přímo pocházejí, nebo jsou podílově vlastněny a ovládány společnostmi se sídlem v USA. Zavedení tohoto oznamovacího systému je povinností uloženou americkým zákonem SOX (tj. Sarbanes-Oxley Act), která se jejich prostřednictvím prosazuje i v rámci EU.

Doposud získané zkušenosti vypovídají o tom, že v rámci tohoto systému dochází primárně ke zpracování a následnému předávání osobních údajů do USA, jelikož na území jiného státu se dosud nenacházejí společnosti, které by v tomto směru poskytovaly společnostem, jež zavedly tento systém, potřebný servis. Nutným funkčním prvkem systému je totiž účast nezávislého a nezaujatého subjektu, který bude vyšetřovat oznámení podaná zaměstnanci, jež budou mířit na vyšší příčky vedení společnosti. V rámci fungování systému pak dochází ke zpracování osobních údajů dvou skupin subjektů, tj. oznamovatele, který k takovému zpracování svým podáním fakticky uděluje souhlas, a oznamovaného, tj. osoby, která je nahlášena jako osoba, která se dopustila škodlivého jednání. Z dosud došlých dotazů a oznámení o zpracování osobních údajů lze usuzovat na to, že společnosti si jsou vědomy existence pracovního dokumentu WP 117 a pokud nejsou, pak instinktivně nastavují své systémy v souladu s ním. Jediným problémem v tomto směru se jeví občasné neujasnění si role správce/zpracovatele, případně jakým způsobem zde plynou toky dat.

PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Povolovací agenda pro posuzování předávání osobních údajů do jiných států podle § 27 zákona o ochraně osobních údajů se opírá o právní principy EU. V poslední době Úřad zaznamenal zvýšený nárůst požadavků posouzení tzv. pravidel Binding Corporate Rules (BCR), které by měly vytvořit základní a nezbytný právní rámec pro předávání osobních údajů v oblasti, kde působí více subjektů, ale se stejnými zájmy nebo kde jeden subjekt působí na území několika států, ať už členů EU nebo nečlenů, a je jeho zájmem přenos osobních údajů vykonávat podle obecných pravidel posouzených a schválených v rámci EU jedním úřadem, zpravidla tím, který vykonává svou působnost ve stejné zemi, kde má takový žadatel o povolení soustředěnu převážnou nebo významnou část své činnosti – očekávaného zpracování osobních údajů.

Žádosti právnických osob se v roce 2008 týkaly, podobně jako v minulých letech, zejména předávání osobních údajů zaměstnanců, popř. uchazečů o zaměstnání, mateřským společnostem v zahraničí, zvláště pak ve Spojených státech amerických. Jako důvody byly nejčastěji uváděny činnosti související s vedením společné personální politiky, plánováním personálního rozvoje zaměstnanců, efektivnějším využíváním pracovních sil zaměstnanců a plánováním dalšího vzdělávání zaměstnanců.

Do států Evropské unie v roce 2008 předávalo 148 registrovaných správců.

Předání osobních údajů do všech ostatních států může dále probíhat v režimu § 27 odst. 2 nebo 3 zákona o ochraně osobních údajů. Dle ustanovení § 27 odst. 2 tohoto zákona mohou být do třetích zemí předány osobní údaje, pokud zákaz omezování volného pohybu osobních údajů vyplývá z mezinárodní smlouvy, k jejíž ratifikaci dal Parlament ČR souhlas a kterou je Česká republika vázána. Jde zejména o ty státy, které ratifikovaly Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat (Rada Evropy, ETS 108, 1981) a Dodatkový protokol, a jejichž právní předpisy by tedy měly zaručovat dostatečnou ochranu osobních údajů odpovídající všem požadavkům směrnice Evropského parlamentu a Rady 95/46/ES. Úmluva pak přímo v čl. 12(2) zavazuje nezakazovat a nepodrobovat zvláštnímu povolení tok dat na území druhé smluvní strany. V současné době se kromě států EU jedná o Andorru, Albánii, Bosnu a Hercegovinu, Černou Horu, Gruzii, Chorvatsko, Island, Lichtenštejnsko, Makedonii, Moldávii, Norsko, Srbsko a Švýcarsko. Prakticky je ovšem situace taková, že Rada Evropy nemá efektivní nástroj nebo mechanismus pro vyhodnocování legislativy přistupujících států.

Podle § 27 odst. 2 zákona o ochraně osobních údajů mohou být také do třetích zemí předány osobní údaje na základě rozhodnutí orgánu Evropské unie. V současnosti jde především o rozhodnutí Komise, která může na základě čl. 25 odst. 6 směrnice, a to postupem podle čl. 31 odst. 2 směrnice, konstatovat, že třetí země zajišťuje odpovídající úroveň ochrany na základě svých národních předpisů, nebo svých mezinárodních závazků (např. rozhodnutí Komise o standardních smluvních doložkách, viz níže). Také v případě předání osobních údajů, na které se vztahuje § 27 odst. 2 zákona o ochraně osobních údajů, není nutné žádat Úřad o povolení.

Z registračních oznámení, podaných v souladu s § 16 zákona v roce 2008 vyplývá, že předání osobních údajů do států, které ratifikovaly Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat (Rada Evropy, ETS 108, 1981) nebo předání, které probíhá na základě některého z rozhodnutí Komise, uskutečnilo 103 (62+41) správců.

Předání osobních údajů do třetích zemí v režimu § 27 odst. 3 zákona o ochraně osobních údajů lze uskutečnit za předpokladu, že na daný případ nelze aplikovat § 27 odst. 1 nebo 2 citovaného zákona a že správce (exportér dat) Úřadu prokáže, že plní některou z podmínek stanovených v § 27 odst. 3 tohoto zákona, uvedené pod písm. a) až g). Na základě předložené žádosti pak Úřad zahájí správní řízení, jehož výsledkem je vydání rozhodnutí o povolení/nepovolení předání osobních údajů do jiných zemí. Toto rozhodnutí bývá vydáno na dobu určitou, zpravidla na 2 – 3 roky.

V roce 2008 byla nejčastěji plněna podmínka, uvedená pod písm. a) výše zmíněného ustanovení, tzn., že šlo o předání osobních údajů se souhlasem nebo na základě pokynu subjektu údajů. K souhlasu je třeba poznamenat, že se jím v souladu s § 4 písm. n) zákona o ochraně osobních údajů rozumí svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním jeho osobních údajů. Poměrně často byla plněna také podmínka uvedená pod písm. e). V těchto případech tedy šlo o předání osobních údajů, které bylo nezbytné pro jednání o uzavření nebo o změně smlouvy, uskutečněné z podnětu subjektu údajů,

nebo pro plnění smlouvy, jejíž smluvní stranou byl subjekt údajů. Tuto podmínku plnili především ti správci, kteří působí jako pojišťovny, cestovní agentury či realitní kanceláře.

V jednom případě také správce (exportér dat) úspěšně prokázal Úřadu, že bude splněna podmínka, uvedená pod písm. b). Šlo tedy o předání do země (USA), ve které byly vytvořeny dostatečné zvláštní záruky ochrany osobních údajů, a to na základě profesních předpisů a bezpečnostních opatření. V tomto případě se jednalo o takové profesní předpisy, které se vztahovaly ke zpracování osobních údajů zákazníků, dodavatelů, konzultantů nebo jiných obchodních partnerů a zaměstnanců. Profesní předpisy splňovaly základní kritéria a zásady pro zpracování a předávání osobních údajů do třetích zemí srovnatelné s BCR (závazná podniková pravidla, viz výše). V těchto dokumentech nazvaných kodexy chování bylo srozumitelným a podrobným způsobem popsáno fungování zabezpečení ochrany osobních údajů v rámci korporace. Kodexy chování byly rovněž schváleny příslušným zmocněncem pro ochranu osobních údajů v Berlíně, úřadu pro ochranu osobních údajů Spolkové republiky Německo, jako adekvátní ochrana umožňující předávání osobních údajů ze Spolkové republiky Německo do USA.

K tomuto případu lze dodat, že původně šlo o učiněné oznámení provedené v souladu s § 16 zákona o ochraně osobních údajů. Až na základě podkladů a skutečností předložených na základě výzvy k doplnění podaného oznámení učinění podle § 16 odst. 4 zákona, dospěl správní orgán k závěru, že ze strany správce došlo k mylnému výkladu zákona a posouzení dané situace. Učiněné podání, formálně označené za „oznámení o zpracování osobních údajů podle § 16“ vykazovalo materiální znaky žádosti o povolení předání.

Standardní smluvní doložky

Jednou z možností, jak lze zajistit ochranu a legálnost zpracování a přenosu osobních údajů do třetích zemí, je použití standardních smluvních doložek. Exportér osobních údajů uzavře s příjemcem osobních údajů ve třetí zemi smlouvu o předávání osobních údajů, jejíž nedílnou součástí budou smluvní doložky podle rozhodnutí Komise Exportér údajů v EU a dovozce údajů v třetí zemi se může rozhodnout, který ze souborů smluvních doložek si zvolí. Podle článku 1 rozhodnutí jsou standardní smluvní doložky uvedené v příloze považovány za dostatečná ochranná opatření s ohledem na ochranu soukromí a základních práv a svobod jednotlivců, jakož i s ohledem na výkon odpovídajících práv v souladu s čl. 26 odst. 2 směrnice. Správci údajů mohou volit mezi soubory I a II v příloze. Nesmějí však měnit doložky, ani kombinovat jednotlivé doložky či soubory.

Standardní smluvní doložky se v soukromém sektoru u nás poměrně dobře rozšířily a jsou používány jako vítaný nástroj, umožňující předávat osobní údaje do třetích zemí, které nezajišťují odpovídající úroveň ochrany osobních údajů. Na druhé straně, protože v těchto případech není nutné žádat o povolení, nemá Úřad příliš povědomí o tom, jak jsou rozhodnutí Komise o standardních smluvních doložkách v praxi aplikována. Jinými slovy, zda v konkrétním případě skutečně jde ze strany exportéra o používání vzorových doložek a zda jsou v nich zohledněny základní principy ochrany dat. Na rozdíl od jiných členských států, které požadují, aby jim byly doložky předkládány k posouzení. V současné době Úřad eviduje 77 subjektů, které deklarovaly, že předávání osobních údajů do třetích zemí bude uskutečněno na základě smlouvy, jejíž součástí budou standardní smluvní doložky podle rozhodnutí Komise.

Úřad v letošním roce posuzoval případ předložení smluvních doložek, které správce považoval za tzv. standardní, podle rozhodnutí Komise. Na základě jejich posouzení však bylo nutné konstatovat, že smluvní doložky v podobě, ve které byly

Úřadu předloženy, nebylo možné považovat za dostatečný nástroj k tomu, aby mohly být na jejich základě předávány osobní údaje zaměstnanců/klientů do třetích států. Jedním z hlavních důvodů byla absence odpovědnosti exportéra a dovozce údajů vůči subjektům údajů za porušení svých smluvních povinností a právo subjektu údajů vynucovat jako oprávněná třetí strana tuto doložku proti dovozci nebo exportérovi údajů, pokud tito poruší své smluvní povinnosti v souvislosti s jeho osobními údaji. Dále byly např. nedostatečným způsobem popsány účely zpracování a nebyla zdůvodněna nutnost předávat i citlivé osobní údaje o subjektech údajů atd. Závěrem tedy bylo nutné konstatovat, že předložené smluvní doložky neposkytují dostatečné záruky ochrany osobních údajů pro předání osobních údajů do třetích zemí ve smyslu čl. 26(2) směrnice a § 27 odst. 3 písm. b) zákona.

Safe Harbour (dále jen SH)

Na některé z žádostí, které se týkaly předávání osobních údajů do USA, bylo možno v souladu s ustanovením § 27 odst. 2 zákona aplikovat Rozhodnutí Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu" a s tím souvisejících „často kladených otázek" vydaných Ministerstvem obchodu Spojených států amerických – případy SH. V tomto případě lze odpovídající úrovně ochrany osobních údajů při jejich předání do USA podle výše zmíněného rozhodnutí dosáhnout v tom případě, pokud by příjemce osobních údajů v USA dodržoval zásady „bezpečného přístavu" pro ochranu osobních údajů a také zásady „často kladených otázek" (Frequently Asked Questions, dále jen „FAQ"), které představují pokyny pro provádění těchto zásad vydaných vládou Spojených států amerických dne 21. července 2000. Při každém předání údajů musejí být splněny dvě zásadní podmínky: Subjekt, který přijímá údaje se jednoznačně a veřejně zavázal dodržovat zásady prováděné v souladu s FAQ a současně tento subjekt podléhá zákonným pravomocím orgánu veřejné správy Spojených států amerických (Federální obchodní komise nebo Ministerstvo dopravy Spojených států amerických), který je oprávněn vyšetřovat stížnosti v případě nedodržení zásad prováděných v souladu s FAQ a poskytnout nápravu proti nekalým nebo klamavým praktikám, jakož i náhradu škody fyzickým osobám, bez ohledu na zemi, bydliště, nebo na jejich státní příslušnost.

Počet správců, jenž využívá tento institut pro předávání osobních údajů do USA, se v posledním roce značně zvýšil. Většinou se tohoto institutu využívá pro předávání v souvislosti se zaměstnaneckými vztahy. Bohužel i v tomto případě platí, co již bylo řečeno o standardních smluvních doložkách, tedy že Úřad nemá dostatečné povědomí o tom, jakým způsobem a zda dostatečným z pohledu zákona a směrnice, tento institut v praxi skutečně funguje. V této souvislosti stojí za zmínku studie, která byla vypracována na základě požadavku Evropské komise, navazující na obdobnou studii z roku 2004, která měla za úkol zhodnotit dosavadní provádění principů SH. Z obsáhlé zprávy vyplývá, že úroveň ochrany osobních údajů poskytované SH ve srovnání s rokem 2004 se nezlepšila, spíše naopak. Především bylo konstatováno, že společnosti, které se přihlásily k dodržování principů SH, mají velké problémy s tím, aby tyto principy v modifikované a životaschopné podobě začlenily do svých interních předpisů, týkajících se ochrany osobních údajů (privacy policy). Nedostatečná a neurčitá je rovněž informovanost o účelech zpracování a rozsahu zpracovávaných osobních údajů. V neposlední řadě je to i nedostatečný nebo nepřehledný přístup k této „privacy policy" pro samotné subjekty údajů, které tak nemají možnost, a pokud ano, tak velmi omezenou, domáhat se v případě potřeby svých práv, např. podáním stížnosti formou dotazníku. Vesměs negativní zprávu o stavu SH je nutno vnímat jako alarmující i z toho důvodu, že počet subjektů v USA,

které se přihlásily k dodržování principů SH od roku 2004 několikanásobně vzrostl a jak již bylo řečeno, i v České republice dochází ve stále větší míře k předávání osobních údajů do USA na základě SH.

Závazná podniková pravidla (Binding Corporate Rules, dále jen BCR)

Za poslední rok se Úřad setkal s několika případy BCR, které mu byly předloženy k posouzení. Ve všech případech se jednalo o posuzování BCR, jejichž vedoucím dozorovým úřadem (dále jen „DPA“) byl DPA z jiné země EU. Doposud ani v jednom případě nebyl Úřad osloven, aby se stal vedoucím DPA.

Úřad se při svém posuzování BCR snaží k těmto přistupovat vždy spíše z koncepčního a principielního hlediska, tj. zaměřuje se na vnitřní logiku BCR a obsahové stránce se věnuje zejména v tom směru, že zjišťuje, zda jsou v BCR obsaženy všechny nezbytné principy a prvky, které by měly mít. V odpovědi pak vždy zdůrazňuje, že toto posuzování je pouze předběžné a že v případě zájmu o předávání osobních údajů na jejich základě z ČR do třetích zemí bude třeba požádat Úřad o povolení dle § 27 odst. 4 zákona. V odpovědi je pak dále upozorňováno zejména na fakt, že z důvodů národních diferencí v různých oblastech právních úprav, zejména v oblasti pracovněprávní, bude třeba BCR odpovídajícím způsobem přizpůsobit národní legislativě, což by bylo případně možné učinit i s pomocí Úřadu po podání žádosti podle § 27 odst. 4 zákona. S tímto úzce souvisejí zkušenosti, které byly načerpány ze zaslaných připomínek některých z ostatních DPA, z nichž vyplývá, že jednotlivé DPA přistupují k posuzování BCR s různou mírou abstrakce a zaměřují se na různé oblasti. Některé DPA se v rámci tohoto snaží fakticky o harmonizaci BCR s jejich národní legislativou, některé oproti tomu posuzování provádí z principielního hlediska. Taková praxe vede k tomu, že ve svém úhrnu dojde vedoucímu DPA od dotčených DPA velké množství nesourodých připomínek, které je třeba vypořádat a začlenit do BCR, což je mnohdy téměř nemožný úkol.

Rovněž je třeba zmínit, že během uplynulého roku byla v rámci EU iniciována široká debata nad procesem schvalování a přijímání BCR, která se zaměřila zejména na urychlení procesu tvorby BCR. Jejím výstupem pak byla deklarace o vzájemném uznávání BCR, jejímž předmětem je prohlášení, že dozorový úřad bude respektovat rozhodnutí vedoucího dozorového úřadu, který se s danou společností podílí na vytvoření BCR, o tom, že dané BCR jsou adekvátním prostředkem pro garanci ochrany osobních údajů předávaných do třetích zemí. Zde je třeba zmínit, že tato deklarace nemění nic na pravomoci každého státu, podmínit předávání osobních údajů do třetích zemí ještě například obdobou povolení, jak je nastaveno v rámci § 27 odst. 4 zákona o ochraně osobních údajů, což se jeví jako vůbec nejlepší řešení, jestliže je v zájmu DPA, aby byla již fakticky předběžně schválená BCR přizpůsobena národní legislativě a aby tak bylo možno, zcela v souladu s celým právním řádem, předávat osobní údaje na jejich základě do třetích zemí ze země příslušného DPA.

VÝKON SPRÁVNÍCH ČINNOSTÍ ÚŘADU

Správní řízení jsou vedena jednak inspektory Úřadu, jednak odborem správních činností.

Agenda odboru správních činností se vztahuje nejen k řízením podle zákona o ochraně osobních údajů, ale také ke všem řízením, která Úřad vede podle zvláštních zákonů. Sem patří zejména zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel) a zákona č. 159/2006 Sb., o střetu zájmů. Dále vede odbor správních činností řízení podle § 17 zákona o ochraně osobních údajů v případech důvodných obav o zákonnosti

Úřadu oznámených zpracování. V rámci činností odboru dochází také k metodickému sjednocování postupů Úřadu v oblasti působnosti správního řádu.

Výkon pravomoci Úřadu v oblasti správního trestání lze členit jednak podle zákonů, které Úřadu pravomoc projednávat správní delikty (přestupky a jiné správní delikty právnických osob a fyzických osob podnikajících) svěřují, ale například i podle toho, kdo je autorem podnětu, který Úřad k projednání obdrží. V oblasti přestupkových řízení vedených pro podezření z porušení zákona o ochraně osobních údajů je v 60% případů zdrojem podnětu Policie České republiky, resp. jiné orgány veřejné správy a samosprávy (přestupkové komise), zbylé případy jsou projednávány na základě informací od soukromých osob (většinou fyzických), které se obrátí na Úřad se svým podnětem přímo. V případě projednávání jiných správních deliktů podle zákona o ochraně osobních údajů a zákona o evidenci obyvatel jsou pak autorem podnětů orgány veřejné zprávy pouze z 20%, 35% připadá na podněty, které jsou výsledkem kontrolních zjištění inspektorů Úřadu, a největší část (45%) na podněty od soukromých osob.

Obsahem podnětů zaslaných Úřadu Policií České republiky je přitom nejčastěji podezření z porušení § 13 zákona o ochraně osobních údajů, tj. nedostatečné zabezpečení zpracovávaných údajů proti jejich neoprávněnému zpracování, ať už tím, že jsou listiny (v lepším případě smluvní dokumentace, v horším případě i třeba dokumentace zdravotnická) nalezeny u kontejnerů, ve sběrných dvorech či pohozené v lese. V těchto případech tedy jde o aktivní postup osob, které listiny na takovém místě ponechají, ať už jsou to jednotliví zaměstnanci nebo samy osoby za zpracování odpovědné z pozice správce či zpracovatele. Druhou skupinu případů tvoří nedbalostní jednání uvedených osob, které ponechají listiny obsahující osobní údaje např. v neuzamčeném vozidle, ze kterého jsou posléze odcizeny.

K tomu je nutno zdůraznit, že splnění povinnosti přijmout dostatečná opatření směřující k tomu, aby osobní údaje nebyly vystaveny riziku neoprávněného zpracování či využití, předpokládá, že odpovědná osoba důsledně zváží veškerá rizika, která jsou s jí prováděným zpracováním osobních údajů spojená, a přijme odpovídající opatření k jejich vyloučení. K naplnění skutkové podstaty správního deliktu porušením povinnosti podle § 13 odst. 1 zákona o ochraně osobních údajů přitom postačí pouze vznik stavu, kdy jsou osobní údaje určitým způsobem ohroženy, přestože doposud nedošlo nebo ani nedojde k jejich neoprávněnému zpracování. Tato povinnost je spojena s objektivní odpovědností za její porušení; tedy pouze v případě, že správce příp. zpracovatel prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil, nebude za případný správní delikt odpovědný (viz § 46 odst. 1 zákona o ochraně osobních údajů).

Uložené sankce

Výsledky řízení, která byla zahájena přímo na základě podnětů doručených Úřadu, neboť příslušný útvar (odbor pro styk s veřejností) došel k závěru, že vše z předložených dokladů a tvrzení nasvědčuje tomu, že nezákonné jednání už bylo ukončeno a současně závadný stav nelze kontrolou napravit, a ve kterých byla uložena vysoká sankce, jsou uvedeny níže. Případy, kde byly uloženy vysoké sankce, ale zjištění, že byl porušen zákon o ochraně osobních údajů, bylo výsledkem provedené kontroly, jsou uvedeny v jiných částech této zprávy.

Z výše uvedených řízení byla pravomocně ukončena následující:

Pokuta ve výši 100 000 Kč byla v letošním roce uložena státnímu podniku, který nezajistil, aby nahrávka telefonní hovoru jeho operátora s panem I. K., která byla následně odvysílána v rádiích a je volně přístupná prostřednictvím internetu, nebyla zpřístupněna neoprávněným osobám a dále o pořízení této nahrávky pana

I. K. nijak neinformoval. Tímto svým jednáním porušil povinnost stanovenou v § 13 odst. 1 zákona o ochraně osobních údajů, tedy povinnost správce 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. Dále porušil povinnost stanovenou v § 11 odst. 1 tohoto zákona, tedy povinnost správce při shromažďování osobních údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, o právu subjektu údajů přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona o ochraně osobních údajů.

K předmětu správního řízení lze konstatovat, že státní podnik tím, že pořizuje nahrávky telefonických hovorů na svoji tísňovou linku, zpracovává osobní údaje volajících (v případě, kdy jsou identifikovatelní, viz dále) ve smyslu § 4 písm. e) zákona o ochraně osobních údajů, neboť systematicky uchovává, a případně dále využívá osobní údaje. Osobním údajem je v souladu s ustanovením § 4 písm. a) zákona o ochraně osobních údajů jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, v daném případě jsou tedy osobními údaji veškeré informace, které o sobě v telefonním hovoru pan I. K. sdělil. Současně je přitom nepochybné, že tyto informace se vztahovaly k určitelnému subjektu údajů, neboť o sobě sdělil natolik konkrétní informace, které ve spojení s datem a časem pořízení nahrávky umožňovaly jeho identifikaci, tedy byl z nich určitelný. Současně byl na základě sdělených informací a ve spojení se svým specifickým hlasem určitelný i pro další osoby, které jej osobně znají.

Ačkoliv § 13 odst. 1 zákona o ochraně osobních údajů nestanovuje konkrétní bezpečnostní opatření, která je správce povinen přijmout, je vodítko uvedeno v § 13 odst. 3 tohoto zákona a v případě automatizovaného zpracování jsou poté povinnosti správce, případně zpracovatele upřesněny v § 13 odst. 4. Podle těchto ustanovení správce v rámci bezpečnostních opatření posuzuje kromě jiného také rizika týkající se plnění pokynů pro zpracování osobních údajů osobami (v naprosté většině případů zaměstnanci správce nebo zpracovatele), které mají bezprostřední přístup k osobním údajům (je zde tedy riziko lidského selhání), čemuž odpovídá současně v případě automatizovaného zpracování povinnost správce dle § 13 odst. 4 písm. b) a c) zákona o ochraně osobních údajů zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, a povinnost pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány.

V popisovaném případě se nepodařilo určit, jakým způsobem došlo ke zpřístupnění předmětných osobních údajů; z vyjádření státního podniku vyplývá, že ani on sám není schopen určit, jakým způsobem ke zpřístupnění osobních údajů došlo. Pokud státní podnik argumentoval lidským selháním, přičemž nebyl schopen sám toto lidské selhání následně odhalit a současně neměl přijata taková opatření, aby riziko lidského selhání minimalizoval, nelze konstatovat, že by vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil.

Na okraj lze uvést, že by bylo možné za naplnění liberační podmínky považovat takovou situaci, kdy by státní podnik „logoval“ každý přístup k jednotlivým zpracovávaným osobním údajům, tj. k nahrávkám (tzn. že by zaznamenával, který zaměstnanec, kdy a případně i za jakým účelem s každou jednotlivou nahrávkou pracoval), a současně by v přiměřených časových intervalech na základě těchto záznamů prováděl nahodilou kontrolu toho, zda ze strany zaměstnanců šlo o oprávněný a důvodný přístup k nahrávce, tedy o oprávněné zpracování osobních údajů.

Pouze takováto opatření by zajistila bezpečnost zpracovávaných osobních údajů a ve vztahu k možnému lidskému selhání zaměstnance by měla dostatečný preventivní účinek.

K podezření ze spáchání správního deliktu porušením povinnosti dle § 5 odst. 2 zákona o ochraně osobních údajů, které bylo v dané věci také prověřováno, lze uvést, že ze spisové dokumentace vyplývá, že záznam hovoru byl pořízen na tísňové lince. Nahrávání telefonických rozhovorů z linek tohoto (krizového) charakteru lze podřadit pod ustanovení § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, kdy pro pozdější řešení krizových situací, stejně jako pro zabránění zneužití těchto linek, je zpracování osobních údajů formou nahrávky nezbytné a současně nepředstavuje zásah do soukromého a osobního života subjektu údajů. V daném případě bylo tedy možné pořídit nahrávku předmětného telefonického rozhovoru pana I. K. bez jeho souhlasu.

Jedna z nejvyšších pokut v roce 2008 byla uložena společnosti, která v souvislosti s poskytováním půjček, zveřejnila na svých webových stránkách údaje 52 dlužníků v rozsahu jméno, příjmení, adresa bydliště a rodné číslo. Tímto svým jednáním porušila povinnost stanovenou v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tedy povinnost zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, za což jí byla uložena pokuta ve výši 52 000 Kč.

Poskytovatel půjček v tomto případě shromažďoval a zpracovával osobní údaje pro účely poskytování půjček fyzickým a právnickým osobám. Nedisponoval však souhlasem těchto osob – subjektů údajů ke zveřejnění jejich osobních údajů na internetu, kterým došlo k jejich zpřístupnění širokému okruhu osob. Zveřejnění osobních údajů dlužníků je přitom nutno považovat za nátlakové jednání, kterým jsou porušována i další ustanovení článku 10 Listiny základních práv a svobod. Zveřejňování osobních údajů v souvislosti se vznikem pohledávek je nepřípustným zasahováním do soukromí osob, neboť zpřístupněním takového údaje, který byl získán na základě soukromoprávního vztahu, může dojít jak k poškození dobrého jména takové osoby v mnoha dalších vztazích, a to jak soukromoprávních, tak i veřejnoprávních, ale i k narušení základních principů ochrany soukromí této osoby. Protože proti rozhodnutí správního orgánu prvního stupně byl rozklad podán opožděně, byl předsedou Úřadu zamítnut a rozhodnutí nabylo právní moci.

Další sankce byla Úřadem uložena společnosti, která v souvislosti s prováděním veřejných dražeb zveřejnila nejméně ve dvou případech přílohu dražební vyhlášky obsahující seznam zaměstnanců navrhovatele předmětu dražby s osobními údaji v rozsahu příjmení, jméno, datum narození, datum začátku pracovního poměru, výši mzdového tarifu, % prémií a celkovou částku mzdy, a to bez souhlasu dotčených zaměstnanců. Tímto jednáním došlo k porušení povinnosti stanovené v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tedy ke zpracování osobních údajů nikoliv pouze v souladu s účelem, k němuž byly shromážděny, za což byla společnosti uložena pokuta ve výši 25 000 Kč. Rozhodnutí správního orgánu prvního stupně bylo napadeno rozkladem, který byl předsedou Úřadu zamítnut, a rozhodnutí tak nabylo právní moci.

K postupu této společnosti lze konstatovat, že problematika veřejných dražeb a tedy i dražebních vyhlášek je upravena zákonem č. 26/2000 Sb., o veřejných dražbách. Podle ustanovení § 20 odst. 1 uvedeného zákona dražebník vyhlásí konání dražby dražební vyhláškou, v níž uvede mj. označení a popis předmětu dražby a jeho příslušenství, práv a závazků na předmětu dražby váznoucích a s ním spojených, pokud podstatným způsobem ovlivňují hodnotu předmětu dražby. V souladu s požadavkem § 11 téhož zákona musejí být osoby a věci označovány způsobem vylučujícím jejich záměnu.

K věci lze dále uvést, že údaje o fyzické osobě v rozsahu jméno, příjmení, její identifikace jako zaměstnance a údaj o mzdě a odměně za práci, jsou nepochybně

osobní údaje. Vzhledem k tomu, že účastník řízení je jejich správcem, je povinen podle § 5 odst. 1 písm. f) zákona o ochraně osobních údajů zpracovávat tyto osobní údaje pouze v souladu s primárním účelem, k němuž byly shromážděny, a pokud zpracovává jejich osobní údaje k jinému účelu, než ukládají zvláštní zákony, pak je k takovému zpracování nutný souhlas subjektu údajů.

Osobní údaje zaměstnanců navrhovatele dražby, které byly shromážděny bez podmínky existence souhlasu, musejí sloužit pro zpracování výstupů v oblasti mzdové, daňové, důchodového, nemocenského a zdravotního pojištění. Za účelem provedení veřejné dražby tedy nelze zveřejnit osobní údaje zaměstnanců navrhovatele dražby, ale jen anonymizované údaje, které by z hlediska potencionálního zájemce o účast v dražbě a o eventuelní vydražení podniku mohly mít vliv na jeho posouzení předmětu dražby. Totéž platí, pokud jde o přesnou výši platu, mzdy a odměny zaměstnance. Finanční částka, kterou zaměstnanec při výplatě obdrží, je osobním údajem, jehož zveřejnění je třeba plně podřídit režimu zákona o ochraně osobních údajů. Vzhledem k tomu, že se na zveřejnění těchto údajů nevztahuje žádná z výjimek podle § 5 odst. 2 písm. a) až f) zákona o ochraně osobních údajů, může společnost provádějící dražbu zveřejnit výši platu, mzdy nebo odměny pouze se souhlasem zaměstnance. Může však bez souhlasu jednotlivých zaměstnanců zveřejnit např. informaci o celkové výši mzdových prostředků vyplacených v podniku nebo jeho úseku. Pokud z této informace není určitelné, jaké konkrétní částky byly vyplaceny jednotlivým pracovníkům, není tento údaj údajem osobním. Taková informace o celkové výši mzdových prostředků vyplácených navrhovatelem dražby zaměstnancům je nepochybně pro informaci a potřeby potencionálního zájemce o účast v dražbě a o eventuelní vydražení podniku postačující.

Řízení podle § 17 zákona o ochraně osobních údajů

Řízení podle § 17 zákona o ochraně osobních údajů navazuje na postup při plnění oznamovací povinnosti podle § 16 tohoto zákona. V případech, kdy ani výzva k doplnění oznámení nevede k tomu, aby byly odstraněny pochyby o zákonnosti oznámeného zpracování, předává odpovědný útvar (samostatné oddělení registrační) spis k provedení správního řízení odboru správních činností. Toto řízení je vedeno snahou odstranit důvodnou obavu, že by při zpracování mohlo dojít k porušení zákona, a to přesto, že by ze zákonné dikce vyplývalo, že by Úřad mohl v případě nezákonností rozhodnout o nepovolení zpracování. Za tím účelem je především vedeno ústní jednání, kde jsou správci vysvětleny jeho povinnosti při zpracování osobních údajů a podmínky, za nichž lze zpracování provádět. V průběhu celého správního řízení může správce parametry oznámeného zpracování volně měnit. Právě takové změny jsou většinou důvodem toho, že odpadá důvodná obava z nezákonnosti zpracování, řízení je posléze zastaveno a oznámené zpracování je (ve změněné podobě) zapsáno do registru zpracování.

Úřad posuzuje v řízení podle § 17 odst. 2 zákona o ochraně osobních údajů oznámené zpracování osobních údajů pouze jako celek. O oznámeném zpracování osobních údajů může být ve správním řízení vedeném podle § 17 zákona o ochraně osobních údajů rozhodnuto tak, že pokud Úřad zjistí, že oznámeným zpracováním neporušuje správce osobních údajů podmínky stanovené zákonem o ochraně osobních údajů, řízení zastaví (nebo, v případě, že oznámené zpracování stanovené podmínky nesplňuje) je rozhodnuto o nepovolení zpracování osobních údajů, což je v souladu se stanovenou koncepcí registrace podle § 16 zákona o ochraně osobních údajů založené na evidenčním principu. Výrok rozhodnutí tak nelze rozdělit na část povolující a část nepovolující. Správní orgán proto musí např. v případě oznámeného zpracování osobních údajů prostřednictvím kamerových systémů posuzovat zpracování osobních údajů komplexně, nikoli u každé kamery zvlášť.

Obecně lze výsledky tohoto typu správních řízení shrnout tak, že cca 80% vedených řízení je zastaveno, neboť odpadla důvodná obava z porušení podmínek stanovených zákonem, 10% zpracování je nepovoleno a zbývajících 10% řízení je zastaveno z procesních důvodů, jako je to, že oznámení o zpracování bylo účastníkem řízení vzato zpět apod.

Počet provedených řízení:

Správní trestání (řízení vedená odborem správních činností)
– správních řízení o porušení zákona č. 101 a č. 133 ---------- 54
– přestupkových řízení o porušení zákona č. 101 a č. 133 ---------- 8
– přestupkových řízení o porušení zákona o střetu zájmů ---------- 0

Řízení podle § 17
z toho
– zastaveno (správce neporušuje podmínky stanovené zákonem) ---- 78
– zastaveno z procesních důvodů (např. oznámení bylo vzato zpět, nebo nedochází ke zpracování osobních údajů) ---------- 9
– nepovoleno ---------- 12

VÝKON PŘEZKUMNÝCH PRÁVNÍCH AGEND

Činnost Úřadu v oblasti přezkumu správních rozhodnutí je soustředěna v odboru právní podpory a schengenské spolupráce (OPS), který vznikl v roce 2008 sloučením odboru právní podpory a odboru schengenské spolupráce a III. pilíře. OPS se podílí především na rozhodování v druhé instanci ve všech případech, kdy je proti právnímu aktu Úřadu podán opravný prostředek, o němž má rozhodovat předseda Úřadu. Konkrétně se jedná o rozhodování o rozkladech podaných proti rozhodnutí o uložení sankce za porušení zákona, jehož dozorem je Úřad pověřen (popř. rozhodnutí podle § 17 zákona o ochraně osobních údajů), anebo rozhodování o námitkách podaných proti kontrolnímu protokolu inspektora Úřadu. OPS v těchto případech připravuje podklady pro jednání rozkladové komise předsedy Úřadu, resp. kolegia inspektorů, a následně také konečné rozhodnutí ve věci. Kromě této činnosti se odbor podílí na formulaci názorů Úřadu, ať již formou reakcí na konkrétní žádosti anebo zobecněním zkušeností Úřadu v podobě publikovaných stanovisek. Další agendou OPS je příprava materiálů vyžádaných soudy po podání žaloby proti rozhodnutí Úřadu.

Zcela samostatnou kapitolou je plnění úkolů vyplývajících Úřadu z pozice orgánu pověřeného dozorem nad ochranou osobních údajů v oblasti schengenské spolupráce, tedy zejména zpracováním dat v národní části Schengenského informačního systému (SIS). Jmenovaný odbor v této souvislosti jednak zajišťuje účast Úřadu na jednání společného dozorového orgánu pověřeného kontrolou centrální části SIS a sjednocením přístupu národních úřadů a jednak se podílí na výkonu kontroly zpracování osobních údajů příslušnými orgány v České republice. Obdobnou činnost vykonává OPS i v související oblasti zpracování osobních údajů v systému Eurodac či v Celním informačním systému.

Vzhledem k tomu, že vybrané oblasti činnosti Úřadu v roce 2008 jsou pojednány na jiném místě této zprávy, bude se tato část věnovat spíše některým specifickým, spíše procesním otázkám, se kterými se OPS setkal v rámci rozhodování v druhé instanci, ať již o rozkladech či o námitkách. Dále budou zmíněny poznatky o problematice žalob podaných proti rozhodnutí Úřadu.

Přehled o počtech případů, které OPS v roce 2008 řešil, ať již v rámci rozhodování v druhém stupni ve správním anebo kontrolním řízení, a také o počtech žalob podaných proti rozhodnutí Úřadu, poskytují v závěru připojené přehledové tabulky.

Správní řízení druhého stupně

V roce 2008 se konalo 16 jednání rozkladové komise (včetně 1x „per rollam“)
– projednáno bylo 36 věcí
– celkem podaných rozkladů: 33 (z toho 4x – §17)
– pravomocných rozhodnutí: 21

V roce 2008 se konalo 12 jednání námitkového kolegia
– projednáno bylo 21 věcí
– celkem podaných námitek proti KP: 25
– pravomocných rozhodnutí: 20 (včetně námitek proti likvidaci)

Soudní řízení vedená na základě žaloby proti rozhodnutí Úřadu

Celkem soudních řízení v roce 2008: 13

Rok	Celkem žalob	v řízení MS v Praze	v řízení NSS / kasační stížnost	Ústavní soud	Ukončené žaloby	Neukončené žaloby
2001	1	–	–	–	1	0
2002	2	–	–	–	2	0
2003	1	–	–	–	1	0
2004	3	–	–	–	3	0
2005	8	2	3	–	3	5
2006	7	4	2	–	1	6
2007	12	9	1	–	2	10
2008	13	12	–	–	1	12

Z přezkumné rozhodovací a dozorové činnosti

Úřad se opakovaně setkává s otázkou účastenství stěžovatelů (tj. osob, které podaly Úřadu podnět týkající se porušení zákona o ochraně osobních údajů, popř. jiného Úřadem dozorovaného právního předpisu) ve správním řízení, které je na základě tohoto podnětu zahájeno.

S ohledem na skutečnost, že Úřad žádné z řízení, které vede, nezahajuje na návrh, ale pouze z moci úřední (ex offo), je případná stížnost pouze podnětem, na jehož základě Úřad uplatňuje svoji pravomoc podle § 29 zákona o ochraně osobních údajů, tedy provést kontrolu předmětného zpracování, anebo zahájit správní řízení o pokutě. Autor podnětu, stěžovatel, se však nestává účastníkem tohoto řízení. Uvedené vyplývá z § 27 správního řádu, kde je stanoveno, že účastníky řízení z moci úřední jsou ty osoby, kterých se výsledné rozhodnutí dotkne v tom smyslu, že jim tímto rozhodnutím bude založeno, změněno nebo zrušeno určité právo či povinnost, případně bude prohlášeno, že toto právo nebo povinnost mají anebo nemají. Účastníky jsou také další osoby, pokud mohou být rozhodnutím přímo dotčeny ve svých právech nebo povinnostech, a také osoby, o kterých to stanoví zvláštní zákon. Jsou-li pochybnosti o tom, zda konkrétní osoba je či není účastníkem řízení, považuje se tato osoba podle § 28 správního řádu za účastníka do té doby, dokud se neprokáže opak. O tom, zda tato osoba je či není účastníkem, vydává Úřad usnesení, proti němuž se lze odvolat (podat rozklad) k předsedovi Úřadu.

Z uvedeného je zjevné, že stěžovatel, jemuž z rozhodnutí o uložení či neuložení pokuty subjektu, na jehož činnost si stěžoval, žádná práva či povinnosti nevyplývají, nemůže být účastníkem těchto řízení. Jak kontrolní, tak i správní řízení je vedeno se správci nebo zpracovateli osobních údajů, předmětem tohoto řízení je dodržování povinností správce nebo zpracovatele podle zákona o ochraně osobních údajů či jiného zákona, za jejichž dodržování je odpovědný. Naopak stěžovatel žádné povinnosti ani odpovědnost z titulu postavení správce či zpracovatele osobních údajů nemá, nehrozí mu zásah do jeho práv, ani sankce, a proto výsledek vedeného řízení nemůže ovlivnit jeho postavení. Podmínky ustanovení § 27 a 28 správního řádu tak nejsou naplněny.

K otázce soudního přezkumu

Obdobně jako podání řádného opravného prostředku proti právním aktům Úřadu (tj. námitek proti kontrolnímu protokolu a rozkladu proti rozhodnutí ve správním řízení) není v praxi Úřadu ničím výjimečným, naopak opravný prostředek je využíván ve velkém počtu případů, je také institut žaloby ke správnímu soudu využíván stále častěji. Pro ilustraci lze uvést, že v roce 2008 bylo podáno 11 žalob proti rozhodnutí nebo kontrolnímu protokolu Úřadu, což je sice počet podobný roku 2007, ale dvojnásobný ve srovnání s roky 2005 a 2006. A stejně tak, jako i v jiných oblastech činnosti Úřadu, jedná se o stále komplikovanější otázky výkladu a aplikace právních norem, na jejichž zodpovězení nečeká pouze žalobce (nejčastěji správce nebo zpracovatel osobních údajů, kterému byla rozhodnutím Úřadu uložena pokuta), ale také Úřad sám, neboť v některých případech může mít rozhodnutí soudu výrazný dopad na praxi Úřadu.

Smutnou realitou situace v justici však je, že naprostá většina žalob dosud podaných proti rozhodnutí Úřadu leží neprojednána u Městského soudu v Praze, který je příslušným správním soudem k projednání žalob směřujících proti Úřadu. Důsledkem tohoto stavu je, že Úřad (zcela oprávněně) pokračuje i ve věcech typově odpovídajících žalovanému případu ve své dosavadní praxi, a v otázkách, kde by nestranný výrok soudu byl pro budoucí postup Úřadu potřebný, se nemůže spolehnout na reakci v horizontu, v němž bude řešení dané otázky ještě aktuální.

V roce 2008 byl pravomocně ukončen pouze jeden spor, byť z hlediska Úřadu poměrně významný, v němž soud přisvědčil názoru Úřadu na využívání rodných čísel exekutory (blíže viz příslušná úvodní kapitola týkající se kontroly).

Úřad však například čeká na rozhodnutí ve věci, kdy uložil pokutu za zveřejnění osobních údajů nájemníků bytů v souvislosti s problematikou tzv. regulovaného nájemného, kdy byly na internetu zpřístupněny poměrně komplexní a rozsáhlé informace o jednotlivých osobách (v rozsahu příjmení, jméno, adresa bydliště, funkce, politická příslušnost, rodné číslo, informace o nemovitém majetku skládající se z přehledů vlastnictví a výpisů z katastru nemovitostí, ve kterých byly uvedeny také osobní údaje spoluvlastníků nemovitostí nebo jiných osob oprávněných z práv, která se zapisují do katastru nemovitostí). V tomto případě se jedná o nejstarší dosud neukončený případ, kdy byla žaloba podána v dubnu roku 2005 a věc nyní (poté, co byl Nejvyšším správním soudem zrušen rozsudek prvního stupně a věc byla vrácena k novému projednání) opět čeká na projednání u Městského soudu v Praze.

Dále není rozhodnuto o žalobě směřující proti rozhodnutí o uložení pokuty za přestupek spočívající ve zveřejnění zápisů z jednání a usnesení rady města týkajících se provozu domova důchodců, včetně osobních údajů v těchto zápisech uvedených, (často vypovídajících o umístění konkrétních osob v domě s pečovatelskou službou, současně s hodnocením sociálních a majetkových poměrů žadatelů) na webových stránkách. V této věci byla současně, v rámci podané žaloby, vznesena závažná otázka konfliktu práva na přístup k informacím o činnosti veřejné správy a práva na ochranu soukromí a osobních údajů těch, o nichž orgány veřejné správy rozhodují.

Jinou, nepochybně zajímavou kauzou, je případ, kdy Úřad sankcionoval advokáty za zveřejnění osobních údajů dlužníka jejich klienta, které zpracovávali v souvislosti s poskytováním právních služeb klientovi – tj. vymáhání pohledávek, když toto zveřejnění již překročilo účel, k němuž byly osobní údaje shromážděny a dále zpracovávány. Tento případ je významný i tím, že se zde jedná o aplikaci zákona o ochranu osobních údajů na činnost advokátů obecně.

V neposlední řadě je pro Úřad podstatné, jak bude posouzena žaloba směřující proti jeho rozhodnutí o pokutě uložené ministerstvu (resp. České republice zastupované příslušným ministerstvem) v souvislosti se zpracováním osobních údajů bezpečnostním sborem spadajícím do jeho působnosti. V tomto případě jde zejména o pasivní legitimaci ministerstva být účastníkem řízení o správním deliktu, k němuž nedošlo jednáním ministerstva, ale jiného správce osobních údajů, který však nedisponuje vlastní právní subjektivitou, a za jehož činnost nese dle názoru Úřadu deliktní odpovědnost právě ministerstvo (jiný subjekt nelze za porušení zákona v tomto případě potrestat).

VYŘIZOVÁNÍ STÍŽNOSTÍ PODLE § 175 SPRÁVNÍHO ŘÁDU A SOUVISEJÍCÍCH PODÁNÍ

I v roce 2008 Úřad řešil stížnosti směřující proti jeho postupu nebo proti nevhodnému chování úředních osob, jejichž použití upravuje § 175 správního řádu. V roce 2008 Úřad vyřídil třicet šest stížností, z nichž pouze dvě směřovaly proti nevhodnému chování úřední osoby, zatímco ostatní se týkaly možného nesprávného postupu Úřadu. Počet stížností dle § 175 správního řádu v porovnání s předchozím rokem značně narostl (téměř na dvojnásobek). Poměr stížností proti nesprávnému postupu Úřadu, které byly po prošetření shledány důvodnými, je naproti tomu obdobný tomu z loňského roku.

Stížnosti proti postupu Úřadu často, ve čtrnácti vyřízených případech, napadaly postup při vyřízení předchozího podnětu stěžovatele příslušným útvarem Úřadu, tedy odborem pro styk s veřejností.

Z devíti stížností směřujících proti postupu odboru pro styk s veřejností při vyřízení předchozího podnětu byly čtyři po prošetření posouzeny jako bezdůvodné, tři jako částečně důvodné a dvě jako důvodné. Pochybení při vyhodnocení předchozího podnětu byla v zásadě dvou druhů – hmotněprávní a procesní.

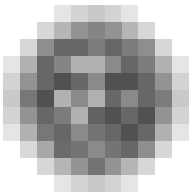
Nesprávný úřední postup spočívající v chybné aplikaci předpisů hmotného práva byl zjištěn např. v otázce samotné aplikace zákona o ochraně osobních údajů, kdy byla odborem pro styk s veřejností v několika případech příliš extenzivně vyložena ustanovení vylučující působnost zákona. V těchto situacích bylo důsledkem přešetření stížnosti postoupení příslušného podnětu ke kontrole nebo k zahájení správního řízení.

V některých případech byl rovněž zjištěn nesprávný úřední postup spočívající v tom, že stěžovatel byl sice řádně informován o tom, že na jím popisovaný případ se nevztahují kompetence Úřadu, ale jiného orgánu veřejné správy, ale jeho podnět již nebyl v rozporu se zásadou spolupráce orgánů veřejné správy dále postoupen. Opatřením přijatým k nápravě tohoto pochybení pak bylo postoupení podnětu příslušnému orgánu.

Úřad rovněž řešil několik stížností, jimiž stěžovatelé napadali postup či závěry inspektorů Úřadu. V této oblasti Úřad řešil např. stížnost na to, že inspektor neumožnil stěžovateli, autorovi podnětu, na jehož základě Úřad zahájil řízení z moci úřední, nahlédnout do příslušného kontrolního spisu. Tato stížnost byla posouzena jako bezdůvodná, protože stěžovatel nebyl účastníkem kontrolního řízení a k nahlédnutí do kontrolního spisu tedy neexistoval právní titul.

Další stížnosti směřovaly proti délce probíhající kontroly. K tomu lze obecně uvést, že ani zákon o ochraně osobních údajů, ani zákon o státní kontrole, které upravují kontrolní proces, pro provedení kontroly nestanoví žádné lhůty. Je tomu tak především proto, aby mohl být ve všech případech naplněn účel kontroly, jímž je zjištění skutečného stavu a jeho doložení příslušnými podklady. Uvedené sice neznamená, že kontrola může probíhat po neomezenou dobu, vylučuje však např. použití obecné lhůty správního řádu v délce třiceti dnů k vyřízení podnětu, na kterou se někteří stěžovatelé odvolávali.

Institut stížnosti podle § 175 správního řádu slouží k ochraně práv dotčených osob, jestliže jim právní předpisy nenabízejí jiné možnosti ochrany. Přestože většina stížností, které Úřad obdržel a řešil, byla shledána bezdůvodnými, opačné případy posloužily jak k nápravě dílčích pochybení, tak i ke komplexnějšímu řešení přístupů Úřadu.



Legislativní činnost

Rok 2008 lze považovat za jedno z významnějších období příprav návrhů klíčových právních předpisů, v rámci jejichž připomínkování také Úřad sděloval své náměty a doporučení, a to jak na základě zkušenosti z dozorové praxe, tak v komparaci s evropskými předpisy. Bezesporu největší připravovanou změnou v právním řádu České republiky byly pokračující práce na přípravě nového kodexu občanského práva a práce na nových elektronických registrech veřejné správy.

V případě **elektronizace státní správy** a zavádění služeb e-governmentu je zřejmé, že se jedná nejen o složitý technický, ale v širší míře společenský problém. Ten nekončí přípravou právních předpisů a nasazením počítačových aplikací, ale je u něj nutno již alespoň souběžně s legislativním procesem řešit osvětu i zvyšovat uživatelskou erudici občanů i úředníků. Přístup Úřadu v této věci byl často vnímán jako zpomalující faktor, neboť Úřad trval na projednání zamýšlených technických záměrů a zhodnocení rizik souvisejících s ochranou a zabezpečením osobních údajů.

V systému klíčovém pro nejbližší dobu v e-governmentu v ČR – systému datových schránek, byla na základě připomínky Úřadu podstatně redukována doba uchovávání údajů v této nové evidenci. Úřad dále zpochybňoval s existencí datových schránek do určité míry související návrh nového elektronického identifikátoru občanů – osobního čísla. Tento identifikátor byl totiž navržen v dosti nejasné podobě s o to jasnějším záměrem, aby byl do budoucna využíván pro další účely podle jiných zákonů (návrh byl později podstatně zúžen pouze na číslo datové schránky). Z hlediska zásad pro řádné zpracování osobních údajů je významné také to, že elektronická komunikace a pořízení datové schránky budou pro občana zajištěny v okamžiku, kdy to bude skutečně potřebné (a nikoliv povinně, resp. od narození, jak bylo původně navrhováno).

Příprava nových elektronických (základních) státních registrů nebyla po stránce legislativní koncem roku 2008 uzavřena. K této problematice se Úřad snažil přispět především konzultační činností, s důrazem na shrnutí zahraničních zkušeností a na význam funkce bezpečných elektronických identifikátorů navzájem odlišných pro jednotlivé agendy (jde o jeden z principů e-governmentu). Úřad přitom poukazoval na nevýhody v současné době nejednotně zabezpečených, propojených a z pohledu ochrany údajů také více zneužitelných stávajících státních registrů. Úřad předpokládá, že obecné povinnosti týkající se ochrany osobních údajů budou platit i v činnostech týkajících se nových elektronických registrů, a tudíž se i na tuto oblast bude vztahovat dozorová činnost Úřadu.

V rámci připomínkování návrhu nového **občanského zákoníku** Úřad kritizoval z pohledu moderního trendu automatizovaného zpracování osobních údajů silně nedostatečnou úpravu pořizování záznamů technickými prostředky. Po vzájemné poradě Ministerstvo spravedlnosti přislíbilo upravit návrh do podoby, která by jasněji vyjádřila podmínky pořizování podobizen a záznamů o jednání lidí, zejména na veřejných prostranstvích a na dalších místech přístupných veřejnosti. V této záležitosti bude možno přihlédnout k výsledkům dvou materiálů týkajících se právní úpravy kamerových systémů, na nichž se Úřad v roce 2008 spolupodílel, připravovaných v rámci poslanecké iniciativy i v rámci výborů Rady vlády pro lidská práva.

Za kladný výsledek považuje Úřad přeformulování návrhu občanského zákoníku v části týkající se identifikace občanů. Tento kodex, který je založen na zásadách přirozeného práva, by měl zdůraznit a svým způsobem shrnout dosavadní pozitivní přístupy, včetně identifikace upravené v resortu justice zejména v procesních předpisech a založené na využívání přirozených identifikačních údajů člověka, jako jsou jméno, příjmení, údaje o narození či adresa bydliště.

S tvorbou výše uvedeného kodexu souvisí i vznik návrhu nového obchodního zákona. Úřad se postavil proti převzetí dosavadní úpravy obchodního rejstříku, kde jsou pravidla zveřejňování osobních údajů stanovena velmi nejasně, navíc podzákonným předpisem. Úřad vítá příslib samostatného zákona o obchodním rejstříku učiněný Ministerstvem spravedlnosti, u něhož bude možno detailně projednat pravidla týkající se zejména elektronického zpracování údajů v rejstříku a jejich zveřejňování na internetu.

V průběhu celého roku budila zájem veřejnosti příprava **zákona o sčítání lidu, domů a bytů** v roce 2011. Zde se ve svých připomínkách Úřad soustředil na to, aby i při nově plánovaném elektronickém sčítání i v rámci práce sčítacích komisařů i při případné spolupráci s externími subjekty byla dána jasná pravidla přístupu k určitým informacím a provedeno zabezpečení dat před zneužitím. Ukázalo se, že velkým problémem byl způsob uchovávání dat po ukončení sčítání, a to v ne zcela anonymizované podobě. Existence tzv. soustavy údajů nejen z plánovaného sčítání, případně doplňovaného z jiných evidencí a bez přesnější úpravy v jiném významném zákonu, zákonu o státní statistické službě, byla v konečné fázi ponechávána k diskusi na úrovni vlády, která navrhovanou úpravu soustavy údajů ze zákona vypustila.

Za dosud společensky podceněnou považuje Úřad problematiku nových předpisů týkajících se **zdravotnických registrů**, u nichž Ministerstvo zdravotnictví ČR neakceptovalo požadavek Úřadu na úplné objasnění koncepce registrů. Úřad požadoval vysvětlení důvodnosti stanovené doby uchovávání údajů v jednotlivých registrech, stejně jako vysvětlení, proč není v případě registrů zohledňován souhlas dotčených osob, tak, jak je tomu v jiných evropských státech. Přitom Úřad doporučoval, aby v zájmu dodržení standardů ochrany velmi citlivých údajů uchovávaných v registrech, byly registry v naznačených otázkách upraveny v zákoně, nikoliv v ministerské vyhlášce či v příloze právního předpisu.

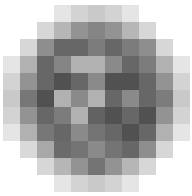
Ve vztahu k zákonu o ochraně osobních údajů vyvolaly některé s Úřadem nekoordinované legislativní přístupy také dotazy dotýkající se dozorové kompetence Úřadu. Kromě obvyklých snah o vyjmutí ze zákonného systému ochrany osobních údajů tím, že se v navrhovaném předpisu stanoví či prostě předpokládá, že v případě určitých informací týkajících se člověka se nejedná o osobní údaje (zde je zjevný rozpor s významově širokou definicí osobního údaje v zákonu o ochraně osobních údajů i v příslušné evropské směrnici) se objevily víceméně neúmyslné případy podřadit dozorovou kompetenci Úřadu některým způsobům prolomení mlčenlivosti podle zvláštních zákonů. Zvláštní úprava v tomto směru je však nadbytečná, neboť oprávnění pracovat s jakkoliv chráněnými osobními údaji, které mají být kontrolovány z hlediska plnění povinností při zpracování osobních údajů, vyplývá v dozorované věci pro příslušné inspektory a kontrolní další pracovníky přímo ze zákona o ochraně osobních údajů. Uvedené je založeno na evropské směrnici, která byla předlohou také při tvorbě kompetenčních a procesních ustanovení zákona o ochraně osobních údajů. Úřad proto přivítal, že eurokonformní výklad potvrdilo také Ministerstvo financí v souvislosti s dozorem Úřadu nad zpracováním osobních údajů podle zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu.

V roce 2008 byla v Parlamentu projednávána iniciativní poslanecká novela (viz sněmovní tisk č. V/171/0) **zákona o střetu zájmů** – z pohledu ochrany osobních údajů velmi problematického. Úřad ve věci novely setrval na svém stanovisku, že navrženou novelu považuje spíše za kosmetickou úpravu, která neřeší podstatné vady zákona o střetu zájmů. Proto se v únoru obrátil na ústavněprávní výbor poslanecké sněmovny Parlamentu a stálou komisi senátu pro ochranu soukromí s žádostí o dopracování tohoto návrhu. K tomu ale nedošlo, neboť senát návrh novely zamítl. V konečném výsledku však novela bez podstatných změn nabyla platnosti a účinnosti jako zákon č. 216/2008 Sb. Je chybou, že zákon o střetu zájmů dostatečně jasně nerozlišuje mezi ústavními, resp. dalšími volenými činiteli, kteří jako veřejné osoby mají často podstatně sníženou míru garance soukromí, a veřejnými úředníky, jejichž ochrana soukromí kromě úřední činnosti musí být v zásadě zachována. Podobu zákona navíc umocňuje způsob zpřístupňování osobních údajů týkajících se majetku a finančních závazků dotčených osob, u něhož není vždy zřejmé, zda a případně jak poslouží k odhalení údajného střetu zájmů. V průběhu legislativních prací Úřad současně podával konzultace týkající se způsobu plnění povinností podle tohoto zákona, a to tak, aby pokud možno nedocházelo k dalším zásahům do soukromí dotčených osob. (Svou konzultační činnost si Úřad nepochybně vysloužil svou působností při udělování pokut podle zákona o střetu zájmů, o tom pojednává jiná část této výroční zprávy.)

Zákon o střetu zájmů, stejně jako jiné právní předpisy často svědčí o nepřipravenosti předkladatelů zákonů zohlednit nové technologie a trendy zpracování osobních údajů, zejména při zpřístupňování a zveřejňování osobních údajů. V souvislosti s návrhem základních registrů Ministerstvo vnitra konečně navrhlo doplnit funkce evidence obyvatel o možnost zprostředkovat lidem za určitých podmínek kontakt na hledanou osobu, tedy o funkci, kterou již Úřad navrhoval doplnit do zákona před lety. Zásadnímu nepochopení často podléhá úprava využití internetu v právních předpisech. Mnohé osoby zodpovědné za zpracování osobních údajů nevědí, že zveřejnění je také formou zpracování osobních údajů podle zákona, kde je nutno zohlednit všechny relevantní zásady ochrany údajů. Místo, aby byly využity nebo naopak zakázány vyhledávací, třídící a přístupové funkce programového vybavení sítě internetu, jsou osobní údaje v rámci seznamů zveřejňovány plošně, bez dalších opatření, která by byla normálně činěna při manuálním zpracování údajů a která je třeba učinit i v elektronické podobě (viz § 13 zákona o ochraně osobních údajů). Příkladem je úprava poskytování informací v praxi obcí, kde stále do-

chází k pracné anonymizaci údajů, neboť je zřejmé, že plošné zveřejnění na internetu zpřístupňuje údaje také uživatelům internetu, jimž poskytnutí osobních údajů projednávaných v rámci obecního zřízení není účelné a zákonné. V lepším případě na základě připomínky Úřadu předkladatel věc odsune k dalšímu projednání (viz případ obchodního rejstříku), v horším případě raději vůbec od záměru něco novelizovat odstoupí, jak se stalo v závěru roku 2008 u balíku novel volebních zákonů (Úřad požadoval kromě jiného vyjasnění otázky, co a z jakého důvodu bude zveřejňováno na internetu).

I přes své omezené kapacity se Úřad v roce 2008 snažil sledovat tvorbu právních předpisů ve všech oblastech, které upravují zpracování osobních údajů. Bohužel ani vládní systém elektronického připomínkování dokumentů nezajistí, aby se Úřad, který podle Legislativních pravidel vlády není ve všech případech povinným připomínkovým místem, včas dozvěděl o přípravě materiálů upravujících zpracování informací o lidech. Za vhodnější proto Úřad považuje včasné oslovení odpovědnými resorty, kterým nabízí při přípravě koncepcí, analýz a věcných záměrů právních předpisů možnost konzultace dopadů na ochranu soukromí a vyhodnocení změn s ohledem na pravidla zákona o ochraně osobních údajů, jak tomu bylo v roce 2008 např. v případě změn zákona o svobodném přístupu k informacím či v nově připravovaném zákonu o kontrole.



Styky se zahraničím a mezinárodní spolupráce

Ve stycích Úřadu se zahraničím zaujímá **spolupráce s orgány EU a partnerskými úřady ve členských státech EU jednoznačnou prioritu**. Proto také hlavní mezinárodní smluvní základnu, ze které vychází činnost Úřadu, tvoří smlouvy zakládající Evropská společenství a Evropskou unii a tedy i veškeré sekundární právo zahrnující závazné právní akty v rámci tzv. acquis communautaire v oblasti ochrany osobních údajů, a rovněž Úmluva č. 108 a další legislativní normy platné pro 3. pilíř EU. Zásadní význam pro ochranu osobních údajů mají dvě směrnice Evropského parlamentu a Rady a několik návazných rozhodnutí Evropské komise. Jde o základní směrnici v dané oblasti – směrnici 95/46/ES, o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, a dále o směrnici 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích); rozhodnutí Evropské komise se většinou týkají adekvátnosti ochrany osobních údajů v některých třetích zemích.

Absence obecné právní normy, která by v dostatečné šíři i hloubce právně zastřešila ochranu osobních údajů v celém 3. pilíři je pociťována stále citelněji, úměrně tomu, jak se rozšiřují, zintenzivňují a propojují jednotlivé mezinárodní bezpečnostní instrumenty. Ty mají svá vlastní specifická ustanovení, což jistě nepřispívá k transparentnosti 3. pilíře. Obecnou zastřešující normou pro ochranu dat ve 3. pilíři

se má stát „Rámcové rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech“ přijaté v závěru roku 2008 po mnohaletých diskusích, o nichž jsme ostatně referovali v předchozích výročních zprávách. Do dvou let by měly členské státy přijmout veškerá opatření vedoucí k zajištění shody, a to jak v právní, tak institucionální oblasti. Právní norma předpokládá působení úřadů nezávislého dozoru na národní úrovni, vybavených silnými kompetencemi. V preambuli se vyslovuje ve prospěch využití stávajících orgánů dozoru zřízených podle prvopilířové směrnice 95/46/ES k této úloze, nicméně poslední rozhodnutí ponechává na členských státech. V oblasti policejních a justičních agend se vztahuje pouze na zacházení s osobními údaji předávanými v rámci mezinárodní spolupráce; pozitivní je nicméně ustanovení preambule, podle kterého by měl národní standard „ladit“ s rámcovým rozhodnutím, avšak může být vyšší. I když výsledný návrh nepovažujeme za ideální a kriticky jsme hodnotili jak některá jeho jednotlivá ustanovení, tak celkovou šíři aplikačního záběru (prosazovali jsme uplatnění i v národních aktivitách bezpečnostních a justičních orgánů), jeho implementace by měla mít oproti současnému nepřehlednému stavu pozitivní efekt. Nicméně obecná úroveň rámcového rozhodnutí si v každém případě i v budoucnu vyžádá, aby při zavádění jednotlivých nových systémů mezinárodní bezpečnostní a justiční spolupráce v EU bylo vždy v příslušné právní normě pamatováno na specifická ustanovení na ochranu osobních údajů, která by přinesla přidanou hodnotu k principům zmíněné obecné normy ve smyslu konkretizace obecných ustanovení ve vazbě na specifické účely a povahu každého instrumentu.

Rozsáhlé diskuse v různých orgánech EU, zejména v pracovních skupinách a výborech Rady/Coreperu, se soustředily na několik témat z bezpečnostní oblasti, z hlediska dopadů do soukromí a ochrany osobních údajů velmi závažných. Souběžně probíhala stejně zaměřená jednání také na domácí mezirezortní úrovni, kde se Úřad často svými komentáři a připomínkami se střídavými úspěchy podílel na vytváření stanovisek a vyjednávacích pozic zastávaných zástupci České republiky v zahraničí. Jednoznačně nejvýznamnějším a současné nejproblematičtějším předmětem diskusí a jednání bylo staronové téma **předávání osobních údajů ze jmenné evidence cestujících v systémech leteckých dopravců (tzv. PNR data) bezpečnostním orgánům**. Po mezinárodních smlouvách, které již dříve Evropská unie uzavřela s USA a Kanadou byla ve sledovaném roce uzavřena také smlouva s Austrálií. Úřad se účastnil projednávání stanoviska ČR k mandátu pro jednání Evropské komise s australskou vládou a je třeba ocenit vstřícný přístup MZV ČR k našim připomínkám.

Mnohem intenzivnější diskuse na platformě orgánů a pracovních skupin Rady/Coreperu i na půdě domácí se vedly k návrhu zavést obdobné opatření formou rámcového rozhodnutí Rady také v Evropské unii. Předpokládá se předávání široké škály údajů o všech cestujících v letecké dopravě, překračujících minimálně vnější hranice EU se třetími zeměmi (o možnosti zahrnutí vnitrounijní dopravy se rovněž diskutuje) do databází zpracovávajících data pro potřeby bezpečnostních orgánů členských států EU, a to bez ohledu na to, zda jde o obyvatele zemí vně či uvnitř Unie. Úřad k tomuto opatření jako takovému měl vždy vyhraněně kritické stanovisko pro jeho neadekvátnost a neproporcionálnost vzhledem k deklarovaným (stále se rozšiřujícím) účelům i neprůkaznost a nedostatečné zdůvodnění bezpečnostních efektů. Přesto však se odborníci Úřadu velmi intenzivně zapojovali do diskusí i k jednotlivým dílčím aspektům ve snaze vnést jistou větší vyváženost alespoň v rovině konkrétních ustanovení.

Nutno konstatovat, že připomínky Úřadu byly MV ČR jakožto hlavním gestorem pro přípravu dokumentu na pracovní úrovni orgánů Rady uplatněny jen sporadicky a okrajově. Zástupci ČR přes vznášení určitých spíše formálních připomínek opatření od samého začátku podporovali, stejně jako tendenci k co nejšíře a nejednoznačně definovanému účelu, daleko překračujícímu původní záměr protiteroristic-

kého opatření. Jistým zadostiučiněním i povzbuzením pro Úřad bylo usnesení Senátu č. 370 z 23. dubna 2008, kterým se horní komora k návrhu rámcového rozhodnutí Rady vyslovila kriticky.

Mezi dalšími tématy projednávanými a diskutovanými v mezinárodním i domácím měřítku zmiňme ještě opatření v rámci programu rušení vízové povinnosti vůči USA (tzv. Visa Waver Programme – VWP), jednání Kontaktní skupiny na vysoké úrovni (HLCG) s USA o přijetí široce platného dokumentu s principy ochrany osobních údajů pokrývajícího různé instrumenty bezpečnostní spolupráce mezi EU a USA a dále například přípravu dokumentu o zřízení Evropského informačního systému rejstříků trestů ECRIS.

Význačné místo v činnosti Úřadu v souvislosti se spoluprací s Evropskou unií zaujímala **příprava na předsednictví České republiky v Radě**.

Úřad v rámci připomínkových řízení, která probíhala v několika stupních, uplatňoval svá stanoviska a své názory při tvorbě dvou základních programových dokumentů, které vláda ČR vypracovala pro potřeby českého předsednictví v Radě: *„Osmnáctiměsíční program předsednictví francouzského, českého a švédského předsednictví“ a „Obsahové priority předsednictví České republiky v Radě Evropské unie v I. pololetí 2009“.*

Hlavním cílem účasti Úřadu na přípravě těchto dokumentů bylo upozornit na problematiku ochrany osobních údajů a příslušná ustanovení organickým způsobem začlenit do plánovaných aktivit. V prvním případě bylo poukazováno na to, že problematika ochrany osobních údajů není pouze technokratickou záležitostí, ale je především součástí základních lidských práv. Dále bylo nutno vzít v úvahu, že má de facto průřezový charakter a víceméně jakékoli aktivita má svůj rozměr i v podobě zpracování a tedy i přiměřené ochrany osobních údajů. Z tohoto prakticky vyplývala potřeba dosáhnout zmínky k problematice ochrany osobních údajů v obecné části materiálů s tím, že by toto bylo konkrétněji rozpracováno pouze v souvislosti s nejvýznamnějšími aktivitami.

Záměr a s ním související náměty navrhované Úřadem se podařilo prosadit jen v malé míře. Projevovala se zjevná neochota zpracovatelů materiálů „komplikovat“ témata určená k prosazování v průběhu předsednictví problematikou lidských práv.

Na sklonku roku probíhaly intenzivně přípravy na tři významné akce pořádané nebo spolupořádané Úřadem v březnu 2009:

(1) Pracovní setkání k vyřizování stížností a podnětů (Case Handling Workshop): Jde o pravidelné setkání odborníků z partnerských úřadů pro ochranu dat z celé Evropy. Na pozvání Úřadu jednání tentokrát proběhne ve dnech 12.–13. března 2009 v Praze. Program se tradičně zaměřuje na výměnu zkušeností a poznatků z běžné praxe. Program se zaměří především na otázky, které jsou z hlediska ochrany dat a soukromí nejvíce aktuální. Sem patří kupříkladu kamerové systémy, biometrie, zpracování údajů v oblasti zaměstnávání nebo problematika ochrany soukromí v novinářské praxi.

(2) Česko-francouzské setkání mezi nejvyššími představiteli Úřadu pro ochranu osobních údajů a CNIL – Commission Nationale de l'Informatique et des Libertés, nezávislého dozorového úřadu ve Francii. Uskuteční se za podpory Francouzského institutu v Praze 3. a 4. března 2009.

(3) Zasedání Pracovní skupiny pro ochranu údajů (Data Protection Working Party, pracovně uváděná také pod kódem G.09), které se má uskutečnit v Bruselu dne 23. března 2009. Tato skupina je jednou z řady pracovních orgánů Rady Evropské unie. Česká republika bude zasedání řídit za odborné podpory Úřadu. Jako předsednická země také bude mít významné slovo při sestavování programu jednání.

Odborníci Úřadu se na přípravu agendy a na řízení samotných akcí intenzivně připravovali. Průběžně se monitoruje vývoj v oblastech spadajících tematicky do oblasti působnosti, u kterých se dá očekávat, že je české předsednictví bude muset řešit. Již jsme upozornili na „žhavé téma" dat leteckých cestujících (PNR). Zástupci některých států k opatření a jeho jednotlivým ustanovením uplatňovali mnoho protichůdných názorů, což diskusi během německého předsednictví v první polovině roku 2008 zavedlo do slepé uličky. Ve snaze o nalezení východiska francouzské předsednictví přerušilo postupné projednávání jednotlivých ustanovení a vrátilo se k rozpravě o obecných východiscích. Je zjevné, že významné posuny, včetně opětného sestoupení na konkrétnější rovinu, se očekávají od předsednictví ČR. Podle předpokladu se na pořad jednání dostanou i další, již výše zmíněné problémy, ale i řada dalších témat, jako je např. problematika všudypřítomných kamerových systémů, zpracování biometrických dat apod.

Nejvýznamnější pracovní platformou pro styk a spolupráci jak s Evropskou komisí, tak s partnerskými orgány dozoru v ostatních státech EU, byla i v uplynulém roce **Pracovní skupina podle článku 29 směrnice 95/46/ES pro ochranu osobních údajů (tzv. WP29)**. Jde o prestižní orgán Evropské komise s poradním a nezávislým statutem, jehož členy jsou přímo předsedové nezávislých orgánů dozoru z členských států EU, kteří se také většiny jeho zasedání osobně účastní. V roce 2008 se konalo celkem 5 zasedání WP29.

Mnoho z výše uvedených aktuálních i dlouhodobých námětů diskutovaných na jiných platformách EU se pochopitelně objevilo i v programu zasedání WP 29. Mezi dalšími specifickými body je možné zmínit např. dlouhodobě projednávaný problém tzv. BCR – Binding Corporate Rules (závazné interní předpisy společností), které prosazují podnikatelské kruhy typu nadnárodních společností jako seberegulační nástroj pro překonání rozdílného legislativního řešení ochrany osobních údajů v různých státech, ve kterých příslušná společnost působí. WP 29 postupně přijímá různá metodická doporučení, která by urychlila dohadovací řízení zúčastněných úřadů pro ochranu osobních údajů vedoucí k uznání jednotlivých BCR jakožto dostatečného nástroje s adekvátními garancemi. Mezi další významné náměty jednání patřily:

- prosazování práva v mezinárodním kontextu (uvnitř EU),
- návrh Světového antidopingového kodexu vč. Mezinárodního standardu pro ochranu soukromí,
- problematika systémů předávání informací zaměstnanců o nekalých praktikách v amerických podnicích v Evropě (tzv. donášení – whistleblowing),
- osobní údaje dětí se zvláštním zaměřením na internet,
- nové požadavky USA v souvislosti s rušením víz (Visa Waver Programme)
- revize směrnice o soukromí a elektronických komunikacích,
- vyhledávače (search engines) poskytovatelů internetových služeb,
- systém sledování ulic (Streetview) společnosti Google.

Pracovní skupina WP29 má řadu pracovních podskupin; Úřad má své zástupce ve čtyřech z nich: Technology Subgroup, Medical Data, Visa and Biometrics, Children and Privacy.

Specifickou platformou pro spolupráci Úřadu s EU je Pracovní skupina pro ochranu dat (G09) Rady EU. Je to politický orgán se zastoupením států a účast Úřadu jakožto nezávislého orgánu je proto zprostředkovaná, protože ČR je zde zastoupena pracovníkem Stálého zastoupení ČR při EU a zástupce Úřadu je v pozici přizvaného experta. Jak bylo již uvedeno výše, nejbližší zasedání bude mít zvláštní význam v souvislosti s předsednictvím ČR pro Úřad jakožto odborného garanta akce.

V roce 2008 pokračovalo aktivní působení Úřadu ve **Společném kontrolním orgánu Europolu** (Joint Supervisory Body of Europol – „JSB"). Zástupkyně Úřadu, inspektorka PhDr. Miroslava Matoušová, byla koordinátorkou kontrolního týmu, kte-

rý provedl v březnu 2008 pravidelnou kontrolu zpracování osobních údajů Europolem v sídle tohoto orgánu a do 26. října 2008 působila jako místopředsedkyně JSB. V roce 2008 se konaly čtyři schůze Společného kontrolního orgánu Europolu a čtyřikrát se sešel také jeho Odvolací výbor, který projednával a řešil dvě stížnosti subjektů údajů – podání britského občana B. a podání finského občana p. N. Klíčovými činnostmi a úkoly JSB byly kontrola v Europolu, nová primární a sekundární legislativa Europolu a nové projekty, jejichž podstatnou součástí je zpracování osobních údajů Europolem. JSB mimo jiné přijal po diskusi s Europolem stanovisko k úrovni ochrany údajů v Ruské federaci. Úřad byl řádně zastoupen na všech plenárních schůzích a na třech schůzích pracovních podskupin, které se uskutečnily v Haagu a Bruselu; dokumenty připravené na těchto jednáních byly posléze společným kontrolním orgánem projednány a přijaty.

Úřad se podílel také na práci nebývale aktivní **Pracovní skupiny pro policii a justici (WP on Police and Justice)**. Skupina je orgánem Konference evropských orgánů ochrany osobních údajů a jejím úkolem je sledovat vývoj ve zpracování osobních údajů orgány činnými v trestním řízení. Schůzky jsou organizovány při příležitosti pracovních jednání společných dozorových orgánů; část práce probíhala korespondenčně. Podíl Úřadu zahrnoval působení ve třech ad hoc pracovních skupinách: pro dotazníkový průzkum oprávnění a postavení dozorových orgánů, pro kontrolní činnost a pro strategickou komunikaci s orgány Evropské unie. Srovnávací průzkum ukázal, že působnost určených vnitrostátních dozorových orgánů není plně srovnatelná a že v řadě evropských zemí platí pro dozor nad zpracováním osobních údajů, prováděném pro potřeby orgánů činných v trestním řízení, jiná pravidla než v ostatních oblastech života společnosti.

Pro úplnost zmiňme významnou aktivitu zástupců Úřadu ve *Společném dozorovém orgánu pro Schengenský informační systém* (Joint Supervisory Authority – JSA Schengen), *Společném dozorovém orgánu pro Celní informační systém* (Joint Supervisory Authority – JSA Customs) a *Koordinační skupině pro dohled nad systémem Eurodac*.

V roce 2008 pokračovaly také společné aktivity zástupců orgánů dozoru nad ochranou dat ze zemí střední a východní Evropy a z Pobaltí, zahájené v roce 2001 z iniciativy českého Úřadu a polského Úřadu generálního inspektora ochrany osobních údajů. Mají formu pracovních setkání a dalších kontaktů, mj. komunikací s využitím společných webových stránek (*www.ceecprivacy.org*). Na posledním setkání v Polsku poblíž Varšavy (Dolny Kazimierz) se diskutovalo o problematice soukromí dětí na internetu, efektivnosti dozorových činností úřadů ochrany dat, zpracování dat finančními institucemi, o využívání kamerových systémům, Schengenském informačním systému. Přijata byla deklarace na podporu dalšího posílení spolupráce zúčastněných zemí a Deklarace o rovném přístupu ke všem národním jazykům členských států EU (se zaměřením na praxi v pracovní skupině WP 29).

Nadále se rozvíjela *bilaterální spolupráce* s partnerskými úřady pro ochranu osobních údajů v různých členských zemích Evropské unie. Nadstandardní a zvláště přínosné jsou zejména kontakty s polským Generálním inspektorem ochrany osobních údajů a slovenským Úradom na ochranu osobných údajov. V návaznosti na projekt pomoci Bosně a Hercegovině ukončený v roce 2007 byly obnoveny kontakty s nově zřízenou Komisí ochrany dat v Sarajevu.

Vedle aktivit v rámci Evropské unie pokračovala také významná spolupráce vyplývající ze závazků České republiky jakožto členské země Rady Evropy a OECD. V ***Radě Evropy*** byl Úřad po řadu let v projektové skupině pro ochranu dat (CJ-PD) a koordinačním výboru (CJ-PD/CG). Aktivní účast pokračovala i ve Výboru pro ochranu dat, zřízeném podle Úmluvy 108 (dále jen T-PD), který je nejvyšším orgánem Rady Evropy zabývajícím se ochranou dat. Úřad je zastoupen v sedmičlenném řídícím byru Výboru PhDr. Hanou Štěpánkovou, tiskovou mluvčí Úřadu. Stejně jako

v předchozím roce patřila k nosným tématům ochrana osobních údajů vrcholových sportovců v souvislosti s antidopingovými aktivitami a materiály agentury WADA – World Anti-Doping Agency. Soutředěně je připravován dokument doporučující zásady aplikace principů Úmluvy 108 v kontextu profilování. Expertizu k problematice technického a technologického procesu profilování s ohledem na Úmluvu 108 pro T-PD připravilo odborné pracoviště univerzity v Namur. Dopracovaný dokument bude rozeslán zástupcům úřadů států, které podepsaly Úmluvu 108 v předstihu, aby o něm mohlo proběhnout hlasování na plenárním zasedání v květnu 2009. Významné v roce 2008 bylo, že Rada ministrů přijala návrh T-PD, aby Úmluva 108 byla otevřena k podpisu rovněž mimoevropským státům. T-PD v roce 2008 na základě žádostí dvou mezinárodnch uskupení ochránců osobních údajů – Agentury frankofonních států a Iberoamerické skupiny – jim udělila statut pozorovatelů.

Pokračuje velmi přínosná spolupráce s ***OECD*** – Organizací pro hospodářskou spolupráci a rozvoj, kde je Úřad partnerem MV ČR pro zastoupení ČR v Pracovní skupině pro informační bezpečnost a soukromí (WPISP). Vzhledem k celosvětové povaze OECD a navíc k její úzké spolupráci s asijským APEC získává Úřad součinností s WPISP mnoho cenných informací a zkušeností i mimoevropské provenience zejména o nových trendech a iniciativách v oblasti informační bezpečnosti a ochraně soukromí. WPISP sama také některé iniciativy vyvíjí, v poslední době jsou to zejména doporučení ohledně spolupráce při vymáhání práva v oblasti ochrany soukromí v mezinárodním měřítku. Mezi dalšími tématy z poslední doby zmiňme problematiku škodlivého softwaru (malware) a správa digitálních identit (digital identity management).

Kromě výše uvedených aktivit v souvislosti s pravidelnou spoluprací v pracovních orgánech mezinárodních organizací a bilaterální spoluprací s partnerskými úřady se odborníci Úřadu účastnili mnoha jednorázových i opakovaných akcí typu konferencí, seminářů a setkání nejrůznějšího druhu, jako například:

(Pozn.: Některé z níže uvedených příkladů akcí s účastí expertů z Úřadu byly specificky zaměřeny na přípravu na předsednictví, s financováním ze zvláštního zdroje).

Diskusní fórum vládních činitelů Evropy: „Modernizace e-Zdravotnictví a školství"

(Berlín, 22. – 23. 1. 2008)

Společnost Microsoft zorganizovala diskusní fórum nejvyšších vládních činitelů z celé Evropy na téma perspektivy modernizace státní správy. Jako hosté se zúčastnili Angela Merkel a Bill Gates. Jednání se soustředilo na to, jak zjistit potenciál modernizace státní správy, za situace, kdy svět elektronických komunikací zasahuje stále více do soukromého světa všech občanů a rozšiřováním elektronizace státní správy je soukromí obyvatel ve stále větším ohrožení.

Schengenská evaluační mise v oblasti ochrany osobních údajů – Švýcarsko

(Bern, 9. – 13. 3. 2008)

Účelem expertní mise s účastí inspektora Úřadu bylo z pověření Rady EU (pracovní skupiny pro schengenské evaluace) ověřit úroveň ochrany osobních údajů Švýcarska s ohledem na požadavky schengenského acquis, a to zejména co se týče postavení a činnosti příslušných dozorových úřadů a budoucích správců údajů v Schengenském informačním systému jak na federální, tak na kantonální úrovni.

Seminář o vztazích mezi předsednictvím v Radě EU a Evropským parlamentem

(Brusel, 27. 3. 2008)

Evropským parlament a Generální ředitelství pro předsednictví uspořádaly prostřednictvím Úřadu vlády ČR a Stálého zastoupení ČR při EU v Bruselu pro zástupce státních institucí z ČR seminář v rámci přípravy na předsednictví ČR. Hlavním cílem bylo: 1. Seznámit se strukturou a způsobem práce EP s ohledem na konkrétní

potřeby státní správy v ČR, 2. Vysvětlit, jaké výzvy stojí před EP, zejména v souvislosti s Lisabonskou reformní smlouvou, 3. Umožnit pracovníkům institucí z ČR navázat osobní kontakty v EP.

17. a 18. pracovní setkání k vyřizování případů (Case Handling Workshop)

(Lublaň, 31. 3. – 1. 4. 2008 a Bratislava, 29. – 30. 9. 2008)
Jednalo se o pravidelné jednání zástupců dozorových orgánů působících v oblasti ochrany osobních údajů ve členských státech EU zaměřené na praktické otázky problematiky ochrany osobních údajů a na konkrétní případové studie.

Jarní konference evropských komisařů pro ochranu dat

(Řím, 17. – 18. 4. 2008)
Jarní konference jsou každoročním setkáním pořádaným vždy jedním z evropských úřadů pro ochranu osobních údajů. Staly se již tradičním mezinárodním fórem významným především možností výměny různých hledisek a názorů jak na práci již vykonanou, tak i na výzvy teprve nadcházejících témat. Letošní konferenci uspořádal italský Úřad „Garante per la protezione dei dati personali".

Evropská vyjednávání v praxi – Intenzivní kurz pro zdokonalení vyjednávacích dovedností

(Bruggy, 21. – 25. 4. 2008)
Jednalo se o kurs pořádaný školou „The College of Europe". Školení bylo součástí přípravy na předsednictví ČR v Evropské Radě EU a v tomto smyslu bezezbytku splnilo svůj účel. Výuka byla založena na kombinaci přednášek s interaktivními cvičeními.

Bilaterální setkání ÚOOÚ ČR a ÚOOÚ SR

(Častá – Papiernička, 5. – 7. 5. 2008)
Setkání se uskutečnilo za účelem vzájemné výměny zkušeností vybraných expertů, a to především na téma osobních dokladů, nejčastějších otázek veřejnosti směřovaných Úřadům, zpracování osobních údajů v rámci centrálních registrů, poskytování součinnosti ze strany státní správy a pravomoci úřadů při výkonu kontroly.

Workshop o komunikačních zařízeních v automobilech, telematice a zabezpečení soukromí

(Brusel, 27. 5. 2008)
Na setkání prezentovali jednotliví účastníci současnou situaci v komunikaci mezi vozidly a silničním dispečinkem, mezi vozidlem a policií a mezi vozidly navzájem. Z hlediska ochrany osobních údajů se jedná o rychle se rozvíjející oblast, která přináší rizika sledování osob prostřednictvím vozidla.

Workshop expertů o evropské pečeti soukromí „EuroPriSE"

(Kiel, 2. – 3. 6. 2008)
Účelem cesty bylo získat informace z workshopu pořádaného Nezávislým zemským centrem pro ochranu dat Šlesvicka-Holštýnska především pro nezávislé experty – právníky a techniky, kteří mají zájem zúčastnit se jako hodnotitelé produktů a služeb IT projektu „European Privacy Seal", jehož cílem je udělování certifikátů garantujících soulad produktů a služeb s evropskými předpisy pro ochranu soukromí a osobních údajů.

Evropská konference k elektronické identitě

(Haag, 10. – 11. 6. 2008)
Konference se zabývala řízením elektronické identity v souvislosti se zabezpečením ochrany osobních údajů v elektronickém bankovnictví, justici, obchodu, podnikání a mobilních systémech.

Jak uspět při předsednictví

(Berlín, 17. – 23. 6. 2008)

Jednalo se o účast na kursu pořádaném Evropskou Akademií v Berlíně jako součást přípravy států EU k jejich předsednictví. Záměrem bylo nastínit obecnější přehled o Evropské Unie a zdrojů, z nichž se formovala.

44. schůzka mezinárodní pracovní skupiny pro ochranu dat v telekomunikacích (IWGDPT) a Mezinárodní sympozium „Soukromí ve věku sociálních sítí"

(Štrasburk, 12. – 14. 10. 2008)

Setkání skupiny se vždy účastní delegáti z celého světa, jsou proto velkým přínosem především z hlediska vzájemné výměny zkušeností. 44. jednání se týkalo krátkých textových zpráv (SMS) z pohledu legislativy a praktik uchovávání jejich obsahu, šifrování s využitím biometrických údajů a provozování bezpečnostních kamerových systémů. Sympozium bylo věnováno rychle se rozšiřujícímu fenoménu virtuálních společenských sítí (SNS).

30. mezinárodní konference komisařů pro ochranu osobních údajů a soukromí

(Štrasburk, 15. – 17. 10. 2008)

Každoročně se scházejí předsedové („komisaři") akreditovaných úřadů pro ochranu osobních údajů na této nejprestižnější akci v jejich působnosti. Konference se konají v různých částech světa vždy na pozvání některého ze zúčastněných úřadů. 30. ročník byl uspořádán hostitelskými úřady z Francie a Německa, které slavily výročí vzniku institucionalizované ochrany dat ve svých zemích. Cílem bylo identifikovat hlavní výzvy v mezinárodním kontextu a globálním měřítku, které vznikají v souvislosti s nástupem nových technologií a s politickým, právním a ekonomickým vývojem.

6. německý antispamový summit a LAP/CNSA konference

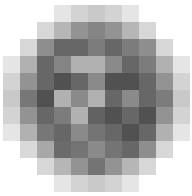
(Wiesbaden, 27. – 29. 10. 2008)

Antispamového summitu se zúčastnili jak zástupci ochránců osobních údajů, tak i zástupci telekomunikačních úřadů a byla zde zastoupena i strana poskytovatelů připojení k internetu. Hlavním tématem byly ukázky toho, jak vypadá elektronický zločin a jak s ním bojovat. Dále byly diskutovány problémy související s internetovým bankovnictvím a riziky, které jsou s tím spojené.

Účast na projednávání případu C-553/07 Rijkeboer před Soudním dvorem ES

(Lucemburk, 19. – 21. 11. 2008)

Šlo o ústní projednání uvedeného případu, k němuž Úřad již vyjádřil své stanovisko zohledněné v písemném vyjádření ČR. Cesta byla uskutečněna z podnětu vládního zmocněnce pro zastupování ČR před Soudním dvorem ES.



Komunikace s médii, šíření znalostí o ochraně osobních údajů

Tiskové konference

V roce 2008 pokračoval zavedený způsob komunikace s médii: Osvědčená čtvrtletní periodicita bilančních tiskových konferencí přivádí na Úřad standardně cca 20 novinářů, mezi nimiž jsou zastoupena tištěná média – jak deníky, tak odborně zaměřený tisk – agentury, hlavní rozhlasové i televizní stanice. Výstupy z tiskových konferencí se pravidelně v průběhu roku objevovaly již v poledním zpravodajství v den konání konference. Dále potom v průběhu následujících 3 dní se ochraně osobních údajů věnuje 30 – 60 výstupů, které se většinou soustřeďují na informování o již dříve mediálně sledovaných kauzách.

Tiskové zprávy i přílohy k nim jsou okamžitě po skončení konference zveřejněny trvale na webových stránkách Úřadu. Je tak mj. také naplňován princip otevřenosti Úřadu vůči veřejnosti

Zvláštní tiskovou konferenci pořádá Úřad u příležitosti Dne ochrany osobních údajů 28. ledna. Tento den byl zvolen Radou Evropy jako připomínka přijetí prvního právně závazného dokumentu zaměřeného na ochranu osobních údajů – Úmluvy 108. Uvedená příležitost dává možnost soustředit pozornost na šíření znalostí o ochraně osobních údajů i nových technologií využívajících a pracujících s osobními údaji, ale také k obecnějšímu pohledu na soukromí jakožto civilizační hodnotu.

V České republice byla u této příležitosti podruhé vyhlášena soutěž pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“, o které se detailněji zmiňujeme níže.

Kontakty s médii

Třikrát v průběhu roku předseda odpovídal v online rozhovoru, uskutečnily se čtyři hodinové relace v rozhlase, dvakrát byl předseda hostem ranního vysílání televize v den konání tiskové konference.

V návaznosti na tiskovou konferenci odpovídá předseda pravidelně na individuální dotazy přítomných novinářů.

V případě jednotlivých individuálních otázek a žádostí novinářů, s nimiž se obracejí na tiskové oddělení, Úřad reaguje zpravidla téhož dne.

Tendence médií k zjednodušování vedla občas, zejména při telefonickém kontaktu, ke zkreslení právní podstaty případu. S obdobným problémem se lze setkat při televizních zprávách, kdy získané reakce nejsou následně předloženy Úřadu k vyjádření, a v důsledku toho dojde k jednostrannému informování veřejnosti.

V průběhu roku 2008 se Úřad setkal i s voluntaristickým pojetím publicisticky sledovaného případu, kdy o vyznění už předem měl redaktor jasno: záběry a výroky sestřihal bez ohledu na vysvětlení o reálné podstatě právního řešení případu. Domáhat se pochopení pro právní podstatu problému je bohužel nevymahatelné a Úřad nenalezl odezvu ani u dozorujícího orgánu. „Úderné“, leč právně nikoli precizní sdělení přitom rozhodně neprospívá posílení právního povědomí veřejnosti.

Naopak jako velmi pozitivní lze hodnotit zájem novinářů o konkrétní životní situace, v nichž se jim jeví, že by mohlo docházet k ohrožení soukromí. Velmi často kontakt novináře s tiskovým oddělením je pro Úřad upozorněním na incident, jímž by se měl zabývat – a také často na základě takového upozornění se případ stává předmětem dozorové či přímo kontrolní činnosti Úřadu.

Obdobně jako rozsáhlé rozhovory v rozhlase jsou přínosem publikace v odborném tisku.

Elektronická komunikace

Fakt, že Národní knihovna zařadila webové stránky Úřadu do nově vytvářeného archivu uchovávajícího ty „weby", které jsou považovány za přináležející k národnímu dědictví, je pro Úřad poctou i radostí.

Webové stránky Úřadu byly v roce 2008 obohaceny o informační bulletin, který přináší poznatky o ochraně osobních údajů a legislativě spojené s ochranou soukromí ve státech, které rozvíjejí tuto stránku ochrany lidských práv. Vznik uvedeného elektronické publikace byl veden poznatkem, k němuž dospěl evropský barometr – o nepříliš valné znalosti o ochraně osobních údajů v zahraničí mezi českými respondenty. Tento informační bulletin obohacuje informace o evropském právním zakotvení ochrany osobních údajů a o obdobné legislativě v dalších státech rozvinutých ekonomik, které jsou průběžně součástí rubriky Zahraničí.

Mezi periodické publikace Úřadu přibyly v roce 2008 tři částky Věstníku. Obsáhly kromě zákonem uloženého zveřejnění zrušených registrací, také řadu dokumentů, jimiž se Úřad vyslovil meritorním způsobem k obecným problémům, pro něž hledal řešení (tzv. Stanoviska); publikována jsou zde rovněž vyjádření a vysvětlení pozice Úřadu ve vztahu k jednotlivým problémům, s nimž se vypořádával, ale také resumé správních rozhodnutí a druhoinstančních rozhodnutí – tedy svého druhu přehled o „judikatuře" Úřadu. Věstník Úřadu také přetiskl řadu dokumentů vydaných původně v Úředním věstníku EU, pokud mají rozhodnou důležitost pro ochranu osobních údajů, nebo dokumentů, jež jsou výstupem z velkých evropských konferencí o ochraně osobních údajů.

Informační bulletin přinesl ve 3 číslech přehled o své práci vždy za uplynulé čtvrtletí a řadu informací o ochraně osobních údajů nebo o ochraně soukromí doma i ve světě v širším slova smyslu. Svou dikcí je toto periodikum určeno široké veřejnosti, která chce být informována o aktuálním dění v oblasti ochrany soukromí. Poslední čtvrtletí roku mapuje 4. číslo Bulletinu, které vychází až v roce 2009. Informační bulletin Úřad vytváří včetně tisku a distribuce silami svého tiskového oddělení.

Obě uvedená periodika Úřadu jsou dostupná také na webových stránkách Úřadu v elektronické podobě.

Knihovna Úřadu

Knihovna nabízí odborné zázemí pro pracovníky Úřadu. V roce 2008 se rozšířila o 135 publikací. Sloužila nadále také jako zázemí pro studenty práv a správních škol. Z jejích zdrojů čerpalo 6 posluchačů vysokých i středních škol pro své připravované práce.

Šíření znalostí o ochraně osobních údajů

Vyjmenovávat všechny přednášky o ochraně osobních údajů, které se v průběhu roku 2008 uskutečnily za přispění odborných pracovníků Úřadu, by bylo velmi rozsáhlé. Je proto účelnější uvést, že pracovníci Úřadu za rok 2008 poskytli 260 hodin přednášek.

Roku 2008 pokračoval program, který Úřad připravil pro pedagogické pracovníky a který byl na 3 roky akreditován MŠMT ČR. Semináře Úřad nabízel v jednotlivých krajích. Semináře se uskutečnily v Hodoníně, Pardubicích a v Ostravě. Na závěr seminářů získávají účastníci osvědčení o absolvování modulu „Ochrana osobních údajů ve vzdělávání" a anonymním testem si mohou ověřit své znalosti. Test slouží Úřadu jako zpětné poznání o schopnosti srozumitelným způsobem sdělit poznatky z oblasti ochrany osobních údajů.

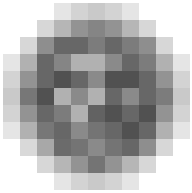
Je třeba říci, že přestože nabídka výjezdních seminářů byla míněna jako služba pedagogům mimo Prahu a zohledňovala jejich časové vytížení – což se dělo samozřejmě s nemalými časovými nároky na přednášející pracovníky Úřadu, neosvědčila se zcela spolupráce se školicími centry v krajích. Odvolávání řady termínů komplikovalo časový harmonogram prací přednášejících. Proto se Úřad rozhodl pořádat v roce 2009 semináře přímo v sídle Úřadu v Praze. Zatím z prosincové reakce pedagogů je zaznamenán velký zájem, už první ze seminářů (v únoru 2009) byl naplněn během týdne po té, co byl inzerován.

Úřad uspořádal v roce 2008 druhý ročník soutěže pro děti a mládež ve výtvarném a literárním projevu s názvem „Moje soukromí! Nekoukat, nešťourat!". Soutěže se v roce 2008 s úspěchem zúčastnily také děti z SOS vesniček v Česku, na Ukrajině, v Kazachstánu, v Rusku a v Bosně a Hercegovině. Úřad velmi vítá spolupráci se Sdružením SOS vesniček. Považuje za potřebné, aby i děti, které vyrůstají mimo úplnou rodinu, byly dostatečně informovány o právech, kterých budou jako plnohodnotní členové společnosti požívat.

Partnerem soutěže byl opět Mezinárodní festival filmů pro děti a mládež ve Zlíně, kde předseda Úřadu a ředitelka Sdružení SOS vesniček v ČR předali ceny vítězům. Spolupráci ve formě účasti na relacích pro děti poskytl ČRo Praha a informace pro děti přinesl i portál MF DNES Alík.

V souvislosti s úspěchem loňského roku, který Úřadu přinesla soutěž a seminář pro pedagogy (Evropská cena za nejlepší službu veřejnosti v oblasti ochrany osobních údajů, udělená v roce 2007 v Madridu), byly práce českých dětí z prvního ročníku soutěže vystaveny u příležitosti vyhlášení Dne ochrany osobních údajů. V týdnu před 28. 1. 2008 byly dětské kresby vystaveny ve vstupní hale Paláce Evropy ve Štrasburku. U příležitosti této výstavky se setkal předseda Úřadu také s velvyslancem ČR při Radě Evropy a s několika řediteli odborů Rady Evropy.

Úřad pokračoval také ve spolupráci s 3. lékařskou fakultou. Na listopadovém semináři věnovaném ohrožením, která se vyskytují pro generaci třetího věku, Úřad participoval přednáškou o smyslu ochrany osobních údajů a šířením znalostí o jejich spojitosti s ochranou soukromí, s důrazem na zvláštní dopady pro život starší generace.



Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 360/2007 Sb., o státním rozpočtu České republiky na rok 2008.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

v tisících Kč

Souhrnné ukazatele

Příjmy celkem ---------- 1 642,48
Výdaje celkem ---------- 88 293,01

Specifické ukazatele – příjmy

Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem ----- 1 642,48

Specifické ukazatele – výdaje

Výdaje na zabezpečení plnění úkolů ÚOOÚ ---------- 88 293,01
v tom: výdaje spojené s výkonem předsednictví ČR v Radě EU ------ 2 159,76
ostatní výdaje na zabezpečení plnění úkolů ÚOOÚ ---------- 86 133,25
Průřezové ukazatele výdajů
Platy zaměstnanců a ostatní platby za provedenou práci ---------- 40 527,82
Povinné pojistné placené zaměstnavatelem*) ---------- 14 207,98

**) pojistné na sociální zabezpečení a příspěvek na státní politiku zaměstnanosti a pojistné na veřejné zdravotní pojištění*

Převod fondu kulturních a sociálních potřeb ---------- 765,72
Platy zaměstnanců v pracovním poměru ---------- 29 341,72
Platy zaměstnanců v pracovním poměru odvozované
od platů ústavních činitelů ---------- 8 979,10

Příjmy

Příjmy byly pro rok 2008 nebyly rozpočtem stanoveny. Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částku 1 642,48 tisíc Kč.
Jednalo se zejména o refundace zahraničních cest zaměstnanců Úřadu Radou Evropy a Evropskou komisí, o sankce uložené podle zákona č. 480/2004 Sb. o některých službách informační společnosti, o náhrady nákladů řízení, o úroky za finanční prostředky uložené na účtech u ČNB, o pojistné náhrady, o převody z vlastních fondů, o příjmy vztahující se k roku 2007 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2007).
Na příjmovém účtu se projevilo použití účelových finančních prostředků z rezervního fondu v celkové výši 49,13 tisíc Kč na výdaje spojené s přípravou předsednictví České republiky v Radě Evropské unie.
Úroky z finančních prostředků uložené na účtech u ČNB činily 2,54 tisíc Kč.
Přijaté sankční platby byly ve výši 352,33 tisíc Kč, pojistné náhrady ve výši 77,00 tisíc Kč, příjmy z prodeje automobilu ve výši 177,66 tisíc Kč, náklady řízení ve vý-

ši 113,49 tisíc Kč a refundace týkající se minulých let ve výši 870,33 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

1. Ostatní běžné výdaje (mimo ISPROFIN)

Čerpání běžných výdajů ve výši 12 208,45 tisíc Kč odpovídá běžným provozním výdajům, které vyplývají z hlavní činnosti Úřadu; jde zejména o položky spojené s nákupem drobného hmotného majetku, materiálu, služeb, cestovného, vzdělávání, údržby a o výdaje související s neinvestičními nákupy.
Výdaje za vodu, plyn a elektrickou energii činily v roce 2008 1 191,74 tisíc Kč.
Výše uvedené částky odpovídají požadavku na účelný a hospodárný provoz Úřadu.

2. Platy zaměstnanců a ostatní platby za provedenou práci

Čerpání rozpočtu na platy zaměstnanců a ostatní výdaje za provedenou práci odpovídají kvalifikační struktuře a plnění plánu pracovníků.
Stav k 31. 12. 2008 byl 92 zaměstnanců.

3. Výdaje na financování programů zařazených v informačním systému Ministerstva financí – ISPROFIN

V souladu se schválenou dokumentací programu 143 010 „Rozvoj a obnova materiálně-technické základny Úřadu pro ochranu osobních údajů“ bylo celkem vyčerpáno 21 348,76 tisíc Kč.
Z toho na investiční výdaje bylo čerpáno 7 273,42 tisíc Kč.
Šlo zejména v programu 143 010 „Rozvoj a obnova materiálně technické základny“ o: podprogram 143 011 „Pořízení, obnova a provozování ICT ÚOOÚ“, kde byly v roce 2008 čerpány investiční systémově určené výdaje SR na:

	v tis.Kč
akci 143 011 0001 „Licenční smlouvy Microsoft – assurance“	439,55
akci 143 011 0002 „Upgrade modulů IS“	353,00
akci 143 011 0004 „Ukládání dat z EKLEP v IS ÚOOÚ“	154,15
akci 143 011 0005 „Pořízení výkonných notebooků“	157,59
akci 143 011 0006 „Rozšíření a obnova licencí antivirového programu“	99,08
akci 143 011 0007 „Pořízení HW pro podporu virtuálních serverů“	281,68
akci 143 011 0008 „Prodloužení smlouvy Enterprise na používání produktů Microsoft“	1 681,90

neinvestiční systémově určené výdaje SR na:

akci 143 011 P004 „Provozování ICT“	8 380,73

podprogram 143 012 „Reprodukce majetku ÚOOÚ“ – kde byly čerpány investiční systémově určené výdaje SR na:

akci 143 012 0005 „Obnova a doplnění vozového parku“	1 606,13
akci 143 012 0006 „Zabezpečení objektu“	1 222,17
akci 143 012 0007 „Implementace měř.a regul.techniky kotelny“	382,08
akci 143 012 0008 „Drobné úpravy budovy“	58,07
akci 143 012 0009 „Klimatizace (chlazení) kanceláří – 5.patro“	838,02

Neinvestiční systémově určené výdaje SR na:

akci 143 012 P006 „Nájemné a služby“	3 379,94
akci 143 012 P007 „Údržba zařízení a DHIM“	2 314,67

Investiční systémově určené výdaje byly čerpány celkem ve výši 7 273,42 tisíc Kč , z toho čerpání na investiční akce v podprogramu 143 011 „Pořízení, obnova a provozování ICT ÚOOÚ“ 3 166,95 tisíc Kč, v podprogramu 143 012 „Reprodukce majetku ÚOOÚ“ 4 106,47 tisíc Kč.

Neinvestiční systémově určené výdaje byly čerpány celkem ve výši 14 075,34 tisíc Kč a byly použity na úhradu provozních nákladů ICT, služeb a údržby zařízení a drobného hmotného dlouhodobého majetku.

4. Interní audit a vnitřní kontrola

Funkce vnitřního auditu je personálně zajištěna od roku 2006.
V květnu roku 2008 byl proveden v souladu s plánem audit informační strategie Úřadu a administrativní náročnost operací. Následně pak v září audit účtování cestovních náhrad a v prosinci audit vnitřního kontrolního systému.

5. Použití rezervního fondu

Část prostředků, účelově určených, uložených v rezervním fondu, byla použita na výdaje spojené s výkonem předsednictví České republiky v Radě Evropské unie, a to ve výši 49,13 tisíc Kč.

Přehled čerpání rozpočtu v roce 2008

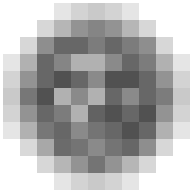
Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2008 v tisících Kč	Upravený rozpočet 2008 v tisících Kč	Skutečnost dle účetních výkazů k 31.12. 2008 v tis. Kč	Skutečnost / Upravený rozpočet v %
	PŘÍJMY CELKEM	**0**	**0**	**1 642,48**	**1 642,48**
501	Platy	38 319	38 348	38 320,82	99,93
5011	Platy zaměstnanců	29 347	29 376	29 341,72	99,88
5014	Platy zaměstnanců odvozované od platů ústavních činitelů	8 972	8 972	8 979,10	100,08
502	Ostatní platby za provedenou práci	2 207	2 207	2 207,00	100,00
5021	Ostatní osobní výdaje	1 807	1 807	1 807,00	100,00
5024	Odstupné	400	400	400,00	100,00
5026	Odchodné	0,00	0,00	0,00	0,00
503	Povinné pojistné placené zaměstnavatelem	14 185	14 195	14 207,98	100,09
5031	Povinné pojistné na sociální zabezpečení	10 538	10 545	10 554,59	100,09
5032	Povinné pojistné na veřejné zdravotní pojištění	3 647	3 650	3 653,39	100,09
513	Nákup materiálu	4 554	3 569	1 985,86	55,64
514	Úroky a ostatní finanční výdaje	50	53	13 68	25,81
515	Nákup vody, paliv a energie	2 250	2 280	1 583,26	69,44
516	Nákup služeb	18 300	18 849	14 372,50	76,25
5167	Školení a vzdělávání	3 220	2 920	1 596,33	54,67
517	Ostatní nákupy	8 249	8 613	5 469,11	63,50
5171	Opravy a udržování	3 204	3 075	1 705,24	55,45
5173	Cestovné	3 715	3 699	2 501,54	67,63

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2008 v tisících Kč	Upravený rozpočet 2008 v tisících Kč	Skutečnost dle účetních výkazů k 31.12. 2008 v tis. Kč	Skutečnost / Upravený rozpočet v %
518	Poskytnuté zálohy	0	0	0	0
519	Výdaje související s neinvestičními nákupy	2 780	2 780	2 090,68	75,20
5342	Převody FKSP	766	766	765,72	99,96
5346	Neinv. převody do RF	0	0	0	0
536	Ostatní neinvestiční transfery jiných veřejných rozpočtů	35	35	2,98	8,51
542	Náhrady placené obyvatelstvu	60	60	0	0
5429	Ostatní náhrady placené obyvatelstvu	60	60	0	0
	BĚŽNÉ VÝDAJE CELKEM	91 755	91 755	81 019,59	88,30
611	Pořízení dlouhodobého nehmotného majetku	3 080	3 410	2 727,68	79,99
612	Pořízení dlouhodobého hmotného majetku	5 180	4 850	4 545,74	93,73
6361	Investiční převody do RF				
	KAPITÁLOVÉ VÝDAJE CELKEM	8 260	8 260	7 273,42	88,06
	V Ý D A J E C E L K E M	**100 015**	**100 015**	**88 293,01**	**88,28**
	z toho: použití rezerv. fondu			49,13	

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 12. 2008

Přehled výdajů spojených s výkonem předsednictví ČR v Radě EU v roce 2008

Položka-název	Schválený rozpočet	Upravený rozpočet	Čerpání
5011/15 – Platy	459	459	494,80
5031/15 – povinné pojistné na SZ	120	120	129,59
5032/15 – povinné pojistné na ZP	41	41	44,38
5342/15 – FKSP	10	10	10,34
5142/15 – Realizované kurz. ztráty	5	8	7,30
5163/15 – Služby peněžních ústavů	0	13	12,08
5167/15 – Školení tuzemské	20	95	57,35
5167/2/15 – Školení zahraniční	1 400	1 025	324,84
5176/1/15 – Účast. popl. na konference	0	300	271,60
5173/2/15 – Cestovné	1 015	999	807,48
Celkem	**3 070**	**3 070**	**2 159,76**



Personální obsazení Úřadu

Pro rok 2008 byl státním rozpočtem schválen počet 96 funkčních míst, z toho jedno funkční místo je určeno na zabezpečení úkolů vyplývajících z výkonu předsednictví ČR v Radě Evropské unie v roce 2009.

K 1. 1. 2008 byl fyzický počet zaměstnanců 92. Průměrný přepočtený stav zaměstnanců za rok 2008 byl 89,841. Stav zaměstnanců zůstává i nadále nenaplněný vzhledem k požadavku vysokoškolského vzdělání právního směru.

V úřadu je 63% vysokoškolsky vzdělaných zaměstnanců. Úřad umožňuje svým zaměstnancům zvyšování kvalifikace a také zajišťuje její prohlubování.Umožňuje a zajišťuje jazykovou výuku v anglickém, francouzském a německém jazyku.

K 31. 12. 2008 měl Úřad pro ochranu osobních údajů 92 zaměstnanců.

Členění zaměstnanců ÚOOÚ podle věku a pohlaví – stav k 31. 12. 2008

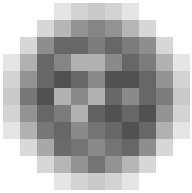
Věk	muži	ženy	celkem	%
18 – 20 let	0	0	0	0,0%
21 – 30 let	6	10	16	17,4%
31 – 40 let	7	6	13	14,1%
41 – 50 let	5	10	15	16,3%
51 – 60 let	21	19	40	43,5%
61 let a více	7	1	8	8,7%
Celkem	46	46	92	100,0%
%	50,0%	50,0%	100,0%	

Členění zaměstnanců ÚOOÚ podle vzdělání a pohlaví – stav k 31. 12. 2008

Vzdělání	muži	ženy	celkem	%
základní	0	0	0	0,0%
vyučen	1	0	1	1,1%
střední odborné	0	1	1	1,1%
úplné střední všeobecné	3	8	11	12,0%
úplné střední odborné	5	15	20	21,7%
vyšší odborné	0	1	1	1,1%
bakalářské	1	0	1	1,1%
vysokoškolské	35	20	55	59,8%
VŠ + vyšší kvalifikace	1	1	2	2,2%
Celkem	46	46	92	100,0%

Celkový údaj o vzniku a skončení pracovních poměrů zaměstnanců v roce 2008

	Počet
nástupy	11
odchody	11



Vyřizování žádostí a podnětů podle zákona o svobodném přístupu k informacím

Úřad v roce 2008 obdržel šest žádostí o poskytnutí informace dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím. Čtyři žádosti se týkaly výsledku správního řízení, které Úřad vedl s konkrétním subjektem. Zbylými dvěma žádostmi byl Úřad dotázán, v kolika případech udělil sankci za porušení povinností při zpracování osobních údajů městem či obcí a kolik Úřad v roce 2007 podal oznámení o skutečnostech nasvědčujících tomu, že byl při nakládání s osobními údaji spáchán trestný čin. Úřad všem uvedeným žádostem o informace vyhověl.

I v roce 2008 byl Úřad v několika případech žádán o konzultaci nebo o vyjádření v oblasti ochrany osobních údajů s tím, že tato žádost byla označena jako žádost o informace dle zákona o svobodném přístupu k informacím. Úřadu však povinnost poskytovat konzultace vyplývá z § 29 písm. h) zákona o ochraně osobních údajů a Úřad tuto svoji zákonnou povinnost naplňuje. Označovat žádost o vyjádření nebo dotaz adresovaný Úřadu za žádost o poskytnutí informace dle zákona o svobodném přístupu k informacím, je tedy nepřesné a nadbytečné. I v takovém případě totiž Úřad dotaz vyřizuje podle výše uvedeného ustanovení zákona o ochraně osobních údajů.