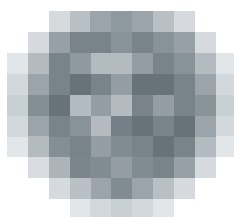


VÝROČNÍ ZPRÁVA

2012



**úřad pro ochranu
osobních údajů**
the office for personal
data protection

Ohlédnutí předsedy Úřadu za rokem 2012



Uplynulý rok je třeba hodnotit jako rok nových trendů a technologií. Úřad pro ochranu osobních údajů je stále konfrontován s realitou, která znamená na jedné straně zvýšení uživatelského komfortu díky miniaturizaci technologií a propojování nejrůznějších systémů – ale na straně druhé nárůst počtu centrálních úložišť dat, těžce zranitelných, dojde-li k útoku zejména na citlivá data.

Do nového roku 2012 Úřad vstoupil vybaven novou kompetencí při tzv. data breaches – tj. v oblasti zpracování osobních údajů v elektronických komunikacích, kdy Úřadu vzniká povinnost sledovat situaci a kontrolovat účinnost jejího řešení podnikatelem poskytujícím veřejně dostupnou službu elektronických komunikací; takový podnikatel, zjistí-li, že došlo k narušení zabezpečení ochrany osobních, provozních a lokalizačních údajů a důvěrnosti komunikace, musí tuto skutečnost Úřadu bez zbytečného odkladu oznámit.

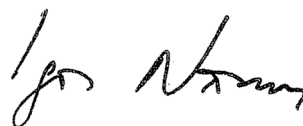
Další výzvou je pro Úřad nový právní rámec ochrany osobních údajů v EU, kde se řada nových trendů jako je „privacy by design“ a „privacy impact assessment“ již stala součástí budoucí právní úpravy podmínek ochrany osobních údajů a nikoliv jen holou proklamací těchto zásad

povinnými osobami na internetu. I když projednávání nového právního rámce Evropskou komisí zatím pokračuje poměrně pomalým tempem, dá se již dnes předvídat, kudy by se měly příští dozorové kompetence Úřadu ubírat. Oceňuji, že v tomto smyslu naše vláda nezůstává pozadu. Pevně také věřím, že od následujícího roku bude systematicky dodržována nová povinnost, kterou vláda schválila, tj. že budou vyhodnocovány dopady do soukromí už při předkládání každé nové právní normy. Předejde se tak situacím, kdy jsou možná úskalí související s ochranou osobních údajů odhalována až poté, co jsou zákony přijaty.

Pokud zmiňuji nové pojmy a trendy v oblasti rozvoje služeb informační společnosti, pak nemohu opomenout doslova každodenně diskutované téma rozvoje a využívání „cloud computingu“. Česká republika rozhodně není žádnou výjimkou a bude se s touto problematikou muset vyrovnat. Proto jsme velmi přivítali, když v červenci 2012 vydala Pracovní skupina pro ochranu údajů, zřízená podle článku 29 směrnice 95/46/ES stanovisko č. 5/2012 zabývající se „cloud computingem“. Z tohoto dokumentu je zřejmé, jak je problematika ochrany osobních údajů úzce spojena s vývojem a aplikací nejnovějších technologií a jak je nezbytné již ve fázi projektování nových služeb mít na mysli jak roli poskytovatele služeb „cloud computingu“, tak postavení uživatelů této služby pod zorným úhlem odpovědnosti jednotlivých aktérů podle zákona o ochraně osobních údajů.

O tom, že nejsme slepí a hluší k nástupu těchto trendů, svědčí řada jednání a vystoupení zástupců Úřadu na konferencích zaměřených právě na nové technologie a ochranu osobních údajů s jejich rozvojem spojenou. Také nové trendy v používání sledovacích systémů a kamer jako jsou fotopasti a další nasazování sledovací techniky – používání kamer sledujících silniční provoz z aut, nebo rozvoj „chytrého“ bydlení – přinesly Úřadu výzvu situací se zabývat nejen z pohledu bezprostřední aplikace zákona o ochraně osobních údajů, ale i v úvahách o možných dopadech na soukromí sledovaných osob.

Jsem rád, že se na Úřad obrací řada občanů a organizací, které upozorňují na nešvary současné doby, kdy je velmi snadné pronikat do dříve ryze soukromých sfér každého z nás. Úřad sice nemá absolutní dozor v oblasti ochrany soukromí, ale v oblasti zpracovávání osobních údajů se snaží vytvářet takové prostředí, aby mohl podporovat ty směry a trendy, které budou zaručovat a posilovat právo jednotlivce na ochranu před neoprávněným zpracováním jeho osobních údajů.



Igor Němec

Obsah

ÚŘAD V ČÍSLECH 2012	9
KONTROLNÍ ČINNOST ÚŘADU	12
■ KONTROLNÍ PLÁN PRO ROK 2012	12
I. Obecná témata pro zaměření kontrolní činnosti inspektorů Úřadu	13
1. Informační systémy veřejné správy	13
2. Informační systémy v oblasti soukromoprávní	14
3. Zpracovávání a zpřístupňování osobních údajů v oblasti prevence kriminality a boje proti terorismu	16
II. Kontroly z kontrolního plánu 2011, dokončené v roce 2012	17
Kontrola ČSÚ – sčítání lidu, domů a bytů v roce 2011	17
Kontrola soukromých subjektů, které podnikají v oblasti poskytování sociální péče	17
Kontrola zaměřená na zpracování osobních údajů v souvislosti s používáním pasivních identifikačních náramků pro pacienty	17
Kontrola zákaznických karet	18
Kontrola údajů zákazníků společnosti Alza.cz	18
Kontrola dodržování pravidel pro zpřístupňování údajů v oblasti telefonie	18
Kontrola povinností vyplývajících ze vztahů mezi správcem a zpracovatelem	19
III. Kontroly zahájené v roce 2012 na základě podnětu předsedy	19
Kontrola Vrchního státního zastupitelství v Praze	19
Kontrola subjektu Česká pošta	19
Kontrola subjektu Vězeňská služba České republiky	19
Kontrola Společenství vlastníků jednotek, Komárov 518	20

IV. Kontroly zahájené v roce 2011 na základě podnětu předsedy a dokončené v roce 2012	20
Kontrola Středočeského kraje – poskytování účelového daru na úhradu regulačních poplatků	20
Kontrola Městského soudu v Praze – zpracování osobních údajů stěžovatelů	21
■ POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI	23
Databáze profilů DNA	23
Zastupitelský úřad v Moskvě	24
Právo na informace při respektování práva na ochranu osobních údajů	26
Zpracování osobních údajů v souvislosti se vznikem nájmu a následným pronájmem bytů ve správě statutárního města	28
Osobní údaje dlužníků zveřejněné na internetových stránkách Společenství vlastníků bytových jednotek	29
FK Teplice	30
Internetové soutěže pro děti	31
Zdravotnictví	32
Kontrola zaměřená na zpracování osobních údajů prostřednictvím elektronické zdravotní knížky – společnost IZIP, a.s.	32
Kontrola zaměřená na zpracování osobních údajů prostřednictvím zákaznických karet – společnost Česká lékárna, a.s. (sítě lékáren Dr. Max)	34
Kontrola zaměřená na předávání údajů o pacientech v rámci screeningu onkologických onemocnění	35
Kontrola vedení zdravotnické dokumentace ve zdravotnickém zařízení	36
Podnět směřující proti Všeobecné zdravotní pojišťovně ČR	38
Kontrola zaměřená na zpracování osobních údajů v souvislosti s používáním pasivních identifikačních náramků pro pacienty – Nemocnice Na Homolce	38
Kamerové systémy	39
Vrchní státní zastupitelství v Praze	39
Kamerový systém v provozovně	41
Kamerový systém v zařízení sociální péče	43
Městský kamerový systém	43
Letiště Praha – kontrola zaměřená na zpracování osobních údajů prostřednictvím záznamů z kamerových systémů umístěných ve veřejně přístupných prostorách letiště	46
Kamerový systém v bytovém domě	48
Nakládání s citlivými osobními údaji klientů Domova důstojného stáří a zpracovávání jejich osobních údajů prostřednictvím kamerového systému s umístěním kamer na pokojích a společných prostorech	52
■ VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ	55
■ POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ	58
„Falešné“ smlouvy	58
Zveřejňování informací (fotografií nebo částí záznamů) pořízených kamerovým systémem za účelem odhalení pachatelů protiprávního jednání	60

■ POZNATKY ZE SOUDNÍCH PŘEZKUMŮ	62
Pravomoc Úřadu ke kontrolní činnosti v oblasti správy daní je dána; zákon o ochraně osobních údajů se na zpracování osobních údajů v oblasti správy daní vztahuje	62
Na výkon dozoru ze strany Úřadu nemá podatel subjektivní právo, a příslušné podání je tedy pouze podnětem k uplatnění dozorčího práva Úřadu, přičemž informace Úřadu o způsobu vyřízení podnětu je toliko sdělením Úřadu, a nikoli rozhodnutím podle § 65 zákona č. 150/2002 Sb., soudní řád správní	63
Za souhlas podle § 4 písm. n) zákona o ochraně osobních údajů nelze považovat pouhé neprojevení nesouhlasu subjektu údajů se zpracováním osobních údajů	64
Za nevyžádané obchodní sdělení podle zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), se nepovažuje individuální reakce na konkrétní nabídku a není jí ani konkrétní protinabídka k nabídce vyplývající z podaného inzerátu	65
Plošné a nerozlišující užití kamerového systému je v rozporu s ustanovením § 5 odst. 2 písm. e) části věty za středníkem zákona o ochraně osobních údajů ukládajícím šetřit právo zaznamenávaných osob na ochranu soukromí a osobního života	65
■ REGISTRACE	66
■ PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ	70
LEGISLATIVNÍ ČINNOST	73
STYKY SE ZAHRANIČÍM A MEZINÁRODNÍ SPOLUPRÁCE	77
ÚŘAD, SDĚLOVACÍ PROSTŘEDKY A KOMUNIKAČNÍ NÁSTROJE	82
Kontakty s médii	83
Šíření znalostí o ochraně osobních údajů	83
Aplikace zákona o ochraně osobních údajů v rámci komunikace Úřadu s odpovědnými subjekty	85
Aktivity Úřadu v komunikaci s odbornou veřejností	86
Knihovna a publikace Úřadu	88
Webové stránky Úřadu	88

INFORMAČNÍ SYSTÉM ORG	89
PROJEKT „OPTIMALIZACE PROCESŮ ÚOOÚ“	92
PERSONÁLNÍ OBSAZENÍ ÚŘADU	94
HOSPODAŘENÍ ÚŘADU	96
POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ	101

Úřad v číslech 2012

Dotazy a konzultace	dotazy ČR	2503
	zahraničí	47
	konzultace	2358
	státní správě	139
	samosprávě	190
	právníkům osobám	307
	fyzickým osobám	
	podnikajícím fyzickým osobám	257 1548
Podání a stížnosti	přijaté podněty dle zákona o ochraně osobních údajů	1319
	stížnosti předané ke kontrole	197
Nevyžádaná obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	7933
	vyřešených podnětů	3772
	zahájených kontrol	87
	ukončených kontrol	88
	správních rozhodnutí o pokutě	23
Kontroly (vyjma kontrol týkajících se zákona č. 480/2004 Sb.)	zahájeno	129
	ukončeno	138
	předáno jiným státním úřadům	2
	napadeno námitkami	16
	námitkám vyhověno	3
	nevyhověno	7
	převážně vyhověno	0
	převážně nevyhověno	5

Správní trestání	správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb.	118
	přestupková řízení podle zákona č. 101/2000 Sb.	21
	správní a přestupkové řízení podle zákona č. 101/2000 Sb. – § 44 a, 45 a	3
	přestupková řízení o porušení zákona č. 159/2006 Sb., o střetu zájmů	0
	rozklady napadená rozhodnutí o porušení zákona	43
	zamítnutých rozkladů	31
	zrušeno a vráceno k novému projednání	4
	zrušených rozhodnutí a zastaveno řízení	8
	změna rozhodnutí	9
	Soudní přezkum (Pozn.: * celkem od r. 2001)	podaných žalob k soudu
	zamítnutých žalob soudem	5
	zrušených rozhodnutí soudem	3
	ukončených/neukončených soudních řízení od r. 2001	59/41
Registrace	přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.)	5169
	zaregistrovaná zpracování	4618
	dosud v řízení	969
	zrušené registrace	78
	oznámení o změně zpracování	811
	řízení podle § 17	108
	zastaveno (nedochází k porušení zákona)	100
	zastaveno z procesních důvodů	
	(např. oznámení vzato zpět)	6
	nepovoleno	2
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	18
	rozhodnutí o povolení předávání	13
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	5
Oznámení podle zákona č. 127/2005 Sb.	došlých oznámení	2
	vyřízených jako opodstatněné	1
	vyřízených jako neopodstatněné	1

Stížnosti podle § 175 správního řádu	přijatých stížností	26
	vyřízených jako důvodné	5
	vyřízených jako částečně důvodné	5
	vyřízených jako bezdůvodné	16
Žádosti podle zákona č. 106/1999 Sb.	přijatých žádostí	42
	zcela vyhověno	29
	částečně vyhověno	10
	odmítnutých žádostí	3
Publikované materiály	Věstník Úřadu (počet částek)	3
	Bulletin Úřadu (počet čísel)	1
Tiskové konference	pravidelné	2
	mimořádné	0
Připomínkované legislativní návrhy	zákony	85
	prováděcí předpisy	94
	návrhy nařízení vlády	14
	návrhy vyhlášek	80
	ostatní	55
	zahraniční materiály	76

Kontrolní činnost Úřadu

KONTROLNÍ PLÁN PRO ROK 2012

V rámci svých dozorových kompetencí vyplývajících ze zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“), zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) a zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), se v roce 2012 Úřad pro ochranu osobních údajů (dále také „Úřad“) zabýval aktuálními tématy a otázkami, které mají široký dopad a ovlivňují zpracovávání osobních údajů v celospolečenském měřítku.

Úřad, který se tradičně zapojil do významných mezinárodních aktivit v oblasti zpracovávání osobních údajů, využil svých dosavadních zkušeností a nabídl možnost společné kontrolní aktivity s některým z úřadů v okolních státech, zejména v oblasti předávání nebo zpřístupňování osobních údajů za situace, kdy je odpovědný subjekt usídlen mimo území České republiky. Výzvou je v tomto ohledu dokument WP 29 č. 8/2010, který se zabývá podmínkami pro aplikovatelnost práva jednoho členského státu na území jiného členského státu EU, případně třetí země.

Dalším novým impulzem pro plánování kontrolních aktivit v roce 2012 byla změna zákona č. 480/2004 Sb., o některých službách informační společnosti, provedená zákonem č. 468/2011 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, a některé další zákony, jež vyplynuly ze změn některých přístupů pro aplikaci práva na ochranu osobních údajů v oblasti služeb informační společnosti. Rovněž tato změna přinesla rozšíření kontrolních kompetencí Úřadu v oblasti služeb elektronických komunikací, kdy nově bude podnikatel poskytující veřejně dostupnou službu elektronických komunikací povinen oznamovat Úřadu porušení ochrany osobních údajů, které zpracovává.

V souladu s § 31 zákona o ochraně osobních údajů vyjádřil předseda Úřadu tento svůj záměr a po projednání s inspektory Úřadu vydal kontrolní plán pro rok 2012:

I. OBECNÁ TÉMATA PRO ZAMĚŘENÍ KONTROLNÍ ČINNOSTI INSPEKTORŮ ÚŘADU

1. INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

Zpracovávání osobních údajů orgány státu patří mezi oblasti, které Úřad pravidelně monitoruje. Proto se i v roce 2012 kontrolní záměry věnovaly jak velkým databázím sdružujícím rozsáhlé skupiny dat a jejich zpracovávání, tak i dílčí problematice v této oblasti, která může vyplývat z povinností odpovědných subjektů vycházejících ze zvláštních zákonů.

V návaznosti na tento záměr byla provedena kontrola zabezpečení ochrany osobních údajů občanů při plnění ustanovení zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, ze strany obcí a měst. Inspektor provedl v rámci tohoto bodu plánu kontrol dvě kontroly: kontrolu Statutárního města Mladá Boleslav v období od 25. dubna do 4. června 2012, která byla zakončena bez zjištění porušení zákona; a kontrolu Města Poděbrady v období od 24. června do 9. října 2012, která byla rovněž ukončena bez zjištění porušení zákona. Více o průběhu a výsledcích těchto kontrol lze nalézt v části *Poznatky inspektorů z kontrolní činnosti*.

Oblastí informačních systémů veřejné správy se měla zabývat také kontrola ochrany osobních údajů v podmínkách Národního zdravotnického informačního systému. Vzhledem k tomu, že počátkem roku 2012 podala skupina senátorů ústavní stížnost týkající se celé právní úpravy zákona č. 372/2011 Sb., o zdravotnických službách, jehož součástí je právní úprava podmínek pro vedení Národních zdravotnických registrů, nebyla kontrola provedena.

Další významnou kontrolou provedenou v této oblasti byla kontrola plánovaná na zabezpečení osobních údajů v Jednotném informačním systému práce a sociálních věcí podle § 4a zákona č. 73/2011 Sb. Ministerstvem práce a sociálních věcí. Kontrola, kterou inspektori zahájili v březnu 2012, nebyla dosud ukončena.

Dále v této oblasti proběhly dvě kontroly na dodržování povinností správce a zpracovatele v souvislosti s vydáváním a využíváním karty sociálních systémů podle zvláštního právního předpisu. V této souvislosti inspektorka zahájila v říjnu 2012 kontrolu Úřadu práce České republiky a v listopadu 2012 kontrolu Ministerstva práce a sociálních věcí jako správce JIS. Kontroly nebyly dosud ukončeny.

V souladu se závazky České republiky v oblasti III. pilíře EU včetně Schengenské úmluvy a v návaznosti na výsledky hodnocení jejího dodržování, které proběhlo v únoru 2012, byla provedena pravidelná kontrola Policie ČR vyplývající z Národního schengenského plánu 2011, který byl vládou schválen dne 5. ledna 2011. Kontrola se zaměřila na oblast vkládání osobních údajů podle článku 96 Schengenské prováděcí úmluvy (SPÚ) a na postup při vyřizování žádostí subjektů údajů o přístup k osobním údajům, uplatnění jejich práva na opravu/výmaz osobních údajů zpracovávaných v SIS (čl. 109 a 110 SPÚ), na bezpečnostní opatření při zajištění přístupu oprávněných subjektů k údajům uloženým v SIS a při následném nakládání s nimi, včetně rozsahu, postupů a účinnosti vnitřní kontroly Policie ČR (kontrola logů, vyplývající z čl. 101 SPÚ).

Kontrola konstatovala porušení ustanovení § 13 odst. 1, 2 a 3 zákona o ochraně osobních údajů, neboť nebyla přijata dostatečná opatření před neoprávněným přístupem k osobním údajům osob v Schengenském informačním systému, když odpovědný subjekt v době provádění kontroly nenevidoval konkrétní důvod dle ustanovení § 63 zákona o Policii ČR při lustraci v SIS, ačkoliv policista má oprávnění k prokázání totožnosti hledané osoby jen na základě důvodů uvedených v tomto ustanovení.

V kontextu závazků ČR v oblasti II. pilíře byla zahájena také kontrola informačního systému EURODAC, která pokračuje i v roce 2013.

Dále byla provedena kontrola plnění dohod v oblasti „Společná zahraniční a bezpečnostní politika“ (předávání a ochrana osobních údajů v silniční dopravě v rámci tzv. Prümské úmluvy v souladu s plněním dohod zemí EU v Schengenském prostoru), která současně vycházela i z obecného záměru této části kontrolního plánu. Kontrola Ministerstva dopravy byla v dané souvislosti zahájena v září 2012. Předmětem kontroly bylo dodržování povinností správce, případně zpracovatele, stanovených zákonem o ochraně osobních údajů při zpracování osobních údajů subjektů údajů v souvislosti s vedením centrálního registru vozidel, se zaměřením na výměnu informací o vozidlech, zejména pak v rámci Prümské úmluvy, anebo jiné mezinárodní právní normy, kterou je Česká republika vázána, včetně převodu systému z Ministerstva vnitra na kontrolovaného a vstupů a výstupů ze systému. Kontrola nebyla dosud ukončena.

2. INFORMAČNÍ SYSTÉMY V OBLASTI SOUKROMOPRÁVNÍ

V návaznosti na aktuální poznatky a zkušenosti se kontrolní aktivity Úřadu v této oblasti zaměřily na:

- **podmínky zpracování osobních údajů v souvislosti s nabídkou a akceptací služeb**, jejichž součástí může být vydávání věrnostních zákaznických karet ve všech typech služeb; Úřad se zaměřil na dodržování povinností odpovědných osob při sběru těchto informací přímo od jednotlivých subjektů a jejich dalšího legitimního zpřístupňování příjemcům;
- **podmínky zpracování osobních údajů cestujících osob; kontrola Českých aerolinií, a.s.**, proběhla ve dnech 25. dubna – 16. října 2012 a nezjistila porušení zákona o ochraně osobních údajů. Kontrolovaný subjekt byl pouze vyzván k provádění pravidelné kontroly aktuálnosti informací na svých webových stránkách ve vztahu k předávání osobních údajů třetím osobám (webové stránky se v době provádění kontroly právě měnily). Kontrolující inspektorka upozornila kontrolovaného, že právě neposkytnutí informací v zákonném rozsahu dle § 11 zákona o ochraně osobních údajů může mít za následek spáchání správního deliktu podle § 45 odst. 1 písm. f) zákona o ochraně osobních údajů;
- **zpracování osobních údajů zákazníků v souvislosti s nabídkou prodeje zboží a služeb** (provoz kamerového systému, zákaznické karty). V rámci plnění tohoto úkolu bylo v roce 2012 zahájeno několik kontrol:
 - Jedna z nejvýznamnějších co do počtu zpracovávaných údajů je databáze CERD. Kontrola tohoto subjektu nebyla v roce 2012 ukončena.
 - Dále byla provedena kontrola společnosti IKEA Česká republika, s.r.o. Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených zákonem o ochraně osobních údajů v souvislosti se zpracováním osobních údajů zákazníků IKEA.

- Kontrola byla ukončena v červnu 2012 a jejím výsledkem bylo zjištění, že kontrolovaný subjekt neporušuje prověřované a posuzované povinnosti ukládané zákonem o ochraně osobních údajů;
- zpracování osobních údajů cestujících osob při provozu kamerových systémů v prostředcích hromadné přepravy**

V roce 2012 byla ukončena kontrola městského kamerového systému v Praze. Předmětem kontroly bylo dodržování povinností stanovených zákonem o ochraně osobních údajů se zaměřením na ochranu osobních údajů, zpracovávaných prostřednictvím Městského kamerového systému hl. m. Prahy. Město určilo účel a prostředky zpracování osobních údajů, je tedy ve smyslu ustanovení § 4 písm. j) zákona o ochraně osobních údajů v pozici správce osobních údajů. Dle § 5 odst. 1 písm. a) uvedeného zákona stanovil správce osobních údajů jako účel zpracování osobních údajů zajišťování veřejného pořádku, ochranu zdraví obyvatel a návštěvníků města, ochranu majetku a bezpečnost silničního provozu.

Dle ustanovení § 5 odst. 1 písm. d) zákona o ochraně osobních údajů je správce povinen „shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu“. Vlastností kamerového systému, vyplývající z jeho fungování, je to, že nepřetržitě shromažďuje záznamy o všech aktivitách veškerých osob, které jsou právě v dosahu jednotlivých kamer. Kontrolou bylo zjištěno, že osobní údaje, resp. záznamy z kamerového systému, shromážděné na veřejných prostorech města v rozsahu zjištěném, významně přispívají k plnění stanovených účelů. Kontrolou nebylo zjištěno zpracování záznamů nad rámec stanovených účelů. Kontrola byla ukončena se závěrem, že hlavní město Praha neporušilo v souvislosti se zpracováním osobních údajů prostřednictvím integrovaného městského kamerového systému hlavního města Prahy zákon o ochraně osobních údajů;
 - podmínky zpracovávání osobních údajů osob při sjednávání nájemních smluv a dalších souvisejících institutů v oblasti bydlení**

Pro naplnění tohoto úkolu se v roce 2012 uskutečnilo několik kontrol, které se zaměřily na dodržování povinností odpovědných subjektů (bytová družstva, společenství vlastníků jednotek, obce) při shromažďování a dalším zpracovávání osobních údajů nájemníků a členů jejich domácností. Výsledkem těchto kontrol byla doporučení oddělovat údaje nezbytné pro sjednávání nájemních a užitelských smluv od údajů potřebných pro uzavření a plnění nájemních a užitelských vztahů. V souladu se záměrem Úřadu byla provedena kontrola zabezpečení ochrany osobních údajů občanů při správě agendy spojené s pronájmem bytů ve vlastnictví obcí a měst. Inspektor provedl kontrolu Statutárního města Kladna v termínu od 26. dubna 2012 do 9. srpna 2012, bez zjištění porušení zákona. Více o průběhu a výsledcích této kontroly lze nalézt v části *Poznatky inspektorů z kontrolní činnosti*;
 - podmínky pro zpracování osobních údajů zákazníků v oblasti nabídky zboží a služeb**

a to nejen v rámci zákona o ochraně osobních údajů, ale i další oblasti působnosti Úřadu týkající se některých služeb informační společnosti ve smyslu zákona, o některých službách informační společnosti. Inspektor provedl kontrolu u společnosti Alza.cz, a.s., a to bez zjištění porušení zákona. Více o výsledcích této kontroly lze nalézt v II. části této kapitoly – *Kontroly z kontrolního plánu 2011, dokončené v roce 2012*;

- **prověření ochrany osobních údajů v podmínkách činnosti výrobní a obchodní společnosti v oblasti fotovoltaiky**
Kontroly dvou soukromých společností, které se ve své činnosti zabývají výrobou elektřiny z fotovoltaických zdrojů, se soustředily na využívání kamerových systémů i k ostraze výrobních zdrojů. Kontroly nezjistily žádné porušení zákona o ochraně osobních údajů;
- **zpracování osobních údajů v souvislosti s nabídkou zboží a služeb v prostředí elektronických komunikací**
Pokud byly kontrolami zjištěny nedostatky spočívající v nedostatečném informování zákazníků, případně odchylky od povinností týkajících se marketingu, byla tato porušení kontrolovaným subjektům vytčena včetně sankcí;
- **provoz sledovacích systémů často souvisí s výkonem činnosti soukromé bezpečnostní služby**
V roce 2012 proběhla kontrola odpovědného subjektu Letiště Praha, která dosud nebyla pravomocně ukončena vzhledem k běhu lhůty pro vyřízení námitek proti kontrolnímu protokolu. Úřad v této souvislosti prověřil provozování bezpečnostního systému monitorujícího pohyb cestujících osob při průchodu letištními prostorami, což úzce souvisí s problematikou uváděnou v části 3., následující.

3. ZPRACOVÁVÁNÍ A ZPŘÍSTUPŇOVÁNÍ OSOBNÍCH ÚDAJŮ V OBLASTI PREVENCE KRIMINALITY A BOJE PROTI TERORISMU

V návaznosti na platnou právní úpravu podmínek pro uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí bylo nezbytné se zaměřit na:

- Plnění povinností České republiky v souvislosti s předáváním a zpracováváním informací v Schengenském informačním systému ve spojení s povinnostmi týkajícími se Vízového informačního systému. V této souvislosti proběhla kontrola dodržování podmínek pro zpracovávání osobních údajů za situace, kdy mezi správcem a zpracovatelem je uzavřena smlouva o zpracování informací podle § 6 zákona o ochraně osobních údajů.
- V této oblasti, která je již tradiční součástí dozorových aktivit Úřadu, se inspektoři zaměřili na kontroly plnění povinností České republiky v souvislosti s předáváním a zpracováváním informací v SIS a VIS. Úřad se proto již několik let věnuje kontrolám plnění povinností správce při ochraně osobních údajů v procesu udělování víz osobám ze zemí mimo schengenský prostor.
- Jako dříve v Makedonii, na Ukrajině a v Mexiku proběhly i tentokrát kontroly na zastupitelských úřadech zemí mimo EU (Kazachstán, Turecko, Rusko), zaměřené na přístup do SIS a zabezpečení osobních údajů žadatelů. Více lze nalézt v části *Poznátky inspektorů z kontrolní činnosti*.
- Podle plánu kontrol byla v září zahájena na Ministerstvu dopravy kontrola se zaměřením na jeho připravenost zpřístupnit v souladu s mezinárodními závazky České republiky některé údaje z **registru řidičů a registru vozidel** zahraničním subjektům. Kontrola nebyla před koncem roku 2012 ukončena.

II. KONTROLY Z KONTROLNÍHO PLÁNU 2011, DOKONČENÉ V ROCE 2012

Kontrola ČSÚ – sčítání lidu, domů a bytů v roce 2011

Ve dnech 2. června 2011 – 25. ledna 2012 proběhla kontrola Českého statistického úřadu, jejímž předmětem bylo celkové posouzení souladu průběhu sčítání lidu, domů a bytů v roce 2011 se zákonem o ochraně osobních údajů.

Kontrola se zaměřila jak na prověření organizačně-bezpečnostních opatření dle § 13 zákona o ochraně osobních údajů, tak na kontrolu způsobu anonymizace sčítacích formulářů, které mají být předány do Národního archivu, a v neposlední řadě na prověření statistických údajů vzešlých ze sčítání, které budou zpracovávány Statistickým úřadem i po ukončení sčítání.

Pokud jde o organizačně-bezpečnostní opatření, kontrolující vyslovili pouze výtku v souvislosti s tím, že obálky s vyplněným formulářem bylo možné odeslat formou vložení do poštovní schránky, kdy se nedá ověřit, zda formuláře s osobními údaji byly skutečně do Statistického úřadu řádně doručeny. Organizačně-bezpečnostní opatření, až na uvedené, byla nicméně v souladu se zákonnou úpravou, ani v uvedené výtce nebylo prokázáno porušení ustanovení § 13 zákona o ochraně osobních údajů.

Předávání formulářů do Národního archivu doposud neproběhlo, tudíž ani nelze konstatovat soulad či nesoulad se zákonem, při kontrole však byly navrženy takové změny postupů, aby byla anonymizace zajištěna. Statistický úřad se k těmto návrhům kontrolujících staví souhlasně.

Ohledně statistických údajů, které budou nadále zpracovávány i po ukončení sčítání, byl ČSÚ rovněž kontrolujícími upozorněn na principy, které musí být dodrženy, což znamená, že po uplynutí tříleté lhůty nelze zpracovávat žádné osobní údaje vzešlé ze sčítání lidu 2011 – tedy žádné takové údaje, které by samotné nebo v kombinaci s jinými údaji mohly osobu – subjekt údajů jednoznačně identifikovat.

Kontrola soukromých subjektů, které podnikají v oblasti poskytování sociální péče

Kontroly byly vykonány u tří společností s r. o. Dvě z těchto kontrol proběhly v součinnosti s Úřadem veřejného ochránce práv a zjistily porušení zákona o ochraně osobních údajů, hlavně při používání kamerových systémů se záznamem, kdy nebyly zcela respektovány podmínky pro zpracovávání těchto informací s ohledem na soukromí monitorovaných osob. Tyto kontroly byly ukončeny sankcí, která byla uložena ve správním řízení. Třetí kontrola byla co do kontrolních úkonů s kontrolovaným subjektem ukončena v roce 2012, ale kontrolní protokol bude dopracován a předán až v lednu 2013.

Kontrola zaměřená na zpracování osobních údajů v souvislosti s používáním pasivních identifikačních náramků pro pacienty

Kontrolou bylo zjištěno, že nedošlo k porušení povinnosti správce osobních údajů při zpracování osobních údajů dle zákona o ochraně osobních údajů v souvislosti s identifikací pacientů prostřednictvím pasivních identifikačních náramků, ani v souvislosti se zveřejněním osobních a citlivých údajů pacienta na internetu. Detailní informace v kapitole *Poznatky inspektorů z kontrolní činnosti*.

Kontrola zákaznických karet

Kontrolováno bylo zpracování osobních údajů prostřednictvím zákaznických karet společností Česká lékárna, a.s. (síť lékáren Dr. Max). Kontrola konstatovala, že ke zpracování dochází na základě souhlasu spotřebitelů – subjektů údajů v souladu s informací, která jim byla náležitě poskytnuta. Detailní informace v kapitole *Poznatky inspektorů z kontrolní činnosti*.

Kontrola údajů zákazníků společnosti Alza.cz

Kontrola proběhla ve dnech 18. listopadu 2011 – 27. června 2012. Jejím předmětem bylo jednak zabezpečení osobních údajů zákazníků a dalších osob v souvislosti s obchodní činností při využití informačního systému a jednak dodržování podmínek stanovených pro šíření obchodních sdělení.

Provedenou kontrolou v oblasti šíření obchodních sdělení byly prověřeny podmínky zasílání obchodních sdělení, tak jak jsou stanoveny zákonem o některých službách informační společnosti. Kontrola poukázala na skutečnost, která není v praxi Úřadu nikterak ojedinělá, tedy že uživatelé e-mailových adres, případně telefonních čísel, poskytnou své údaje v souvislosti s nákupem zboží či učiní registraci na internetových stránkách poskytovatele služby. Kontrolovaný subjekt jednoznačně prokázal, že veškeré e-mailové adresy i telefonní čísla byla získána v souvislosti s prodejem jeho výrobků nebo služby. Proto v souvislosti se zasíláním obchodních sdělení nebyl vyžadován předchozí souhlas a údaje zákazníků byly využívány na základě jejich nákupu zboží.

Kontrola konstatovala, že na rozdíl od e-mailové komunikace neměli zákazníci využívající služby sms zpráv jasně a zřetelně poskytnuté možnosti jednoduchým způsobem, zdarma nebo na účet odesílatele odmítnout souhlas s takovýmto využitím svého elektronického kontaktu. V této souvislosti kontrola upozornila na problematiku plnění popsané povinnosti, a to zejména v případech obchodních sdělení zasílaných formou sms zpráv. Odesílatelé obchodních sdělení obvykle splní povinnost formou informace ve všeobecných obchodních podmínkách, nikoli však při každém jednotlivém sdělení. Proto bylo kontrolovanému subjektu inspektorem Úřadu doporučeno, jak má upravit texty sms zpráv, aby obsahovaly informaci o tom, jak lze jednoduchým způsobem zdarma nebo na účet odesílatele odmítnout souhlas se zasíláním sms zpráv obsahujících obchodní sdělení. Kontrolou současně nebylo prokázáno, že by se kontrolovaný dopustil porušení zákona o ochraně osobních údajů při zpracování osobních údajů zákazníků a dalších osob v souvislosti s obchodní činností.

Kontrola dodržování pravidel pro zpřístupňování údajů v oblasti telefonie

V souvislosti se záměrem Úřadu byl prověřen podnět směřující proti subjektu Telefónica O2, která doložila příslušnými dokumenty, že externí obchodník použil jednu e-mailovou adresu pro více účastníků. V dubnu 2012 bylo příslušným manažerem společnosti Telefónica O2 toto pochybení zjištěno, chybná e-mailová adresa byla z databáze účastníků odstraněna a obchodník byl potrestán. Vzhledem k výše uvedenému zjištění a v souladu s ustanovením § 29 odst. 1 písm. c) zákona o ochraně osobních údajů bylo zjištěné porušení zákona předmětem správního řízení vedeného Úřadem. Řízení bylo uzavřeno uložením pokuty.

Další kontrola telefonie se týkala zpracování údajů klientů společnosti Vodafone a předávání jejich údajů do databáze dlužníků vedené společností SOLUS. Kontrola konstatovala porušení § 5 odst. 1 písm. d) zákona – konkrétně zpracování nepřesných osobních údajů. Také v tomto případě bylo předmětné zjištění důvodem k zahájení správního řízení, které bylo uzavřeno uložením pokuty.

Kontrola povinností vyplývajících ze vztahů mezi správcem a zpracovatelem

za podmínek § 6 zákona o ochraně osobních údajů. V této souvislosti bylo provedeno několik kontrol odpovědných subjektů, které se v rámci zpracovávání osobních údajů rozhodly využít pro naplnění svých povinností správce součinnosti s druhým subjektem, jenž je v postavení zpracovatele. Z výsledků kontrol vyplývá, že nebyla zjištěna závažná pochybení týkající se obsahu jednotlivých smluv.

III. KONTROLY ZAHÁJENÉ V ROCE 2012 NA ZÁKLADĚ PODNĚTU PŘEDSEDY

Kontrola Vrchního státního zastupitelství v Praze

byla zahájena v návaznosti na veřejně publikované informace (záznam z kamerového systému) a s ohledem na podnět veřejnosti a předseda Úřadu rozhodl o provedení kontroly Vrchního státního zastupitelství v Praze, týkající se kamerových záznamů pořízených v sídle kontrolovaného, vzhledem k důvodnému podezření, že postupem jednajících osob odpovědných za provoz a zpřístupnění informací – osobních údajů monitorovaných osob – došlo k porušení povinností správce (případně zpracovatele) podle zákona o ochraně osobních údajů.

Impulem byla skutečnost, že vrchní státní zástupce uspořádal mimořádnou tiskovou konferenci, na které veřejně prezentoval záznam pořízený kamerovým systémem provozovaným kontrolovaným v budově Vrchního státního zastupitelství. Více o průběhu a výsledcích této kontroly lze nalézt v části *Poznátky inspektorů z kontrolní činnosti*.

Kontrola subjektu Česká pošta

navázala na podnět k zahájení správního řízení, který se týkal monitorování zaměstnanců České pošty, a byla reakcí na medializované informace o monitorování zaměstnanců České pošty prostřednictvím technologie GPS, jejich lokalizace, kdy zřejmě docházelo k nezákonnému zpracování osobních údajů zaměstnanců, získaných z osobních terminálů poštovních doručovatelů. Ke kontrole došlo také proto, že Úřad poskytl České poště konzultace a vyjádřil při nich už v letech 2010 a 2011 doporučení, která byla se zaznamenanou praxí v příkrém rozporu.

Kontrola proběhla ve dnech 25. dubna – 25. září 2012 a konstatovala porušení ustanovení § 5 odst. 2 zákona o ochraně osobních údajů, neboť neshledala právní titul pro soustavné zpracovávání osobních údajů, resp. monitorování pohybu doručovatelů/doručovatelek po okrsku určeném k výkonu jejich povolání. Česká pošta proti kontrolnímu zjištění podala námitky, které jsou v současné době předmětem posouzení předsedy Úřadu.

Kontrola subjektu Vězeňská služba České republiky

v souvislosti s veřejnou publikací fotografií vazebně stíhaných osob. Z veřejně dostupných zdrojů bylo zřejmé, že byly dne 2. a 5. června 2012 publikovány fotografie vazebně stíhaných osob, původně pořízené pro účely výkonu vazby a s ní souvisejícím zpracováváním osobních údajů.

Kontrola proběhla ve dnech 22. června – 3. prosince 2012 a konstatovala porušení ustanovení § 13 zákona o ochraně osobních údajů, neboť došlo k úniku osobních údajů z Vězeňského informačního systému. Na základě zásahu kontrolující inspektorky došlo k zásadní změně přístupových práv zaměstnanců Vězeňské služby. K osobním údajům vězňů osob

umístěných v jiné věznici mají nadále přístup pouze ti zaměstnanci Vězeňské služby ČR, kteří údaje nezbytně potřebují k výkonu své služby.

Kontrola Společenství vlastníků jednotek, Komárov 518

V roce 2012 se Úřad zabýval podnětem, jehož obsah se týkal porušení zákona o ochraně osobních údajů v souvislosti s instalací kamerového systému se záznamem v domě, v němž bydlí stěžovatel, který uvedl, že způsob provozu kamerového systému nepřípustně zasáhl do jeho soukromí a soukromí jeho rodiny. Protože tento stav podle názoru stěžovatele dále přetrvával i poté, co SVJ, Komárov 518, byla Úřadem uložena pokuta za porušení povinností správce podle zákona o ochraně osobních údajů, byla opakovaně provedena kontrola splnění uložených nápravných opatření určených kontrolním protokolem. Všechna uložená nápravná opatření však byla splněna, tudíž nebylo shledáno, že dochází k porušení zákona.

IV. KONTROLY ZAHÁJENÉ V ROCE 2011 NA ZÁKLADĚ PODNĚTU PŘEDSEDY A DOKONČENÉ V ROCE 2012

Kontrola Středočeského kraje – poskytování účelového daru na úhradu regulačních poplatků

Kontrola proběhla ve dnech 16. prosince 2011 – 15. února 2012 a konstatovala porušení ustanovení § 13 zákona o ochraně osobních údajů tím, že Středočeský kraj zveřejnil na webových stránkách www.kr.stredocesky.cz seznamy s osobními údaji těch, kterým byl poskytnut dar na úhradu regulačních poplatků u lékaře, či naopak bylo poskytnutí daru odmítnuto. Středočeský kraj tím umožnil neoprávněný přístup k osobním údajům třetím osobám. Předseda Úřadu nevyhověl námitkám, které podal Středočeský kraj, a Úřad rozhodl o správním postřetí a uložil pokutu.

Úřad v tomto řízení konstatoval, že je třeba postup Rady Středočeského kraje v dané věci posoudit z hlediska proporcionality mezi právem na informace a právem na ochranu soukromí, tedy zda je v dané věci vyšší zájem na poskytnutí informace, či na ochraně osobních údajů, a to vzhledem k tomu, že se jedná o velký rozsah osobních údajů, o velký počet subjektů údajů a u většiny žadatelů současně o relativně malé finanční částky. Informace o poskytnutí daru na úhradu regulačních poplatků je přitom svým charakterem obdobná poskytnutí veřejných prostředků v sociální, resp. zdravotní oblasti ve smyslu § 8b odst. 2 zákona č. 106/1999 Sb., jelikož z výše daru lze dovozovat i výši regulačních poplatků uhrazených konkrétní osobou. Při zveřejňování informace je obecně nezbytné rozlišovat dvě situace, a to na jedné straně zveřejnění informace určené pro oprávněné osoby (tj. v tomto případě žadatele) a na druhé straně zveřejnění prostřednictvím webových stránek, kdy dochází ke zpřístupnění informací včetně osobních údajů nejen uvedeným (oprávněným) osobám, ale neomezenému počtu příjemců. Podle § 5 odst. 7 zákona č. 106/1999 Sb. může povinný subjekt za podmínek stanovených tímto zákonem zveřejnit i další informace (než informace povinně zveřejňované podle tohoto zákona, resp. informace poskytované na základě žádostí jednotlivců). Protože však zákon č. 106/1999 Sb. pro poskytování osobních údajů odkazuje v § 8a na podmínky plynoucí ze zákona o ochraně osobních údajů, je nutné i v tomto případě uplatnit test proporcionality, jenž je ve vztahu k osobním údajům vyjádřen především v § 5 odst. 3 a § 10 zákona o ochraně osobních údajů.

Zveřejňování osobních údajů způsobem umožňujícím dálkový přístup (prostřednictvím internetu) pro předem neurčený okruh osob z vlastní iniciativy povinného subjektu přitom

zjevně zasahuje do osobní sféry jednotlivce daleko podstatnějším způsobem než jejich zpřístupnění na základě individuální žádosti konkrétní fyzické nebo právnické osoby.

Omezení základních práv a svobod je podle testu proporcionality možné pouze tehdy, jedná-li se o zásah, který je pro dosažení sledovaného cíle vhodný, nutný a přiměřený. Kritériem pro nutný zásah je skutečnost, že není možné ze strany daného subjektu užití jiného, objektivně srovnatelného prostředku, jímž by docházelo k menšímu zásahu do chráněných zájmů na straně dotčených subjektů údajů. Za přiměřený je považován takový zásah, kdy je možno očekávat, že dosažený prospěch realizací dané činnosti bude větší nežli nepříznivý následek jí způsobený – v tomto případě zejména v podobě míry zásahu do osobnostních práv dotčených subjektů údajů.

V případě žadatelů, jejichž žádosti byly vráceny, tito zjevně nebyli v danou chvíli příjemci veřejných prostředků, tudíž nebyl žádný právní důvod ke zveřejnění jejich osobních údajů. V případech úspěšných žadatelů pak Úřad uvážil, že Středočeský kraj svou povinnost informovat o vynaložení veřejných prostředků mohl splnit tak, že by prostřednictvím svých webových stránek poskytl informaci o celkovém počtu příjemců, kterým byl dar poskytnut, a o celkové výši finančních prostředků takto vynaložených, o struktuře těchto veřejných prostředků apod.

Výše uvedené tak vede k jednoznačnému závěru, že ani právo na přístup k informacím není neomezené; i pokud by bylo možné považovat za zákonný podklad jednání Středočeského kraje zákon č. 106/1999 Sb. a legitimním cílem jeho jednání by bylo zvýšení transparentnosti, resp. veřejná kontrola použitých veřejných prostředků, nelze zveřejnění osobních údajů žadatelů prostřednictvím internetu v rozsahu vymezeném ve výroku tohoto rozhodnutí považovat za přiměřené, resp. nezbytné, neboť způsobuje nepřiměřený zásah do práva na ochranu soukromého a osobního života.

Kontrola Městského soudu v Praze – zpracování osobních údajů stěžovatelů

Úřad obdržel stížnost od podatele pro důvodné podezření, že o jeho osobě soud nezákonně a nedůvodně sbírá informace a údaje a tyto následně šíří, přičemž mu bylo odmítnuto nahlédnutí do spisu usnesením soudce. Stěžovatel měl za to, že soud provádí zpracování osobních údajů, které je v rozporu s ochranou jeho soukromého a osobního života a dále je v rozporu se zákonem o ochraně osobních údajů, neboť osobní údaje jsou nepřesné a jsou dále šířeny směrem k policejním složkám, zpravodajské službě a dalším subjektům, a žádal Úřad o prošetření, včetně vyžádání příslušných spisů soudu.

Dále Úřad obdržel stížnost jiné stěžovatelky na porušení zákona o ochraně osobních údajů totožným soudem v souvislosti se ztrátou, event. odcizením spisu. Z podání vyplynulo, že přestože je stěžovatelka oprávněnou osobou, je jí od určitého data odepíráno právo nahlédnout do předmětného spisu s tím, že se ztratil a nyní se rekonstruuje.

Ze strany soudu byly v této souvislosti uváděny různé důvody a je zjevné, že v evidenci archivovaných soudních spisů je chaos, odpovědné osoby nemají přehled o pohybu předmětného spisu, soud nepřijal všechna potřebná opatření, aby nemohlo dojít k neoprávněnému přístupu, zpracování či jinému zneužití osobních údajů, čímž porušil povinnosti uvedené v § 13 zákona o ochraně osobních údajů. Jelikož z podání vyplývalo možné porušení plnění povinností soudu podle § 13–15 zákona o ochraně osobních údajů, byla kontrola zaměřena na jejich plnění. Kontrola proběhla ve dnech 30. listopadu 2011 až 4. dubna 2012.

Soud je orgánem státní správy soudů a jeho úkolem je vytvářet soudům podmínky k řádnému výkonu soudnictví, zejména po stránce personální, organizační, hospodářské, finanční

a výchovné, a dohlížet způsobem a v mezích zákona na řádné plnění úkolů soudům svěřených (§ 118 a 119 zákona č. 6/2002 Sb., o soudech a soudcích, v platném znění).

Předmětný spis obsahující osobní údaje stěžovatele, který byl předmětem stížnosti stěžovatele, byl soudem založen poté, co bylo zjištěno jeho časté zastupování účastníků řízení jako obecný zmocněnec. Příslušné ustanovení občanského soudního řádu upravuje možnost rozhodnutí soudce o nepřipuštění zastoupení obecným zmocněncem v případě, že vystupuje v různých věcech opětovně. Přehled o zastupování stěžovatele ve funkci obecného zmocněnce byl získán z evidenčních pomůcek kontrolovaného soudu a byl následně poskytnut k případnému využití soudcům odvolacích senátů soudu, předsedům obvodních soudů. Uvedený postup byl v souladu s výkonem státní správy soudů dle § 118 zákona o soudech a soudcích. Kontrolovaný soud jako orgán státní správy postupoval v případě stěžovatele v souladu s ustanovením § 118 zákona č. 6/2002 Sb., o soudech a soudcích v platném znění, a nedošlo tak ke shromažďování osobních údajů v rozporu se zákonem o ochraně osobních údajů.

Dále bylo kontrolou v souvislosti s namítanou ztrátou spisu stěžovatelky prověřeno plnění přijatých opatření při zabezpečení osobních údajů vyplývajících z ustanovení § 13 zákona o ochraně osobních údajů, jejich kontrola podle § 14 a plnění povinnosti mlčenlivosti podle § 15. Nebylo zjištěno, že by došlo k neoprávněnému nebo nahodilému přístupu k osobním údajům nebo k jinému zneužití osobních údajů ze spisu.

Z vedené evidence oběhu spisu bylo pouze dohledáno, že spis byl vrácen z Krajského soudu, ale pracovníkem soudu již nebylo vyznačeno jeho další zařazení. Pracovník kontrolovaného soudu tak porušil povinnost dle § 14 zákona o ochraně osobních údajů, neboť nezajistil řádné uchování spisu (potvrzující dohledatelnost spisu) v rozporu s pokynem soudu.

Kontrolou bylo prokázáno, že soud přijal nejen potřebná opatření ve smyslu § 13 zákona o ochraně osobních údajů, ale zajistil také splnění povinnosti mlčenlivosti podle § 15 téhož zákona (jmenovitě v pracovních smlouvách zaměstnanců).

Nad rámec uvedeného právního závěru bylo konstatováno, že k uvedenému pochybení došlo v listopadu 2008 a případná odpovědnost právnické osoby za správní delikt již podle § 46 odst. 3 zákona o ochraně osobních údajů zanikla. Soud pak v průběhu kontroly nad rámec povinností dle vnitřního kancelářského řádu provedl další opatření.

Porušení právní povinnosti fyzickou osobou (zaměstnancem) dle § 14 zákona o ochraně osobních údajů nenaplňovalo skutkovou podstatu přestupku dle § 44 tohoto zákona.

POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

DATABÁZE PROFILŮ DNA

Velmi lákavou se jeví myšlenka, že prostřednictvím databáze profilů DNA všech obyvatel České republiky (nebo ještě lépe všech lidí na Zemi) by bylo možno při vyšetřování kteréhokoli trestného činu pomocí srovnání profilů DNA snadno nalézt pachatele. A pokud se nejedná o reálnou existenci databáze profilů DNA všech občanů České republiky, tak lze alespoň uvažovat o existenci databáze profilů DNA všech zločinců, míněno osob odsouzených za úmyslný trestný čin, protože určitá míra recidivy těchto osob po odpykání trestu je velmi častým, statisticky podloženým jevem. Je třeba si ovšem uvědomit, že se vychází ze dvou předpokladů: jedná se o trestný čin, při kterém je hledání pachatele prostřednictvím DNA možné (tam ovšem nepatří trestné činy, jako jsou např. daňové úniky a jiná hospodářská kriminalita, neplacení alimentů i nejčastější trestný čin – pomluva); navíc je třeba mít na paměti, že recidivou se míní opakování podobného trestného činu.

V roce 2008 byla provedena kontrola Národní databáze DNA (dále ND DNA) s tím, že bylo uloženo Policii ČR postupovat podle ustanovení § 42e odst. 3 zákona o policii: Citlivé osobní údaje mohou být zpracovávány pouze tehdy, *je-li to s ohledem na povahu trestného činu nezbytné pro plnění úkolů policie v souvislosti s trestním řízením*; proto jako výsledek kontroly bylo nařízeno zlikvidovat všechny profily DNA u těch pachatelů trestných činů, kteří nesplňují výše uvedená kritéria. Policie toto nápravné opatření nesplnila, naopak proti pokutě podala žalobu ke správnímu soudu.

Na základě mnoha stížností a vzhledem k novému zákonu o policii byla zahájena nová kontrola v polovině roku 2011, která byla ukončena v září 2012.

Základním východiskem pro kontrolu byl § 79 nového zákona o policii, podle kterého může Policie ČR zpracovávat osobní údaje včetně citlivých údajů bez souhlasu osoby, jíž se tyto údaje týkají, pouze **pokud je to nezbytné pro plnění jejích úkolů**. Z dvaceti náhodně vybraných profilů DNA, které byly uloženy v ND DNA, se u dvanácti z nich ukázalo, že neodpovídají kritériím nezbytnosti, přičemž:

- ve třech případech se jednalo o osoby zproštěné obžaloby,
- v jednom případě se jednalo o svědka,
- v jednom případě se jednalo o osobu, která v době odběru DNA již nebyla v postavení obviněného, neboť to bylo zrušeno jako nedůvodné,
- ve třech případech se jednalo o trestné činy hospodářské (neodvedení daně, platby na sociálním pojištění),
- ve čtyřech případech se jednalo o bagatelní trestné činy (maření výkonu úředního rozhodnutí, podmíněný trest na jeden rok).

Při výkladu pojmu nezbytnosti je třeba vycházet mj. z Doporučení R (92) 1 Výboru ministrů členských států o využívání analýzy deoxyribonukleové kyseliny v rámci systému trestní justice, kde se uvádí: *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. Pojem „nezbytnost“ musí tudíž obstát, jak co se týče kritéria dostatečné závažnosti trestného činu* (tj. závažné trestné činy ohrožující život, zdraví nebo

bezpečnost osob – a lze tedy logicky dovodit, že pod toto kritérium jistě nespádají méně závažné trestné činy, ale naopak spíše trestné činy ve formě zločinů dle ustanovení § 14 odst. 3 trestního zákoníku), **tak co se týče kritéria důvodnosti** (rozhodnutí Evropského soudu pro lidská práva – nelegální je zpracovávání osobních údajů osob v minulosti podezřelých a obviněných z páchaní trestné činnosti, kterým se však vina nikdy neprokázala) **i co se týče kritéria faktické použitelnosti** (některé trestné činy použitelnost vylučují z podstaty svého charakteru, např. zanedbání povinné výživy nelze dokázat na základě použití citlivých údajů podezřelého či pachatele).

Zákon o ochraně osobních údajů obsahuje v § 3 odst. 6 písm. d) výjimku z povinností správce, která bude aplikována při *předcházení, vyhledávání, odhalování trestné činnosti a stíhání trestných činů*. Výjimka se ovšem týká pouze povinností stanovených v § 5 odst. 1 a § 11 a 12 zákona o ochraně osobních údajů a nevztahuje se na povinnosti stanovené v § 5 odst. 2 a v § 9 zákona o ochraně osobních údajů.

Podle definice obsažené v § 4 písm. b) zákona o ochraně osobních údajů je citlivým údajem mj. *jakýkoli biometrický nebo genetický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů*, což profil DNA bezesporu je.

Podle § 9 zákona o ochraně osobních údajů lze zpracovávat citlivé údaje, kterým je i profil DNA, pouze se souhlasem subjektu údajů, nebo pokud *se jedná o zpracování podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách*.

Rozsáhlé odebrání bukálního stěru obviněným v případě, kdy není potřebný k prokázání jeho viny či nevinu ani k jinému vyšetřování daného trestného činu tzv. pro budoucí identifikaci, tj. pro vyšetřování zatím neexistujících trestných činů, tudíž neodpovídá nezbytnosti takového zpracování ve smyslu ustanovení § 79 zákona o policii ani ústavním principům zákonnosti a přiměřenosti.

Proto bylo v kontrolním protokolu konstatováno porušení § 9 zákona o ochraně osobních údajů a požadována likvidace profilů DNA v ND DNA, což potvrdil i odvolací orgán, tj. předseda Úřadu. Pokuta ještě nebyla uložena.

ZASTUPITELSKÝ ÚŘAD V MOSKVĚ

Ve dnech 3.–5. října 2012 proběhlo v rámci kontrol plnění povinností správce osobních údajů místní šetření na konzulárním úseku Velvyslanectví České republiky v Moskvě. Podnětem ke kontrole bylo doporučení expertní komise pro schengenské hodnocení členských států na úseku ochrany osobních údajů.

Moskevský konzulát je počtem udělovaných víz největším českým konzulátem ve světě. Kromě běžných konzulárních povinností, jako je vydávání náhradních dokladů, pomoc českým občanům v nepředvídatelných situacích, je zde ročně žadatelům vydáno 280–300 tisíc krátkodobých víz a cca 3000 dlouhodobých víz a povolení k pobytu. Žadatelé o víza požívají z hlediska osobních údajů obdobné ochrany jako občané EU. Mají právo, aby byli informováni, co se s jejich osobními údaji děje, jaké údaje jsou o nich shromažďovány, komu jsou předávány a komu si mohou v případě pochyb stěžovat.

Kontrola se zaměřila především na informační povinnost správce a na povinnost při zabezpečení osobních údajů, tj. zejména naplnění ustanovení § 11 a § 13 zákona o ochraně osobních údajů, za použití ustanovení zákona č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

Pokud jde o krátkodobá víza, jsou žádosti přijímány zejména prostřednictvím vízového centra, které je následně předá konzulárnímu úseku; nicméně žadatel se může na konzulární úsek obrátit sám po předchozím objednání. Veškeré žádosti, které konzulární úsek ráno obdrží od vízového centra, jsou ten den zpracovány, tzn. zaneseny do vízového systému. Na základě každé žádosti je tedy vytvořen spis, který má svou spisovou značku, z níž lze mimo jiné odvodit datum podání žádosti.

Od žadatelů jsou požadovány dokladové náležitosti, které jsou součástí příslušného formuláře žádosti, a to vyplněný formulář žádosti, cestovní doklad (konzulární pracovník vytvoří kopii datové stránky cestovního dokladu, na kterém je jméno, příjmení, pohlaví, číslo dokladu) a kopie nebo originály jednotlivých potvrzení dle vízového kodexu. Kopie předložených dokladů jsou zakládány do spisu. V případě krátkodobých víz mohou být s žadatelem prováděny pohovory, ale v praxi se tak děje spíše výjimečně.

Žádost založená do elektronické aplikace (vízového systému) je předložena ke kontrole orgánům v ČR, resp. dojde k předání žádosti do IS Ministerstva vnitra ČR za účelem ověření žadatele v SIS; žádost je takto vyřízena cca do 24 hodin.

Postup při přijímání a vyřizování žádostí o dlouhodobá víza a povolení k pobytu je obdobný jako v případě krátkodobých víz. V těchto případech ale není žádost přijímána na vízovém centru, ale pouze na konzulárním úseku, a to po předchozím internetovém objednání. Ve dvou třetinách případů je s žadatelem veden pohovor, přičemž u podnikatelů vždy. O pohovoru je sepsán záznam, který je součástí spisu.

Pokud jde o vedení spisu, je kopie spisu uložena na konzulárním úseku, přičemž originál spisu je poslán zabezpečenou poštou na MZV a odtud je postoupen na MV, odbor azylové a migrační politiky. Odpověď je zasílána jak elektronicky, tak v případě neudělení víza i písemně. Spisy žadatelů o krátkodobá i dlouhodobá víza, se kterými jednotliví konzulární pracovníci pracují, tj. jsou aktivní, mají u sebe v kanceláři a poté je ukládají do skladu, který je opatřen uzamykatelným zámekem, kam mají přístup pouze určení zaměstnanci. Spisy jsou archivovány po dobu 5 let, a pak jsou na základě rozhodnutí skartační komise skartovány. Přístup do vízového systému má 21 konzulárních pracovníků, a to na základě jména a hesla. Přístupová práva jsou přidělena na základě žádosti konzula o zřízení přístupu do systému, přístupová práva a účet jsou vytvořeny administrátory MZV. Administrátorská oprávnění mají i dva IT pracovníci, kteří jsou ve struktuře ZÚ zařazeni do sekretariátu velvyslance. Jeden z nich má na starosti údržbu místní sítě a druhý je šifrant velvyslanectví. Administrátorská práva k systému mají též prostřednictvím vzdáleného přístupu IT pracovníci MZV.

Celkem je na konzulárním úseku 28 zaměstnanců, z toho 7 místních sil (3 pracovníci ostrahy, 2 pracovnice u přepážek, 1 pracovnice v agendě dlouhodobých víz a 1 sekretářka). Nikdo z těchto 7 pracovníků nemá přístup do vízového systému.

Dále proběhla kontrola v prostorách čekárny konzulárního úseku za účelem posouzení dodržování povinností dle ustanovení § 11 zákona o ochraně osobních údajů, tzv. informační povinnost. Mimo toho, že byly kontrolovaným předloženy tiskopisy žádostí, byl zkontrolován též prostor čekárny pro žadatele, ve které jsou umístěny nástěnky s podrobnými informacemi pro žadatele (v českém i ruském jazyce).

Byla provedena kontrola zabezpečení vízových štítků. Ty jsou uloženy v trezoru v samostatné místnosti. Klíče od trezoru má pouze konzul, který zajišťuje jejich příjem a výdej referentům. Je vedena evidence denního výdeje vízových štítků. Jednotliví referenti mají své malé trezory, kde jsou umístěny stornované štítky. Skartace probíhá za účasti skartační komise.

Vchod, čekárna a prostor, kde jsou umístěny přepážky, jsou monitorovány kamerovým systémem (celkem 14 kamer jak on-line, tak i se záznamem). Tyto prostory jsou opatřeny informací o monitorování kamerovým systémem v ruském jazyce.

Prostory pro zaměstnance konzulárního úseku jsou, dle názoru kontrolujícího, dostatečně separovány od prostor pro veřejnost.

Celý objekt je dále zabezpečen EZS. Archiv je umístěn v areálu Zastupitelského úřadu. Zabezpečení bylo shledáno dostačujícím.

Lze konstatovat, že přístup k ochraně osobních údajů, informační povinnosti a zabezpečení nosičů osobních údajů (fyzických i elektronických) je na vysoké úrovni a má skutečně příkladný charakter.

V obdobném rozsahu proběhly **kontroly provedené na Generálním konzulátu ČR v Istanbulu a v hlavním městě Republiky Kazachstán v Astaně**, jejichž předmětem bylo rovněž do držování povinností správce osobních údajů v souvislosti s činností konzulárního úřadu při zpracování osobních údajů v rámci vízového řízení a využívání Schengenského informačního systému, s přihlédnutím k § 11 a § 13 zákona o ochraně osobních údajů byly rovněž uzavřeny s pozitivními poznatky o respektování ochrany osobních údajů, obdobně jako v předchozím roce v Makedonii, na Ukrajině a v Mexiku.

PRÁVO NA INFORMACE PŘI RESPEKTOVÁNÍ PRÁVA NA OCHRANU OSOBNÍCH ÚDAJŮ

Stále častěji jsou obce žádány svými občany i členy zastupitelstev o poskytnutí informací o činnosti orgánů obce, o záměrech do budoucna a o rozhodnutích, které obce učinily v rámci své rozhodovací pravomoci. Typické jsou žádosti o poskytnutí kopií smluv nebo žádosti o sdělení výše odměn členů statutárních orgánů anebo výši platů zaměstnanců úřadu.

Kontrolní plán a některé incidenční kontroly v roce 2012 se zaměřily na to, zda jsou v praxi tyto žádosti vyřizovány v souladu se zákonem, neboť někdy bývá nejen obtížné určit, zda poskytnutí informace nebrání zákonná ochrana (např. ochrana osobních údajů) nebo obchodní tajemství, ale i to, zda informaci má či musí obec poskytnout.

Zkontrolována byla dvě města a jedna městská část. Prvním kontrolovaným bylo statutární město, druhým město s rozšířenou působností III. typu a třetím městská část hlavního města Prahy. U všech kontrolovaných subjektů bylo kontrolou zjištěno, že ani v jednom případě nebyl porušen zákon o ochraně osobních údajů v souvislosti s vyřizováním žádostí o poskytnutí informací podle zákona 106/1999 Sb., o svobodném přístupu k informacím. Postup kontrolovaných byl vždy v souladu se zákonem: obce zveřejňovaly vyžádané informace, jak jim ukládá zvláštní právní předpis, blokovaly osobní údaje žadatele o informaci a také dbaly o ochranu soukromého a osobního života subjektu údajů, jehož se informace týkala.

Při první kontrole bylo zjištěno, že kontrolované město v rámci plnění povinností o svobodném přístupu k informacím přijalo vlastní pravidla, která upravují přesný postup při vyřizování jednotlivých žádostí, a to s ohledem nejen na vyřízení příslušné žádosti, ale i s ohledem na povinnosti stanovené zákonem o ochraně osobních údajů. Byla stanovena konkrétní odpovědnost vedoucích pracovníků za vyřízení žádosti, včetně odpovědnosti za poskytování informací vypovídajících rovněž o projevech osobní povahy, o soukromí fyzické osoby a o odpovědnosti za poskytování informací o osobách, které jsou příjemci veřejných prostředků v oblasti sociální, jimž jsou poskytovány zdravotní služby, pomoc hmotného zabezpečení a podpora v nezaměstnanosti. Město v rámci své činnosti mělo zpracovanou

metodikou vnitřní kontroly pro dodržování povinností stanovených zákonem o svobodném přístupu k informacím.

Bylo zkontrolováno poskytnutí všech jednotlivých informací v roce 2011 podle zákona o svobodném přístupu k informacím, a to nejen informace poskytnuté konkrétním žadatelům, ale i jejich zveřejnění na internetových stránkách města. V uvedeném období město poskytlo celkem 18 odpovědí. Větší část žádostí se týkala činností města v oblasti investic, stavebnictví, veřejných zakázek a životního prostředí; v jednom případě se dotaz vztahoval k fyzické osobě.

Ve všech případech město postupovalo v souladu s platnou právní úpravou, a to včetně zveřejnění poskytnutých informací v anonymizované podobě – tedy bez osobních údajů subjektů údajů i žadatelů o informaci.

Kontrola, která se uskutečnila ve statutárním městě, se týkala čtrnácti dotazů a odpovědí, které město za kontrované období poskytlo. Charakter žádostí byl rozmanitý – od běžných žádostí vztahujících se zejména k činnosti magistrátu přes žádosti vztahující se k činnosti města v oblasti investic a stavebnictví až po žádost, jejíž odpověď byla žadatelkou využita pro diplomovou práci.

V jednom případě byla podána žádost vztahující se k poskytování poradenské služby magistrátu – jak advokátními kanceláři, tak i fyzickými osobami. V daném případě magistrát žadatele nejdříve informoval o výši nákladů, které vzniknou v souvislosti s vypracováním odpovědi. Protože žadatel uvedenou částku neuhradil, byla tato žádost odložena.

Město mělo zpracovanou metodiku organizačního a pracovního zajištění plnění povinností podle zákona o svobodném přístupu k informacím, včetně zajištění ochrany osobních údajů ve smyslu tohoto zákona. Žádosti jsou přijímány prostřednictvím podatelny, podklady pro vyřízení žádosti vypracovává příslušný úředník, který žádost, včetně návrhu odpovědi, předává kanceláři tajemníka magistrátu. Následně je vypracována a odeslána definitivní odpověď a současně je v anonymizované podobě zveřejněna na internetových stránkách města v části povinně zveřejňované informace. Město má přijata i opatření pro zpětnou kontrolu informací zveřejňovaných na svých webových stránkách.

Veškeré žádosti podle zákona č. 106/1999 Sb. jsou centrálně evidovány.

Kontrolou nebylo zjištěno ani v jednom případě, že by postup města byl v rozporu s příslušnými zákony.

Třetím kontrovaným subjektem v roce 2012 byla městská část Prahy. Jednalo se o incidentní kontrolu, na základě konkrétní stížnosti. Stěžovatel uváděl, že sám na městskou část podal žádost podle zákona č. 106/1999 Sb. Žádostí se domáhal informace o tom, kterým osobám podávala městská část informace podle zákona č. 106/1999 Sb. o něm jakožto fyzické osobě. Na základě odpovědi, kterou obdržel a z níž vyplývalo, že v odpovědi zpracované a odeslané městskou částí jiné žadatelce bylo uvedeno jeho jméno, příjmení a adresa bydliště, žádal o prověření daného postupu.

V rámci kontroly bylo zjištěno, že žadatelka požadovala konkrétní informace týkající se řízení, ve kterém stěžovatele sama označila a identifikovala jménem, příjmením a adresou. Městská část tedy ve své odpovědi nesdělila žádné jiné informace než ty, které žadatelka sama poskytla. Informace, kterou městská část stěžovateli poskytla, byla zveřejněna na webových stránkách městské části v anonymizované podobě.

Dále bylo kontrolou zjištěno, že stěžovatel vede několik sporů s žadatelkou a jejich osobní údaje jsou jim navzájem známy. Město v daném případě postupovalo v souladu s ustanovením § 8b zákona č. 106/1999 Sb.

S ohledem na řadu oprávněných stížností, které byly následně řešeny přímo ve správním řízení, se Úřad obrátil přímo na Ministerstvo spravedlnosti ČR s upozorněním na nezbytnost dodržování zákona v souvislosti se zveřejňováním osobních údajů žadatelů.

V roce 2012 šlo o třináct správních řízení ve věci neoprávněného zveřejňování osobních údajů v souvislosti s poskytováním informací dle zákona č. 106/1999 Sb.

Úřad na základě poznatků z kontrolní činnosti, správního řízení, i své konzultační činnosti a z odpovědí tazatelům konstatuje, že v rámci plnění povinností uložených povinným subjektům zákonem o svobodném přístupu k informacím nedochází k žádnému závažnému porušování zákona o ochraně osobních údajů.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI SE VZNIKEM NÁJMU A NÁSLEDNÝM PRONÁJMEM BYTŮ VE SPRÁVĚ STATUTÁRNÍHO MĚSTA

V rámci kontrolního plánu byla uskutečněna kontrola ve věci dodržování povinností správce osobních údajů v souvislosti se vznikem nájmu a následným pronájmem bytů, které jsou ve správě velkého statutárního města.

Město, v souladu se zákonem č. 128/2000 Sb., o obcích, v rámci své samostatné působnosti má mimo jiné povinnost vytvářet podmínky pro rozvoj sociální péče a uspokojování potřeb svých občanů. Podstatnou částí této povinnosti je uspokojování potřeby bydlení.

Město hospodář s bytovým fondem v rozsahu cca dva tisíce bytů, které má ve svém vlastnictví. V rámci kontroly bylo prověřováno nejen to, jakým způsobem město nakládá s osobními údaji osob, které žádají o uzavření nájemní smlouvy, ale rovněž jakým způsobem jsou dodržovány povinnosti správce osobních údajů těch občanů a jejich členů domácností, kteří již mají smlouvu uzavřenou.

Město hospodář s bytovým fondem, který se skládá nejen z běžných bytů, ale rozhoduje o uzavření nájemní smlouvy se zájemci o tzv. startovací byty, tedy byty určené pro řešení sociálních problémů svých občanů, včetně bytů určených pro seniory.

V průběhu roku město uzavírá zhruba 150 nových nájemních smluv. Rozsah zpracovávaných osobních údajů v souvislosti s pronájmem bytů je značný, protože jsou v tomto případě zpracovávány osobní údaje nejen o nájemcích, ale i o všech osobách, které s nimi žijí v domácnosti. Z podstaty uvedených specifických podmínek zpracování osobních údajů je zřejmé, že pronajímatel v průběhu trvání smlouvy shromažďuje a získává významné informace vypovídající mimo jiné o rodinných i sociálních poměrech nájemce. V době trvání nájmu totiž běžně dochází k narození nového člena domácnosti, ke svatbám, k rozvodům a úmrtím (s nimiž souvisí například přechod nájemního práva).

V rámci činnosti města, jakožto správce osobních údajů zpracovávaných v souvislosti s činností správce bytového hospodářství, jsou zpracovávány osobní údaje žadatelů v rozsahu jméno, příjmení, rodné číslo, trvalé bydliště, kontaktní telefon, zaměstnání, státní příslušnost, číslo bankovního účtu, kód/název peněžního ústavu. Takové osobní údaje jsou evidovány i u rodinných příslušníků, resp. členů domácnosti. Prověřována je rovněž bezdlužnost žadatelů. V případě žadatelů o byty pro seniory jsou dále shromažďovány informace o státní příslušnosti, druhu důchodu, který pobírají, jeho měsíční výši, a také informace o dalších příjmech žadatele, o tom, zda pobírá příspěvky na péči, zda je držitelem průkazu ZTP, informace o jeho zdravotním stavu, o tom, zda je pohyblivý, soběstačný. Stejně informace se vyžadují i od žadatelčina/žadatelova manžela/manželky. Současně je od žadatele požadován

souhlas se zveřejněním jeho identifikačních osobních údajů na úřední desce města za účelem informování občanů o přidělení bytu.

U žadatelů o uzavření nájmu bytu pro mladé rodiny ve startovacích bytech je vyžadováno: jméno, příjmení, věk, rodné číslo, trvalé bydliště, kontaktní telefon, zaměstnání, stav a státní příslušnost. Stejně osobní údaje jsou požadovány u partnera žadatele, u dětí žijících ve společné domácnosti pak jméno, příjmení, věk a rodné číslo. Dále jsou nad rámec běžných informací shromažďovány osobní údaje o druhu spoření, o výši měsíčních příspěvků, ale rovněž informace o tom, zda je manželka žadatele nebo žadatelka těhotná, včetně pořizování kopie těhotenského průkazu, a to jak na základě povinností vyplývajících z povinností obcí zabezpečovat potřeby svých občanů ve smyslu zákona o obcích, tak i se souhlasem žadatelů.

Zpracování osobních údajů v souvislosti s bytovým hospodářstvím je upraveno nejen zákonem o ochraně osobních údajů, ale základní povinnosti pronajímatele i nájemce vyplývají zejména z občanského zákoníku a z předpisů upravujících zvyšování nájmu, výpočet a úhradu služeb souvisejících s bydlením, ale například i v souvislosti s předpisy o registrovaném partnerství.

V průběhu kontroly bylo zjištěno, že město má v rámci této problematiky přijatá dostatečná technicko-organizační opatření k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům. Uzavírání smluv se řeší podle vnitřního předpisu – manuálu správce osobních údajů, který upravuje rozdílný přístup při shromažďování osobních údajů žadatelů podle jednotlivých kategorií bytů. Upraven je postup přístupu k datům v návaznosti na rozhodovací kompetence jednotlivých funkcionářů města.

Kontrola se zaměřila rovněž na zpracování osobních údajů v rámci IT systému, jejich zabezpečení, oprávněnost administrátorských přístupových práv, vedení informací o přístupech k osobním údajům (logování). Kontrolou nebylo zjištěno porušení povinností správce osobních údajů uložených zákonem.

OSOBNÍ ÚDAJE DLUŽNÍKŮ ZVEŘEJNĚNÉ NA INTERNETOVÝCH STRÁNKÁCH SPOLEČENSTVÍ VLASTNÍKŮ BYTOVÝCH JEDNOTEK

Kontrolou bylo u Společenství vlastníků jednotek (dále též SVJ) při zpracovávání osobních údajů v souvislosti se zveřejněním osobních údajů dlužníků – členů SVJ – na webové stránce kontrolovaného zjištěno, že je možné získat ze zveřejněných zápisů z jednání výboru SVJ informace o šesti dlužnících – členech SVJ v rozsahu jméno, příjmení a výše dluhu.

Pokud jde o oprávnění evidovat dluhy a vést záznamy o projednávání způsobu vymáhání těchto dluhů, pak k tomuto Společenství souhlas dlužníků nepotřebuje, protože lze uplatnit výjimku podle ustanovení § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, podle něhož je možné zpracovávat osobní údaje, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.

Zpracování osobních údajů z důvodu potřeby vedení evidence dluhů a jejich vymáhání je nepochybně v zájmu SVJ a jeho členů. Není přitom v rozporu s právem subjektu údajů na ochranu soukromí, pokud probíhá způsobem, kdy k osobním údajům nezbytným k vymáhání dluhu mají přístup pouze osoby, které jsou členy SVJ, a tudíž de facto jsou věřiteli dlužníků.

Pokud jde o zpracování osobních údajů formou zveřejnění jmen dlužníků s výší jejich dluhu na internetové stránce SVJ, tak v tomto případě nelze uplatnit výjimku uvedenou v ustanovení

§ 5 odst. 2 písm. e) zákona o ochraně osobních údajů ani žádnou jinou výjimku. K uveřejnění jmen dlužníků by byl v tomto případě nutný jejich souhlas dle ustanovení § 5 odst. 2 uvedeného zákona. Zpracování formou uveřejnění jmen může mít zásadní dopad do soukromí osob, neboť zpřístupněním takového údaje, který byl získán na základě soukromoprávního vztahu, může dojít k poškození dobrého jména takové osoby v mnoha dalších vztazích, a to jak soukromoprávních, tak i veřejnoprávních.

Ke zveřejněným osobním údajům mají přístup nejen věřitelé dlužníků, ale i široký okruh dalších osob vstupujících na internetové stránky SVJ. Takto široký zásah do soukromí je pak obvykle v nepoměru k možným efektům plynoucím ze zlepšení platební morálky dlužníků.

Tím, že SVJ zpřístupnilo na svých internetových stránkách osobní údaje dlužníků a nezajistilo přístup pouze pro členy SVJ, a tudíž dostatečně nezabezpečilo zpracovávané osobní údaje, které obsahovaly zápisy z jednání výboru SVJ, porušilo ustanovení § 5 odst. 2 a ustanovení § 13 odst. 1 zákona o ochraně osobních údajů.

Protože kontrolovaný nezákonný stav odstranil zaheslováním internetových stránek obsahujících osobní údaje dlužníků se zabezpečeným přístupem pouze pro členy výboru SVJ, nebyla nápravná opatření uložena. Za porušení zákona byla kontrolovanému, i přes odstranění závadného stavu již v průběhu kontroly, uložena odpovídající pokuta.

FK TEPLICE

Jedním z míst, kde se shromažďuje velké množství lidí a kde může reálně dojít k ohrožení zdraví návštěvníků nebo škodám na majetku, jsou sportovní stadiony. Ze zkušenosti víme, že návštěva sportovní akce může být jen záminkou k násilnostem a ničení majetku.

Sportovní kluby musely reagovat na odchod policie ze stadionů a přijmout různá bezpečnostní a organizační opatření k zajištění pořádku při zápasech. To se týká především fotbalových stadionů. Jedním z těchto opatření byla instalace kamerových systémů na stadionech, které monitorují zmíněný prostor a napomáhají organizátorům zvládnout krizové situace.

Úřad se v rámci své kontrolní činnosti rozhodl prověřit, zda jsou kamerové systémy instalované ve sportovních areálech v souladu se zákonem o ochraně osobních údajů a zda je jejich činnost přiměřená.

FK Teplice, jakožto jeden z registrovaných provozovatelů kamerového systému, má přehledné a vyjasněné majetkové poměry vzhledem k vlastnictví stadionu a jeho odpovědnost vůči návštěvníkům je nezpochybnitelná. Je zároveň členem Českomoravského fotbalového svazu a své zkušenosti z provedené kontroly může předávat zástupcům ostatních klubů a přispět tak k jejich informovanosti.

Kapacita fotbalového stadionu v Teplicích je přes 18 tisíc diváků, což samozřejmě klade značné nároky na pořadatelskou službu. Té pomáhá platný *Návštěvní řád*, který je rozmístěn na různých místech stadionu a jenž diváky informuje o jejich právech a povinnostech. Pořadatelská služba má pouze organizační funkci. FK Teplice má dohodu s městskou policií, která je při zápasech na stadionu rovněž přítomna a která může, na upozornění pořadatele, nevhodně se chovajícího návštěvníka ze stadionu vyvést.

Kamerový systém instalovaný na stadionu včetně ovládacího a záznamového zařízení je ve vlastnictví policie, která má uvnitř stadionu vlastní detašované pracoviště. Na tomto pracovišti je neustále přítomen zaměstnanec městské policie, který funkčnost kamerového systému zajišťuje.

Klub neprodává vstupenky na jméno, neviduje žádné osobní údaje, a to ani na permanentkách nebo VIP kartách. Všechny typy vstupenek jsou prodávány bez vazby na identitu kupujícího. Vstupenka na kryté tribuny obsahuje poučení, že návštěvník zakoupením vstupenky souhlasí s návštěvním řádem FK Teplice.

Klub neorganizuje FANKLUB, a tedy ani k tomuto účelu neshromažďuje žádné osobní údaje.

Ze závěrů kontroly vyplývá, že FK Teplice, a. s. má svůj vztah k návštěvníkům zorganizován a zabezpečen způsobem, který nevyžaduje shromažďování a zpracovávání jejich osobních údajů.

INTERNETOVÉ SOUTĚŽE PRO DĚTI

Na základě podnětů provedl Úřad několik kontrol zaměřených na internetové soutěže, kterých se účastní děti. V těchto kontrolách byly konstatovány následující závěry:

Občanský zákoník v § 8 říká: *Způsobilost fyzické osoby vlastními právními úkony nabývat práv a brát na sebe povinnosti (způsobilost k právním úkonům) vzniká v plném rozsahu zletilostí. A § 9 upřesňuje: Nezletilí mají způsobilost jen k takovým právním úkonům, které jsou svou povahou přiměřené rozumové a volní vyspělosti odpovídající věku. Opačně, rodiče mají zodpovědnost za citový, rozumový a mravní vývoj nezletilého dítěte (viz § 31 zákona o rodině a § 217 a 217a trestního zákona).*

Způsobilost uzavírat typ „soutěžní smlouvy“, resp. dát souhlas se zpracováním osobních údajů, v soutěžích uvedeného typu bude zřejmě často chybět u dětí mladších 15 let, tudíž zde bude nezbytné k uzavření uvedené smlouvy souhlasu zákonného zástupce, neboť tyto děti nemohou posoudit všechny dopady vzniku této smlouvy, resp. uděleného souhlasu se zpracováním osobních údajů. Kontrolující si jako rozhodující kritérium zvolili věk 15 let, neboť dosažením tohoto věku by již žáci mohli mít vzhledem k rozvinuté informační době povědomí, že jejich údaje v určitém rozsahu budou někým zpracovávány, a že pokud by se s jejich osobními údaji nakládalo neoprávněně, je možnost domoci se svých práv (byť pouze prostřednictvím svých zákonných zástupců).

Je jasné, že určitý typ soutěží bude probíhat na internetu, neboť je to po všech stránkách nejjednodušší a pro dnešní dobu je to typické. Je přitom ale třeba zachovávat maximální zodpovědnost při zpracování osobních údajů. Na základě provedených kontrol dospěla inspektorka k určitým zásadám, aby zpracování osobních údajů odpovídalo úpravě dle zákona o ochraně osobních údajů (§ 5 odst. 1 písm. e/ a f/), které stanoví, že zpracovávání osobních údajů lze provádět jen k danému účelu, a to v rozsahu k tomuto účelu nezbytném. K prvotnímu přihlášení účastníka do soutěže je třeba vyžadovat minimálně údaje, většinou stačí pouze e-mailová adresa, popř. věk dítěte. Pokud je do soutěže zapojena i škola a dítě souhlasí s tím, že bude informována, je možno přiřadit i název a adresu školy. V každé takové internetové přihlášce musí být i okénko pro vyjádření souhlasu rodiče se zpracováním osobních údajů dítěte. Nepochybně v mnoha případech se stane, že děti vyplní souhlas samy, ale to už je do jisté míry založeno na vztahu dětí a rodičů a na jejich vzájemné důvěře. Jinými slovy: lepší aspoň určitý odkaz na souhlas zákonných zástupců než žádný. Nicméně je nutné uvést, že odpovědnost za to, že souhlas byl řádně udělen, nese provozovatel soutěže. Teprve v případě, kdy dítě vyhraje nějakou věcnou cenu, je možno požádat o adresu, další souhlas s vysvětlením, že osobní údaje mohou být použity pouze k poslání ceny. Takto získané osobní údaje – e-mailové adresy, popř. jména a adresy vítězů, je možno používat pouze v rámci dané soutěže, maximálně pro nabídku jejího dalšího kola. Každý, kdo takovou soutěž organizuje, se musí registrovat u Úřadu pro ochranu osobních údajů, neboť se v každém případě jedná o zpracování osobních údajů.

ZDRAVOTNICTVÍ

KONTROLA ZAMĚŘENÁ NA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PROSTŘEDNICTVÍM ELEKTRONICKÉ ZDRAVOTNÍ KNÍŽKY – SPOLEČNOST IZIP, A.S.

Inspektorka Úřadu ukončila v roce 2012 kontrolu ve společnosti IZIP, a.s. Kontrola byla provedena v souladu s kontrolním plánem pro rok 2010 a dále na základě stížností a podnětů, které Úřad obdržel v roce 2010 a 2011. Předmětem kontroly bylo plnění povinností správce osobních údajů, případně zpracovatele při zpracování osobních údajů držitelů elektronické zdravotní knížky IZIP (dále jen „EZK/IZIP“).

Ze stížností a podnětů, které Úřad obdržel, vyplývalo jednak podezření z porušení zákona o ochraně osobních údajů při tzv. „fiktivní“ registraci klientů EZK/IZIP a dále podezření na možnost přístupu společnosti IZIP, a.s. k osobním údajům vedeným v databázi pojištěnců Všeobecné zdravotní pojišťovny ČR (dále jen „VZP ČR“), resp. k osobním údajům pojištěnců všech zdravotních pojišťoven, vedeným v Centrálním registru pojištěnců, jehož správcem je VZP ČR, a to cestou propojení počítačových sítí IZIP, a.s. a VZP ČR. Další z podnětů se týkal podezření na neoprávněné nakládání s osobními údaji fyzických osob a podezření na jejich nedostatečné zabezpečení před zneužitím.

V případě tzv. „fiktivních“ registrací Úřad nezjistil pochybení společnosti IZIP, a. s. Pro navýšení akvizice pojištěnců VZP ČR a klientů EZK/IZIP uzavřela společnost IZIP, a. s. zpracovatelské smlouvy s několika společnostmi, jež prostřednictvím svých obchodních zástupců zajišťovaly registraci nových klientů, jak pojištěnců VZP ČR, tak registraci klientů EZK/IZIP. Obchodní zástupci, tzv. „získatelé“, kteří se na základě těchto smluv podíleli na akvizici pojištěnců VZP ČR a klientů EZK/IZIP, byli společností IZIP, a.s. proškoleni, získali osvědčení o absolvování školení a testů pro obchodní zástupce, podepisovali čestné prohlášení získatele a zavázali se dodržovat Kodex získatele – Obchodní manuál pro partnery společnosti IZIP, a. s. Součástí Čestného prohlášení je kromě jiného ustanovení o přiměřené identifikaci klienta a záruka, že veškeré tiskopisy jsou klienty, na základě jejich souhlasu, vlastnoručně podepsány. Součástí Kodexu získatele v části, jež stanoví, co získatel zejména nesmí, je uvedeno: „nechat podepsat přihlášku nezletilým klientem, nechat podepsat přihlášku ‘za někoho jiného’, např. za manželku, babičku, vnučku či za nesvéprávnou osobu, a podepsat se za klienta sám“.

Přihlášky byly následně zpracovávány ve společnosti IZIP, a. s. v dobré víře, že se jedná o klienty, kteří sami podepsali přihlášku. V několika případech se však jednalo o tzv. „fiktivní“ přihlášky, které obchodní zástupci vyplnili a podepsali sami a které obsahovaly údaje osob, jež tito obchodní zástupci použili bez jejich vědomí, a tedy v rozporu se zákonem o ochraně osobních údajů. Kontrolou bylo zjištěno, že společnost IZIP, a. s. takové kontaktní údaje zpracuje, vytvoří prázdnou EZK/IZIP, avšak v okamžiku, kdy klienta kontaktuje zasláním přístupových údajů na kontaktní adresu uvedenou v přihlášce a klient sám sdělí, že takovou přihlášku nepodepsal nebo se doručení IZIP, a. s. vrátí, společnost osobní údaje takového klienta zlikviduje – stejně tak vytvořenou EZK/IZIP. Společnost IZIP, a. s. tedy postupuje v souladu s ustanovením § 5 odst. 1 písm. d) zákona o ochraně osobních údajů.

Činnost obchodních zástupců prověřovaly v několika případech orgány činné v trestním řízení. Úřad v rámci součinnosti požádal Policii ČR a státní zastupitelství o sdělení výsledků šetření, ze kterých vyplývá, že pouze v jednom případě bylo sděleno podezření pro přečin poškození cizích práv podle ustanovení § 181 odst. 1 písm. a) trestního zákoníku. Podle § 179 g odst. 2 trestního řádu byla podezřelému stanovena zkušební doba v trvání osmi měsíců.

V daném případě zjištěné skutečnosti nenasvědčovaly spáchání přečinu neoprávněného nakládání s osobními údaji podle § 180 trestního zákoníku. V době ukončení kontroly se externí společnosti na akvizici nových klientů EZK/IZIP již nepodílely.

Kontrolou bylo dále zjištěno, že společnost IZIP, a.s. nemá přístup do Centrálního registru pojištěnců VZP ČR, vybrané kontaktní údaje sdílí s VZP ČR pouze u těch pojištěnců, kteří se registrovali k EZK/IZIP na základě Přihlášky klienta, na níž zároveň vyjádřili svůj souhlas s tímto sdílením. IZIP, a.s. dále pro klienty EZK/IZIP zprostředkovává vytvoření a zpřístupnění výpisu z Osobního účtu pojištěnce u VZP ČR za určitý kalendářní rok, a to na základě jednak předchozího souhlasu klienta a jednak jeho jednorázového požadavku na tento výpis.

EZK/IZIP je elektronickou kopií zdravotnické karty klienta u praktického lékaře, případně u specialistů, a záleží pouze na samotném klientovi, jak informace ze zdravotní karty využívá. Přihlášení klienta a veškerá další komunikace probíhá zabezpečeným přenosem (protokol https) přes webové rozhraní IZIP. Klient zadá své identifikační číslo a následně osobní heslo (původně vygenerované společností IZIP, a. s., které si však po zprovoznění EZK/IZIP může kdykoli změnit), které lze ještě zajistit prostřednictvím tzv. SMS hesla; klient může EZK/IZIP autentizovat i prostřednictvím certifikátu – takovéto další nastavení zabezpečení je dobrovolné. Údaje ze zdravotnické dokumentace klienta do EZK/IZIP zadává zdravotnické zařízení prostřednictvím zdravotnického pracovníka, jenž je registrován v systému IZIP, a. s., a to na základě výslovného souhlasu klienta, který stvrzuje svým podpisem na Přihlášce klienta. Klient si sám volí, kdo ze zdravotnických pracovníků a v jakém rozsahu může do jeho EZK/IZIP vstupovat.

Zdravotnický pracovník, který do EZK/IZIP vstupuje, musí být registrován v systému, při vstupu do EZK/IZIP konkrétního klienta vyplňuje prohlášení o oprávnění přístupu a musí zadat své přístupové heslo a PIN. O všech přístupech do své EZK/IZIP je klient informován prostřednictvím záznamů v Historii záznamů, jež se v jeho EZK/IZIP zobrazují. V případě nouzových situací mohou k údajům v EZK přistupovat zdravotničtí pracovníci záchranné služby bez souhlasu držitele EZK, a to za úzce vymezených podmínek. O této skutečnosti je klient EZK/IZIP informován v Provozním řádu IZIP.

Účelem EZK/IZIP je především shromažďování a další zpracování údajů a informací o klientech, zdravotnických zařízeních a zdravotnických pracovnících tak, aby prostřednictvím zabezpečené veřejné datové sítě byla jednak zajištěna okamžitá dostupnost úplných zdravotních informací pro klienta a s jeho souhlasem i pro všechny ošetřující jej zdravotnické pracovníky a další poskytovatele zdravotní péče. Klient EZK/IZIP může vyslovit svůj souhlas i s předáváním svých údajů z EZK/IZIP do zahraničí, pouze však do zemí EU, přičemž platnost tohoto souhlasu může omezit pouze na určité období. Úřad věnoval při kontrole zvláštní pozornost prověření naplnění ustanovení § 13 zákona o ochraně osobních údajů, tj. přijatým technicko-organizačním opatřením k zabezpečení ochrany osobních údajů. Prověřována byla opatření týkající se zabezpečení přístupů k osobním údajům, opatření proti zneužití osobních údajů, prověřena byla příslušná vnitřní dokumentace, dále to, zda společnost IZIP, a. s. posoudila rizika a zda na jejich základě přijala patřičná opatření. Kontrolou byl prověřen systém logování – aby bylo možno zpětně ověřit, kdo, kdy a za jakým účelem přistoupil k osobním údajům jednotlivých klientů. Prověřováno bylo zároveň zabezpečení serverů, včetně jejich dohledu a detekce podezřelých událostí, vnitřní sítě a přenosů jednotlivých zpráv a informací v informačním systému, včetně přenosů záznamů o vydaných léčivých přípravcích z lékárny. Úřad neshledal porušení § 13 zákona o ochraně osobních údajů.

Společnost IZIP, a. s., jako správce osobních údajů klientů EZK/IZIP, má uzavřeny smlouvy se společnostmi MD Access, a. s a UNIQSOL, a. s., jejichž předmětem je zpracování osobních

údajů klientů EZK/IZIP. Smlouvy jsou uzavřeny v souladu s § 6 zákona o ochraně osobních údajů.

Společnost IZIP, a.s. poskytuje informace o systému IZIP, a.s. svým klientům prostřednictvím Provozního řádu při podpisu přihlášky a prostřednictvím webových stránek.

Ze skutečností zjištěných při kontrole vyplývá, že společnost IZIP, a.s. jako správce osobních údajů držitelů EZK/IZIP neporušila povinnosti vyplývající jí ze zákona o ochraně osobních údajů.

KONTROLA ZAMĚŘENÁ NA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PROSTŘEDNICTVÍM ZÁKAZNICKÝCH KARET – SPOLEČNOST ČESKÁ LÉKÁRNA, A. S. (SÍŤ LÉKÁREN DR. MAX)

Kontrola byla provedena v souladu s kontrolním plánem Úřadu pro rok 2011 a na základě stížnosti podané Úřadu, jejímž předmětem bylo podezření z porušení ustanovení § 20 a § 21 zákona o ochraně osobních údajů. Předmětem kontroly, která byla dokončena v roce 2012, bylo plnění povinností správce osobních údajů, případně zpracovatele osobních údajů v souvislosti se zpracováním osobních údajů zákazníků v síti lékáren Dr. Max, kteří využívají klientskou kartu Dr. Max.

Společnost zpracovává osobní a citlivé údaje klientů klientské karty Dr. Max v databázi související se softwarem FaRMIS, který společnost využívá ke splnění povinností vyplývajících ze zákona č. 378/2007 Sb., o léčivech. Dle § 82 odst. 3, písm. d) jsou provozovatelé oprávněni k výdeji; dle zákona jsou (farmaceuti) „povinni zajistit při výdeji léčivých přípravků uvedených v § 75 odst. 1 písm. a) a b) evidenci výdeje pomocí jejich kódů a tuto evidenci uchovávat po dobu 5 let; dále jsou povinni poskytovat Státnímu ústavu pro kontrolu léčiv údaje o vydaných léčivých přípravcích; rozsah údajů a způsob jejich poskytování formou hlášení zveřejní Ústav ve svém informačním prostředku“. Údaje jsou zpracovávány systematicky a automatizovaně, jsou ukládány na nosiče informací, vyhledávány a používány.

Společnost prostřednictvím přihlášky klienta klientské karty Dr. Max a dalším zpracováním údajů v klientské kartě Dr. Max získává osobní a citlivé údaje za účelem jejich dalšího uložení na nosič informací, tyto informace dále zpracovává. Společnost vede databázi osobních a citlivých údajů klientů klientské karty Dr. Max v podobě, která je přístupná pracovníkům příslušné lékárny, ve které klient založil klientskou kartu. Údaje jsou v databázi uchovávány v takové podobě, že je umožněno jejich další zpracování, tj. přiřazování dalších údajů o vydaných léčivých a zdravotních doplňcích.

Společnost pro zřízení a vedení klientské karty Dr. Max stanovila jako účel zpracování osobních a citlivých údajů klientů této karty vedení lékové karty klienta. Společnost údaje z této lékové karty využívá pro kontrolu interakcí vydávaných léčiv, kontrolu kontraindikace léčiv v návaznosti na poskytnuté údaje o diagnózách, sleduje alergické reakce na léčiva a jejich včasné odhalení mezi podávanými léky, dohledání nevhodných kombinací a vedlejších účinků při podávání léků nebo kombinací, informování klientů o novinkách a pokroku v oblasti zdravotní péče a poskytnutí bonusů za vyzvednuté léky.

Klient klientské karty Dr. Max je s účelem zpracování osobních a citlivých údajů vedených v klientské kartě seznámen při podpisu přihlášky do klientského programu. Součástí přihlášky je poskytnutí souhlasu klienta ke zpracování osobních údajů dle požadavků zákona o ochraně osobních údajů, přihlášku klient stvrzuje vlastnoručním podpisem.

V rámci kontroly bylo prověřováno, zda společnost přijala dostatečná technicko-organizační opatření ve smyslu § 13 zákona o ochraně osobních údajů tak, 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. Kontrolou bylo zjištěno, že společnost povinnosti vyplývající jí z § 13 zákona o ochraně osobních údajů neporušila.

Dále byl prověřován postup společnosti při vyřizování žádosti subjektu údajů o likvidaci osobních údajů v souladu s § 20 a 21 zákona o ochraně osobních údajů. Na základě zjištěných skutečností bylo konstatováno, že společnost porušila ustanovení § 20 a § 21 zákona o ochraně osobních údajů tím, že neprodleně neprovedla likvidaci osobních údajů klienta, ačkoli klient o likvidaci svých osobních údajů, resp. zrušení své klientské karty Dr. Max požádal. Kontrolou bylo zjištěno, že společnost uvedenou likvidaci neprovedla, a to z důvodu nedostatečného proškolení personálu, jak postupovat v případě žádosti o zrušení klientské karty Dr. Max. V průběhu kontroly však byl uvedený nedostatek společností napraven.

S ohledem na kontrolní zjištění a nápravu postupu při likvidaci osobních údajů klienta nebyla společnosti uložena žádná nápravná opatření.

KONTROLA ZAMĚŘENÁ NA PŘEDÁVÁNÍ ÚDAJŮ O PACIENTECH V RÁMCI SCREENINGU ONKOLOGICKÝCH ONEMOCNĚNÍ

Inspektorka Úřadu provedla na základě podnětu kontrolu Institutu biostatistiky a analýz MU Brno (dále jen „IBA MU“), jejímž předmětem bylo dodržování povinností správce osobních údajů, stanovených zákonem o ochraně osobních údajů v souvislosti se shromažďováním a zpracováním osobních údajů za účelem správy dat při monitoringu onkologických screeningových programů.

Kontrolou bylo zjištěno, že screeningové programy (screening nádorů kolorekta, karcinomu prsu a děložního hrdla) byly zahájeny na základě směrnice Evropské unie 2003/878/EC – „European Council Recommendation of 2 December 2003 on cancer screening“ a ve spolupráci s Českou onkologickou společností byly postupně realizovány. Legislativní rámec (rozsah a metodika) provádění screeningů byly do současného stavu postupně upravovány vyhláškami a Věstníky Ministerstva zdravotnictví ČR.

Na základě prověřených skutečností bylo konstatováno, že ID klientky v případě mamografického screeningu a ID pacientky v případě screeningu karcinomu děložního hrdla jsou bezvýznamové identifikátory, které jsou jedinečné v rámci příslušného zdravotnického zařízení, resp. laboratoře, nejsou však jedinečné v rámci celé České republiky. Takto definované skupiny údajů, vztahující se k jednotlivým subjektům vyšetření a ke zdravotnickému zařízení, jsou dostatečné k naplnění stanovených účelů, tedy k vytváření statistik, založených na lokalitě či věku, a dalších agregovaných ukazatelů s přijatelnou statistickou chybou. Na základě zjištěných skutečností kontrolující konstatovali, že údaje shromažďované v rámci výše uvedených screeningových programů nejsou dostatečné k identifikaci dotčených subjektů, a ve smyslu ustanovení § 4 písm. a) zákona o ochraně osobních údajů se tedy nejedná o osobní údaje.

IBA MU v Brně neshromažďuje osobní údaje ve smyslu ustanovení § 4 písm. a) zákona o ochraně osobních údajů. Na zpracování programů mamografického screeningu, screeningu karcinomu děložního hrdla a screeningu karcinomu kolorekta způsobem a v rozsahu popsaným v kontrolním protokolu tedy nelze aplikovat zákon o ochraně osobních údajů.

Následně zástupce IBA MU zaslal Úřadu písemnou žádost o stanovisko k možnosti použití ID ve formě jednostranného otisku rodného čísla vytvořeného hašovacím algoritmem za podmínky dodržení konkrétních bezpečnostních opatření. Uvedený postup dle sdělení IBA MU umožní v rámci screeningových programů identifikovat vícenásobný výskyt jedné osoby v databázi, což je pro účely centrálního sběru nezpochybnitelná nutnost.

Úřad na základě písemného dotazu zástupce IBA MU sdělil tazateli stanovisko, že budou-li jednotlivá zdravotnická zařízení zasílat data do centrálního úložiště screeningových programů upravená takovým způsobem, který jakoukoliv další identifikaci dotčených pacientů umožní právě a pouze jenom odesílajícím zdravotnickým zařízením, zatímco provozovatel centrálního úložiště nebude schopen jakýmkoliv způsobem přímo ani nepřímo konkrétní pacienty identifikovat, a pokud IBA MU, jakožto provozovatel centrálního úložiště, bude přijatá data zpracovávat pouze pro účely vlastní, statistické, analytické atd., lze konstatovat, že uvedený způsob bude analogický ke způsobu zpracování, které bylo předmětem předcházející kontrolní činnosti popsané v kontrolním protokolu, pak popsaný způsob použití jednoznačného identifikátoru, jímž by byl popsaný otisk rodného čísla s hašovacím algoritmem a s dalšími uvedenými zabezpečeními, nelze posuzovat jako postup, který by byl ve smyslu zákona o ochraně osobních údajů zpracováním osobních údajů.

Dále Úřad IBA MU sdělil, že bude-li proces probíhat způsobem, jaký je shrnut v předchozím odstavci, pak lze uvést, že provozovatel centrálního úložiště dat screeningových programů nebude v postavení správce osobních údajů ve smyslu zákona o ochraně osobních údajů. Nebude totiž mít přístup k takovým informacím, které by byl schopen přímo či nepřímo přiřadit ke konkrétním fyzickým osobám, a tudíž se nebude jednat o osobní údaje dle definice § 4 písm.a) uvedeného zákona. Zákon jako celek proto nebude na jeho činnost dopadat.

KONTROLA VEDENÍ ZDRAVOTNICKÉ DOKUMENTACE VE ZDRAVOTNICKÉM ZAŘÍZENÍ

Inspektorka Úřadu provedla na základě podnětu kontrolu na oční klinice (dále jen „Klinika“), ze které vyplývalo možné podezření z porušení § 13 zákona o ochraně osobních údajů, jehož se mohl dopustit správce, tj. zdravotnické zařízení.

Stěžovatelka v podnětu uvedla, že se domnívá, že Klinika porušila povinnosti uložené zákonem o ochraně osobních údajů, a to zejména povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů, dále povinnost zpracovávat pouze přesné údaje a povinnost shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Klinika dle stěžovatelky zpracovala její osobní údaje v rozporu s jejím právem na zachování lidské důstojnosti a v rozporu s ochranou jejího soukromého a osobního života. Stěžovatelka zaslala na Kliniku žádost o poskytnutí veškerých informací shromážděných v její zdravotnické dokumentaci (dále jen „ZD“), avšak odpověď obdržela ve lhůtě překračující 30 dnů, tedy ve lhůtě, která neodpovídala příslušnému ustanovení pro vyřizování takových žádostí, stanovenému zákonem č. 20/1996 Sb., o péči o zdraví lidu. V zasláné kopii ZD bylo u jednoho z vyšetření uvedeno datum, ve kterém stěžovatelka Kliniku nenavštívila, a při osobní návštěvě Kliniky jí její ZD nebyla poskytnuta k nahlédnutí s odůvodněním, že písemné dokumenty (ZD) jsou zasílány do archivu na pobočce Kliniky a tam ZD stěžovatelky také primář odvezl. Sestra ani manažer stěžovatelce neumožnili nahlédnout do její ZD, neboť tvrdili, že nahlédnout do ZD lze pouze za přítomnosti ošetřujícího lékaře. Stěžovatelce bylo nabídnuto, že jí budou originály ZD v archivu oskenovány a zaslány na Kliniku. Dále stěžovatelka ve své stížnosti uvedla, že bylo následně zasláno asi šest papírů, o kterých se domnívala, že nejsou úplné; na papírech také nebyla razítka. Zároveň požadovala veškeré snímky z vyšetření na topografu, tyto jí byly poskytnuty, avšak snímky z autorefraktometru nebyly dohledány. Stěžovatelka se dále domnívala, že v její dokumentaci

byly dopisovány či měněny údaje, zejména se domnívala, že byly měněny či dopisovány údaje v lékařské zprávě o zákroku.

Úřad požádal odbor zdravotnictví příslušného krajského úřadu o prověření stížnosti stěžovatelky, a to z hlediska plnění povinností nestátních zdravotnických zařízení při vedení ZD dle zákona č. 20/1966 Sb., o péči o zdraví lidu, v platném znění, a Vyhlášky Ministerstva zdravotnictví ČR č. 385/2006 Sb., a to v návaznosti na oprávnění krajského úřadu provádět v přenesené působnosti kontroly na úseku zdravotnictví.

Krajský úřad podal Úřadu následující vysvětlení: *„vzhledem k tomu, že jmenovaná nepodala ke krajskému úřadu stížnost na poskytnutou zdravotní péči, ale řeší poškození zdraví soudní cestou, nemá tedy úřad zákonnou možnost vyžádat si její ZD a zkontrolovat náležitosti založených zpráv a komplexnost dokumentace. Kontrolu ZD pacientky by neumožnilo ani dodatečné podání stížnosti na poskytnutí zdravotní péče, protože podle příslušné směrnice krajského úřadu, schválené usnesením rady krajského úřadu, se vyřizování stížnosti zastavuje v případě, že o totožných skutečnostech probíhá trestní, občanskoprávní, správní nebo daňové řízení. Podněty, které vyplývají z podání stěžovatelky ke spolupráci jmenovaných zdravotnických zařízení, či se týkají vedení ZD, si krajský úřad samozřejmě ověří a v obecné rovině zjistí i způsob vedení ZD, její uložení, skartaci, apod. V kompetenci krajského úřadu však není posuzování a ověřování komunikace jmenované s personálem při uplatňování jejich práv podle § 67b odst. 12 písm. b) a c) zákona č. 20/1966 Sb.“*

Stěžovatelka Úřadu sdělila, že věc neřeší soudní cestou, ve věci neprobíhá žádné trestní, občanskoprávní, správní ani daňové řízení. Vyzvala proto Úřad, aby pokračoval v prošetření dané věci.

Úřad zaslal na Ministerstvo zdravotnictví ČR žádost o výkladové stanovisko ve věci oprávněnosti kompetentního orgánu k provádění kontrolní činnosti v oblasti zpracování osobních údajů z hlediska oprávněnosti a úplnosti zápisů do ZD v návaznosti na poskytování zdravotní péče, tj. požádal o sdělení, který dozorový orgán je oprávněn provádět dozorovou činnost v uvedené oblasti.

Ministerstvo zdravotnictví ČR zaslalo Úřadu stanovisko k otázce určení správního orgánu k doзору nad vedením ZD: *„primárně je stanoven dozor nad dodržováním povinností vyplývajících ze zvláštních zákonů, se kterými ale souvisí vedení a nakládání se ZD; proto je v souvislosti s touto dozorovou činností umožněno nahlížet do ZD (viz např. § 67b odst. 10 zákona č. 20/1966 Sb.). Pokud jde o stížnost směřující k tomu, že nějaký pacient se domnívá, že jeho ZD je neúplná, neboť neobsahuje všechny zdravotnické výkony, a že záznamy ve ZD byly podle něj pozměňovány, uvádíme, že tento pacient je oprávněn si svoji dokumentaci vyžádat, včetně kopie, a po prostudování uvážit, zda záznamy v ní odpovídají skutečnosti. V případě, že tomu tak není, musí pacient sám pro sebe dovést, jakou odpovědnost a případně jaké nároky chce z tohoto tvrzení uplatnit.“* Dále MZd ČR dodalo, že: *„padělání nebo úmyslná neoprávněná změna lékařské zprávy nebo zdravotnického průkazu anebo zneužití lékařské dokumentace je přestupkem dle § 29 odst. 1 písm. d) přestupkového zákona; obdobně trestní zákoník. Zákon neoznačuje jeden jediný správní orgán povoláný k tomu, aby dozoroval pouze vedení ZD, a tudíž jím není ani Úřad pro ochranu osobních údajů.“*

Úřad následně zahájil na Klinice kontrolu, jejímž předmětem bylo dodržování povinností správce osobních údajů stanovených zákonem o ochraně osobních údajů se zaměřením na zpracování osobních údajů pacientů Kliniky, a s tím související kontrolu zabezpečení zpracovávaných osobních údajů ve zdravotnické dokumentaci dle ustanovení § 13 zákona o ochraně osobních údajů.

Kontrolou bylo prokázáno, že Klinika porušila vlastní interní předpis, týkající se vedení ZD, čímž porušila ustanovení § 13 odst. 2 zákona o ochraně osobních údajů, a to tím, že nepřijala dostatečná technicko-organizační opatření pro takovou situaci, kdy převážel ZD přímo primář kliniky, tj. přesný postup pro nakládání se ZD v případě, že o nahlédnutí do ZD, která je uložena v archivu pobočky Kliniky, požádá pacient přímo na Klinice. Dále Klinika tím, že zaslala kopii ZD stěžovatelce na její žádost ve lhůtě 37 dnů, porušila ustanovení § 67bb odst. 4 zákona č. 20/1966 Sb. o péči o zdraví lidu, a dále porušila ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů, resp. ustanovení § 67b odst. 4 zákona č. 20/1966 Sb., neboť ve ZD stěžovatelky nevedla přesné údaje o zdravotní péči, která jí byla na Klinice poskytnuta.

Klinice byla uložena opatření k nápravě, spočívající v povinnosti přijmout taková opatření, aby osobní údaje pacientů vedené ve ZD dle zvláštního zákona byly vedeny ve smyslu ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů a doplnit interní předpis tak, aby obsahoval technicko-organizační opatření pro případ, kdy nakládá se ZD přímo ošetřující lékař při nahlížení pacienta nebo oprávněné osoby do ZD.

Klinika následně informovala Úřad, že uložena opatření k nápravě splnila.

PODNET SMĚŘUJÍCÍ PROTI VŠEOBECNÉ ZDRAVOTNÍ POJIŠŤOVNĚ ČR

Úřad prostřednictvím elektronické pošty obdržel podnět směřující proti Všeobecné zdravotní pojišťovně ČR (dále jen „VZP“) s žádostí o prošetření, zda VZP může na svých webových stránkách (www.vzp.cz/platci/dluznici) vystavovat údaje svých dlužníků.

Na výše uvedených stránkách jsou prostřednictvím excelové tabulky zveřejňovány údaje o osobách (fyzické i právnické) v rozsahu jméno, příjmení, název, IČ/datum narození, adresa a informace o dlužné částce.

Inspektorka Úřadu provedla analýzu podnětu, který následně odložila s odůvodněním, že z hlediska zákona o ochraně osobních údajů jsou údaje, které se vztahují k fyzické osobě, osobními údaji ve smyslu ustanovení § 4 písm. a) tohoto zákona, avšak VZP je za účelem zpřístupňování informací o dlužnících na veřejném zdravotním pojištění oprávněna zpracovávat osobní údaje subjektů údajů ve smyslu ustanovení § 5 odst. 2 písm. a) zákona o ochraně osobních údajů, tedy bez souhlasu subjektu údajů, neboť ve smyslu ustanovení § 23 odst. 3 zákona č. 592/1992 Sb., o pojistném na všeobecné zdravotní pojištění, ve znění pozdějších předpisů, se povinnost zachovávat mlčenlivost, vztahující se k zaměstnancům zdravotní pojišťovny, nevztahuje na údaje týkající se dluhu na pojistném, včetně výše dlužného penále, o nichž bylo rozhodnuto pravomocnými platebními výměry, nebo jedná-li se o pohledávku na pojistném a penále, kterou zdravotní pojišťovna uplatňuje ve veřejné dražbě nebo která byla zjištěna v insolvenčním řízení podle zvláštního právního předpisu.

O tomto stanovisku byl stěžovatel inspektorkou Úřadu informován.

KONTROLA ZAMĚŘENÁ NA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI S POUŽÍVÁNÍM PASIVNÍCH IDENTIFIKAČNÍCH NÁRAMKŮ PRO PACIENTY – NEMOCNICE NA HOMOLCE

Inspektorka Úřadu provedla v souladu s kontrolním plánem Úřadu pro rok 2011 kontrolu dodržování povinností správce osobních údajů v souvislosti s používáním elektronických, resp. pasivních identifikačních náramků v Nemocnici Na Homolce (dále jen „Nemocnice“). Předmět kontroly byl rozšířen v průběhu kontroly na základě stížnosti, kterou Úřad obdržel, v níž stěžovatel doložil záznam z internetu, na kterém byl zveřejněn záznam ze zákroku, kde bylo

zobrazeno rodné číslo pacienta, včetně jeho jména i části příjmení, které bylo odvoditelné. Kontrola byla dokončena v roce 2012.

V průběhu kontroly bylo zjištěno, že Nemocnice používá pasivní identifikační prvky – náramky obsahují informace, které jsou na nich umístěné ve formě samolepky vytištěné z nemocničního informačního systému (dále jen „NIS“). Při příjmu pacienta k hospitalizaci je pacient vybaven identifikačním štítkem s údaji: jméno a příjmení pacienta, datum narození a čárový kód obsahující číslo pacienta z registru pacientů nemocnice. Sestra na oddělení, na které je pacient přijat, nalepí tento štítek na identifikační náramek, umístěný na zápěstí pacienta. Standardně se v Nemocnici používá náramek modré barvy, pro pacienty s vyšším rizikem upadnutí náramek žluté barvy. Údaje na náramku jsou jedním ze základních prostředků zajištění kvality a bezpečnosti pacienta při jeho pobytu v nemocnici. Kontrolou údajů na identifikačním náramku se zajistí, aby nedošlo k záměně pacientů nebo přiřazení výsledků vyšetření k dokumentaci jiného pacienta. Mají zcela zásadní funkci při provádění diagnostických nebo léčebných výkonů, a to zejména mimo příslušné oddělení, na kterém je pacient hospitalizován (zobrazovací vyšetřovací metody, laboratorní vyšetření, operační zákrok atp.). Nezastupitelnou úlohu mají při identifikaci dezorientovaných, zmatených pacientů a pacientů pod vlivem léčiv (celková anestézie apod.). Všechny údaje uvedené na náramku jsou automaticky i součástí každého listu zdravotnické dokumentace. Čtečky na čárový kód jsou umístěny u počítačů, kde je možný vstup do NIS (jedná se o místnosti, kde je poskytována zdravotní péče, tj. na oddělení, ambulanci a podobně). Čárový kód na náramku je možno snímat pouze na vzdálenost cca 10–20 cm při přímé viditelnosti, což vylučuje možnost sledování pohybu pacienta v areálu nemocnice.

K uveřejnění záznamu z lékařského zákroku na internetu a zároveň zveřejněným údajům v rozsahu rodné číslo, jméno a část příjmení pacienta Nemocnice v průběhu kontroly předložila pacientem podepsaný „Souhlas pacienta k mediálnímu použití provedeného diagnostického/léčebného výkonu“, jehož součástí byl i výslovný souhlas s použitím jména, příjmení, data narození, rodného čísla, textové informace, obrazových a zvukových záznamů konkrétní podoby či podoby částí těla a dále projevu či jiných prvků osobní povahy. Kontrolovaný dále uvedl, že tento záznam byl již z internetových stránek odstraněn, jelikož Nemocnice fakticky neměla v úmyslu rodné číslo příslušného pacienta zveřejňovat, a to navzdory tomu, že měla od příslušného pacienta udělen písemný souhlas.

Kontrolou bylo zjištěno, že Nemocnice neporušila povinnosti správce osobních údajů při zpracování osobních údajů dle zákona o ochraně osobních údajů v souvislosti s identifikací pacientů prostřednictvím pasivních identifikačních náramků, ani v souvislosti se zveřejněním osobních a citlivých údajů pacienta na internetu.

KAMEROVÉ SYSTÉMY

VRCHNÍ STÁTNÍ ZASTUPITELSTVÍ V PRAZE

Na základě podnětu předsedy Úřadu proběhla kontrola Vrchního státního zastupitelství v Praze. Důvodem bylo posouzení dodržování povinností stanovených Vrchnímu státnímu zastupitelství při zpracování osobních údajů získaných prostřednictvím kamerového systému provozovaného kontrolovaným v jeho sídle. Impulsem byla skutečnost, že vrchní státní zástupce uspořádal mimořádnou tiskovou konferenci, na které veřejně prezentoval záznam pořízený kamerovým systémem provozovaným kontrolovaným v budově Vrchního státního zastupitelství.

Vrchní státní zástupce uspořádal dne 24. února 2012 tiskovou konferenci, na které novinářům přehrál záběry z kamerového systému ze dne 17. února 2012 a doplnil je svým komentářem. Záznam z tiskové konference byl umístěn na internetu.

Bylo zjištěno, že kontrolovaný má registrována Úřadem od 19. května 2009 dvě zpracování osobních údajů.

Účelem obou oznámených zpracování osobních údajů je ochrana a bezpečnost osob, majetku a informací ve střežených prostorách Vrchního státního zastupitelství v Praze. O době uchovávání záznamů deklaruje, že: Záznamy budou uchovávány v rámci časové smyčky nepřetržitě po dobu 3 dnů.

Vrchní státní zastupitelství vydalo v rámci plnění povinností vyplývajících ze zákona o ochraně osobních údajů vnitřní předpisy Opatření vrchního státního zástupce v Praze č. 4/2011 k zajištění ochrany osobních údajů při provozování kamerového a záznamového systému a Zásady ochrany osobních údajů v systému na Vrchním státním zastupitelství v Praze. Ochrana snímacích a záznamových zařízení před neoprávněným nebo nahodilým přístupem či přenosem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním je zabezpečena souborem organizačních, technických, elektronických a softwarových opatření. Na používání video-monitoringu v traktu B na chodbě ve 2. patře viditelně upozorňoval nápis: „prostor je monitorován kamerovým systémem se záznamovým zařízením“ a piktogram. Přístup k záznamům měly dvě osoby.

Kontrolou byl zjištěn rozdíl doby Úřadem registrované pro uchování záznamu a doby, po niž byl záznam skutečně uchován, což bylo způsobeno nastavením kvality ukládaného záznamu v závislosti na velikosti ukládaných dat. Zařízení neumožňuje časové nastavení smyčky. Dobu záznamu odhadl pro účely registrace dodavatel zařízení.

Vrchní státní zástupce na základě podnětu svého podřízeného využil svého oprávnění přístupu k záznamům kamerového systému a uložil kopie těchto záznamů do PC ve své kanceláři.

Jako základ rozhodování o souladu s právní úpravou byla vzata ustanovení zákona o ochraně osobních údajů a dalších právních předpisů. Nejprve byla určena odpovědnost kontrolovaného za zpracování osobních údajů podle zákona o ochraně osobních údajů; poté byly posouzeny relevantní povinnosti kontrolovaného podle tohoto zákona.

Porušení povinností vyplývajících ze zákona o ochraně osobních údajů shledal kontrolující u § 13 odst. 3 a § 16 odst. 1. Opatření k zabezpečení osobních údajů kontrolovaný sice přijal, ne však důsledně, což je patrné zejména ze zjištění učiněného vrchním státním zástupcem, že záznamy jsou pět dní staré (nikoli tři dny), a z výpisu auditních záznamů/logů, které do dne zahájení kontroly prokazatelně nikdo neposuzoval. Dále nelze jednoznačně určit, která z oprávněných osob systém použila. Kontrolovaný také nesplnil oznamovací povinnost, když zjištěný rozdíl mezi dobou skutečného uchovávání a dobou registrovanou neoznámil Úřadu.

Kontrolní zjištění byla promítnuta do nápravných opatření uložených inspektorem. Vrchní státní zastupitelství v Praze výsledky kontroly akceptovalo a Úřadu podalo zprávu o realizovaných nápravných opatřeních.

Z kontrolních zjištění ale vyplynulo i pochybení zaměstnance kontrolovaného, tedy osoby zplnomocněné se systémem pracovat. Kontrolující došli k závěru, že vrchní státní zástupce zveřejněním záběrů z kamerového systému porušil povinnost mlčenlivosti, neboť jejich zveřejnění nebylo v souladu s účelem, ke kterému byly určeny.

Toto porušení zákona o ochraně osobních údajů je řešeno v rámci správního řízení Úřadu. Rozhodnutí Úřadu ke konci roku 2012 nenabýlo právní moci.

KAMEROVÝ SYSTÉM V PROVOZOVNĚ

Inspektorka Úřadu provedla kontrolu kamerového systému v provozovně palírny (dále jen „kontrolovaný“). Předmětem kontroly bylo dodržování povinností stanovených zákonem o ochraně osobních údajů, se zaměřením na zpracování osobních údajů prostřednictvím kamerového systému se záznamem, instalovaného v místě podnikání.

Kontrola byla zahájena na základě podnětu – souseda kontrolovaného (dále jen „stěžovatel“). Obsahem jeho stížnosti bylo podezření z porušení zákona o ochraně osobních údajů. Dle stěžovatele jeho sused, kontrolovaný, na budově své provozovny instaloval kamerový systém, jehož prostřednictvím monitoroval nejen svůj pozemek, ale i pozemek stěžovatele, kde stěžovatel má svůj dům, a dále okolní pozemky, které jsou ve vlastnictví manželky stěžovatele. Dle sdělení stěžovatele kontrolovaný tak monitoroval veškerou činnost, která byla prováděna na okolních pozemcích. Zejména upozornil na to, že kontrolovaný monitoruje vchod s vjezdem k jeho bydlišti (k rodinnému domu se zahradou).

Stěžovatel se písemně obrátil na kontrolovaného se žádostí, aby ukončil monitorování jeho pozemků a domu, což je v rozporu s dobrými sousedskými mravy. Na tuto výzvu kontrolovaný stěžovateli neodpověděl.

Stěžovatel následně podal stížnost na příslušný obecní úřad s žádostí o zjednání nápravy a o pomoc v návratu k právnímu stavu. Obecní úřad stěžovateli sdělil, že v rámci šetření nebylo zjištěno, že by jednáním kontrolovaného došlo ke spáchání přestupku dle zákona č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů, a věc odložil.

V průběhu místního šetření bylo zjištěno, že kontrolovaný instaloval kamerový systém na své provozovně prostřednictvím externí společnosti před cca jedním rokem. Důvodem pro instalaci kamerového systému byla ochrana vlastního majetku. Řídící jednotka s monitorem je umístěna v kanceláři provozovny. Kamerový systém se skládá ze čtyř kamer. Současně je na plášti budovy umístěna jedna maketa kamery. Záznam z kamer se ukládá na harddisku řídicí jednotky. Kamerový systém snímá barevný obraz, a to nepřetržitě. Nemá funkci zoomu a kamery nejsou mobilní (otočné). Doba uchovávání závisí na naplnění harddisku. Naplnění disku trvá cca 10–14 dnů. Poté se záznamy automaticky mažou, zpětně od nejstaršího data. Z řídicí jednotky lze nahrát příslušnou sekvenci (konkrétní nahrávku) na přenosné záznamové zařízení flash. Kontrolovaný sdělil, že tuto funkci nevyužil a záznamy nikdy nikomu nepředával.

Přístup do prostor provozovny, a to jak venkovních, tak vnitřních, má kontrolovaný a jeho rodinní příslušníci a dále zákazníci kontrolovaného. Provozovna ani vnitřek provozovny nejsou označeny žádnou informační tabulkou s informací o provozování kamerového systému.

V průběhu ústního jednání a místního šetření bylo projednáno se zástupcem externí společnosti, že změní nastavení zorného úhlu jedné z kamer tak, aby v záběru byl monitorován výhradně pozemek kontrolovaného, a tuto skutečnost neprodleně sdělil Úřadu.

Kontrolovaný prostřednictvím zástupce externí společnosti zaslal Úřadu fotodokumentaci, ze které vyplývá, že došlo ke změně nastavení zorného úhlu kamery tak, že v současné době zabírá pouze pozemek kontrolovaného (horní okraj záběru zabírá hranici mezi pozemkem kontrolovaného a veřejnou cestou). Kontrolovaný nebyl v době zahájení kontroly registrován v registru správců osobních údajů vedeného Úřadem. Kontrolovaný dne 19. prosince 2011 zaslal registraci správce osobních údajů shromažďovaných prostřednictvím kamerového systému se záznamem. Z činnosti Úřadu ani ze stížnosti nevyplývá, že by kontrolovaný využíval pořízené záznamy.

Kontrola byla ukončena s následujícím závěrem: doba 10 až 14 dní, po kterou jsou záznamy pořízené kamerovým systémem uchovávány, neodpovídá době nezbytné, neboť vzhledem

k umístění a chodu provozovny je nepochybné, že o případném excesu, který je zachycen prostřednictvím kamerového systému, získá kontrolovaný informaci minimálně nejbližší následující pracovní den. Po zjištění případného excesu má kontrolovaný možnost zajistit neprodlené přehrání a uchování záběru na přenosné médium k dalšímu využití. V ostatních případech jsou záznamy uchovávány bez jakéhokoliv důvodu, a to až po dobu 14 dnů. Kontrolovaný tým, že zpracovává osobní údaje osob, jejichž jednání je zaznamenáváno po dobu, která není nezbytná pro naplnění stanoveného účelu, porušil ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů. Správce osobních údajů je povinen při shromažďování osobních údajů informovat subjekt údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat, komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce osobních údajů musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona o ochraně osobních údajů. Vzhledem k tomu, že kontrolovaný neinformuje ani informační tabulkou třetí osoby o tom, že v provozovně jsou shromažďovány osobní údaje prostřednictvím kamerového systému, natož o dalších náležitostech zpracování osobních údajů, porušil povinnost uloženou mu jako správci osobních údajů § 11 odst. 1 zákona o ochraně osobních údajů.

Kontrolovaný tým, že neoznámil písemně Úřadu před zpracováním osobních údajů záměr zpracovávat osobní údaje prostřednictvím kamerového systému se záznamem, porušil povinnost uloženou mu jako správci osobních údajů dle § 16 odst. 1 zákona o ochraně osobních údajů.

Kontrolovaný prostřednictvím kamerového systému zpracovává osobní údaje svých a sousedových rodinných příslušníků a dále jednotlivých návštěvníků provozovny, přičemž lze presumovat, že ke zpracování osobních údajů rodiny kontrolovaného má kontrolovaný k dispozici jejich souhlas. Od návštěvníků provozovny kontrolovaný souhlas nevyžaduje a jejich osobní údaje shromažďované prostřednictvím kamerového systému se záznamem zpracovává bez jejich souhlasu. Právo kontrolovaného na ochranu svých práv a svých právem chráněných zájmů, které realizoval instalací kamerového systému monitorujícího jeho majetek, lze v tomto případě nadřadit právu jednotlivých návštěvníků na ochranu jejich soukromého a osobního života, neboť záznamy vypovídající o jednorázových, nahodilých návštěvách pánenice do osobnostních práv nezasahují zásadním způsobem.

Kontrolovaný prostřednictvím kamerového systému, resp. prostřednictvím jedné kamery zaznamenával i část příjezdové cesty k bydlišti stěžovatele. Vzhledem k nastavení kamerového systému byly zaznamenávány všechny příchody a odchody (příjezdy a odjezdy) všech osob, které měly bydliště v sousedním domě. V tomto případě tedy docházelo k pravidelnému a systematickému sledování osob, které k takovému shromažďování osobních údajů nedaly souhlas, a ke zpracování osobních údajů bez souhlasu subjektu údajů nelze přisvědčit žádnou z výjimek uvedených v ustanovení § 5 odst. 2 pod písmenem a) až g) zákona o ochraně osobních údajů. Kontrolovaný tým, že zpracovával osobní údaje subjektů údajů bez jejich souhlasu, porušil povinnost uloženou mu jako správci osobních údajů v § 5 odst. 2 zákona o ochraně osobních údajů.

V průběhu kontroly kontrolovaný zajistil změnu zorného úhlu monitorovaného prostoru, čímž ukončil monitorování vjezdu do sousedního domu, a tedy i shromažďování osobních údajů osob bez jejich souhlasu.

Na základě zjištěných skutečností byla kontrolovanému uložena opatření k nápravě, a to splnit povinnost informovat subjekty údajů dle ustanovení § 11 odst. 1 zákona o ochraně osobních údajů, a to označením monitorovaného prostoru prostřednictvím informačních

tabulek, a současně informovat subjekty údajů o dalších náležitostech zpracování osobních údajů dle ustanovení § 11 odst. 1 tohoto zákona, a to minimálně prostřednictvím písemného sdělení umístěného v provozovně; a neuchovávat osobní údaje shromažďované prostřednictvím kamerového systému se záznamem po dobu, která není nezbytná pro naplnění stanoveného účelu.

KAMEROVÝ SYSTÉM V ZAŘÍZENÍ SOCIÁLNÍ PÉČE

Při místním šetření příspěvkové organizace poskytující sociální služby byly oblastním inspektorátem v rámci inspekce práce zjištěny nedostatky, které se týkaly provozování kamerového systému. Na základě těchto zjištění byl Úřadu zaslán podnět upozorňující na možné porušení zákona o ochraně osobních údajů. Kontrolou bylo zjištěno, že organizace má v objektu, kde provozuje sociální služby, instalovaný kamerový systém za účelem ochrany osob před napadením agresivní osobou, ochrany majetku před krádeží, jakož i před jinou protizákonnou či trestnou činností, dále v zájmu předcházení nežádoucím jevům, zejména proti ničení společného majetku a vandalismu.

V daném případě zpracováním osobních údajů kamerovým systémem nedochází k zásahům do práv subjektů údajů (zaměstnanci, klienti, návštěvy apod.) na ochranu soukromého a osobního života subjektů údajů a práva na zachování lidské důstojnosti, neboť z umístění kamer se záznamem je zřejmé, že jsou zaměřeny na vchody a vstupy do objektu kontrolovaného a prostory, kde monitorování není v rozporu s právem na ochranu soukromého a osobního života. Doba uchování pořízených záznamů z kamerového systému je přiměřená účelu jejich zpracování.

V rozporu se stanoveným účelem však došlo k použití záznamu při šetření stížnosti klienta, a tím organizace porušila svou povinnost zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. K jinému účelu lze osobní údaje zpracovávat, tedy záznam použít, pokud k tomu dal subjekt údajů souhlas. Jelikož takovým souhlasem kontrolovaný nedisponoval a nadto nesplnil oznamovací povinnost Úřadu v době před zpracováním osobních údajů instalovaným kamerovým systémem, bylo kontrolou konstatováno porušení zákona o ochraně osobních údajů a organizaci byla uložena pokuta.

MĚSTSKÝ KAMEROVÝ SYSTÉM

Předmětem kontroly bylo dodržování povinností stanovených zákonem o ochraně osobních údajů se zaměřením na zpracování osobních údajů prostřednictvím městského kamerového dohlížecího systému se záznamem městskou policií.

Podnět ke kontrole Úřadu podalo obvodní oddělení Policie ČR. Následně zaslala Policie ČR spisový materiál, shromážděný na základě prověřování trestního oznámení osoby (stěžovatele), ve věci zneužití pravomoci úřední osobou (neoprávněné sledování stěžovatele kamerovým systémem a pořízení zvukové nahrávky jeho stížnosti na jednání městského policisty), kterého se měl dopustit ředitel městské policie a místostarosta města, v návaznosti na zajišťování důkazů protiprávního jednání stěžovatele při projednávání jeho dopravního přestupku. O údajném protiprávním jednání ředitele městské policie a místostarosty města se stěžovatel dozvěděl v souvislosti se svým trestním stíháním, a to pro útok na úřední osobu (veřejného činitele), kterého se měl stěžovatel dopustit při projednávání jeho dopravního přestupku městskou policií. Inspektorka Úřadu na základě uvedeného podnětu zahájila kontrolu daného města. V průběhu kontroly bylo zjištěno, že kontrolovaná osoba – Město, na základě § 7 odst. 1 zákona č. 128/2000 Sb., o obcích (obecní zřízení), spravuje své záležitosti

samostatně; do samostatné působnosti patří ve smyslu § 35 odst. 2 zákona o obecním zřízení mimo jiné i vytvoření podmínek pro rozvoj sociální péče a pro uspokojování potřeb svých občanů. Jde především o uspokojování potřeby bydlení, ochrany a rozvoje zdraví, dopravy a spojů, potřeby informací, výchovy a vzdělávání, celkového kulturního rozvoje a ochrany veřejného pořádku. Za účelem plnění úkolů v samostatné působnosti Město, ve smyslu § 35a odst. 2 zákona o obcích, zřídilo obecní (městskou) policii, jejíž činnost je upravena zákonem č. 553/1991 Sb. o obecní policii. Městská policie k plnění úkolů uvedených v § 2 zákona o obcích je ve smyslu § 24b odst. 1 téhož zákona oprávněna pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu zákroku nebo úkonu. Na základě výše uvedeného provozuje městská policie kamerový systém se záznamem (dále také jen „MKDS“) jako zpracovatel, za účelem ochrany majetku a zdraví občanů a majetku Města a dalších subjektů. Šetřením Policie ČR bylo zjištěno, že zvukový záznam stížnosti stěžovatele byl pořízen v únoru 2009 na služebně městské policie bez jeho vědomí. O pořízení zvukového záznamu byl stěžovatel informován po skončení jednání. Pořízená audionahrávka byla poskytnuta jako důkazní materiál vyšetřovateli Služby kriminální policie a vyšetřování Policie ČR.

Záznamy z kamerového systému Města, se záběry osoby stěžovatele, pocházely z ulic města a byly pořízeny kamerovým systémem městské policie, o poskytnutých důkazech se stěžovatel dozvěděl až následně od policejního orgánu.

Policie ČR uvádí, že městská policie stěžovatele zaznamenala na kamerovém systému náhodně, v souvislosti s jeho přestupkovým jednáním. Přestupek se týkal motorového vozidla stěžovatele, které parkovalo na zákazu stání. Tato událost byla službu konajícím strážníkem zaznamenána do služební pomůcky – knihy událostí. Dle Policie ČR došlo k zálohování záznamů se záběry, které pořídil kamerový systém, i když na nich není zachyceno žádné porušení veřejného pořádku, ani nelze dovodit podezření z protiprávního jednání. Policie ČR v závěru podnětu konstatovala, že záznamy byly archivovány v rozporu se směrnicí upravující provoz kamerového systému Města, a domnívala se, že mohl být porušen zákon o ochraně osobních údajů. O pochybení strážníků informovala Policie ČR Město, současně s podáním podnětu k projednání porušení pracovních povinností strážníka. Policie ČR se domnívala, že kamerové záznamy byly archivovány nepřiměřenou dobu, aniž by obsahovaly protiprávní jednání stěžovatele, respektive neurčitě uváděla, že se mělo většinou jednat o náhodné záběry pohybu osoby stěžovatele ve Městě a jejího přestupkového jednání (parkování vozidla stěžovatele v zákazu stání). Zálohování (neupřesněných) kamerových záznamů je údajně v rozporu se směrnicí na provoz kamerového systému Města.

Kontrolou bylo prověřováno zpracování osobních údajů prostřednictvím kamerového systému Města, příslušné směrnice i postupy při využívání záznamů z kamerového systému Města.

Kontrolním šetřením byly zjištěny dvě žádosti Policie ČR o poskytnutí kamerového záznamu. V žádostech je uvedený důvod poskytnutí kamerového záznamu, označení dne a pravděpodobný čas šetřené události. Žádost je podepsána dvěma policisty. Na žádostech je na místě označeném „podpis ředitele městské policie“ další nečitelný, neidentifikovatelný podpis. Kontrolou celkového zabezpečení operačního střediska a také evidence pořízených záznamů a jejich likvidace v PC nebyly zjištěny nedostatky.

Kontrolující inspektorka ukončila kontrolu s tím, že osobní údaje, resp. záznamy z kamerového systému, shromážděné ve veřejných prostorách Města, v rozsahu zjištěném v průběhu kontroly, jednoznačně přispívají ke stanovenému účelu a záznamy nejsou zpracovávány nad rámec stanoveného účelu, kterým je ochrana majetku a zdraví občanů a majetku Města a dalších

subjektů, doba tří až deseti dnů, po kterou jsou záznamy z kamerového systému zálohovány, považuje Úřad v daném případě za přípustnou dobu, po kterou lze osobní údaje na záznamovém zařízení shromažďovat ke stanovenému účelu. Policie ČR v postoupení záležitosti Úřadu uvedla podezření, že záznamy z kamerového systému (záběry stěžovatele) byly městskou policií archivovány bezdůvodně po delší dobu, cca dva měsíce, kdy došlo k předání záznamů z kamerového systému vyšetřovateli Služby kriminální policie a vyšetřování Policie ČR. Jak je uvedeno v dopisu Policie ČR, byly záznamy dle městské policie archivovány z důvodu řešení protiprávního jednání, popřípadě pro potřeby vyhodnocení činnosti a reakce operátora na oznámení, či vyhodnocení činnosti strážníků městské policie. Jak vyplývá z dožádání Policie ČR k provozu MKDS, Město také uvedlo, že se v daném případě jednalo o náhodné zaznamenávání a zálohování dat prostřednictvím kamer v okolí autobusového nádraží, kde byly zaznamenány stížnosti na „popíjení“ mládeže. Jednalo se o různá časová období, aby bylo možné posléze vyhodnotit úspěšnost této preventivní akce. Město také v dožádání uvedlo, že si vyšetřovatel SKPV Policie ČR vybral nahrávky zcela náhodně ze souboru jiných. Město také kontrolujícím sdělilo, že maximální doba v délce tří měsíců pro smazání zálohovaných záznamů, jež jsou uloženy, se týká nahrávek, které jsou uloženy na přenosných záznamových zařízeních. Dle ředitele městské policie dochází k zálohování nahrávek z kamerového systému v rámci preventivních akcí a k jejich pozdějšímu vyhodnocení a dále v případech, kdy ve věci probíhá šetření na základě oznámení občanů, a to pro zdokumentování stavu přijatých opatření. Zálohované záznamy se vymažou v době, kdy je již zřejmé, že nebude nahrávka potřebná k dalšímu využití. Kontrolující v daném případě akceptovali vysvětlení Města k době zálohování záznamů a konstatovali, že v souvislosti s uložením záznamů se záběry stěžovatele po dobu cca dvou měsíců nebylo porušeno ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů.

Dle názoru kontrolující inspektorky byla audionahrávka výpovědi stěžovatele na služebně městské policie pořízena v souladu s výše uvedeným ustanovením § 24b odst. 1 zákona č. 553/1991 Sb. Taktéž pořízení záběrů jeho osoby z ulic města prostřednictvím kamerového systému bylo v souladu s výše uvedeným ustanovením. Dle názoru kontrolující zpracovávala městská policie osobní údaje stěžovatele, které byly shromážděné audiozáznamem a prostřednictvím záznamů z kamerového systému Města v souladu s § 5 odst. 2 písm. e) zákona o ochraně osobních údajů. Dle tohoto ustanovení může správce osobních údajů zpracovávat osobní údaje bez souhlasu subjektu údajů v případě, že je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Jak je uvedeno výše, byly záznamy z kamerového systému pořízeny náhodně v rámci preventivní akce městské policie. V různých časových obdobích bylo zaznamenáváno trvajících protiprávní jednání v prostoru autobusového nádraží, aby bylo možno posléze vyhodnotit úspěšnost této preventivní akce. Vyšetřovatel SKPV si vybral nahrávky zcela náhodně ze souboru jiných.

Kontrolující je toho názoru, že pořízené záznamy se stěžovatelem (a jinými osobami) byly pořízeny a zálohovány v souladu s veřejným zájmem, který byl v daném případě postaven nad zájem na ochranu soukromého a osobního života stěžovatele. Kontrolující nebylo prokázáno neoprávněné zpracování záznamů ani jejich jiné zneužití, které by vážně narušilo soukromý a osobní život jmenovaného.

V závěru kontroly inspektorka Úřadu konstatovala, že Město neporušilo v souvislosti se zpracováním osobních údajů stěžovatele prostřednictvím městského kamerového systému zákon o ochraně osobních údajů. Z toho důvodu nebyla uložena žádná opatření k nápravě.

LETIŠTĚ PRAHA – KONTROLA ZAMĚŘENÁ NA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PROSTŘEDNICTVÍM ZÁZNAMŮ Z KAMEROVÝCH SYSTÉMŮ UMÍSTĚNÝCH VE VEŘEJNĚ PŘÍSTUPNÝCH PROSTORÁCH LETIŠTĚ

Kontrola ve společnosti Letiště Praha, a.s. byla zahájena na základě Kontrolního plánu Úřadu na rok 2012. Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených zákonem o ochraně osobních údajů při zpracování osobních údajů cestujících a zaměstnanců Letiště prostřednictvím kamerových systémů, se zaměřením na dodržování jeho § 13, tj. technického a organizačního zabezpečení osobních údajů a na dodržování povinností při jejich předávání. V průběhu kontroly přijal Úřad podnět ve věci systému rozpoznávání registračních značek vozidel na parkovištích Letiště. Na základě tohoto podnětu rozhodla kontrolující inspektorka o rozšíření rozsahu probíhající kontroly o kontrolu uvedeného systému.

Kamerový systém na Letišti je v provozu od roku 1995, v roce 2006 proběhla jeho digitalizace a začal být pořizován záznam. Účelem kamerového systému se záznamem (dále také jen CCTV) je zajištění bezpečnosti a ochrany letecké přepravy – plnění povinností dle národního bezpečnostního programu civilního letectví, zejména pracoviště bezpečnostních kontrol, prostor kontroly palubních vstupenek pro cestující v schengenském prostoru a pracoviště pasového odbavení, dále zajištění plynulosti odbavení cestujících, dohled nad vlastním provozem Letiště (letištní plochy, třídící systémy zavazadel a další).

Ke dni místního šetření bylo v areálu Letiště instalováno 1226 kamer, které sledují vnitřní prostory Letiště, v nichž se pohybují cestující a další osoby, dále jsou sledovány vnitřní prostory Letiště, ve kterých je umístěna provozní technologie, vnější veřejné prostory před Letištěm, letištní plocha a prostory parkovišť a parkovacích domů (instalován je systém identifikace registračních značek vozidel). Kamerový systém se záznamem je v nepřetržitém provozu 24 hodin denně, 7 dnů v týdnu s tím, že i záznam je pořizován nepřetržitě.

Letiště zároveň provozuje systém rozpoznávání registračních značek vozidel na krátkodobých parkovištích (dále jen „Parkovací systém“). Pro řízení a případné zpoplatnění provozu na krátkodobých parkovištích před halami terminálů využívá Letiště systém pro kontrolu vjezdu a výjezdu z parkovišť založený na elektronickém rozpoznávání registračních značek motorových vozidel. U vjezdů na tato parkoviště jsou umístěny kamery, které automaticky snímají registrační značky vjíždějících vozidel, přičemž Parkovací systém současně rozezná text na registrační značce. Tento údaj je následně odeslán na server Parkovacího systému, kde je přiřazen k číslu parkovacího lístku. Při odjezdu vozidla z parkoviště je opět sejmuto a rozpoznána registrační značka a dvojice údajů „text registrační značky / číslo parkovacího lístku“ je na serveru parkovacího systému porovnávána s dvojicí údajů pořízených při vjezdu vozidla na parkoviště. Současně s údaji o registrační značce vozidla a o vjezdu / výjezdu vozidla jsou ukládány i vlastní snímky. Parkovací systém zároveň ovládá závory na vjezdu a výjezdu z parkoviště. U výjezdu z parkovišť je stanoviště obsluhy, kde zaměstnanci Letiště asistují např. při placení poplatku za překročení bezplatné doby parkování nebo zasahují v konfliktních případech. Na sloupku před závorami parkoviště, ve kterém je umístěn přístroj pro výdej parkovacích lístků, je informační štítek s piktogramem kamery a nápisem „OBJEKT JE SLEDOVÁN KAMEROVÝM SYSTÉMEM“ a „OBJECT IS MONITORING BY CAMERA SYSTEM“. Nad sloupkem je umístěna rovněž tabule „Výňatek z provozního řádu odstavných ploch na Letišti Praha“ v českém jazyce. Dále je na sloupku umístěn Ceník parkovního s uvedením podmínek bezplatného parkování.

Primárním účelem Parkovacího systému je kontrola dodržování provozního řádu krátkodobých parkovišť, zejména pak dodržení doby bezplatného pobytu na parkovišti, dodržení minimálního časového intervalu pro další bezplatný vjezd, zpoplatnění delšího pobytu, zamezení nežádoucí nebo podvodné manipulaci s parkovacími lístky a dalších podvodných praktik. Dle Provozního řádu a Ceníku parkovného, platného od 1. 7. 2012, je na krátkodobých parkovištích možno bezplatně parkovat 15 minut, přičemž mezi jednotlivými vjezdy musí být dodržen interval delší než 1 hodina.

Parkovací systém dále umožňuje trvale vložit registrační značky pro další funkce, a to nepovolení vjezdu vozidla s určitou registrační značkou, upozornění obsluhy parkoviště při vjezdu určitého vozidla a umožnění automatického otevření závory pro volný vjezd a výjezd určitého vozidla bez vydání parkovacího lístku. Doba uchování všech pořízených údajů včetně snímků přední masky vozidla s registrační značkou je 90 dnů. Tato doba je nastavena dodavatelem, Parkovací systém neumožňuje uživatelské nastavení doby uchování ani parametrické mazání údajů, např. v určitém intervalu poté, co vozidlo řádně opustilo parkoviště, nebo dle jiných kritérií. Doba uchování 90 dnů je nastavena i s ohledem na potřeby Letiště pro vyhodnocování provozu a pro postihování řidičů, kteří se opakovaně dopouštějí porušení Provozního řádu parkovišť v delším časovém intervalu. Záměrem je použít funkci upozornění obsluhy parkoviště v případech, kdy vozidlo s určitou registrační značkou hrubě poruší Provozní řád více než pětkrát v průběhu tří měsíců.

Kontrolující inspektorka v závěru konstatovala, že Letiště pro zajištění především bezpečnosti a ochrany letecké přepravy využívá systém CCTV se záznamem, je tedy správcem osobních údajů, pořízených systémem CCTV. Pro řízení a zpoplatnění provozu na krátkodobých parkovištích využívá Parkovací systém založený na snímání a rozeznávání registračních značek vozidel. Letiště je tedy správcem osobních údajů pořízených Parkovacím systémem. Na základě zjištěných skutečností inspektorka konstatovala, že technická a organizační opatření přijatá Letištěm jsou dostatečná k naplnění povinností stanovených § 13 zákona o ochraně osobních údajů. Dle vnitřní směrnice pro nakládání se záznamy CCTV je export dat ze systému CCTV (trvalé uložení na přenosný nosič informací) prováděn ve dvou exemplářích, přičemž jeden exemplář je určen pro žadatele o export, druhý exemplář je určen pro evidenci, a to bez stanovení doby, po kterou má být export archivován, a bez udání účelu archivace. V průběhu místního šetření bylo kontrolujícím sděleno, že archivace exportů záznamů ze systému CCTV je trvalá, bez časového omezení, přičemž účelem uchování je řešení případných rozporů s žadatelem o export, objasnění případů možného zneužití předaných exportů a dalších obdobných situací. Vzhledem k tomu, že účel trvalé archivace exportů záznamů ze systému CCTV není explicitně stanoven v interních řídicích dokumentech a současně nelze takovou archivaci podřadit pod ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů ve znění „Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví“, kontrolující konstatovali, že trvalé uchování exportů záznamů ze systému CCTV je v rozporu s ustanovením § 5 odst. 1 písm. e) zákona o ochraně osobních údajů.

Dle § 11 odst. 1 uvedeného zákona je správci uložena tato povinnost: „Správce je při shromažďování osobních údajů 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, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21.“ U vstupů do terminálů jsou

umístěny informační štítky s piktogramem kamery a textem „OBJEKT JE SLEDOVÁN KAMEROVÝM SYSTÉMEM“ a „OBJECT IS MONITORING BY CAMERA SYSTEM“. Dle kontrolující inspektorky není tato informace dostatečná ke splnění povinností uložených správci v § 11 odst. 1 zákona o ochraně osobních údajů.

V souvislosti s provozem Parkovacího systému kontrolující inspektorka doporučila Letišti uchovávat snímky registračních značek vozidel, jejichž řidiči neporušili platný Provozní řád, a s tím související zpracovávané údaje, pouze po dobu, která je nezbytná ve smyslu stanoveného účelu, tedy pro zajištění provozu a zpoplatnění parkovišť v souladu s platným Provozním řádem a Ceníkem, nejdéle však po dobu 24 hodin.

Na sloupku u vjezdu do parkoviště je umístěn informační štítek s piktogramem kamery a textem „OBJEKT JE SLEDOVÁN KAMEROVÝM SYSTÉMEM“ a „OBJECT IS MONITORING BY CAMERA SYSTEM“. Rozsah takto poskytovaných informací je nutno hodnotit jako nedostatečný ve smyslu výše citovaného ustanovení § 11 odst. 1 zákona o ochraně osobních údajů.

Dle § 13 odst. 4 písm. c) uvedeného zákona je správce nebo zpracovatel v oblasti automatizovaného zpracování osobních údajů v rámci opatření podle odstavce 1 povinen také „pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány“. Aplikace Parkovacího systému shromažďuje a zpracovává pouze provozní údaje o pohybu vozidel na parkovišti, žádné další údaje, např. o přístupu k uloženým údajům a jejich následném zpracování, neukládá. Letiště provozováním aplikace Parkovacího systému tedy dle kontrolující inspektorky neplní povinnost uloženou v § 13 odst. 4 písm. c) zákona o ochraně osobních údajů.

Zpracováním osobních údajů prostřednictvím systému CCTV se záznamem porušilo Letiště ustanovení § 5 odst. 1 písm. e) a § 11 odst. 1 zákona o ochraně osobních údajů a prostřednictvím Parkovacího systému s rozeznáváním registračních značek vozidel porušilo ustanovení § 11 odst. 1 a § 13 odst. 4 písm. c) tohoto zákona. Kontrolující inspektorka uložila Letišti neprodleně upravit informační štítky o systému CCTV u vstupů do terminálů tak, aby byla splněna povinnost uložená v § 11 odst. 1 zákona o ochraně osobních údajů, a informační štítky o systému CCTV u vjezdů na krátkodobá parkoviště tak, aby byla splněna povinnost uložená v § 11 odst. 1 zákona o ochraně osobních údajů, a to i pro specifické podmínky zpracování osobních údajů prostřednictvím Parkovacího systému. Dále uložila do tří měsíců zajistit, aby kopie záznamů ze systému CCTV (tzv. exporty) byly uchovávány pouze po dobu nepřesahující 90 dnů, do tří měsíců zlikvidovat dosud pořízené kopie záznamů ze systému CCTV, jejichž stáří přesahuje stanovenou dobu, zajistit ve lhůtě šesti měsíců takové úpravy aplikačního programového vybavení Parkovacího systému, aby byly splněny požadavky kladené § 13 odst. 4 písm. c) zákona o ochraně osobních údajů. Současně byla Letišti stanovena povinnost podat kontrolující inspektorce písemnou zprávu o přijatých opatřeních, a to neprodleně po realizaci každého jednotlivého opatření.

KAMEROVÝ SYSTÉM V BYTOVÉM DOMĚ

Inspektorka Úřadu ukončila opakovanou kontrolu kamerového systému instalovaného Společenstvím vlastníků jednotek (dále jen „SVJ“) v bytovém domě v Příbrami, jejímž předmětem byla kontrola plnění nápravných opatření, stanovených kontrolou Úřadu a uvedených v kontrolním protokolu (dále jen „KP“) z února 2010. Této kontrole předcházela kontrola probíhající v roce 2009, která byla ukončena v únoru 2010, a to s následujícími zjištěními a právním hodnocením porušení ustanovení zákona o ochraně osobních údajů: SVJ porušilo povinnost

stanovenou v § 5 odst. 2 uvedeného zákona, tedy povinnost zpracovávat osobní údaje se souhlasem subjektů údajů a bez tohoto souhlasu pouze na základě výjimek podle § 5 odst. 2 písm. a) až g) tohoto zákona, SVJ porušilo povinnost stanovenou v § 11 odst. 1 zákona o ochraně osobních údajů, tedy povinnost informovat subjekty údajů při shromažďování osobních údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat, komu mohou být osobní údaje zpřístupněny, a nepoučilo je o jejich právu na přístup k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona. SVJ porušilo ustanovení § 16 zákona o ochraně osobních údajů, tedy povinnost oznámit Úřadu pro ochranu osobních údajů skutečnost, že hodlá zpracovávat osobní údaje, a to před zpracováním osobních údajů, a tím spáchalo správní delikt podle § 45 odst. 1 písm. e), f) a i) zákona o ochraně osobních údajů, neboť zpracovávalo osobní údaje bez souhlasu subjektů údajů mimo případy uvedené v zákoně, neposkytlo subjektům údajů informace v rozsahu nebo zákonem stanoveným způsobem a nesplnilo oznamovací povinnost podle tohoto zákona.

SVJ podalo v únoru 2009 námitky ke KP. V rámci námitkového řízení vydal v květnu 2010 předseda Úřadu rozhodnutí, jímž námitkám kontrolovaného nevyhověl v plném rozsahu. SVJ byla v souladu s § 45 odst. 3 zákona o ochraně osobních údajů uložena pokuta ve výši 30 000,-Kč a dále podle § 79 odst. 5 správního řádu povinnost nahradit náklady řízení ve výši 1 000,- Kč. Proti tomuto rozhodnutí podal účastník řízení v červenci 2010 (SVJ) rozklad.

V září 2010 bylo vydáno předsedou Úřadu rozhodnutí v odvolacím řízení, ve kterém bylo konstatováno, že rozklad účastníka řízení se zamítá.

Opakovaná kontrola byla zahájena na základě stížnosti dvou obyvatelek domu (dále jen „stěžovatelky“) z července 2011. V dané stížnosti stěžovatelky uváděly, že v květnu 2009 zaslaly Úřadu podnět ve věci stížnosti na provoz kamerového systému ve Společenství. Dále uvedly, že *obdržely oznámení od výboru Společenství o opětovném spuštění kamerového systému s tím, že dne 17. ledna 2011 byl kamerový systém registrován na Úřadě, čímž byla splněna jedna z podmínek provozu. Stěžovatelky se ovšem domnívají, že je i nadále porušován zákon č. 101/2000 Sb., a to tím, že s provozem kamerového systému několik vlastníků nesouhlasí a dále je monitorován vchod i výtah a nelze zde aplikovat výjimku dle ust. § 5 odst. 2 písm. e) zákona, dochází k porušování § 11 zákona, neboť není známo, kdo a jakým způsobem bude informace zpracovávat a kdo bude mít k informacím přístup. Jelikož i při prvním spuštění kamerového systému docházelo k hrubým zásahům do soukromého života (fotografie pořizované z kamer, slovní napadání předsedou Společenství), stěžovatelky se domnívají, že se bude situace opakovat. Chápu riziko vandalismu, ale výbor Společenství nevyužil žádné jiné možnosti na ochranu majetku Společenství. Jsou-li nefunkční vstupní dveře, výbor situaci několik dní vůbec neřeší, potom pozbývá smysl kamerový systém.* Opětovně tedy požádaly o zvážení a prošetření této situace. Podle jejich názoru osoba předsedy Společenství a jeho jednání je spíše vrací do dob totality, kdy sledování, vyhrožování a pomluvy byly běžným prvkem.

Při ústním jednání a místním šetření, konaném v rámci opakované kontroly, zástupci SVJ seznámili kontrolující se změnami, které SVJ na základě předcházející kontroly při provozu kamerového systému se záznamem uskutečnilo. Zástupci SVJ sdělili, že nemají souhlas všech osob, tzn. vlastníků bytových jednotek, ale že s provozem kamer nesouhlasí pouze stěžovatelky. Zjištěno bylo, že SVJ změnilo nastavení pouze u jedné z kamer, ostatní kamery byly instalovány na stejném místě; místo jedné kamery proti vstupu do výtahu v přízemí je umístěna pouze maketa kamery (původní kamera byla odpojována a zůstala využita jako maketa). Pokud se jedná o plnění informační povinnosti, bylo kontrolujícím dokumentováno vylepení

upozornění na provoz kamerového systému a informace umístěná na nástěnce SVJ v přízemí domu. Dále bylo zjištěno, že řídicí jednotka je umístěna na stejném místě v suterénní uzamykatelné místnosti s tím, že není vybavena monitorem. Zástupci SVJ uvedli, že přístup k pořízeným záznamům má na základě smlouvy pouze zástupce servisní firmy. Dále uvedli, že v případě, že se něco stane, zavolají Policii ČR, za jejíž přítomnosti je záznam přehrán na přenosné médium. Uvedli, že důvodem pro umístění kamery byla skutečnost, že v sousedství došlo ke zdemolování výtahového zařízení. Dále sdělili, že záznam se pořizuje ze všech čtyř kamer a je uchováván po dobu cca tří dnů. Kontrolující bylo demonstrováno, že v provozní knize nebyl od poslední kontroly žádný záznam, kromě zápisu, že systém byl v červenci 2010 vypnut a v lednu 2011 byl opětovně zapnut.

Záměrem kontrolující bylo znovu objasnit SVJ základní principy ochrany osobních údajů zpracovávaných prostřednictvím kamerových systémů se záznamem v bytových domech.

SVJ bylo připomenuto, že základní problematika, která byla posuzována v jejich bytovém domě, je uvedena jak v rozhodnutí předsedy Úřadu o námitkách, tak i v rozhodnutí o udělení pokuty v rámci správního řízení, které bylo se Společenstvím vedeno.

Stěžovatelky zaslaly Úřadu opakovanou stížnost, v níž uvedly, že jsou monitorovány vstupní dveře, kamera je umístěna přímo ve výtahové kabině, SVJ nemá souhlas všech dotčených vlastníků a obyvatel domu. Dále stěžovatelky uvedly, že v poslední době osoba předsedy SVJ zneužívá kamerový systém ve svůj prospěch na ochranu své osoby. K dopisu přiložily i obrazový materiál. Vzhledem k závažnosti sdělení byly stěžovatelky písemně požádány o doplnění podnětu, které následně Úřadu zaslaly.

Na základě postoupení podnětu se věcí zabýval Městský úřad Příbram. Ze spisové dokumentace postoupené MÚ Příbram vyplývá, že předseda SVJ při podávání trestního oznámení na PČR Příbram ve věci podezření ze spáchání trestného činu proti občanskému soužití, spochybujícímu v diskreditaci jeho osoby, sdělil, že prostor nástěnky je monitorovaný kamerovým systémem, ze kterého je pořizován záznam. Tento záznam je uchováván po dobu tří dnů a záznam je oprávněn stáhnout pouze pracovník společnosti ČIP plus, s.r.o., a to za účasti PČR. Ze spisové dokumentace dále vyplývá, že v listopadu 2011 byl na základě žádosti předsedy SVJ vyslán příslušník PČR do bytového domu, kde za přítomnosti pracovníka externí společnosti spravující kamerový systém bylo provedeno kopírování záznamu, který měl dokumentovat činnost stěžovatelek. Příslušník PČR pořízený záznam převzal a vložil do spisové dokumentace. Záznam dokumentuje činnost stěžovatelek, konkrétně jejich jednání, kterak jedna z nich přichází k nástěnce a umísťuje na ni nějakou listinu.

Z vyjádření Policie ČR Příbram, které bylo vyžádáno v průběhu kontroly v roce 2009, vyplývá, že v uvedeném domě dochází ke zvýšenému pohybu zájmových osob policie a dále že při řešení několika oznámení byly využity záznamy pořízené kamerovým systémem v bytovém domě.

Kontrolující inspektorka konstatovala, že dle § 5 odst. 1 písm. a) zákona o ochraně osobních údajů je: „*správce povinen stanovit účel, k němuž mají být osobní údaje zpracovávány*“. Současně je dle § 16 odst. 1 téhož zákona „*ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle tohoto zákona, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováním osobních údajů*“. Dle § 16 odst. 3 uvedeného zákona lze „*zahájit zpracování osobních údajů po uplynutí lhůty 30 dnů ode dne doručení oznámení o zpracování*“. SVJ dle kontrolujících jako správce osobních údajů určilo účel ve výrazně větším rozsahu, než sdělilo Úřadu prostřednictvím registrace, přičemž dle zjištění kontrolujících je základním účelem zpracování osobních údajů prostřednictvím kamerového systému se záznamem sledování osob, konkrétně všech osob, které vcházejí a odcházejí do bytového

domu. Dle § 5 odst. 2 zákona o ochraně osobních údajů „*má správce povinnost zpracovávat osobní údaje pouze se souhlasem subjektu údajů*“, přičemž dle § 4 písm. n) zákona o ochraně osobních údajů se rozumí souhlasem subjektu údajů „*svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů*“. Bez tohoto souhlasu může správce zpracovávat osobní údaje pouze při splnění některé z výjimek uvedených v § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů. Dále dle § 5 odst. 4 zákona musí být správce schopen souhlas subjektu údajů se zpracováním osobních údajů prokázat po celou dobu zpracování.

V rámci kontroly bylo zcela bezpochyby zjištěno, že SVJ disponuje v současné době souhlasem se zpracováním osobních údajů prostřednictvím kamerového systému od sedmnácti osob, které jsou současně vlastníky bytů. Kontrolou v roce 2009 bylo konstatováno, že souhlas se zpracováním osobních údajů, získaný dle pravidel stanovených zákonem o bytech, tedy souhlas pouze nadpoloviční většiny vlastníků bytových jednotek, nemůže být považován za souhlas se zpracováním osobních údajů dle zákona o ochraně osobních údajů.

K absenci souhlasu všech osob žijících v domě SVJ ve svém vyjádření argumentuje právem většiny vlastníků společenství bytových jednotek garantovaným Listinou základních práv a svobod na ochranu zdraví a života a dalších práv zajišťujících ostatním vlastníkům práva touto listinou a zákony nad právem dvou vlastníků. SVJ dále uvádí, že zajistit pořádek v domě nelze jiným způsobem než prostřednictvím sledování osob. Listina práv a svobod ve svém článku 10 rovněž zajišťuje ústavní právo jednotlivce na ochranu před neoprávněným zasahováním do soukromého a rodinného života a právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.

I přes upozornění a vysvětlení střetu těchto dvou základních práv zaručených ústavou se SVJ ani v jednom případě nezabývalo právem menšiny na zachování jejího práva, práva na ochranu soukromí. SVJ se rovněž nevypořádalo s možností zajistit bezpečnost chráněných zájmů jinými prostředky. SVJ se nevypořádalo s podmínkou, danou zákonem o ochraně osobních údajů, která spočívá v nezbytnosti shromažďování a zpracování, tak jak je uvedena v § 5 odst. 1 písm. d) a v § 5 odst. 2 písm. e) zákona o ochraně osobních údajů.

Z podkladů shromážděných v rámci kontroly vyplývá, že SVJ zcela přehlíží právo osob, které vyjádřily svůj nesouhlas. Všechna vyjádření a podklady SVJ se de facto opírají o nesouhlas s postojem stěžovatele. Je nezbytné zcela odmítnout jako nepřípustné, aby zastavení provozu kamerového systému se záznamem bylo svalováno na spolubydlící, když z pravomocného rozhodování Úřadu je zcela zřejmé, že za nezákonné využívání informací z kamerového systému odpovídá výbor, resp. předseda Společenství.

Při aplikaci stanoviska č. 1/2008 – Umístění kamerových systémů v bytovém domě kontrolující konstatuje, že u kamery v kotelně lze aplikovat zákonnou výjimku podle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů.

SVJ rozhodlo, že bude chránit svůj majetek, ale tento majetek chrání prostřednictvím shromažďování informací o osobách, které do bytového domu vstupují. Prostřednictvím monitorování osob dochází k neproporcionálnímu sledování osob, a ne k ochraně majetku, k čemuž využívá zcela nevhodné argumenty, které nemají oporu ve skutečnosti (případ usmrčeného dítěte s kalkulací na strach rodičů o děti, argumentace o poškození výtahu v jiném bytovém domě, zabránění shromažďování osob před prostranstvím domu).

Z uvedeného vyplývá, že výjimku dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů lze aplikovat pouze u kamery umístěné v kotelně. Na ostatní kamery uvedenou výjimku aplikovat nelze.

SVJ v případě provozování kamerového systému se záznamem prostřednictvím kamer u vchodových dveří do domu, u poštovních schránek a ve výtahu porušilo ustanovení § 5 odst. 2 tím, že shromažďovalo a zpracovávalo osobní údaje získané prostřednictvím uvedených kamer bez souhlasu subjektů údajů.

Podezření stěžovatelek, že předseda SVJ zneužil pořízené záznamy z kamerového systému se záznamem, tedy podezření na porušení ustanovení § 13 odst. 1 zákona o ochraně osobních údajů, je neoprávněné, neboť fotografie jednání stěžovatelek, které jsou součástí spisové dokumentace přestupkové komise MÚ Příbram, byly do spisu vloženy na základě rozhodnutí příslušného útvaru Policie ČR, které šetřilo trestní oznámení.

Dle přijatých vnitřních pravidel SVJ mohou být osobní údaje shromážděné prostřednictvím kamerového systému se záznamem použity pouze v případě trestného činu, a to za přítomnosti Policie ČR. Využití záznamů k řešení osobního sporu, ke kterému došlo mezi předsedou SVJ a rodinou jedné ze stěžovatelek, je porušením těchto vlastních pravidel. Současně je nezbytné konstatovat, že o předání pořízeného záznamu nebyl proveden záznam v provozní knize. Z podstaty sporu, který nejenže nebyl trestným činem, ale ani přestupkem, je zřejmé, že pořízené záznamy měly být využity pouze k osobnímu zájmu předsedy SVJ. SVJ tím, že neoprávněně předalo záznamy k jinému účelu, než bylo deklarováno, porušilo ustanovení § 13 odst. 1 zákona o ochraně osobních údajů.

SVJ v souvislosti s kontrolou plnění nápravných opatření provedených předcházející kontrolou z roku 2010 nepřijalo taková opatření v souvislosti s provozováním kamerového systému, která by odpovídala ustanovení zákona o ochraně osobních údajů. SVJ provozováním kamerového systému se záznamem prostřednictvím kamer u vchodových dveří do domu, u poštovních schránek a ve výtahu porušilo povinnost uloženou SVJ jako správci osobních údajů v ustanovení § 5 odst. 2 a § 13 odst. 1 zákona o ochraně osobních údajů.

V souladu s § 40 odst. 1 zákona o ochraně osobních údajů uložila inspektorka Úřadu SVJ opatření k odstranění zjištěných nedostatků a stanovila lhůtu pro jejich odstranění: neshromažďovat a dále nezpracovávat osobní údaje osob nacházejících se ve sledovaných prostorách domu prostřednictvím kamerových záznamů pořizovaných kamerami (u vchodu a poštovních schránek) způsobem porušujícím platnou právní úpravu tak, aby byl minimalizován zásah do soukromí osob procházejících chodbami v přízemí bytového domu a současně byla zachována nebo zvýšena úroveň ochrany majetku SVJ, neshromažďovat a dále nezpracovávat osobní údaje osob nacházejících se v kabinách výtahů prostřednictvím kamerových záznamů pořizovaných kamerou způsobem porušujícím platnou právní úpravu a uvést do souladu informace předané do veřejného registru správců osobních údajů, vedeného Úřadem pro ochranu osobních údajů, týkající se souhlasu zpracování osobních údajů, se skutečným stavem.

NAKLÁDÁNÍ S CITLIVÝMI OSOBNÍMI ÚDAJI KLIENTŮ DOMOVA DŮSTOJNÉHO STÁŘÍ A ZPRACOVÁNÍ JEJICH OSOBNÍCH ÚDAJŮ PROSTŘEDNICTVÍM KAMEROVÉHO SYSTÉMU S UMÍSTĚNÍM KAMER NA POKOJÍCH A SPOLEČNÝCH PROSTORÁCH

Předmětem kontroly u společnosti s ručením omezeným, která provozovala, a to do doby výpovědi pronajímatele z nájemních prostor pro neplacení nájemného, tzv. Domov důstojného stáří, bylo dodržování povinností při zpracování osobních údajů seniorů trpících v různých stádiích Alzheimerovou chorobou a demencemi jiného typu, Parkinsonovou nemocí,

roztroušenou sklerózou apod. Kontrola se uskutečnila na základě podnětu příbuzného jednoho z ubytovaných klientů.

Při kontrole, při níž bylo zjištěno porušení zákona o ochraně osobních údajů, při neoprávněném nakládání s osobními, resp. citlivými údaji klientů Domova důstojného stáří podle obchodního zákoníku, vyplynulo ze součinnosti zejména s Veřejným ochráncem práv dále podezření, že Domov důstojného stáří poskytoval zdravotní služby, aniž k tomu měl oprávnění, a stejně tak poskytoval bez oprávnění podle ustanovení § 107 odst. 1 zákona č. 108/2006 Sb., o sociálních službách, tj. bez registrace, o níž rozhoduje krajský úřad příslušný podle sídla Domova důstojného stáří.

Výsledkem kontroly bylo prokázáno, že Domov důstojného stáří zpracovával osobní údaje klientů komerčního ubytovacího zařízení prostřednictvím kamerového systému se záznamem, s umístěním na jednotlivých pokojích klientů, chodbách a v místnosti označené „sesterna“ v rozporu se zákonem o ochraně osobních údajů. V souladu s ustanovením § 5 odst. 1 písm. d) tohoto zákona může správce shromažďovat osobní údaje odpovídající stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Je zřejmé, že pořizování kamerového záznamu v jakémkoliv rozsahu z důvodu sledování vývoje zdravotního stavu, případně prevence pádu z postele u ubytovaných klientů, je zbytečné. Zásadní pro naplnění tohoto účelu by měla být osobní péče pečovatelek či zdravotních sester doplněná v krajních případech kamerovým systémem s on-line přenosem, což by bylo ovšem možné pouze u zařízení poskytujícího zdravotní nebo sociální služby podle zvláštního zákona. Tuto podmínku však kontrolovaný nesplňoval, proto nebylo možné kamerový systém s on-line přenosem pro tento účel případně doporučit. Záznam z kamer má spíše funkci dokumentační a nemůže plnit preventivní účel, jak jej stanovil kontrolovaný. Provozováním kamerového systému se záznamem nebyla splněna povinnost stanovená v ustanovení § 5 odst. 1 písm. d) zákona o ochraně osobních údajů. Vzhledem k tomu, že samo shromažďování kamerových záznamů neodpovídalo stanovenému účelu, nebylo možno ani dobu sedmi dnů pro uchovávání osobních údajů ve smyslu ustanovení § 5 odst. 1 písm. e) uvedeného zákona považovat v tomto případě za přiměřenou, ačkoliv v případě účelnosti pořizování záznamu z kamerového systému je tato doba obvykle za přiměřenou považována. Kontrolovaný neprokázal, že by disponoval platným souhlasem všech osob, jejichž osobní údaje byly ve smyslu ustanovení § 5 odst. 2 zákona o ochraně osobních údajů prostřednictvím kamerového systému zpracovávány, ani nebylo možné uplatnit žádnou z výjimek v tomto ustanovení pod písm. a) – g) uvedenou.

Monitorování jednotlivých pokojů obývaných klienty a monitorování zaměstnanců v místnosti, kde se převážně zdržují, je zásahem do jejich soukromí intenzivnější, a proto i v případě individuálního obecného souhlasu nemohl být považován za informovaný ve smyslu ustanovení § 11 odst. 1 zákona o ochraně osobních údajů. Vzhledem k tomu, že se nejednalo ani o splnění podmínek uvedených v ustanovení § 4 písm. n) a § 5 odst. 4 tohoto zákona, kdy se musí jednat o svobodný a vědomý projev vůle a vyžaduje se informovaný souhlas subjektu údajů, mohl být nekonkrétní souhlas uvedený ve smlouvě o ubytování považován za neplatný souhlas se zpracováváním osobních údajů podle ustanovení § 5 odst. 2 zákona o ochraně osobních údajů. Kontrolovaný rovněž nedisponoval svobodným a informovaným souhlasem klientů, jejichž citlivé údaje zpracovával v jejich osobních kartách. I v případě, že by klienti kontrolovanému podepisovali svobodně informovaný souhlas se zpracováním osobních údajů, tak by vzhledem k diagnóze klientů, z nichž řada má snížené intelektuální schopnosti související zejména s Alzheimerovou či Parkinsonovou chorobou, bylo v některých případech nutné souhlas považovat za neplatný v souladu s ustanovením § 38 odst. 2 občanského zákoníku,

a to ačkoli klient nebyl zbaven ani omezen ve způsobilosti k právním úkonům. Toto posouzení by ovšem bylo nezbytné vztáhnout k jednotlivým klientům a k jejich zdravotnímu stavu v době udělení souhlasu, což vzhledem k obecnému posouzení udělených souhlasů se zpracováním jako neplatných nebylo dále kontrolou zjišťováno.

Instalování a následný provoz kamerového systému se záznamem na pokojích klientů s nepřetržitým monitorováním těchto prostor je zcela zásadním zásahem do práva na soukromí klientů kontrolovaného. Nepřetržité monitorování těchto klientů v místech, kde by měli požívat té nejvyšší míry soukromí, a to bez jejich souhlasu a bez náležitého informování o jejich právech, jakož i bezdůvodné pořizování záznamu z tohoto monitorování, je zásadním zásahem do lidské důstojnosti klientů zařízení. Tento zásah je o to intenzivnější, že klienti jsou často ve vážném zdravotním stavu, který jim neumožňuje se tomuto nepřetržitému sledování efektivně bránit. Rovněž je nepřipustné s odkazem na zákon č. 262/2006 Sb., zákoník práce, monitorování zaměstnanců kontrolovaného při jejich práci.

Zdravotnická dokumentace klientů nebo její část, v daném případě kontrolovaným uváděna jako osobní karta klienta, obsahující citlivé údaje, musí požívat zvýšenou ochranu při nakládání s ní. Nelze považovat za dostatečné, pokud je tato dokumentace volně přístupná v místnosti označené jako „sesterna“ bez k tomu odpovídajícího zabezpečeného a řádně uzamkatelného prostoru, včetně provedení technicko-organizačních opatření k zajištění ochrany osobních údajů v souladu s ustanovením § 13 zákona o ochraně osobních údajů.

Kontrolovaný rovněž nesplnil oznamovací povinnosti vůči Úřadu podle ustanovení § 16 zákona o ochraně osobních údajů.

S ohledem na zjištění, že právnická osoba vedla záznamy o klientech, zejména pak o jejich zdravotním stavu a užívaných lécích, včetně zpráv z ošetření klientů, písemností vážících se k příspěvkům na péči či k posuzování způsobilosti k právním úkonům, a osobní dokumentace obsahovala propouštěcí zprávy při hospitalizaci v nemocnici, a to bez informovaného souhlasu, a tyto dokumenty byly uloženy v listinné podobě v nevhodných a nezajištěných prostorách, byla inspektorem uložena opatření k nápravě, a to provést likvidaci osobních údajů klientů zařízení, včetně citlivých, v souladu s ustanovením § 20 zákona o ochraně osobních údajů. Za porušení povinností uložených zákonem o ochraně osobních údajů byla Domovu důstojného stáří uložena pokuta s tím, že v případě zjištění dalšího či opakujícího se porušení povinností při obdobné podnikatelské činnosti v jiné provozovně dle výsledků šetření Veřejného ochránce práv v souvislosti s podezřením na porušení zejména zákona č. 108/2006 Sb., o sociálních službách, bude možné uložit v souvislosti s porušením zákona o ochraně osobních údajů další pokutu, včetně pokuty za nesplnění uložených nápravných opatření.

■ VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ

Na rozdíl od roku 2011, kdy nárůst nebyl tak výrazný, zaznamenal odbor pro styk s veřejností Úřadu opětovně standardní nárůst počtu podnětů a stížností na protiprávní jednání při zpracování osobních údajů, který dlouhodobě meziročně činí cca 20 %. Úřad obdržel celkem 1 319 podání a oproti roku 2011 tak došlo k celkovému nárůstu o 18 %.

Situace dosáhla v letošním roce stavu, který za současného personálního obsazení Úřadu (přičemž nelze navýšit počet kontrolních pracovníků) není řešitelný, neboť není reálné zahájit v jednom kalendářním roce téměř tisíc incidenčních kontrol. S ohledem na zkušenosti obdobných dozorových orgánů v Evropské unii a připravovaný nový evropský základní rámec ochrany osobních údajů by to ani neměla být hlavní náplň činnosti Úřadu.

Po vyhodnocení průběžné analýzy informací získaných za více než dvanáctiletou existenci dospěl Úřad k závěru, že ochrana osobních údajů je primárně věcí subjektů údajů. Právní vědomí občanů v této oblasti se neustále prohlubuje a dosáhlo úrovně, kdy drtivá většina z nich je schopna a ochotna využívat svá práva daná zákonem o ochraně osobních údajů. To byly hlavní důvody, které vedly Úřad k novele citovaného zákona spočívající v odstranění možnosti občanů obracet se přímo na Úřad, aniž by se alespoň pokusili řešit věc sami formou písemné žádosti příslušnému správci osobních údajů o vysvětlení, odstranění závadného stavu, případně blokaci nebo likvidaci svých osobních údajů. Teprve poté, co nebude jejich oprávněným nárokům vyhověno, mohou se obrátit na Úřad s tím, že meritum věci alespoň základním způsobem doloží, např. kopiemi příslušné korespondence se správcem.

Uvedená legislativní změna zákona o ochraně osobních údajů (ukončení platnosti bývalého ustanovení § 21 odst. 4) byla hlavním důvodem nárůstu (o 27 %) počtu stížností, které byly odloženy jako nedůvodné. Počet ostatních forem řešení stížností zůstal víceméně na úrovni předchozích let, což je zejména u počtu stížností předaných ke kontrole (cca 200 ročně) skutečně hraniční mezí možností Úřadu.

Statistika stížností vyřízených v roce 2012

Celkem	1 319
z toho: předáno ke kontrole	197
předáno na zahájení řízení	69
postoupeno příslušným orgánům	13
odloženo jako nedůvodné	1 040

Stejně jako v roce 2011 byl zaznamenán největší nárůst počtu podání v oblasti moderních informačních technologií obecně označitelných jako prostředí internetu (547 podání). Oblast sociálních sítí, zejména nejdynamičtěji celosvětově se rozvíjející Facebook, který se blíží 1 miliardě uživatelů, ale i různá diskusní fóra, „soukromé“ databáze dlužníků, neplatičů apod., se tak poprvé stala nejčastějším předmětem stížností dotčených občanů.

V souvislosti s nabytím účinnosti zákona o trestní odpovědnosti právnických osob dnem 1. 1. 2012 byl zaznamenán významný nárůst stížností zaměstnanců na jejich protiprávní monitorování na pracovišti a ve společných prostorách zaměstnavatele. Zdaleka již nejde jen o kamerové systémy se záznamovým zařízením, ale o zneužívání stále sofistikovanějších

technických prostředků k monitorování telefonických hovorů, elektronické pošty, skryté instalování fotopastí, nasazování systémů využívajících k lokalizaci pohybu zaměstnanců principů GPS, WiFi atd.

Analýzou obsahu podání tohoto typu lze dospět k závěru, že zaměstnavatelé jsou si dobře vědomi rizik, které jim může neodpovědný zaměstnanec způsobit, včetně výmazu společnosti z Obchodního rejstříku. Vědomě překračují zákonná oprávnění s cílem vybrat si skutečně spolehlivé pracovníky a ty, často opět za hranou zákona, kontrolovat, monitorovat, sledovat na pracovišti, ve společných prostorách a dokonce i v mimopracovní dobu.

Ochrana osobních údajů zpracovávaných v rámci pracovněprávních vztahů tvoří značnou část dozorové činnosti Úřadu. Jeho posláním je především chránit subjekty údajů, tedy zaměstnance, před neoprávněným nebo jinak protiprávním zpracováním osobních údajů. Současně se Úřad snaží být naprosto nestranný ve smyslu přístupu i k oprávněným zájmům zaměstnavatelů majícím postavení správců osobních údajů. V rámci správního uvážení je schopen reflektovat a respektovat, že základním zájmem zaměstnavatelů je dosažení zisku a perspektiva dalšího rozvoje společnosti v rámci svobodného podnikání, samozřejmě ovšem v mezích zákona o ochraně osobních údajů jakožto základního lidského práva. Trvalým jevem byl v roce 2012 nesprávný postup tzv. povinných subjektů, nejčastěji obecních úřadů, spočívající ve zveřejňování osobních údajů tazatelů podle zákona o svobodném přístupu k informacím (blíže viz kapitolu této VZ Právo na informace při respektování práva na ochranu osobních údajů).

Úřad se snažil o systémové řešení cestou spolupráce s věcně odpovědným Ministerstvem vnitra, které vydalo v tomto směru metodický pokyn pro všechny orgány veřejné správy. Obdobný problém se objevil i u soudů všech stupňů, a protože by bylo opět velmi neefektivní řešit každý ad hoc případ samostatně, byl dopisem předsedy Úřadu osloven ministr spravedlnosti, který přislíbil zjednání nápravy rovněž vydáním metodického pokynu k odstranění uvedené nežádoucí praxe.

Úřad obdržel řadu požadavků orgánů veřejné správy i neziskových organizací v souvislosti s pořizováním video a audiozáznamů z jednání zastupitelstev. V současné době Úřad připravuje samostatné stanovisko k této problematice, přestože výklad podal již ve výroční zprávě za rok 2011. Na tomto místě lze proto jen opakovaně konstatovat, že Úřad musí respektovat platnou právní úpravu, zejména zákon o obcích, který zatím stále ještě rozlišuje dvě kategorie osob z hlediska přístupu k zápisu z jednání zastupitelstva, potažmo tedy i k pořizování záznamu, a to v zásadě na občany s trvalým pobytem v obci, kterým je zápis zpřístupňován v plném rozsahu, a ostatní, kterým zákon o obcích právo přístupu k zápisu nepřiznává. Znamenán byl posun v přístupu orgánů obcí, které upouštějí od pořizování záznamu a na internet přenášejí on-line přenos z jednání zastupitelstva. Takováto činnost sice již přesahuje působnost Úřadu, neboť se nejedná o zpracování ve smyslu zákona o ochraně osobních údajů, nicméně z pohledu potenciálních zásahů do soukromí občanů není zveřejněním celého průběhu jednání neomezenému počtu osob zásadní rozdíl. Shodný názor prezentoval i Veřejný ochránce práv v informačním bulletinu Úřadu č. 2/2011 věnovaném kamerovému sledování, a již tedy více než před rokem doporučil přijetí adekvátních legislativních opatření.

Z poskytnutých osobních konzultací pro ilustraci uvádíme následující subjekty a řešení otázky: Ministerstvo školství, mládeže a tělovýchovy – integrace cca padesáti vedených agend do jediné centralizované databáze (projekt „Nedir“) nebyla doporučena; Národní ústav pro vzdělávání – získávání adresných údajů absolventů odborných škol za účelem studie jejich úspěšnosti na trhu práce musí respektovat příslušná ustanovení školského zákona; Český

statistický úřad – oprávnění uvažovaného vedení samostatné databáze osobních údajů nemá oporu ve zvláštním zákoně, a bylo by tedy v rozporu i se zákonem o ochraně osobních údajů; Úřad pro civilní letectví – možnost vydávání karet posádkám letadel na základě Chicagské úmluvy nahrazujících vízum do Ruské federace nebyla shledána v rozporu se zákonem; České dráhy, a.s. – zřízení „Centra sdílených služeb“, které by centrálně spravovalo veškerou personální a mzdovou agendu všech dceřiných společností, s výjimkou ČD Cargo, a.s., zákon o ochraně osobních údajů nebrání; Volksbank CZ, a.s.– pro požadované předávání osobních údajů tzv. „matce“ se sídlem v Ruské federaci je nezbytné postupovat podle ustanovení § 27 zákona o ochraně osobních údajů; společnost Lidl – po posouzení pilotního projektu „Centrální pokladní zkouška“ bylo konstatováno, že použité postupy nelze považovat za sledování zaměstnanců na pracovišti ve smyslu zákoníku práce a nejsou ani v rozporu se zákonem o ochraně osobních údajů; Merck Sharp & Dohme, s.r.o. – při posuzování možností retrospektivního sběru dat byla doporučena anonymizace osobních údajů tak, že jednotlivá zdravotnická zařízení obdrží pouze agregovaná data bez možnosti jejich vztažení ke konkrétním pacientům.

K nejčastějším a současně nejzávažnějším porušením zákona správci nebo zpracovateli osobních údajů zjišťovaným v roce 2012, na které bude soustředěna i nadále pozornost Úřadu, patří: nepřijetí adekvátních opatření k zabezpečení zpracovávaných osobních údajů, jejich neoprávněné shromažďování, zveřejňování a další formy zpracovávání bez souhlasu subjektu údajů.

■ POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

„FALEŠNÉ“ SMLOUVY

Úřad se častěji než v předešlých letech setkával v roce 2012 s případy smluv o poskytování různého typu služeb (a méně často smluv kupních), pro které byly osobní údaje subjektů údajů využity neoprávněně a bez jejich vědomí. Došlo tedy k porušení zákona o ochraně osobních údajů. Typické pro tyto případy je, že se jedná nikoli o přímé uzavření smlouvy mezi zájemcem a poskytovatelem služby, ale že uzavření smlouvy probíhá prostřednictvím obchodních zástupců. Často se jedná o situaci, kdy obchodní zástupce jako fyzická osoba podnikající pracuje pro společnost (případně jinou fyzickou osobu podnikající), a teprve ta má uzavřenou smlouvu se samotným poskytovatelem služeb. Vztahy mezi jednotlivými osobami a s tím související odpovědnost za zpracování osobních údajů se tak stávají velmi nepřehlednými.

Zpravidla Úřadu podněty k projednání z této oblasti předává k vyřízení Policie České republiky, která je šetří na základě trestního oznámení údajného klienta, jenž se o zneužití svých osobních údajů nějakým způsobem dozvěděl – typicky tak, že je jakožto údajný klient osloven poskytovatelem služby s požadavkem finančního plnění. V některých případech je trestní oznámení podáváno poskytovatelem služby, který měl být smluvní stranou falešné smlouvy, opět na základě podnětu klienta, jenž se na provozovatele obrátí ve chvíli, kdy po něm jsou vymáhány nějaké finanční závazky. Obvyklým závěrem orgánů činných v trestním řízení je, že nebyly naplněny požadované znaky trestného činu, konkrétně pak odpovídající společenská škodlivost, příp. trestním zákonem požadovaná výše škody. Většinou je totiž po upozornění ze strany dotčeného subjektu údajů smlouva poskytovatelem služeb bez větších problémů stornována a údajný klient tak nese spíše náklady časové než finanční. Tyto skutky jsou dále projednávány jako správní delikty na úseku ochrany osobních údajů. Nejvyšší sankcí, kterou Úřad v těchto případech uložil, byla pokuta ve výši 50 000 Kč.

Je také zajímavé zmínit, že, jak vyplývá z dále uvedených případů, není vždy motivem jednání obchodního zástupce neoprávněné získání provize. Je to však motiv jistě převládající. V některých ze zjištěných případů bylo cílem „pouze“ naplnit požadovaný počet uzavřených smluv a obchodní zástupce zjevně počítal s tím, že, ještě než se o neoprávněném použití svých údajů údajný klient dozví, bude možno smlouvu stornovat.

Důležité je uvést též skutečnost, že v řadě případů je součástí souboru neoprávněně využívaných osobních údajů také rodné číslo jako obecný identifikátor občana. V důsledku nadměrného používání tohoto údaje v soukromoprávních vztazích, na které Úřad opakovaně upozorňuje, se tak paradoxně a v rozporu s očekáváním druhé smluvní strany stává smlouva, která rodné číslo uživatele služby obsahuje, nikoli automaticky přesná a důvěryhodná.

Je třeba zdůraznit, že předejití uzavírání „falešných“ smluv nastavením vnitřních procesů je povinen vždy též poskytovatel služeb, v jehož prospěch jsou smlouvy uzavírány. Jako možný postup, jak co nejdříve odhalit problematrické smlouvy, se jeví například odeslání „uvítacího dopisu“ všem novým klientům se shrnutím obsahu uzavřené smlouvy. Skutečnost, že je třeba v případě zjištění neoprávněně uzavřených smluv určitým obchodním zástupcem prověřit důkladně všechny jím uzavřené smlouvy, snad není třeba zdůrazňovat. V případě, že by tak přímý poskytovatel služeb (případně jeho obchodní zástupce, s nímž na základě smlouvy spolupracuje ten obchodní zástupce, který problematrickou smlouvu uzavřel) neučinil, je nutno uvažovat o tom, že na něj přechází částečná odpovědnost, a to i z hlediska ochrany osobních údajů.

Z popisu konkrétních případů je zřejmé, že některé jejich okolnosti se vyskytují opakovaně. Takovou je například skutečnost, že údaje byly získány z vyúčtování, které sám subjekt údajů obchodnímu zástupci předložil k nahlédnutí, neboť mu byly nabízeny finančně výhodnější služby. Úřad se tak musí připojit k varování nejrozličnějších spotřebitelských organizací, které dlouhodobě před smlouvami uzavíranými na schodech či mezi dveřmi varují (totéž se týká i „pouhého“ předávání podkladů pro případné pozdější uzavření takové smlouvy).

Následuje shrnutí některých Úřadem v roce 2012 projednávaných případů:

Obchodní zástupce získal osobní údaje konkrétního subjektu údajů v rámci jednání o uzavření smlouvy, která však nebyla platně uzavřena (byla stornována). Obchodní zástupce pak použil údaje tohoto subjektu bez jeho souhlasu k uzavření úvěrové (a následně pak kupní) smlouvy pro zcela jiný subjekt údajů, a to proto, aby tento subjekt „dosáhl na úvěr“, a tedy mohl jeho prostřednictvím uzavřít kupní smlouvu, za jejíž uzavření by obchodní zástupce samozřejmě získal příslušnou provizi.

Obchodní zástupce společnosti použil údaje, které získal ze své dřívější (blíže neurčené) činnosti k vyplnění přihlášky klienta, zájemce o elektronickou zdravotní knížku. Tyto přihlášky přitom byly sjednávány pro třetí společnost (tj. nikoli pro tu, se kterou měl uzavřenou smlouvu o obchodním zastoupení). Současně nepravdivě uvedl jako zpracovatele přihlášky namísto sebe jinou osobu, která pro něj dříve tuto činnost vykonávala. Důvodem pro jeho jednání byla potřeba splnit plán, do čehož mu ještě několik přihlášek chybělo.

Obchodní zástupce společnosti uzavíral bez vědomí údajných klientů smlouvy o půjčce, a to za použití jejich osobních údajů. Celkem se jednalo o sedmáct smluv, na jejichž základě získal od společnosti, pro kterou jako obchodní zástupce pracoval, neoprávněně cca 370 000 Kč. Údaje některých lidí přitom znal (např. se jednalo o jeho sestru, bývalou přítelkyni, osobu, jejíž údaje získal v souvislosti s vymáháním pohledávky), další údaje získal v rámci výkonu svého předchozího zaměstnání, u některých osob, jak tvrdil, údaje zjistil z poznámkového sešitu, který náhodně našel. Za své jednání byl odsouzen k trestu odnětí svobody v délce jednoho roku s podmíněným odkladem trestu na zkušební dobu v délce tří let za přečin úvěrového podvodu a za přečin zpronevěry. Úřad však došel k závěru, že skutek, za který byl odsouzen, není totožný se skutkem, pro který bylo s tímto obchodním zástupcem vedeno správní řízení. Předmětem trestního řízení totiž nebylo neoprávněné zpracování osobních údajů domnělých klientů, ale jednání související s jeho vztahem ke společnosti, pro kterou pracoval. Proto sankci za jednání (pokračující správní delikt), které trvalo cca devět měsíců, uložil Úřad ve výši 50 000 Kč.

Autorizovaný energetický poradce uzavřel bez vědomí údajných klientů dvě smlouvy o sdružených dodávkách elektřiny a plynu ve prospěch třetí společnosti. Osobní údaje jednoho z údajných klientů poradce získal tak, že tuto osobu oslovil v místě jejího trvalého bydliště a požádal ji o předložení zálohových faktur na odběr elektrické energie a jako obchodní zástupce společnosti jí nabídl změnu dodavatele, vyplnil návrh smlouvy o sdružených dodávkách elektřiny a plynu, do které vyplnil nezbytné osobní údaje, a ačkoli tato osoba podepsat návrh smlouvy následně odmítla, odnesl si vyplněný návrh s sebou. Z jakého zdroje obchodní zástupce získal osobní údaje druhého z klientů, se nepodařilo šetřením Policie České republiky ani v následném správním řízení vedeném Úřadem zjistit.

Obchodní zástupce společnosti použil osobní údaje bez vědomí subjektu údajů pro uzavření Rámcové smlouvy na dodávku elektřiny a plynu, plné moci, kterou měl subjekt údajů zmocnit společnost k jednání o podmínkách dodávek elektřiny a plynu, a pro odstoupení od uvedené smlouvy. Osobní údaje přitom získal obchodní zástupce při návštěvě údajného klienta v místě jeho trvalého pobytu z klientem zapůjčeného vyúčtování za odběr plynu a elektřiny. Následně se obchodní zástupce doznal k vyplnění uvedených listin s tím, že mu chybělo ještě několik přihlášek na to, aby splnil plán.

Závěrem je třeba k této problematice konstatovat následující: S ohledem na výše popsanou rozmáhající se nezákonnou praxi bude Úřad nucen se této oblasti výrazněji věnovat ve všech součástech své dozorové činnosti. Jeví se totiž jako potřebné zaměřit se nejen na zjištěné případy porušení zákona o ochraně osobních údajů v reakci na zjištěné delikty, nýbrž též na předcházení takovéto praxi. K takovému proaktivnímu přístupu lze přitom jistě přispět kontrolní činností, v jejímž rámci budou posuzována opatření poskytovatelů služeb k odhalování neoprávněně uzavíraných smluv. Úřad bude dále muset důsledně vyhodnocovat závažnost jednání pachatele správního deliktu a od ní odvozené výše sankce, a to přesto, že má za to, že výše popsaná jednání jsou primárně otázkou porušení občansko- či obchodněprávních vztahů. Zásah do soukromí a do práva na ochranu osobních údajů však v žádném případě nelze přehlížet.

ZVEŘEJŇOVÁNÍ INFORMACÍ (FOTOGRAFIÍ NEBO ČÁSTÍ ZÁZNAMŮ) POŘÍZENÝCH KAMEROVÝM SYSTÉMEM ZA ÚČELEM ODHALENÍ PACHATELŮ PROTIPRÁVNÍHO JEDNÁNÍ

Ve společnosti bylo během roku 2012 velmi rozporuplně vnímáno několik řízení, která Úřad vedl ve věci zveřejňování informací soukromými osobami za účelem dopadení pachatelů protiprávních jednání (přestupků nebo trestných činů). Jednalo se přitom zejména o publikování fotografií zachycených kamerovým systémem instalovaným v místě, kde měl být údajný protiprávní čin spáchán, prostřednictvím sociálních sítí (resp. obecně internetu).

K tomuto tématu je nutno předeslat, že podle článku 90 Ústavy České republiky pouze soud rozhoduje o vině a trestu za trestné činy. Právě toto ustanovení ve spojení s článkem 7 (Ne-dotknutelnost osoby a jejího soukromí je zaručena.) a článkem 10 (Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.) Listiny základních práv a svobod pak musí být základem pro posuzování všech případů, které mohou ve svém důsledku prolamovat takové základní zásady právního státu, jako je presumpce nevinny apod.

Z hlediska zákona o ochraně osobních údajů vždy platí, že zpracování osobních údajů, tedy provoz kamerového systému se záznamem, včetně případného dalšího zpracování údajů, které byly takovým systémem shromážděny, musí mít svůj právní titul. Tím může být souhlas subjektu údajů nebo některá z výjimek dle § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů. V případě provozu kamerových systémů obvykle dochází ke zpracování osobních údajů bez souhlasu subjektu údajů na základě výjimky dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, tj. je-li to nezbytné pro ochranu práv a právem chráněných zájmů (jako je např. ochrana majetku) správce, příjemce nebo jiné dotčené osoby a nejedná-li se o nepřiměřený zásah do soukromí sledovaných osob.

Právě posouzení a vyvážení dvou kritérií (tedy práva na ochranu majetku a práva na soukromí) je zásadní pro vyhodnocení legálnosti většiny kamerových systémů. Jednou ze základních vlastností kamerového systému přitom je, že shromažďuje a uchovává osobní údaje, tj. informace o soukromém životě, v naprosté většině běžných osob, které se žádného protiprávního jednání nedopouštějí. Proto je možné provozovat kamerové systémy bez souhlasu subjektu údajů jenom tehdy, je-li bezpodmínečně zabezpečeno, že osobní údaje z tohoto kamerového systému nebudou nijak zveřejněny ani jiným způsobem šířeny (s výjimkou, která bude uvedena dále).

Tento princip je vyjádřen v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, podle kterého lze zpracovávat osobní údaje jen v souladu s účelem, ke kterému byly shromážděny, a k jinému účelu jen se souhlasem subjektu údajů. Je-li účelem kamerového systému (zpracování osobních údajů) ochrana majetku, znamená to, že v případě odcizení majetku nebo způsobení jiné škody může kamerový systém, resp. záznam z něj, napomoci zjištění pachatele. Vyhledávání pachatelů trestných činů a shromažďování důkazů o jejich vině je ovšem v demokratickém právním státě rolí orgánů činných v trestním řízení (tj. orgánů státu), a nikoliv provozovatele kamerového systému. Proto je každý správce osobních údajů z kamerového systému v souladu s účelem ochrany majetku oprávněn pouze k předání záznamu orgánům činným v trestním řízení, ale již nesmí sám tyto záznamy zveřejnit. Orgány činné v trestním řízení jsou za zákonem stanovených podmínek, na základě svých znalostí a zkušeností, a po vyhodnocení všech jim dostupných důkazů a informací, oprávněny zahájit proti konkrétní osobě trestní řízení, které je výrazem toho, že je daná osoba důvodně podezřelá z trestného činu, případně vyhlásit po takové osobě pátrání. V případě pátrání po pachateli trestného činu je poté Policie České republiky v souladu s § 81 písm. a) bodu 2. zákona č. 273/2008 Sb., o Policii České republiky, oprávněna zveřejnit osobní údaje (tedy např. i fotografii podezřelé osoby pořízenou kamerovým systémem) v rozsahu nezbytném k plnění úkolů policie v souvislosti s pátráním po osobách. Pokud tedy provozovatel kamerového systému, jako správce osobních údajů, sám zveřejnil na svých stránkách na sociální síti fotografii podezřelé osoby pocházející z jím provozované kamery, jednalo se o zpracování osobních údajů k jinému účelu, než ke kterému byly osobní údaje shromážděny, proto tedy zveřejněním došlo k porušení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů.

■ POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

Úřad pro ochranu osobních údajů je účastníkem celé řady soudních sporů. Pokud jde o poznatky z rozhodovací praxe za rok 2012, lze poukázat na pět dále uvedených významných oblastí, týkajících se správy daní, povahy podnětu nebo stížnosti subjektu údajů, souhlasu subjektu údajů se zpracováním osobních údajů, pojmu obchodní sdělení a provozování kamerových systémů.

PRAVOMOC ÚŘADU KE KONTROLNÍ ČINNOSTI V OBLASTI SPRÁVY DANÍ JE DÁNA; ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ SE NA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V OBLASTI SPRÁVY DANÍ VZTAHUJE

Úřad čelil názorům, že jednak není orgánem oprávněným ke kontrolní činnosti při zpracování osobních údajů při výkonu správy daní, a dále že zákon o ochraně osobních údajů na zpracování osobních údajů v oblasti správy daní nedopadá.

Ohledně vlastní aplikace zákona o ochraně osobních údajů v oblasti správy daní bývá argumentováno výjimkou zakotvenou v ustanovení § 3 odst. 6 písm. f) zákona o ochraně osobních údajů, podle něhož se ustanovení § 5 odst. 1 a § 11 a § 12 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. V této záležitosti Městský soud v Praze v odůvodnění rozsudku sp. zn. 11 Ca 91/2009 ze dne 5. června 2012 uvedl, že „je nutné toto ustanovení aplikovat vždy s ohledem na konkrétní situaci, na kterou je zákon aplikován a že není možné zobecnit, že by se zákon o ochraně osobních údajů nevztahoval na žádná daňová řízení“. Posouzení, zda se na konkrétní situaci vztahuje uvedená výjimka z důvodu, že je zajišťován významný finanční zájem České republiky, by mělo být uskutečněno v součinnosti mezi Úřadem a příslušným finančním úřadem.

Stejně tak bylo v uvedených souvislostech argumentováno, že daňový řád obsahuje zvláštní autonomní právní úpravu mlčenlivosti, poskytující vyšší ochranu všem zpracovávaným údajům, které byly získány při správě daní, než zákon o ochraně osobních údajů. Odůvodnění rozsudku sp. zn. 11 Ca 91/2009 ze dne 5. června 2012 k tomu uvádí, že „podle ustanovení § 2 odst. 5 daňového řádu jakékoliv osoby, s výjimkou daňových subjektů v daňovém řízení o jejich daňové povinnosti, 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 nezprostřuje správce daně povinnosti poskytnout údaje osobě, která prokáže, že je oprávněna tyto údaje získat podle zvláštního právního předpisu. Těto povinnosti mohou být zproštěny jen za podmínek stanovených tímto zákonem. Z citovaného ustanovení vyplývá, že povinnost mlčenlivosti finančních úřadů je omezená za situace, že finanční úřad je požádán o poskytnutí údajů subjektem, který je oprávněn k jejich získání, což je v daném případě ... Úřad pro ochranu osobních údajů, který je oprávněn se s osobními údaji seznamovat a sám je také vázán povinností mlčenlivosti.“

Ohledně dalšího názoru, podle něhož Úřad není orgánem oprávněným ke kontrolní činnosti při výkonu správy daní, a to z důvodů, že není vázán mlčenlivostí podle § 24 odst. 11 či § 25 zákona č. 337/1992 Sb., o správě daní a poplatků, a že není orgánem, který by vykonával správu daní, bylo v odůvodnění rozsudku sp. zn. 11 Ca 91/2009 ze dne 5. června 2012 konstatováno, že Úřad „neprovádí kontrolu výkonu daňové správy, ale pouze kontroluje, zda

dochází ke zpracování osobních údajů v souladu s příslušnými právními předpisy a zákonem č. 101/2000 Sb. Při posouzení této otázky je nutno vyjít ze vztahu zákona č. 101/2000 Sb. a zákona č. 337/1992 Sb., které mají oba stejnou právní sílu, platí současně a v oblasti pravidel pro zpracovávání osobních údajů je zákon č. 101/2000 Sb. zákonem obecným. Vzhledem k tomu, že zákon č. 337/1992 Sb. je zákonem speciálním v této oblasti, je nutné posoudit, zda upravuje veškeré otázky shodně se zákonem obecným či nikoli a podle toho posoudit, který zákon se použije.“

Soud pak dospěl k závěru, že zákon č. 337/1992 Sb., o správě daní a poplatků, neobsahuje komplexní úpravu povinností při zpracování osobních údajů (např. požadavky odpovídající ustanovení § 5 nebo práva subjektů údajů dle § 12 a 21 zákona o ochraně osobních údajů), a proto se v této oblasti zákon o ochraně osobních údajů uplatní v plném rozsahu.

Obdobné závěry Městský soud v Praze vyvodil i v rozsudcích č. j. 10 A 46/2010-62 ze dne 8. srpna 2012 a č. j. 9 A 251/2011-90 ze dne 17. října 2012. Na obecné platnosti těchto závěrů nic nemění ani fakt, že zákon č. 337/1992 Sb., o správě daní a poplatků, byl nahrazen zákonem č. 280/2009 Sb., daňový řád, nicméně zároveň je třeba upozornit, že všechny uvedené rozsudky byly napadeny kasační stížností.

NA VÝKON DOZORU ZE STRANY ÚŘADU NEMÁ PODATEL SUBJEKTIVNÍ PRÁVO, A PŘÍSLUŠNÉ PODÁNÍ JE TEDY POUZE PODNĚTEM K UPLATNĚNÍ DOZORČÍHO PRÁVA ÚŘADU, PŘIČEMŽ INFORMACE ÚŘADU O ZPŮSOBU VYŘÍZENÍ PODNĚTU JE TOLIKO SDĚLENÍM ÚŘADU, A NIKOLI ROZHODNUTÍM PODLE § 65 ZÁKONA Č. 150/2002 SB., SOUDNÍ ŘÁD SPRÁVNÍ

V této souvislosti bylo usnesením rozšířeného senátu Nejvyššího správního soudu č. j. 1 As 93/2009 ze dne 4. září 2012 konstatováno, že „Zákon o ochraně osobních údajů jakožto zákon zvláštní k zákonu o státní kontrole ovšem nestanoví, že by se státní kontrola zahajovala podáním žádosti subjektu údajů o zjednání nápravy při neoprávněném zpracování osobních údajů. I tento systémový argument potvrzuje, že podání subjektu údajů je pouhým podnětem, jímž se nezahajuje správní řízení.“

Dále pak bylo v předmětném usnesení uvedeno, že § 29 zákona o ochraně osobních údajů nezakládá Úřadu pravomoc vést správní řízení o žádostech subjektů údajů a že ustanovení § 21 odst. 3 či 4 tohoto zákona neupravují možnost subjektů údajů podávat žádosti o uložení nápravných opatření ze strany Úřadu zpracovatelům či správcům osobních údajů, o kterých by Úřad musel rozhodovat. Protože Úřadu nebyla tato pravomoc svěřena, je zřejmé, že opačný výklad by vedl k rozporu s Ústavou i s Listinou. Pokud subjekt údajů neuspěje u Úřadu se svým podnětem, může se ochrany svých práv domoci žalobou (vůči správci) na ochranu osobnosti dle § 13 občanského zákoníku, na který § 21 zákona o ochraně osobních údajů odkazuje. Obdobně projednání nároku subjektu údajů na zajištění opatření k nápravě způsobené nemateriální újmy a náhradu škody svěřil zákon o ochraně osobních údajů do pravomoci soudů v občanském soudním řízení.

Uvedené usnesení pak uzavírá konstatování, že: „podání subjektu osobních údajů podle § 21 odst. 3 i odst. 4 zákona o ochraně osobních údajů, jímž tento subjekt žádá žalovaného o uložení opatření k nápravě zpracovateli či správci osobních údajů, má charakter podnětu k uplatnění dozorových pravomocí Úřadu. Toto podání nemá za následek zahájení správního řízení. Sdělení žalovaného o způsobu vyřízení podnětu je pouhým sdělením úřadu straně, nikoli rozhodnutím ve smyslu § 65 s. ř. s., a není proto přezkoumatelné ve správním soudnictví dle § 70 písm. a) s. ř. s.“

Tyto závěry pak ve svém důsledku byly potvrzeny i zákonem č. 468/2011 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, a některé další zákony, který s účinností od 1. ledna 2012 ustanovení § 21 odst. 3 a 4 zákona o ochraně osobních údajů zcela vypustil.

ZA SOUHLAS PODLE § 4 PÍSM. N) ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ NELZE POVAŽOVAT POUHÉ NEPROJEVENÍ NESOUHLASU SUBJEKTU ÚDAJŮ SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ

V případě, který vyústil rozsudkem Městského soudu v Praze sp. zn. 6 Ca 378/2008 ze dne 16. října 2012, bylo posuzováno zpracování osobních údajů uchazeče o zaměstnání i po ukončení výběrového řízení na uvolněné pracovní místo, a to bez výslovného souhlasu tohoto subjektu údajů.

V odůvodnění předmětného rozsudku Městský soud v Praze nejprve uvedl, že pro zpracování osobních údajů po dobu trvání výběrového řízení nebyl potřebný souhlas, a to vzhledem k ustanovení § 5 odst. 2 písm. b) zákona o ochraně osobních údajů, jelikož se jednalo o údaje poskytnuté subjektem údajů spolu s jeho návrhem na uzavření smlouvy. Zároveň však platí, že podle § 20 odst. 1 zákona o ochraně osobních údajů je nezbytné osobní údaje zlikvidovat, jakmile pomine účel jejich zpracování. V případě výběrového řízení je tímto účelem jednání o uzavření smlouvy na základě nabídek jednotlivých uchazečů. Ve vztahu k jednotlivým uchazečům tedy účel zpracování osobních údajů pomine ve chvíli, kdy potenciální akceptant projeví své stanovisko vůči návrhu na uzavření smlouvy (ofertě). V posuzovaném případě bylo subjektu údajů sděleno, že se na jeho ofertu nereflektuje. Tímto okamžikem zanikl účel zpracování jeho osobních údajů, a mělo tedy být postupováno podle § 20 odst. 1 zákona o ochraně osobních údajů, ledaže by k dalšímu zpracování byl získán souhlas subjektu údajů ve smyslu § 4 písm. n) uvedeného zákona. Takový souhlas však žalobce od subjektu údajů neobdržel. Nicméně zároveň subjekt údajů nereagoval na výzvu k tomu, aby projevil svůj nesouhlas s dalším zpracováním osobních údajů.

K tomu pak Městský soud v Praze uvedl, že podle zmiňovaného ustanovení § 4 písm. n) zákona o ochraně osobních údajů se souhlasem subjektu údajů rozumí svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním osobních údajů, a tedy „tím, že zákon stanoví jako obsahovou náležitost svolení subjektu údajů, vylučuje právě praxi, kterou žalobce v posuzovaném případě využil, tj. konstruovat presumpci souhlasu na základě toho, že nebude projevem nesouhlas se zpracováním osobních údajů. Takový postup by byl zjevným obcházením zákona a neodpovídá jasně dikci ustanovení § 4 písm. n) zákona o ochraně osobních údajů.“

Obdobně Městský soud v Praze v rozsudku sp. zn. 6 Ca 343/2008 ze dne 1. listopadu 2012 uvedl, že pouhý vstup do hotelových prostor není souhlasem s monitorováním prostřednictvím kamerového systému, který by korespondoval s podmínkami § 4 písm. n) a § 5 odst. 4 zákona o ochraně osobních údajů. Hlavním důvodem pro tento závěr je, že posledně citovaná ustanovení stanoví jako obsahovou náležitost svolení subjektu údajů a vyžadují pro udělení souhlasu poučení o účelu a rozsahu zpracování osobních údajů. To opět vylučuje konstruovat presumpci souhlasu na základě toho, že nebude projevem nesouhlas se zpracováním osobních údajů, případně konstrukci konkludentního souhlasu na základě prosté informace, že objekt je monitorován kamerami.

ZA NEVYŽÁDANÉ OBCHODNÍ SDĚLENÍ PODLE ZÁKONA Č. 480/2004 SB., O NĚKTERÝCH SLUŽBÁCH INFORMAČNÍ SPOLEČNOSTI A O ZMĚNĚ NĚKTERÝCH ZÁKONŮ (ZÁKON O NĚKTERÝCH SLUŽBÁCH INFORMAČNÍ SPOLEČNOSTI), SE NEPOVAŽUJE INDIVIDUÁLNÍ REAKCE NA KONKRÉTNÍ NABÍDKU A NENÍ JÍM ANI KONKRÉTNÍ PROTINABÍDKA K NABÍDCE VYPLÝVAJÍCÍ Z PODANÉHO INZERÁTU

V rozhodnutí č. j. 10 A 217/2010-39 ze dne 14. června 2012 Městský soud v Praze uvedl, že protinabídku na inzerát s veřejnou nabídkou určité nemovitosti může, aniž by byl porušen zákon o některých službách informační společnosti, učinit i realitní kancelář, zastupuje-li zájmy konkrétního klienta, který si ji najal k obstarání koupě určité nemovitosti. Zároveň však uvedené rozhodnutí zdůraznilo, že se musí jednat o individualizovanou reakci na konkrétní inzerát.

O takovouto konkrétní reakci se však nejedná, pokud zpráva s totožným textem byla odeslána více různým osobám a pokud tato zpráva obsahuje toliko telefonní číslo centrály odesílatele, a nikoli konkrétní kontakt na makléře pověřeného k zastupování konkrétního zájemce o některou nemovitost nabízenou inzerujícím.

Další okolností, vylučující klasifikovat zprávu jako konkrétní nabídku, je několikeré odeslání zprávy s totožným textem témuž adresátovi, a to i v rozmezí několika dnů. Obdobně je třeba hodnotit formulace textu jednotlivých zpráv, které korespondují s formulacemi užívanými v reklamě, jako je „vsadte na jistotu“, „neváhejte využít této šance“ apod. Konečně je možno vyloučit charakter předmětných zpráv jako individuální reakci na konkrétní nabídku pro případ, že tyto zprávy byly odesílány i osobám, které již v době odeslání zpráv žádnou nemovitost nenabízejí, nebo v případě, kdy oslovená osoba zjistí, že odesílatel zprávy ve skutečnosti žádného konkrétního zájemce o jeho nemovitost nemá. Uvedené okolnosti vylučují, aby byly odesílané zprávy vnímány jako konkrétní reakce na konkrétní nabídku. Naopak je nutno jednoznačně dovodit, že tyto zprávy jsou určeny k přímé či nepřímé podpoře služeb žalobce, a jde tedy o obchodní sdělení.

Kasační stížnost proti rozsudku č. j. 10 A 217/2010-39 ze dne 14. června 2012 Nejvyšší správní soud usnesením 8 As 89/2012 ze dne 31. října 2012 odmítl.

PLOŠNÉ A NEROZLIŠUJÍCÍ UŽITÍ KAMEROVÉHO SYSTÉMU JE V ROZPORU S USTANOVENÍM § 5 ODS. 2 PÍSM. E) ČÁSTI VĚTY ZA STŘEDNÍKEM ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ UKLÁDAJÍCÍM ŠETŘIT PRÁVO ZAZNAMENÁVANÝCH OSOB NA OCHRANU SOUKROMÍ A OSOBNÍHO ŽIVOTA

Městský soud v Praze v rozsudku sp. zn. 6 Ca 343/2008 ze dne 1. listopadu 2012 uvedl, že pokud je kamerový systém užitý plošně, tedy snímá plošně prostory, v nichž se klientela hotelu zdržuje, a není např. zaměřen na objekty, které by se mohly stát cílem protiprávního jednání (tedy např. na místa určená k odkládání věcí), nelze uvažovat o tom, že by konkrétní způsob pořízení kamerových záznamů vyhovoval požadavku ustanovení § 5 odst. 2 písm. e), části věty za středníkem, zákona o ochraně osobních údajů, tedy šetřil právo zaznamenávaných osob na ochranu soukromí a osobního života.

Uvedený způsob instalace kamerového systému je, podle názoru soudu, zjevně neproporcionální. Zájem na ochraně před drobnými krádežemi, vandalstvím a případným excesem některé osoby totiž nelze jednostranně upřednostňovat před zájmy na ochranu soukromí a osobního života.

REGISTRACE

Trend nárůstu počtu registračních oznámení pokračoval i v roce 2012. V tomto roce Úřad přijal 5169 oznámení o zpracování podle § 16 zákona o ochraně osobních údajů. Oproti předchozímu roku se jednalo o 17% nárůst. S narůstajícím počtem registračních oznámení souvisí i počet oznamovaných změn či doplnění již zaregistrovaných zpracování. Změny se nejčastěji týkaly adresních údajů, doplnění rozsahu zpracovávaných osobních údajů, kategorií subjektů údajů, doplnění účelů zpracování. V roce 2012 Úřad zaznamenal 811 žádostí o změnu či doplnění.

Vedle posuzování přijatých registračních oznámení vydává Úřad rozhodnutí o zrušení registrace podle § 17a odst. 2 zákona o ochraně osobních údajů. V letošním roce bylo zrušeno celkem 78 zpracování na žádost správce, nejčastěji z důvodů zániku či sloučení společnosti, zrušení podnikatelské činnosti nebo ukončení zpracování osobních údajů. Jednalo se o nárůst 59 %. Informace o zrušených registracích Úřad povinně zveřejňuje ve svém Věstníku. V případě, že oznámení neobsahuje všechny náležitosti, které jsou nezbytné pro samotné posouzení zpracování, je správci zaslána výzva k doplnění informací. V roce 2012 Úřad zahájil celkem 969 řízení o registraci podle § 16 odst. 4 zákona o ochraně osobních údajů. Z velké části se řízení týkala zpracování prostřednictvím kamerových systémů, zpracování citlivých údajů, zpracování osobních údajů bez právního titulu. Pokud v rámci tohoto řízení vznikne, resp. trvá důvodná obava z porušení zákona, zahajuje Úřad správní řízení ve smyslu § 17 zákona o ochraně osobních údajů, jehož závěrem může být i rozhodnutí o nepovolení oznámeného zpracování.

Do českého právního řádu byla zákonem č. 468/2011 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů, transponována směrnice Evropského parlamentu a Rady 2007/66/ES. Novela zákona, která nabyla účinnosti dne 1. ledna 2012 zavádí nový nástroj ochrany osobních údajů a soukromí. Poskytovatelům služeb elektronických komunikací se výslovně stanoví povinnost řešit případy porušení ochrany osobních údajů (tzv. data breaches), včetně povinnosti takové porušení oznámit Úřadu pro ochranu osobních údajů. Kompetence související s přijímáním a posuzováním zaslanych oznámení byla svěřena registračnímu odboru Úřadu. V souvislosti s novou kompetencí byla vytvořena zvláštní rubrika na webových stránkách („Oznámení podle zákona č. 127/2005 Sb.“), kde jsou uvedeny odkazy na právní předpisy, vytvořen formulář k plnění oznamovací povinnosti a jsou zde definovány některé pojmy a postupy ukládané oznamovateli. Úřadem vytvořený formulář má sloužit především oznamovatelům a ulehčit jim plnění povinnosti vyplývající ze zákona o elektronických komunikacích. Formulář zároveň obsahuje všechny nezbytné náležitosti, které je nutné Úřadu sdělit, aby mohl dané oznámení posoudit.

V souvislosti s novou povinností uloženou zákonem o elektronických komunikacích poskytovatelům elektronických komunikací přijal registrační odbor několik podání. Ve většině případů se však jednalo o podání subjektu údajů týkající se podezření na porušení povinností uložených správci osobních údajů zákonem o ochraně osobních údajů, a byly tudíž postoupeny věcně příslušnému útvaru k vyřízení. V jednom případě se jednalo o případ porušení ochrany osobních údajů podle zákona o elektronických komunikacích, ale podaný subjektem, na nějž se oznamovací povinnost podle tohoto zákona nevztahuje. Teprve koncem října obdržel Úřad první opodstatněné oznámení týkající se porušení ochrany osobních údajů. Spočívalo v tom,

že od povinného subjektu byly za jeden měsíc rozeslány faktury některých zákazníků – fyzických osob a ty byly doručeny na adresy jiných zákazníků – převážně právnických osob. Ze strany oznamovatele porušení byla přijata odpovídající technická opatření a dotčené subjekty údajů byly o této věci informovány.

Zatím tedy nelze hovořit o zkušenostech s těmito případy oznámení v České republice. Nicméně věcně příslušné úřady v jiných zemích Evropské unie mají již konkrétnější zkušenosti, i když také ne příliš rozsáhlé. Je však již možno uvést příklady oznamovaných porušení ochrany osobních údajů:

- osobní údaje zaslány nesprávnému adresátovi (např. e-mailem, dopisem),
- krádež nebo ztráta hardware s osobními údaji,
- zpřístupnění osobních údajů neoprávněným osobám (zálohování dat na P2P sítích, nedokonalé vymazání záznamů na prodávaných použitých zařízeních, použití „ostrých“ dat při testování nových aplikací, nevhodná úschova přihlašovacích údajů nebo chybné nastavení systému a aplikací),
- ztráta nebo nesprávná likvidace papírové dokumentace s osobními údaji,
- hackerské útoky (napadení webu, napadení interních informačních systémů, napadení komunikačních sítí),
- výsledky napadení škodlivými programy vedoucí k porušení ochrany osobních údajů (znepřístupnění dat, zveřejnění dat apod.).

V souvislosti s rozvojem informačních technologií se stále častěji objevují zvláštní typy zpracování prováděné právě prostřednictvím nových technologií. Týká se to např. technologií zabezpečujících vstup do režimových pracovišť, nejčastěji na základě snímání otisku prstů či snímku duhovky oka. Pokud jsou otisky prstů převedeny do jednostranně zašifrovaného binárního řetězce čísel, z něhož nelze zpětně reprodukovat otisk prstu, pak se o zpracování citlivého biometrického údaje nejedná. Úřad registroval zpracování prováděné společností zabývající se vývojem hardwaru a softwaru v oblasti identifikace osob na základě rozpoznání otisků prstů. Otisk prstů zaměstnanců je zpracováván za účelem vedení a zpracování databáze otisků prstů pro účely testování vyvíjených technologií a programů. Pro účely vývoje těchto technologií je třeba ověřit, jakým způsobem se otisk prstu bude měnit v rámci ročních období a zda nebude docházet k anomáliím při identifikaci osob při různých teplotách a dalších fyziologických vlivech. Zpracování se děje se souhlasem testovaného zaměstnance. Další zajímavý případ registrovaný Úřadem je zpracování oznámené bankou, týkající se podpisu jako biometrického údaje – konkrétně údaje týkajícího se jeho velikosti a dynamiky, tlaku při podepisování a časové délce podpisu za účelem zajištění a uplatnění právních nároků v případě pochybností nebo sporů o pravost podpisu. Ve dvou posledně uvedených případech šlo skutečně o zpracování citlivých biometrických údajů.

K častým omylům v souvislosti se zpracováním biometrických údajů dochází při použití antropometrických charakteristik (váha, míra, věk, pohlaví, velikost oblečení atd.). V případech izolovaného využití uvedených antropometrických údajů se však o biometrické údaje nejedná, neboť neumožňují přímou identifikaci nebo autentizaci subjektu údajů, jak vyžaduje zákon o ochraně osobních údajů. Tyto údaje zpracovávají zejména castingové a modelingové agentury za účelem vytváření databází hostesek a modelek či společnosti zabývající se aktivitami v oblasti výživového či dietologického poradenství, případně seznamovací agentury zpracovávající tyto údaje v souvislosti se svou činností.

Rozvoj informačních technologií se odráží rovněž ve způsobech, jakými jsou nebo mohou být monitorováni zaměstnanci na pracovištích. Vedle již klasických prostředků, jako jsou kamerové systémy, jsou to i stále sofistikovanější nástroje schopné sledovat činnost zaměstnance. Jako příklad lze uvést softwarové systémy pracující na obdobném principu jako např. antispamový software. Jsou založeny na automatizované kontrole klíčových slov.

Deklarovaným účelem zpracování je uváděna nejčastěji ochrana důvěrných informací. Zpracování osobních údajů probíhá automatizovanou neadresnou kontrolou pracovní elektronické komunikace zaměstnanců na základě klíčových slov. V případě těchto zpracování může vzniknout nejistota ohledně povinnosti takové zpracování registrovat u Úřadu. Vždy bude záležet na vymezení jednotlivých účelů zpracování. Pokud účelem zpracování bude ochrana obchodního tajemství ve smyslu § 17 ObchZ, lze konstatovat, že takové zpracování je nezbytné pro dodržení právní povinnosti správce, a tudíž by se aplikovala výjimka z registrační povinnosti podle § 18 odst. 1, písm. b) zákona o ochraně osobních údajů. Zpracování musí ovšem vždy probíhat pouze v rozsahu nezbytně nutném pro naplnění uvedeného účelu.

Podobně jako v letech předešlých bylo registrováno několik subjektů provádějících výzkum v oblastech medicíny a genealogie za účelem zjištění četnosti určitého znaku v populaci, dále zpracování molekulárně genetických testů příbuzenství osob v různých variantách, jako je test otcovství, mateřství, sourozenectví, test identity dvojčat apod. Dále zpracování genetických analýz, na základě kterých je možné zjistit předky, nalézt ztracené příbuzné, určit pravděpodobnost příbuznosti s jinou osobou, zjistit predispozice lidských vlastností a určit biologické vztahy s jinými osobami. Genetický rozbor prováděný na základě stěru ze sliznice dutiny ústní, prostřednictvím kterého lze zjistit, zda klient má či nemá vrozené dispozice k přibližně 20 chorobám (jaké je riziko, že klient může danou nemocí onemocnět), a na základě výsledků je mu pak doporučena prevence. Všechna tato zpracování předpokládají zpracování citlivých údajů vypovídajících o zdravotním stavu a genetických citlivých údajů. Zpracování se vždy musí dít se souhlasem subjektu údajů.

Je třeba rovněž zmínit oznámené zpracování, které naznačuje určitý trend v oblasti komerčního poskytování zdravotní péče. Jedná se o zpracování oznamující záměr nabízet službu monitorování tělesných a zdravotních parametrů klientů, kde jsou všechna měření v reálném čase přenášena bezobslužně a bezdrátově na server. Koncová data aplikace pouze nezobrazí, ale zpracuje je dle medicínsky podložených algoritmů a klientovi zašle patřičná doporučení, případně na přání klienta upozorní jeho lékaře či jinou oprávněnou osobu, např. osobního trenéra. Je čistě na volbě klienta, které přístroje si objedná, např. tlakoměr, glukometr, krokoměr apod. Zpracování správce provádí výlučně na základě výslovného souhlasu klienta.

Podobně jako v minulém roce pokračoval i letos trend zpracovávat osobní údaje formou zveřejnění audiovizuálního záznamu ze zasedání zastupitelstva na webových stránkách. V rámci registračního řízení oznamovatelé ve většině případů deklarovali, že budou zpracovávat osobní údaje zastupitelů bez jejich souhlasu na základě ustanovení § 5 odst. 2 písm. f) zákona o ochraně osobních údajů, zatímco osobní údaje přítomné veřejnosti a osobní údaje obsažené v projednávané agendě zpracovávány nebudou nebo budou anonymizovány.

Nejčastějším druhem zpracování (cca 42 %), které se v tomto roce objevovalo, bylo podobně jako v letech minulých zpracování prostřednictvím kamerových systémů. Celkem je v registru zpracování osobních údajů zapsáno 8621 subjektů, které podaly oznámení o zpracování osobních údajů kamerovými systémy. V roce 2012 podalo oznámení 1886 subjektů, což je nárůst oproti roku 2011 o 25,3 %.

Přehled počtu subjektů, které podaly oznámení o zpracování osobních údajů ke kamerovým systémům

Rok	Počet subjektů
do 2005	32
2006	386
2007	890
2008	1399
2009	1255
2010	1268
2011	1505
2012	1886
Celkem	8621

V roce 2012 došlo k úpravě a celkovému zjednodušení doplňujícího formuláře ke kamerovým systémům, který je součástí formuláře oznámení o zpracování osobních údajů tak, aby lépe vyhovoval současným podmínkám a zároveň byl pro oznamovatele uživatelsky přívětivější. Z původních deseti bodů doplňujícího formuláře zůstalo pouze osm bodů. V posledním osmém bodě je navíc poptáváno, zda oznamovatel provedl analýzu vhodnosti, účelnosti a nezbytnosti nasazení kamerového systému, což bývalo častým dotazem v rámci prováděných registračních řízení. Touto změnou došlo k zjednodušení a urychlení procesů vyřízení registračních oznámení týkajících se zpracování kamerovými systémy.

Při zodpovídání dotazů týkajících se zpracování prostředky kamerových systémů se pracovníci registračního odboru setkávali často s dotazy, které se týkaly náležitostí souhlasu subjektu údajů se zpracováním osobních údajů, náležitostí informačních tabulí umístěných u sledovaných prostor a podobně. Proto registrační odbor ve spolupráci s dalšími útvary připravil *Metodiku pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů*. Metodika má subjektům provozujícím kamerové systémy (tedy správcům či zpracovatelům) usnadnit přípravu nasazení a provozování kamerových systémů tak, aby byly v souladu se zákonem o ochraně osobních údajů, a to s využitím některých definovaných postupů a vzorů. Metodika je zájemcům k dispozici v tištěné i elektronické podobě a byla rovněž přeložena do anglického jazyka.

■ PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Ustanovení § 27 zákona o ochraně osobních údajů upravuje zvláštní režim pro předání osobních údajů z České republiky do třetích zemí. Třetí zemí se v tomto smyslu rozumí všechny země mimo Evropský hospodářský prostor. Účelem a smyslem tohoto ustanovení je zajištění ochrany osobních údajů subjektů údajů, které mají být předány a následně zpracovávány ve třetích zemích. V zásadě mohou být osobní údaje předávány do země mimo EU, pokud tato země zaručuje „odpovídající úroveň ochrany“. Odpovídající úroveň ochrany ve třetí zemi mohou zajišťovat buď obecné právní předpisy, nebo odvětvová pravidla dotyčné třetí země, nebo tuto ochranu může garantovat sám správce (vývozce údajů) prostřednictvím odpovídajících ochranných opatření, která zajistí, že úroveň ochrany předávaných osobních údajů bude v zemi příjemce srovnatelná se standardy ochrany obsaženými v zákoně o ochraně osobních údajů. Takové záruky mohou vyplývat zejména ze smlouvy mezi správcem a příjemcem dat, jejíž nedílnou součástí budou standardní smluvní doložky vytvořené rozhodnutím Komise. Pokud správce osobních údajů zvolí variantu vytvoření jiných druhů odpovídajících ochranných opatření, musí tato svá vlastní ochranná opatření obhájit v rámci povolovacího řízení podle § 27 odst. 4 zákona o ochraně osobních údajů.

V roce 2012 se zlomil dlouhodobý trend klesajícího počtu podávaných žádostí o povolení předání osobních údajů. Úřad přijal za rok 2012 celkem 17 žádostí o povolení k předání osobních údajů do třetích zemí a vydal celkem 18 rozhodnutí (v loňském roce to bylo pouze 8 rozhodnutí). Geograficky šlo jako obvykle především o předání do Spojených států amerických, Turecka, Indie a oblasti jihovýchodní Asie a Pacifiku (Jižní Korea, Malajsie, Hongkong, Austrálie), ale nově častěji také do oblasti východní Evropy (Rusko, Ukrajina). Z těchto 18 rozhodnutí Úřad v jednom případě řízení zastavil, neboť žadatel vzal svou žádost zpět; ve čtyřech případech Úřad věc odložil, buď z toho důvodu, že se žadatel nakonec rozhodl předpokládané předání údajů ošetřit smlouvou s dovozcem údajů, jejíž nedílnou součástí budou standardní smluvní doložky, nebo žadatel omezil předání pouze na státy Evropské unie, nebo od svého záměru zcela ustoupil. Ve zbývajících 13 případech Úřad předání povolil.

Předávat osobní údaje do třetích zemí, nezajišťujících přiměřenou úroveň ochrany osobních údajů, lze rovněž na základě výjimek uvedených v § 27 odst. 3 písm. a) až g) zákona o ochraně osobních údajů. Naplnění některého právem uznaného důvodu musí být správce (vývozce) schopen prokázat jak před započítím předávání, tak po celou dobu jeho trvání. Nejčastějšími právními tituly, na jejichž základě bylo povolení vydáno, byla ustanovení § 27 odst. 3 písm. a), tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů, a ustanovení § 27 odst. 3 písm. e), tedy předání údajů nezbytné pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů. Na základě každého z uvedených právních titulů bylo vydáno pět povolení. Jedno povolení bylo vydáno na základě splnění podmínek daných § 27 odst. 3 písm. d) a f), kdy předání bylo nezbytné pro uplatnění důležitého veřejného zájmu vyplývajícího ze zvláštního zákona nebo z mezinárodní smlouvy, kterou je Česká republika vázána, a zároveň bylo předání nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou, nebo pro uplatnění jiných právních nároků.

Konečně lze konstatovat, že nový trend na poli předávání osobních údajů do zahraničí se odráží ve dvou případech, kdy bylo vydáno povolení na základě § 27 odst. 3 písm. b) zákona o ochraně osobních údajů, neboť žadatel vytvořil ve třetí zemi dostatečné zvláštní záruky ochrany osobních údajů.

V jednom z těchto dvou případů byly dostatečné zvláštní záruky vytvořeny smlouvou uzavřenou mezi správcem (vývozcem) a zpracovatelem (dovozcem) v Indii. Na základě zjištěných skutečností, zejména na základě textu smlouvy o zpracování osobních údajů uzavřené mezi správcem a zpracovatelem, bylo možné konstatovat, že uvedená smlouva o zpracování osobních údajů vytvoří dostatečné zvláštní záruky ochrany osobních údajů ve třetí zemi, a že tedy při předání osobních údajů bude plněno ustanovení § 27 odst. 3 písm. b) zákona o ochraně osobních údajů. V druhém případě žadatel doložil vytvoření zvláštních záruk pro předání osobních údajů v rámci nadnárodní korporace, do níž žadatel patří, předložením tzv. závazných podnikových pravidel (Binding Corporate Rules) skupiny, které byly schváleny ze strany některého z unijních úřadů pro ochranu osobních údajů jakožto „lead Data Protection Authority“ v rámci zvláštní schvalovací procedury, jejíž náležitosti a průběh jsou definovány Pracovní skupinou pro ochranu dat podle článku 29 (Working party 29) v pracovních dokumentech WP 74, WP 107, WP 108, WP 133, WP 153, WP 154 a WP 155. Vedle právě zmíněného případu se o předání osobních údajů v rámci skupiny na základě závazných podnikových pravidel pokusily požádat další dva subjekty a Úřad zodpovídal rovněž několik dotazů, ze kterých vyplynulo, že se tazatelé připravují k podání žádosti o povolení, avšak nemají jasno v některých otázkách: především v otázce, kdo má žádost podat, v jakém jazyce má být žádost sepsána, zda a v jakém jazyce mají být přiloženy přílohy, zvláště pak příslušná závazná podniková pravidla skupiny, a jaké jsou další náležitosti žádosti.

V rámci své povolovací činnosti Úřad řešil v roce 2012 žádosti o povolení předání osobních údajů cestujících leteckých společností na Ukrajinu, která začala na základě Nařízení vlády Ukrajiny No 291/506/228 v souvislosti s fotbalovým šampionátem nově vyžadovat od leteckých společností předání předběžné informace o cestujících Státní pohraniční stráží Ukrajiny a Státní celní správě Ukrajiny, a to v rozsahu těchto údajů: číslo letu, kód přepravce, datum a čas odletu, jméno a příjmení, státní příslušnost, datum narození, pohlaví a číslo cestovního dokladu, a dále rovněž předběžné informace o nákladech včetně tranzitního zboží. S ohledem na získané informace a předložené podklady dospěl Úřad k názoru, že v posuzovaném případě bude naplněna podmínka § 27 odst. 3 písm. e) zákona o ochraně osobních údajů, tzn. že předání bude nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů. Správní orgán tak dospěl ke stejnému závěru jako ve starších obdobných případech předání osobních údajů leteckých cestujících do Kuvajtu a na Kubu. Úřad při svém rozhodování zohlednil skutečnost, že účastník řízení hodlá předávat osobní údaje svých cestujících pouze prostřednictvím systému APIS, a tedy pouze v omezeném rozsahu osobních údajů, které jsou de facto součástí cestovního dokladu a letenky; nikoliv prostřednictvím svých rezervačních a odbavovacích systémů, jak je tomu v případech předání údajů ze jmenné evidence cestujících (PNR data). Úřad při svém rozhodování vzal dále v úvahu také článek 13 Úmluvy o mezinárodním civilním letectví, sjednané 7. prosince 1944 (Chicagská úmluva), publikované pod č. 147/1947 Sb., podle kterého musí dopravce respektovat zákony a nařízení smluvního státu, které se týkají vstupu a výstupu cestujících na území tohoto státu.

Úřad rovněž řešil žádost o povolení předání osobních údajů klientů bankovní skupiny, jejichž údaje měly být v rámci cloudového řešení centralizovány na serverech provozovaných hardwarově i softwarově mateřskou společností se sídlem ve třetí zemi s nedostatečnou ochranou

osobních údajů. Žadatel se však v průběhu řízení rozhodl věc vyřešit jiným způsobem a vzal svou žádost zpět.

V souvislosti s předáváním osobních údajů řeší Úřad stále častěji otázku spojenou s poskytováním cloudových služeb ze strany poskytovatelů usazených mimo EU, resp. EHP. Obecně lze konstatovat, že cloud computing přináší mnoho rizik z pohledu ochrany osobních údajů a jedním z nich je rovněž riziko spojené s mezinárodním předáváním osobních údajů. Osobní údaje se mohou nacházet ve velmi krátkém čase v jiném datovém centru na jiném serveru. Uživatel cloudu tak může lehce ztratit kontrolu nad svými daty, za které je jako správce primárně odpovědný.

V rámci zpracování údajů v cloudu je nutné rozlišit role dvou hlavních aktérů: uživatele a poskytovatele cloudu. Podle stanoviska WP29 z 1. července 2012 ke cloud computingu (WP 196) je ve všech typech základních cloudů (IaaS, PaaS, SaaS) poskytovatel cloudových služeb v pozici zpracovatele. V případě, že se data v cloudu dostanou i mimo území ČR (do tzv. třetích zemí neposkytujících adekvátní úroveň ochrany), bude docházet k jejich předávání ve smyslu § 27 zákona o ochraně osobních údajů. V těchto případech bude nutné, aby správce sám přijal odpovědnost za bezpečné předávání údajů a legalizoval takové předání tím, že využije některý z nástrojů zajišťujících přiměřenou ochranu předávaným údajům, jako např. standardní smluvní doložky nebo BCR. V souvislosti s poskytováním cloudových služeb byl vytvořen stanoviskem WP29 z 6. června 2012 (WP 195) další nástroj pro bezpečné předávání osobních údajů do třetích zemí, kterým je BCR pro zpracovatele.

Legislativní činnost

Za nejvýznamnější komplexní agendu s řadou problémů týkajících se stanovení řádných zákonných pravidel pro zacházení s informacemi, včetně zpracování osobních údajů, Úřad v roce 2012 **považoval vládní agendu boje s korupcí a zajištění transparentnosti rozhodování veřejné správy**, která byla doprovázena řadou, nejen legislativních, opatření. Úřad v probíhajících připomínkových řízeních předkládal dotčeným resortům podklady, které ve vládních materiálech mnohdy zcela chyběly, zejména dosažené zahraniční zkušenosti v této oblasti – pro ČR relevantní judikaturu a evropské právo. Úřad přitom upozorňoval na problematičnost jednání, v němž byly veřejnosti z důvodu „zajištění transparentnosti“ předkládány neutříděné informace, obsahující množství osobních údajů, navíc dlouhodobě publikované na internetu. Úřad poukazyval na zahraniční zkušenosti, že cíli transparentnosti (veřejné správy) nelze plošně přiznávat automatickou přednost před právem na ochranu osobních údajů jednotlivců. Úřad přitom za jedno z hlavních korupčních rizik považuje vysokou nepřehlednost informací, které správní úřady publikují. Veřejnost je tak zahlcena informacemi, v nichž však nemá možnost se vyznat. Úřad naopak nebrání zákonnému poskytnutí úplných informací v případech, kdy jasně převažuje veřejný zájem a je prokázán příslušný právní nárok.

Ukázkovým příkladem nerespektování elementárních pravidel zpracování osobních údajů byl návrh úpravy **zveřejňování příjemců dotací** v novele zákona o rozpočtových pravidlech. Úřad v připomínkovém řízení upozornil, že předkladatel se v důvodové zprávě nijak nevyptával s klíčovým rozsudkem ESD Schecke a Eifert v. Hessensko. Podle legislativního návrhu se měly paušálně zveřejnit všechny dokumenty, včetně řady osobních údajů. Předkladatel sice obsáhle popsal, co vše se má zveřejnit, ale tento rozsah zveřejnění téměř neodůvodnil. Nezhlednil tak skutečnost, že zveřejnění osobních údajů je zásahem do soukromí. Podle uvedeného judikátu však nemá být zveřejňování příjemců dotací, včetně podnikatelů, paušální: *„Není zpochybňováno, že částky, které dotčení příjemci dostávají ... představují část, často značnou, jejich příjmů. Zveřejnění jmenovitých údajů o uvedených příjemcích a přesných částkách, které obdrželi, na internetové stránce tak vzhledem k tomu, že se tyto údaje stávají dostupnými třetím osobám, představuje zásah do jejich soukromého života ve smyslu čl. 7 Charty.“*

V připomínkovém řízení se předkladatel s tímto rozsudkem nijak nevypořádal, ačkoliv zhodnocení souladu navrhované právní úpravy s mezinárodními smlouvami a slučitelnost s akty práva Evropských společenství je povinnou součástí obecné části důvodové zprávy. Na výzvu k nápravě nereagoval ani zákonodárny sbor, když předseda Úřadu upozornil na nedostatky předsedu příslušného výboru poslanecké sněmovny. Vzhledem k pochybení ministerstva financí jako předkladatele návrhu právního předpisu i nevypořádání připomínek, které Úřad uplatnil, vydal Úřad v závěru roku stanovisko, v němž konstatoval rozpor čerstvě přijatého zákona se zákonnou ochranou osobních údajů.

Úřad výslovně upozornil, že jeho připomínky zásadně neomezují právo veřejnosti na informace a možnost kontrolovat nakládání s veřejnými prostředky. Vedou ke stejnému cíli, který český zákonodárce vytyčil, ovšem při plném respektování oprávnění na soukromí. Jejich základem je mj. § 5 odst. 3 zákona o ochraně osobních údajů, který zní: „*Provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů.*“ Z uvedeného vyplývá nutnost pečlivého přístupu zejména při zveřejňování údajů, pak např. na základě aplikace principu přiměřeného zpracování osobních údajů by drobné dotace nebo návratné finanční výpomoci konkrétním lidem neměly být zveřejňovány vůbec, protože ochrana soukromí převáží nad oprávněním na informace.

Úřad dále vyzval k respektování § 8b odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, který upravuje poskytování informací o příjemcích veřejných prostředků, z něhož lze dovodit, že u větších dotací nebo návratných finančních výpomocí fyzickým osobám se poskytnou tyto druhy osobních údajů: „jméno, příjmení, rok narození, obec, kde má příjemce trvalý pobyt, výše, účel a podmínky poskytnutých veřejných prostředků“. V neposlední řadě Úřad upozorňoval, že ve zveřejňovaných dokumentech by se neměly objevovat osobní údaje třetích osob.

Výše uveden byl pouze jeden z případů, které dokládají, že celkový stav legislativních návrhů v České republice z hlediska pravidel pro zacházení s informacemi, provozováním informačních systémů a zpracováním osobních údajů nebyl uspokojivý a ve srovnání s předchozími roky nedoznal zlepšení. Nedostatky se týkaly zejména zkracování lhůt pro vypracování legislativních materiálů, lhůt připomínkových řízení, „nestandardního“ – neprůkazného vypořádání připomínek i absencí odůvodnění pro nová zpracování dat navrhovaná v zákonech. Tuto situaci plasticky dokreslila veřejná **debata ohledně sociální karty**, která ukázala, že řada podstatných náležitostí celé agendy vůbec nebyla předmětem připomínkového řízení k příslušnému zákonu.

Z výše uvedených důvodů Úřad uvítal, že v závěru roku byla přijata inovovaná legislativní pravidla vlády s novou **povinností vyhodnocovat dopady navrhovaných právních norem do ochrany soukromí a osobních údajů**, a to nejen při zpracování věcných záměrů zákonů, ale i důvodových zpráv. Vyhodnocení dopadů z hlediska potřeb ochrany soukromí je běžné v řadě evropských států, neboť směrnice Evropského parlamentu a Rady 95/46/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, předpokládá, že během přípravy legislativního opatření vnitrostátního parlamentu (nebo opatření založeného na tomto legislativním opatření) bude provedeno předběžné šetření či posouzení okolností a rizik a ochranných opatření týkajících se zpracování. Úřad očekává, že vyhodnocení dopadů do soukromí přispěje ke zkvalitnění legislativního procesu, pomůže lépe nastavovat zákonná pravidla pro zacházení s informacemi o občanech a objasňovat nezbytnost sběru, předávání a sdružování osobních údajů zejména v rámci přípravy státních informačních systémů.

V oblasti elektronických komunikací Úřad v roce 2012 přivítal vládní návrh na změnu zákona o elektronických komunikacích, trestního řádu a některých dalších zákonů, jehož výlučným obsahem je **uchovávání a využívání provozních a lokalizačních údajů k elektronické komunikaci**. Úřad ocenil, že nová zákonná úprava je něčím víc než jen prostou náhradou ustanovení zrušených Ústavním soudem. Především obsahuje výslovné podmínky, které omezují možnost využívat údaje, jež budou uchovávány po dobu šesti měsíců. Provozní a lokalizační údaje jsou v zákoně o elektronických komunikacích nově definovány na základě vypovídací hodnoty jednotlivých údajů. Uživatel služby elektronických komunikací, jehož totožnost je soudu nebo orgánu činnému v trestním řízení známa, bude zásadně o nařízeném zjišťování těchto údajů dodatečně z úřední povinnosti informován. Konceptně a rozsahem je tak navrhovaná úprava srovnatelná s již tradiční úpravou zpracování osobních údajů vázaných na odposlech a záznam telekomunikačního provozu. Zástupce Úřadu se dále aktivně podílel na přípravě prováděcí vyhlášky, v níž se aktivně zasadil o podstatné zpřesnění úpravy předávání údajů mezi tzv. oprávněnými orgány a provozovateli (sítí a služeb) a o stanovení povinnosti provozovatelů po uplynutí doby uchování údajů stanovené zákonem o elektronických komunikacích údaje zlikvidovat způsobem, který trvale znemožní jejich obnovení a který je stanoven v příslušném technicko-organizačním předpise.

Úřad v uplynulém roce uplatnil připomínky ve dvou oblastech, které se týkají jeho postavení a dozorových kompetencí.

V případě **úpravy státní služby** Úřad upozornil na čerstvou evropskou judikaturu týkající se postavení dozorových úřadů ochrany osobních údajů v Německu a Rakousku a na potřebu, aby právní úprava splňovala kritéria nezávislosti dozorového úřadu požadovaná směrnicí 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.

V souvislosti se schválením nového zákona o kontrole (kontrolního řádu) Úřad vypracoval a projednal s Ministerstvem vnitra změnu vybraných zákonných ustanovení, podle nichž Úřad postupuje v kontrole. V **kontrolní novele zákona o ochraně osobních údajů**, která bude v balíku jiných změnových zákonů souvisejících s kontrolním řádem předmětem připomínkového řízení v roce 2013 a nabude účinnosti s kontrolním řádem v roce 2014, je kromě odstranění duplicit s kontrolním řádem navrženo několik novinek vylepšujících organizaci kontrolního mechanismu Úřadu, zejména **kolegium inspektorů** jako kolektivní orgán, který by měl zajišťovat sjednocování kontrolních závěrů Úřadu, zejména tím, že bude projednávat námitky kontrolovaných osob, závěry z výsledků kontroly, kontrolní metodiku a návrhy kontrolního plánu nebo jeho změny.

Z dosavadní úpravy kontrolního procesu Úřadu se v zákonu o ochraně osobních údajů ponechává zejména zákonné oprávnění založené unijní směrnicí 95/46/ES, která požaduje pro orgány dozoru jednak pravomoc přístupu k údajům, které jsou předmětem zpracování, jednak pravomoc shromažďovat veškeré informace nezbytné pro splnění svého úkolu dozoru. Toto oprávnění se týká zejména citlivých a dalších údajů chráněných zvláštními druhy mlčenlivosti. Dále je v novele ve prospěch kontrolního procesu řešen souběh s jiným řízením vedeným Úřadem, o registraci zpracování osobních údajů. Po vzoru jiných kontrolních úřadů se v novele navrhuje nová zásadní pravomoc Úřadu uvážít, zda a v jakých případech je nutno uložit pokutu za porušení povinností při zpracování osobních údajů. Dlouhodobé poznatky Úřadu pro ochranu osobních údajů ukazují, že se v oblasti ochrany dat vyskytuje řada drobných či krátkodobých pochybení, která nejsou systémovými pochybeními, případně zásadně

neohrožují bezpečnost osobních údajů. Takové nedostatky jsou mnohdy operativně odstraněny kontrolovaným již v bezprostřední souvislosti s kontrolou, často na základě doporučení inspektora. Nevyhnutelnost správního trestání u nevýznamných případů se jeví jako nadbytečná i z pohledu evropského práva, které zavádí nové postupy alternativní k trestní represi (Jedná se zejména o čerstvě zavedenou zákonnou povinnost provozovatelů v oblasti elektronických komunikací oznamovat porušení ochrany osobních údajů Úřadu a případně o tomto stavu dále vyrozumět dotčené osoby.).

V případě **novelizace zákona týkající se tzv. praní špinavých peněz** Úřad upozornil Ministerstvo financí na nutnost zpřesnění vybraných postupů. Skutečnost, že v této složité agendě není s ohledem na § 3 odst. 6 zákona o ochraně osobních údajů třeba postupovat podle některých ustanovení tohoto zákona neznamená, že správce agendy nemá povinnost aplikovat principy ochrany osobních údajů jiným, specifickým způsobem; to se týká například poskytování informací subjektům údajů.

Oblastí, v níž Úřad v roce 2012 postrádal zásadní nezbytné změny v ochraně osobních údajů, je **oblast informačních systémů veřejné správy a základních registrů**. Jistým důvodem tohoto stavu byl postup prací při realizaci základních registrů a vazeb na jednotlivé „agendové“ informační systémy veřejné správy. Dílčí výsledky těchto prací a souvisejících analýz mohou poukázat na některé nedostatky, zejména duplicitu systémů či dat ve veřejné správě, případně nepatřičné sdružování údajů. Mimoto Úřad na expertních jednáních doporučoval ústředním správním úřadům více se zaměřit na jeden ze základních pilířů fungování e-governmentu, a to na praktické využití elektronického veřejného dokladu, jeho použití v soukromém (zejména finančním) sektoru, včetně zabezpečení v případě ztráty a související ochrany před zneužitím identity (veřejná garance platnosti dokladu a informací na něm uvedených a autorizovaná služba hlášení ztracených a ukradených dokladů). Nezhledněna zůstala připomínka Úřadu upozorňující na nutnost zpřísnění legislativní konstrukce oprávnění pro vyžadování a vzájemné předávání dat v elektronických registrech. Úřad upozornil, že v době propojených informačních systémů veřejné správy a systematického nastavování účelného předávání údajů se může stávat více zneužitelným běžně využívané zákonné zmocnění, zavedené původně v systému evidence obyvatel, totiž že ze všech „poskytovaných údajů“ mohou příslušné úřady v konkrétním případě použít vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu“.

Styky se zahraničím a mezinárodní spolupráce

Na počátku roku 2012 Evropská komise představila legislativní návrh **komplexní reformy ochrany osobních údajů** v EU. Dne 25. ledna 2012 zveřejnila materiál „Ochrana soukromí v propojeném světě – Evropský rámec pro ochranu údajů pro 21. století“ a spolu s ním návrhy dvou právních předpisů: návrh nařízení Evropského parlamentu a Rady o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně údajů; dále jen „GDPR“) a návrh směrnice o ochraně fyzických osob v souvislosti se zpracováváním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů a o volném pohybu těchto údajů (dále jen „JHAD“).

Úřad jako ústřední správní instituce v oblasti ochrany osobních údajů vypracoval, společně s dotčenými resorty, návrh rámcové pozice ČR k návrhu GDPR pro jednání v pracovních orgánech Rady EU, který zároveň posloužil jako stanovisko pro Parlament (poslaneckou sněmovnu i senát). V této pozici i v navazujících postupech se Úřad zaměřil kriticky především na následující oblasti: modernizované zásady zpracování osobních údajů, zpřesnění povahy a formy souhlasu se zpracováním, (re)definice základních pojmů, jako např. vztah citlivých údajů a rizikových zpracování, přehodnocení rolí subjektů odpovědných za zpracování osobních údajů (správce a zpracovatel), jasnější úprava zpracování osobních údajů nezletilých a vybraná oprávnění v souvislosti se zvláštním zpracováním osobních údajů pro účely vynucování práva. Úřad si v souvislosti všech komentářů i připomínek kladl zejména otázku, zda navrhovaný text nových evropských pravidel ochrany osobních údajů, který má ambici široce regulovat každodenní chování jednotlivců, podnikatelů i institucí, je formulován přesně, srozumitelně a účelně tak, aby dostál požadavkům vyplývajícím z formy nařízení, tj. předpisu přímo aplikovatelného, fakticky rovného zákonu.

Dne 29. února 2012 vládní Výbor pro EU přijal usnesení, které uložilo ministru vnitra, aby převzal gesci za návrh obecného nařízení o ochraně údajů a aby zajistil přípravu instrukcí či mandátů pro jednání o obecném nařízení o ochraně údajů v rámci EU a dále aby v rámci Výboru pro EU i nově zřízené meziřesortní pracovní skupiny pro problematiku ochrany údajů v rámci EU zajistil průběžné informování o stavu vyjednávání návrhu obecného nařízení o ochraně údajů. V předmětném rozhodnutí o **převzetí gesce** tak bylo přihlédnuto k názoru ministerstva vnitra a některých dalších ministerstev, že gesce Úřadu za přípravu evropských předpisů je nevhodná, protože Úřad je nezávislým správním úřadem – není součástí vlády a není vázán jejími pokyny. Úřad následně v pozici jednoho z mála aktivních připomínkových míst komentoval návrhy instrukcí k jednotlivým etapám projednávání; některé jím formulované postoje a návrhy byly uplatněny jako součást oficiálního postoje České republiky. Týkalo se to zejména projednávání návrhu GDPR, z jehož obsahu byla v roce 2012, na celkem osmi pracovních jednáních skupiny DAPIX, diskutována téměř polovina textu.

Aktivně vystupoval Úřad i v případě návrhu JHAD, jehož předložení a projednávání bez jasné prodiskutované definitivní podoby hlavního předpisu ochrany osobních údajů (GDPR) však považoval za předčasné. Připomínky Úřad uplatnil rovněž v rámci Pracovní skupiny pro ochranu údajů (WP29), nezávislého poradního orgánu Evropské komise, a jejích odborných podskupin, která v roce 2012 vydala k aktuálně diskutovaným tématům reformy ochrany osobních údajů dvě obsáhlá stanoviska.

Úřad se rovněž prostřednictvím své zástupkyně na plenárních zasedáních a na jednáních výboru skupiny T-PD Rady Evropy, kde plní funkci místopředsedy, podílel na připomínkování a dopracování **návrhu modernizace Úmluvy 108**. Ačkoliv byl T-PD dopracován definitivní návrh modernizované Úmluvy 108, bylo rozhodnuto, že v roce 2013 bude ještě ad hoc komisí, již ustaví Rada ministrů, harmonizován s návrhem GDPR, připravovaným Evropskou komisí.

Jednou z podstatných otázek při přípravě nového právního rámce ochrany osobních údajů je problém nezávislého **postavení a kompetencí národních dozorových úřadů pro ochranu osobních údajů**. Rozsudek Evropská komise v. Německo z roku 2010 již naznačil žádoucí poměr nezávislých dozorových úřadů ke státní službě, v případě Evropská komise v. Rakousko pak v roce 2012 zazněl jasný obdobný výrok, že Rakouská republika nepřijala veškeré právní předpisy nezbytné k tomu, aby právní úprava platná v Rakousku, týkající se Datenschutzkommission (komise pro ochranu osobních údajů) splňovala kritérium nezávislosti. Právní úpravou (na jejímž základě je tajemník Datenschutzkommission spolkovým úředníkem, podléhající služebnímu dohledu, přičemž kancelář Datenschutzkommission je začleněna do struktury spolkového kancléřství a současně má spolkový kancléř bezpodmínečné oprávnění k informacím ohledně všech aspektů řízení Datenschutzkommission), Rakousko nesplnilo povinnosti, které pro něj vyplývají z čl. 28 odst. 1 druhého pododstavce 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.

Tématem, kterému Úřad věnoval pozornost nejen v souvislosti s přípravou nového právního rámce ochrany osobních údajů, bylo **přeshraniční vynucování práva na ochranu osobních údajů**. Zásady dobré praxe (tzv. Best practices) i návrh dílčích metodik celosvětové spolupráce mezi více orgány dozoru v Evropě i v zámoří byly projednávány v rámci expertní skupiny OECD. Na úrovni WP29 pak byly diskutovány praktické poznatky z dozoru nad mimoevropskými správci osobních údajů, zejména takovými, kteří provozují populární internetové portály a služby.

Poznatky ze zemí, v nichž jsou tito správci usazení, nebo zde provozují úložiště dat, prokazují sice, že formálně byly naplněny požadavky ochrany osobních údajů, současně však odhalují problematičnost splnění všech zásad a patřičných záruk ochrany osobních údajů, pokud již při návrhu internetových aplikací nebylo přihlédnuto k požadavkům vyplývajícím z evropského práva (typickým příkladem je Facebook). S přihlédnutím k této skutečnosti Úřad v roce 2012 podpořil v rámci WP29 ta rozhodnutí, která pověřila vybrané národní dozorové úřady posoudit u vybraných poskytovatelů internetových služeb aktuálně realizované změny podmínek ochrany osobních údajů (např. Google či Microsoft).

Již tradičně byl v roce 2012 **Úřad zapojen do projektů** podpory dozorovým orgánům v zemích usilujících o přistoupení k Evropské unii. Čtyři zaměstnanci Úřadu přijali jakožto experti pozvání přednášet na seminářích kolegům v partnerských institucích, především v Makedonii, Albánii a Moldávii. Nejvíce žádanými tématy byly aspekty ochrany osobních údajů v oblasti finančnictví a policie a dále také výkon dozoru, komunikace s veřejností a mezinárodní předávání údajů. Úřad předpokládá, že účast jeho pracovníků v těchto akcích otevřela dveře pro trvalejší bilaterální spolupráci pro příští léta.

Úřad dále obdržel finanční prostředky z programu Celoživotního učení/Leonardo da Vinci – Partnerství na realizaci **mezinárodního projektu „Zvýšení povědomí o ochraně dat mezi zaměstnanci pracujícími v EU“**. Tento projekt navazuje na předchozí úspěšnou spolupráci z minulých let, kdy se v rámci téhož programu Úřad podílel na projektu, který téma ochrany dat zkoumal z pohledu zaměstnavatelů. Nový projekt je zaměřen na ochranu osobních údajů a soukromí na pracovišti, ať už v rámci klasického shromažďování a uchovávání osobních a citlivých údajů určených k realizaci pracovních vztahů či prostřednictvím moderních sledovacích a monitorovacích technologií. Cílem projektu je sestavit srozumitelnou, přehlednou a v praxi použitelnou příručku, která by, spolu s dalšími aktivitami, přispěla k prohloubení informovanosti zaměstnanců. Na realizaci projektu Úřad spolupracuje s partnerskými organizacemi v Polsku (koordinátor projektu), Bulharsku a Chorvatsku.

První schůzka, kde partneři projektu vypracovali osnovu příručky a dohodli časový harmonogram postupu prací včetně kontrolních termínů, proběhla v listopadu 2012 ve Varšavě.

V roce 2012 se Úřad vyjadřoval také k aspektům zpracování osobních údajů ve dvou zásadních politicko-právních tématech s mezinárodním prvkem:

V případě **zavedení nové informační povinnosti finančních institucí vyžadované daňovou správou Spojených států amerických** podle Foreign Account Tax Compliance Act (dále jen „**FATCA**“) Úřad upozornil na potřebu vyjasnění právního titulu pro zjišťování, shromažďování a další operace s údaji osob s „americkými indiciemi“ a na nutnost příslušných legislativních změn, bez nichž by docházelo k porušování zákona o ochraně osobních údajů. Současně se Úřad zapojil do diskuse nad zákonnou úpravou předávání osobních údajů shromážděných v rámci agendy FATCA finančními institucemi nebo daňovou správou v České republice do Spojených států amerických za podmínek § 27 zákona o ochraně osobních údajů.

Sjednávání obchodní dohody proti padělatelství mezi Evropskou unií a jejími členskými státy, Austrálií, Kanadou, Japonskem, Korejskou republikou, Spojenými státy mexickými, Marockým královstvím, Novým Zélandem, Singapurskou republikou, Švýcarskou konfederací a USA (ve zkratce „**ACTA**“) ukázalo nedostatky, jimiž se vyznačují tradiční přístupy vynucování práva ve složitém prostředí internetu. Do dohody ACTA nebyla zahrnuta žádná podrobná

ujednání výslovně odkazující na standardy, jimiž se ochrana osobních údajů v Evropské unii a jejích členských státech řídí. Nebylo však pochyb o tom, že osobní údaje budou na základě této dohody zpracovávány. Úřad proto považoval návrh ustanovení dohody týkající se zpracování informací (tedy i osobních údajů) za nejasný a z hlediska zásad ochrany osobních údajů za nevyvážený, neboť návrh ACTA nestanovil, jaká úroveň a jaké odpovídající nástroje ochrany osobních údajů mají být aplikovány. Ve svém stanovisku zaslaném Ministerstvu průmyslu a obchodu a na ně navazujících jednáních Úřad upozornil, že obchodní dohoda ACTA je z velké části založena na zpracování osobních údajů v oblasti nových technologií (internetu) a zasahuje do několika specificky regulovaných oblastí, jako je důvěrnost komunikací, zpracování provozních a lokalizačních údajů, zpřístupňování komunikace pro specifické účely vynucování práva, zpracování velkého množství údajů týkajících se nejen účastníků dvoustranných právních vztahů, ale zejména třetích osob (jak dodavatelů – poskytovatelů služeb a sítí elektronických komunikací, tak poskytovatelů služeb informační společnosti, jejich zaměstnanců, účastníků a uživatelů služeb).

V návrhu ACTA Úřad zejména považoval za vadné nástroje, které naváděly k tomu, aby mimo účel soudního vymáhání práva byly vedeny a shromažďovány informace o třetích osobách. Úřad upozornil, že pro účely tzv. *enforcementu* nelze nastavovat nové datové toky a nařizovat zpřístupnění informací (mnohdy původně zpracovávaných pro jiné účely), aniž by bylo současně vymezeno, jakým způsobem má k předávání a zpřístupňování informací docházet. Úřad proto doporučil přehodnocení širšího rámce dotčených právních předpisů. Dohoda ACTA nebyla v roce 2012 ojedinělým případem, kdy proces navrhování dokumentu zásadní povahy postrádal expertní zhodnocení, veřejnou konzultaci a hlubší věcné posouzení příslušných gestorů státní správy, z něhož by bylo patrné, za účelem jakých opatření, příp. změn je dokument přijímán a jakou přesnou oporu mají navrhované novinky v právním řádu ČR.

Práce v **expertních komisích Pracovní skupiny pro ochranu údajů (WP29)**, poradního orgánu Evropské komise, jejímž je Úřad členem, a jeho předseda je jejím místopředsedou, vyústila v roce 2012 ve vydání čtyř dokumentů týkajících se zpracování osobních údajů s využitím nových technologií. Jednalo se o stanoviska k rozpoznávání tváře u on-line a mobilních služeb, k vývoji biometrických technologií, k výjimkám požadavků na souhlas u cookies a k tématu, které bylo v uplynulém roce diskutováno odbornou veřejností nejčastěji – ke **cloud computingu**.

Částí odborné veřejnosti je stále jako problematická vnímána poslední novelizace evropské směrnice o soukromí v elektronických komunikacích, která inovovala pravidla o **zacházení s cookies** tak, aby uživatelé, kteří provádějí činnosti na internetu, jež by mohly vést k uchování údajů o nich, nebo k přístupu k těmto údajům, měli k dispozici jasné a srozumitelné informace o zpracování a mohli vyjádřit souhlas se zpracováním cookies (může být např. vyjádřen vhodným nastavením prohlížeče nebo jiné aplikace). V rámci EU byl tímto zaveden restriktivnější přístup a změny ve funkčnosti cookies z principu opt-out na opt-in, čímž došlo k posílení ochrany uživatelů internetu, neboť je vyžadováno poskytnutí informací a získání souhlasu uživatele ještě předtím, než bude cookie uložena, či bude získán přístup k již uchovávaným informacím v počítači uživatele.

O povinnostech dopadajících na cookies jakožto na osobní údaje reflektovala již stanoviska skupiny WP29 z roku 2010, týkající se behaviorální reklamy, a z roku 2009, týkající se vyhledávacích nástrojů a společenských sítí na internetu. V těchto dokumentech je mj. jasně deklarováno a vysvětleno, proč některé druhy cookies umožňují preciznější identifikaci uživatelů než např. IP adresy. To, že mnohé cookies jsou informacemi vypovídajícími o chování

jednotlivců a úzce souvisejí se soukromím uživatelů, jasně ukazují i nastavení cookies v internetových prohlížečích, obvykle v sekcích týkajících se „privacy settings“. Stanovisko poradní skupiny WP29 z července 2012 pak podrobněji rozvádí, k jakým druhům cookies je třeba aplikovat některé z principů a metod ochrany osobních údajů. Úřad se v roce 2012 zapojil do aktivit v rámci WP29, které předpokládají analýzu stavu zpracování cookies v aktuálních službách na internetu, a to ve spolupráci s Ministerstvem průmyslu a obchodu a Českým telekomunikačním úřadem.

Úřad, sdělovací prostředky a komunikační nástroje

V roce 2012 Úřad uspořádal tradičně tiskovou konferenci u příležitosti Dne ochrany osobních údajů. Jako obvykle byla tato konference příležitostí vyhlásit další ročník soutěže pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“ (bližší informace viz níže). Tato tisková konference nabídla přítomným novinářům také bilanci činnosti Úřadu za uplynulé půlroční období. Druhá bilanční tisková konference proběhla v druhé polovině roku.

Stejně jako v předcházejících letech byli tiskovým konferencím přítomni novináři ze všech druhů médií (tištěná, elektronická, zástupci rozhlasu a televize, agenturní novináři). Výstupy z tiskových konferencí se pravidelně objevovaly již v poledním zpravodajství v den konání konference, obdobně také telefonický rozhovor nejčastěji s předsedou Úřadu v poledních rozhlasových zpravodajských relacích.

V následujících dvou dnech po lednové konferenci bylo zveřejněno rekordních 90 příspěvků o ochraně osobních údajů – zatímco každodenní počet závažnějších mediálních zpráv o ochraně osobních údajů se pohybuje v průměru mezi 5–9 zprávami.

V přílohách k tiskovým zprávám poskytuje Úřad informace o ukončených kontrolách, správních řízeních a druhoinstančním řízení. Důležitá je nejen otevřenost, s níž hovoří o výsledcích své práce, ale především informování o důvodech uložených pokut. Toto Úřad považuje za příspěvek k prohlubování právního povědomí ve vztahu k zákonu o ochraně osobních údajů i způsobu jeho aplikace.

Po skončení tiskové konference jsou zveřejněny už trvale na webových stránkách Úřadu tiskové zprávy a další informační materiály. Široká veřejnost tak může dohledat jakoukoliv zprávu i zpětně a sledovat kontinuitu práce i rozhodování Úřadu.

KONTAKTY S MÉDIÍ

Každodenní servis poskytovaný médiím se týká bezprostředního poskytování odpovědí na dotazy novinářů, eventuálně příjem jejich podání spojený s případy, kdy se novináři setkávají s problematikou ochrany osobních údajů a které jsou pro Úřad důležitou zpětnou vazbou a někdy i orientací pro jeho dozorovou činnost.

Z témat, jimž se média v roce 2012 věnovala zejména, je třeba uvést ta obzvlášť frekventovaná: smlouva proti padělatelství ACTA, Google Street View, PNR data (předávání údajů o cestujících leteckých společnostech mezi USA a Evropskou unií), portál znamylekar.cz, zveřejňování dlužníků, kamery ve veřejné dopravě, osobní údaje a IZIP, zveřejňování fotografií domnělých zlodějů, zveřejňování platů veřejných činitelů – Metodika vydaná MV a ÚOOÚ k této problematice, fotopasti, sledování poštovních doručovatelů s použitím GPS, výše uložených pokut v souvislosti s nevyžádanými obchodními sděleními, pokuta uložená MŠMT za zveřejnění osobních údajů romských stipendistů, únik fotografií z policejního spisu, sledování na pracovištích, kamerový systém na Vrchním státním zastupitelství v Praze, krádeže osobních údajů, odhlasování německého zákona umožňujícího prodej osobních údajů „městy“ soukromým firmám, sledování národnosti turistů v ČR pomocí mobilních telefonů, otázka policejní databáze DNA, skipasy a zveřejňování záznamů z jednání obecních zastupitelstev.

Z uvedeného každodenního servisu poskytovaného médiím lze soudit, že problematika ochrany osobních údajů je značně frekventovaným mediálním tématem a že otevřenost, s níž o ní Úřad informuje, znamená přínos právnímu povědomí veřejnosti. Nicméně poslední jmenované v médiích frekventované téma – zveřejňování záznamů z jednání obecních zastupitelstev – se stalo v loňském roce naprosto nepochopeným. A to přesto, že Úřad již v roce 2011 přinesl ve své výroční zprávě obsáhlý právní výklad a objasnil spojitost se zákonem o obcích, z čehož plyne nepřipustnost zveřejňování záznamů prostřednictvím internetu. Tento výklad, jak se ukázalo, zůstal většinou nepochopitelný pro média a v rozporu s vůlí Otevřené společnosti o.p.s., jak vykládat právní rámec; a tak byla Úřadu touto společností udělena anticena Zavřeno. Nešlo tedy o nepřístupnost informací, jak by se jevílo logické z názvu udíleného ocenění, ale o „odmítaný“, byť reálný výklad zákonného rámce Úřadem. Bylo tedy bohužel nutné konstatovat, že vztah k českému právnímu řádu může z důvodu zarytého voluntarismu postrádat právní přesnost a ochotu přistupovat k zákonu standardními demokratickými postupy.

Kromě tiskových zpráv a sdělení Úřadu vydávaných mimořádně, kdy je třeba se vyjádřit k jednotlivé události v chodu prací Úřadu, informovat o ní či uvést na pravou míru médií publikovanou zprávu, poskytuje tiskový odbor individuální servis novinářům. Prostředkem je jak e-mailová komunikace, tak telefonické spojení – novináři stále oblíbenější, ačkoliv pro přenos informace, jak se opakovaně potvrzuje, nezaručující zdaleka dokonalou přesnost.

ŠÍŘENÍ ZNALOSTÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Příležitost Dne ochrany osobních údajů (28. ledna) dává možnost hovořit také o ochraně osobních údajů v obecnější rovině – v kontextu práva na soukromí jakožto základního lidského práva. Již pošesté vyhlásil Úřad soutěž pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“. V rámci šíření znalostí o ochraně osobních údajů (která je stavěna mezi důležité úkoly úřadů pro ochranu osobních údajů ve všech státech, v nichž tyto instituce působí) se v roce 2012 Úřad zaměřil na stále palčivější problém – využívání internetu mladými lidmi

a pobídl je k zamýšlení, zda si dostatečně uvědomují důsledek svých přístupů k tomuto svému oblíbenému způsobu komunikace:

**Úřad pro ochranu osobních údajů
u příležitosti „Dne ochrany osobních údajů“ 28. ledna 2012**

vyhlašuje

VI. ročník soutěže pro děti a mládež

„Moje soukromí! Nekoukat, nešťourat!“

Jeden z hlavních problémů umístění informací na internetu se týká ztráty kontroly nad těmito informacemi: Jakmile se zveřejní, stanou se dostupné pro vyhledávače a lze je zaregistrovat a dále předávat pomocí síťových nástrojů, jako jsou sociální sítě apod.

Co si o té věci myslí mladá generace? Dva níže rozehrané příběhy, v nichž je uvedený problém zápletkou, mohou dle vlastní fantazie děti **do 18 let** dotvořit.

Mohou napsat povídku, úvahu, filmovou povídku, scénář, nebo mohou také příběh, který si vymyslí, sehrát, natočit na video, případně ztvárnit v podobě comicsu, a poslat (s uvedením jména, adresy a věku*) **do 15. dubna 2012** buď elektronicky na adresu: soutez@uouu.cz (soubory do velikosti 3 MB), anebo na adresu **Úřad pro ochranu osobních údajů, tiskové oddělení, Pplk. Sochora 27, 170 00 Praha 7** (obálku označit heslem „Soukromí“).

Autor nejlepšího zpracování bude pozván na Mezinárodní festival filmů pro děti a mládež, kde mu bude slavnostně předáno ocenění.

Příspěvky všech zúčastněných zveřejníme a vydáme v brožované publikaci.

Aktuální informace o soutěži budou průběžně k dispozici na webových stránkách Úřadu www.uouu.cz v rubrice Pro mládež.

*Adresa bude použita jen v rámci soutěže, jméno a věk případně v rámci propagačních účelů ochrany osobních údajů. Pokud neobdržíme výslovné přání, že zasláná práce k uvedené propagaci nesmí být použita.

CO SE STALO, KDYŽ...

...**Milan** byl tak trochu doma mazánek. Rodiče se v něm od malička viděli, protože dlouho čekali, než se jim synek narodil. Když přišel na svět, zaznamenávali v deníku, ale i fotoaparátem a videokamerou každý jeho krůček. Obrázky i natočené „scény“ ze synova života posílali babičkám, kamarádům a umísťovali na internet, kde si zřídili blog a uvažovali o vývoji svého dítěte. A tak nahatý Milánek pózoval na kožešině i na písku a v bazénu, smál se i brečel, seděl a způsobně se snažil na nočníčku... Byl roztomilý a rostl...

Ve škole byl šikovný kluk, rád se učil a také rád a slušně hrál na klavír. Byl oblíbený mezi kamarády, s učiteli neměl žádné konflikty. Myslel si, že se mu podaří jít na konzervatoř. Ale byl trémista, a kdoví – zkoušku prostě neudělal. Nakonec si řekl, že půjde na gymnázium a pak na pedák a stane se učitelem hudební výchovy a češtiny. Tohle mu vyšlo. Jenomže protože uměl dobře jednat s lidmi, byl dobrý pedagog i organizátor, nechal se kolegy přesvědčit a šel do konkurzu na ředitele školy. A tohle také vyšlo. Škola běžela, ale... Na nástěnce se jednoho dne objevily obrázky stažené z internetu: nahatý Milánek pózoval na kožešině a způsobně se snažil na nočníčku, jenomže tentokrát s patřičným komentářem o panu řediteli... A pak začaly fotografie kolovat po internetu...

...**Marcela** dostala k patnáctým narozeninám od mámy senzační prádýlko. Večer šli rodiče na večeři a Marcela dostala k dispozici byt, aby si s kamarády udělali párty. Zapařili a došlo i na tanečky. A Marcela se nechala od holek vyprovokovat, aby si zahrála Go-go tanečnici a předvedla dárek od mamči... Petr vytáhl mobil a poslal pár fotek Honzovi, který ležel s angínou. Protože se doma nudil, jako počítačový maniak fotky hned hodil do počítače a zpracoval prezentaci, kterou poslal Marcelce jako dárek k narozeninám. Bylo z toho velké gaudium, protože Honza

doplnil Marcelinu produkci vtipným komentářem o profesionálkách, jaké rostou na jejich škole. Po škole se šířil odkaz na prezentaci, která byla nakonec na internetu.

Běžel čas, Marcela vystudovala práva. Měla velké ambice, byla koneckonců premiantka, a tak poslala životopis na několik míst, lukrativních a prestižních, taky u zahraničních společností. Co se stalo, když se její internetový dárek od Honzy objevil mezi materiály, které si o ní dohledala výběrová komise...

Partnery v pořádání soutěže v roce 2012 byly Český rozhlas Praha, MFF pro děti a mládež Zlín (kde byly předány ceny vítězům) a také Svaz knihovníků a informačních pracovníků (SKIP), disponující sítí kontaktů na knihovny z celé České republiky, které se velmi aktivně věnují dětem a mládeži, jak potvrdila už spolupráce v roce 2011.

O výsledcích soutěže podrobně informují webové stránky Úřadu ve speciální rubrice „Pro mládež“.

APLIKACE ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ V RÁMCI KOMUNIKACE ÚŘADU S ODPOVĚDNÝMI SUBJEKTY

Také v roce 2012 se zaměstnanci Úřadu zúčastnili řady odborných přednášek a konferencí, které se zabývaly problematikou, kde Úřad vykovává své dozorové pravomoci. Z mnoha akcí lze zmínit přednášky pořádané subjekty, jako je: Advokátní kancelář Wolf Theiss; Sokolovská uhelná, a.s.; Úřad městské části Praha 8; Společnost medicínského práva (účast na diskusním fóru); Krajský úřad Olomouckého kraje; LP-EFEKT, vzdělávací agentura; Policejní prezidium ČR; InBIT Česká republika, s.r.o.; F.S.C. Bezpečnostní poradenství; Národní centrum bezpečnějšího internetu ve spolupráci se Senátem Parlamentu ČR; EELA European Employment Lawyers Association; Grémium Alarm, o.s. (konference AGA); Pro Centre s.r.o.; Justiční akademie; Plzeňský Prazdroj; Asociace inkasních agentur; Software 602; BOVA Polygon; 1. VOX a.s., přednáška pro Město Chrudim; Jasanská & co advokátní kancelář; Ministerstvo financí; Právnická fakulta UK v Praze; Ministerstvo vnitra ČR; Bankovní institut Vysoká škola, a.s.; Norton Rose v.o.s. advokátní kancelář; Nakladatelství FCC Public – Perspektivy bydlení; Svaz českých a moravských bytových družstev; Magistrát hl. města Prahy.

Těchto akcí bylo celkem 31 a některé z nich byly speciálně přizpůsobeny po dohodě s pořadatelem s ohledem na okruh posluchačů (kdy šlo například jen o zaměstnance pořadatele); jiné byly obecnějšího charakteru, případně specializované dle projednávané problematiky (problematika obcí, elektronických informací, činnost policie při zpracování osobních údajů, bezpečnost dat apod.).

Speciálně byla v roce 2012 věnována pozornost šíření znalosti o kompetenci Úřadu v rámci provozu základních registrů, tedy Informačního systému ORG jako součásti systému základních registrů, která zajišťuje procesy spojené s identifikací fyzických osob a se zabezpečením jejich osobních údajů: Dopady zavedení IS ORG do života, celostátní konference ISSS, Hradec Králové (duben 2012); v dubnu až červnu proběhly semináře pro úředníky (Praha, Olomouc, Ostrava, Brno, Plzeň, Praha); v červnu proběhla přednáška Informační systém ORG – bezpečnost základních registrů pro Kancelář veřejného ochránce práv v Brně; v září pak v Mikulově na celostátní konferenci eGovernment přednáška Základní registry – dva měsíce provozu IS ORG a v prosinci na konferenci eGovernment 2012 přednáška Informační systém ORG v systému Základních registrů v Praze.

AKTIVITY ÚŘADU V KOMUNIKACI S ODBORNOU VEŘEJNOSTÍ

V roce 2012 Úřad pokračoval ve svých aktivitách, které vyvolává společenská potřeba: O některých záměrech povinných osob je nejprve třeba diskutovat a teprve následně je realizovat. Zatím se většina těchto aktivit odehrávala prostřednictvím konzultačních aktivit v rámci § 29 písm. h) zákona o ochraně osobních údajů.

Jak řečeno mj. výše, odborníci Úřadu se účastnili mnoha konferencí a seminářů pořádaných k jednotlivým tématům ochrany osobních údajů.

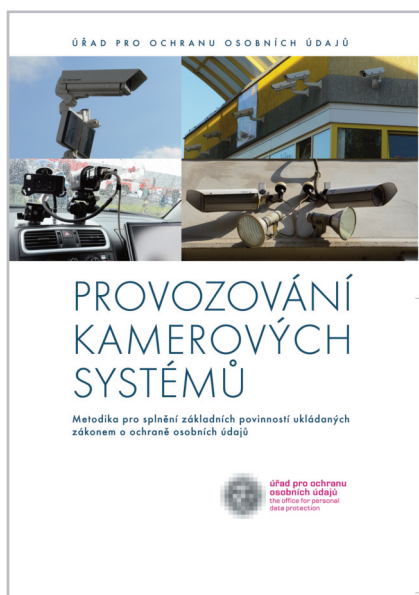
V roce 2012 však Úřad sám takovou konferenci již organizoval. Šlo o třetí ročník konference s názvem Bezpečnost a ochrana osobních údajů, kde se odborná veřejnost a zástupci Úřadu pravidelně už podvkrát setkali a diskutovali o novinkách v této oblasti z pohledu podmínek ochrany osobních údajů. Pořadatelem se tentokrát stal Úřad a jeho partnerem Česká asociace bezpečnostních manažerů.

Novinkou v komunikaci s odbornou veřejností jsou od roku 2012 kulaté stoly, které se pořádaly k různým tématům.

V lednu 2012 byl u příležitosti Dne ochrany osobních údajů (28. ledna) uspořádán kulatý stůl, jehož tématem byla problematika přístupů médií k ochraně osobních údajů. Přítomní zástupci médií a odborné veřejnosti se shodli na potřebě sebereflexe novináře publikujícího informace, které se mohou dotýkat soukromí jednotlivých osob a jejich okolí.

Další kulatý stůl, který Úřad organizačně zajistil společně se společností ORSEC, se konal v říjnu, a jeho hlavním nosným tématem byly kamerové systémy. Vzhledem k rozsahu tohoto tématu byly pro diskusi odborníků vybrány oblasti provozu kamerových systémů v bytových domech a v dopravě. Úřad se v této souvislosti zavázal dopracovat v krátké době metodiku ke

kamerovým systémům, což ještě do konce roku 2012 splnil. Brožura „Provozování kamerových systémů (Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů)“ se setkala se zájmem nejen účastníků uvedeného kulatého stolu. Zůstala dostupná na vyžádání v tištěné podobě v tiskovém odboru Úřadu i zveřejněna na webu Úřadu.



V závěru roku 2012 se v součinnosti s advokátní kanceláří Kinstellar konal kulatý stůl, jehož tématem byly právní aspekty sledování zaměstnanců, i v kontextu trestní odpovědnosti právníků osob; jako téma druhé byly diskutovány podmínky pro předávání osobních údajů do zahraničí. I v tomto případě lze akci hodnotit jako úspěšnou – dokladem toho byla bohatá a otevřená diskuse přítomných zástupců firem a společností se zástupci Úřadu o konkrétních problémech v aplikaci zákona o ochraně osobních údajů.

Díky pozitivním zkušenostem s kulatými stoly Úřad bude v jejich pořádání pokračovat.



Kulatý stůl, 16. října 2012, ve spolupráci se společností ORSEC

KNIHOVNA A PUBLIKACE ÚŘADU

Knihovna je odborným zázemím pro pracovníky Úřadu. Je ovšem otevřena na individuální vyžádání též odborné veřejnosti. Využívají ji studenti pro své seminární a diplomové práce dotýkající se ochrany osobních údajů. V roce 2012 poskytla svůj fond třem studentům a získala jednu diplomovou práci, která těžila z jejího fondu. Fond knihovny se rozrostl o 78 svazků – z toho 64 bylo zakoupeno, 14 získáno darem.

V roce 2012 Úřad publikoval částky 61–63 svého Věstníku. Zde publikovaná stanoviska Úřadu jsou určena odborným pracovištím a státním institucím, stejně jako závažné zahraniční dokumenty věnované ochraně osobních údajů. Trvale jsou tyto dokumenty s malým časovým odstupem od vydání Věstníku dostupné rovněž na webových stránkách Úřadu.

V roce 2012 vyšlo číslo Informačního bulletinu, které se tematicky zaměřilo na problematiku základních registrů v zájmu toho, aby se k širší veřejnosti dostaly informace od představitelů každé ze součástí základních registrů (tedy nejen jeho součásti ORG, kompetenčně příslušející Úřadu), které budou, jak se dá předpokládat, v průběhu času ovlivňovat život občanů a jsou vytvářeny jako systém se záměrem učinit komunikaci s úřady a institucemi komfortnější a časově méně náročnou.

Vydání bylo podpořeno z finančních zdrojů vyčleněných pro prezentaci základních registrů z Evropského fondu regionálního rozvoje.

WEBOVÉ STRÁNKY ÚŘADU

Na své tiskové konferenci na podzim roku 2012 informoval Úřad o tom, že vytvoří nové webové stránky, které budou nejen vizuálně inovované, ale především uživatelsky komfortnější a také výkonnější co do vyhledávacích možností. Na tomto systému se začalo pracovat poté, co Úřad prostřednictvím diskusního fóra ověřil názory a potřeby uživatelů stránek a jako dodavatel byla vybrána společnost Webhouse. Stránky se v počátku roku 2013 dostanou do zkušebního provozu.

V současné době ovšem stávající webové stránky poskytují službu uživatelům v rozsahu, na který byli zvyklí a jenž dle zjištění prostřednictvím diskusního fóra nebyl vystaven žádným připomínkám zásadního dosahu. Nicméně není pochyb o tom, že nové webové stránky budou nabízet uživatelům dokonalejší službu.

Informace zveřejňované na webových stránkách jsou výběrově poskytovány informačnímu systému, který používá na svém území Městská část Praha 7. Úřad považoval za vhodné spolupracovat s městskou částí Prahy, kde sídlí, a poskytovat jejím obyvatelům svého druhu nadstandardně informace jako výraz společné územní příslušnosti.

Informační systém ORG

Rok 2012 byl ve znamení dokončení projektu „Informační systém ORG v systému základních registrů“ a ostrého startu tohoto systému. Zákon č. 111/2009 Sb., o základních registrech (dále zákon č. 111/2009 Sb.) a jeho změna zákonem č. 100/2010 Sb., přinesl Úřadu nový úkol – do 30. 6. 2012 vytvořit Informační systém ORG jako součást systému Základních registrů, která bude zajišťovat procesy spojené s identifikací fyzických osob.

Informační systém ORG v systému základních registrů je realizován v rámci Integrovaného operačního programu, prioritní osa Modernizace veřejné správy – Cíl Konvergence, oblast podpory Rozvoj informační společnosti ve veřejné správě. Odbor strukturálních fondů MV ČR schválil uvedený projekt dne 30. 11. 2009.

Smyslem začlenění Informačního systému ORG do systému základních registrů je ochrana identity občanů před zneužitím jejich osobních údajů. ORG je jedinou institucí, která dokáže převádět agendové identifikátory z jedné agendy do agendy druhé.

Na základě již zmiňovaného zákona č. 111/2009 Sb. jsou založeny čtyři základní registry (dále ZR) a další součásti systému:

- Registr obyvatel,
- Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (registr osob),
- Registr územní identifikace, adres a nemovitostí (registr územní identifikace),
- Registr agend orgánů veřejné moci a některých práv a povinností (registr práv a povinností),
- Informační systém základních registrů,
- Informační systém pro přidělování a tvorbu identifikátorů a vedení jejich seznamů (ORG).

Projekt byl rozdělen na čtyři etapy výstavby:

Etapa BASE	9. 2. 2011 – 30. 9. 2011
Etapa ADVANCED	1. 10. 2011 – 16. 1. 2012
Etapa FULL	17. 1. 2012 – 30. 6. 2012
Etapa DOKONČENÍ PROJEKTU	1. 7. 2012 – 31. 12. 2012
17. 1. 2012	zahájena třetí etapa FULL
1. 4. 2012	spuštěn pilotní provoz
15. 5. 2012	předán HW druhého datového centra a toto zprovozněno
30. 5. 2012	ukončena třetí etapa FULL
1. 7. 2012	zahájena etapa DOKONČENÍ PROJEKTU

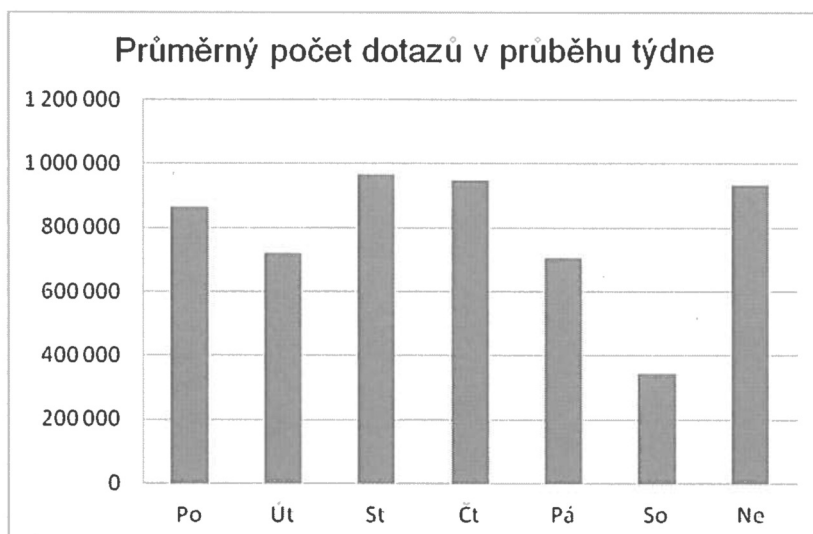
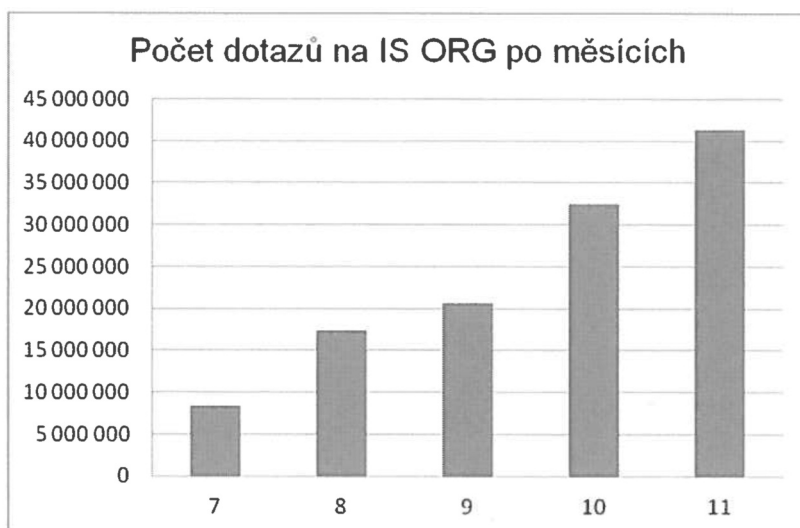
Pro potřeby pilotního provozu Úřad generoval, z dodaných údajů, data pro testování provozu jednotlivých registrů. Jen pro provoz registru ROB (registr osob) bylo založeno a generováno přes 16 milionů agendových identifikátorů (AIFO). Celkem bylo během pilotního provozu vygenerováno a založeno 29 milionů AIFO.

Na konci etapy FULL již ORG disponoval plnou funkcionalitou, 100% výkonem a redundantním provozem v primární a sekundární lokalitě (z důvodu poskytování bezvýpadkových služeb).

Od 1. 7. 2012 systém běží v ostrém provozu – etapa DOKONČENÍ PROJEKTU

Etapa DOKONČENÍ PROJEKTU 1. 7. 2012 – 31. 12. 2012

Provoz základních registrů je provozován ve dvou datových centrech, spojených do geo-clusteru. Na IS ORG jsou kladeny vysoké nároky na dostupnost služeb, neboť poskytování referenčních údajů ze strany ZR je podmíněno dodáním příslušného agendového identifikátoru z ORG.



Maximum: neděle 25. 11. 2012 9 168 298

Pro pracovníky odboru ORG v tomto roce proběhla řada odborných školení. Školení provedli pracovníci dodavatele systému TESCO SW a.s. Olomouc. Týkala se správy a sledování systému ORG, vzdáleného sledování zabezpečení a hlášení požadavků na opravu a úpravu SW. Řídicí pracoviště je vybudováno přímo v budově Úřadu a je zajištěn dohled na provoz 24 hodin 7 dní v týdnu. V současné době má odbor základních identifikátorů pět pracovníků.

Bohatá byla propagační a osvětová činnost ředitelky odboru Ing. E. Vrbové, která proběhla na celostátních konferencích věnovaných e-Governmentu a přednáškách k objasnění fungování systému ORG a s tím spojené ochraně osobních údajů. Přednesla příspěvky na celostátních konferencích v Hradci Králové – duben, Mikulově – září a Praze – prosinec. S fungováním systému byla obeznámena i kancelář ombudsmana ČR v Brně. Problematice registrů byl věnován i Informační bulletin 1/2012 Úřadu.

Dne 20. 11. 2012 byla podepsána trojstranná „Smlouva o poskytování sdílených služeb datových center“ mezi Správou základních registrů, TESCO SW a Úřadem.

V září 2012 proběhly penetrační testy provedené AEC, spol. s r.o., která zajišťovala analýzu a definici bezpečnostních požadavků informačního systému ORG, hodnocení plnění bezpečnostních požadavků informačního systému ORG v průběhu jeho implementace a vyhodnocení splnění bezpečnostních požadavků informačního systému ORG po jeho implementaci. Penetrační testy proběhly v obou datových centrech, na Úřadu a na zálohovacím datovém centru, kde je uložena testovací a vývojová verze ORG. Výsledkem je závěrečná bezpečnostní zpráva, ve které je konstatováno, že na základě provedených penetračních testů a bezpečnostních auditů je informační systém ORG velmi dobře zabezpečen, a to zejména vůči případnému vnějšímu útoku.

Administrativní zajištění projektu a souvisejících poradenských a administrativních činností měla na starosti společnost Eunice Consulting a.s. Vypracovala „Monitorovací zprávy“ a „Žádosti o platbu“ na etapu ADVANCED, FULL a PROVOZ, které byly předány na Odbor strukturálních fondů MV ČR. Žádosti byly kladně vyřízeny a prostředky převedeny na účet Úřadu.

Tento projekt byl z 85 % financován z prostředků Evropské unie a zbývajících 15 % financí bylo zajištěno ze státního rozpočtu usnesením vlády č. 1019/2009.

Publicita je povinnou součástí každého projektu Evropské unie; pro projekt IS ORG v systému základních registrů ji zajišťovala firma Tristarpromotion s.r.o. – zajistila koordinaci publicity s ostatními projekty základních registrů, propagaci článků o IS ORG, tisk bulletinu a výrobu propagačních materiálů.

Projekt „Optimalizace procesů ÚOOÚ“

Úřad zakončil druhý rok realizace projektu „Optimalizace procesů ÚOOÚ“, jehož cílem je zvýšení kvality a efektivity interních procesů a nastavení systému řízení projektů. Úřad tak naplňuje cíle vládní strategie Smart Administration, jejímž smyslem je zkvalitnění služeb veřejné správy s využitím prostředků ze strukturálních fondů. Projekt je finančně podpořen z Evropského sociálního fondu v rámci Operačního programu Lidské zdroje a zaměstnanost, a to konkrétně z prioritní osy „Veřejná správa a veřejné služby (Konvergence)“ a oblasti podpory „Posilování institucionální kapacity a efektivnosti veřejné správy“.

Projekt se ve svých klíčových aktivitách zaměřil na vytvoření projektové kanceláře, která centralizuje projektové aktivity Úřadu na jednom místě – dohled nad jednotlivými projekty realizovanými útvary Úřadu, jejich koordinace, metodická podpora a zajištění potřebných standardů a optimalizace provozních, ekonomických a personálních procesů přípravou nových směrnic.

V rámci provozních procesů byla navržena SW podpora řízení provozních služeb – elektronizace procesů (helpdesk). Jedná se především o zajištění autoprovozu, technických služeb a IT požadavků. SW podpora řízení provozních služeb bude spuštěna na začátku roku 2013.

Součástí optimalizace byla také úprava stávajících interních předpisů a tvorba nových interních předpisů podle změn v jednotlivých procesech dle nového organizačního řádu. Většina nových předpisů se nachází v připomínkovacím řízení, přičemž se předpokládá, že začátkem roku 2013 vejdou tyto předpisy v platnost.

V roce 2012 byla vytvořena metodika projektového řízení a zaveden systém projektového řízení do prostředí Úřadu. Ve sledovaném monitorovacím období proběhlo testování metodiky na pilotním projektu, kterým byl stanoven přímo projekt „Optimalizace procesů“. Za účelem snadné a přehledné administrace projektů byl na Úřadě implementován elektronický nástroj – Projektový portál.

Projekt bude probíhat ještě v roce 2013, kdy budou schválené změny postupně implementovány do chodu Úřadu. Do projektu jsou průběžně zapojováni nejen zaměstnanci Úřadu, ale i další organizace působící ve veřejné správě, které budou moci profitovat z realizace projektu v rámci přenosu příkladů dobré praxe. Projekt potrvá do léta 2013 a jeho výstupy budou prezentovány například zástupcům Úřadu pro ochranu hospodářské soutěže, Nejvyššího kontrolního úřadu, Energetického regulačního úřadu, České školní inspekce, Českého telekomunikačního úřadu a České obchodní inspekce.

Personální obsazení Úřadu

Počet funkčních míst v Úřadu je stanoven státním rozpočtem na 102, tento počet zůstal stejný jako v předchozím roce.

Fluktuace zaměstnanců byla o něco vyšší než v předchozím roce. Během roku nastoupilo 10 nových zaměstnanců a 13 zaměstnanců odešlo. Z toho 1 zaměstnanec dostal výpověď z organizačních důvodů, 2 zaměstnankyně odešly na mateřskou dovolenou a 1 zaměstnanec odešel do starobního důchodu.

Ke dni 1. 1. 2012 měl Úřad 100 zaměstnanců a ke dni 31. 12. 2012 byl jejich počet 97. Průměrný evidenční počet zaměstnanců za rok 2012 byl 98,5.

V průběhu roku se v Úřadu uskutečnily dvě organizační změny. Důvodem bylo nové uspořádání činností útvarů a jejich nové postavení, v důsledku toho byly i některé útvary přejmenovány.

K zajištění pomocných činností a odborných, úzce specializovaných činností a jako členy zvláštní komise zaměstnává Úřad na základě dohod o pracovní činnosti nebo dohod o provedení práce externí zaměstnance. Spolupráce s těmito externími zaměstnanci funguje velmi dobře.

Věková struktura zaměstnanců (viz tabulka) zůstává stejná jako v předchozím roce. Nejpočetnější skupinu tvoří zaměstnanci ve věku od 51 do 60 let (37,11 %), v předchozím roce to bylo 36,4 %. Při porovnání s rokem 2011 se objevil jediný rozdíl, a to u žen. Druhou nejpočetnější skupinou po skupině ve věku od 51 do 60 let byly ženy ve věku od 31 let do 40 let. V roce 2012 je na druhém místě skupina žen ve věku od 21 let do 30 let.

Struktura vzdělání (viz tabulka) zůstává také skoro totožná s rokem předešlým, nejvyšší počet zaměstnanců Úřadu má vysokoškolské vzdělání (62,89 %), v předešlém roce to bylo 62,6 %. Vysoké procento souvisí s požadavkem Úřadu na vysokoškolské vzdělání, především právní a IT, na převážnou většinu pracovních míst.

Úřad si uvědomuje důležitost vzdělání zaměstnanců, a proto jim umožňuje prohlubovat si odbornou kvalifikaci, případně si ji i zvyšovat, pokud je to v souladu s potřebami Úřadu. Zaměstnanci v pracovním poměru mají také možnost navštěvovat jazykové kurzy. Jazykové znalosti jsou nepostradatelné pro výkon některých funkcí, pro spolupráci s úřady jiných zemí a pro dobrou reprezentaci Úřadu.

Rok od roku se zvyšuje i zájem studentů a absolventů středních a vysokých škol o získání odborné praxe nebo absolvování stáže v Úřadu.

Členění zaměstnanců ÚOOÚ podle věku a pohlaví – stav k 31. prosinci 2012

Celý soubor	muži	ženy	celkem	%
do 20 let	0,00	0,00	0,00	0,00
od 21 do 30 let	5,00	11,00	16,00	16,49
od 31 do 40 let	8,00	6,00	14,00	14,43
od 41 do 50 let	9,00	6,00	15,00	15,46
od 51 do 60 let	14,00	22,00	36,00	37,11
61 a více	13,00	3,00	16,00	16,49
Celkem	49,00	48,00	97,00	100,00

Členění zaměstnanců ÚOOÚ podle vzdělání a pohlaví – stav k 31. prosinci 2012

Celý soubor	muži	ženy	celkem	%
H – Střední odborné + VL	1	1	2	2,06
J – Střední odborné	0	1	1	1,03
K – Úplné střední všeobecné	2	5	7	7,22
L – Úplné střední odborné + VL	1	1	2	2,06
M – Úplné střední odborné	5	17	22	22,68
N – Vyšší odborné vzdělání	0	1	1	1,03
T – Vysokoškolské	40	21	61	62,89
V – VŠ + vyšší kvalifikace	0	1	1	1,03
Celkem	49	48	97	100,00

Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 455/2011 Sb., o státním rozpočtu České republiky na rok 2012.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

Souhrnné ukazatele	v tisících Kč
Příjmy celkem	89 566,00
Výdaje celkem	203 555,71
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	89 566,00
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	84 991,88
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	4 574,12
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	203 555,71
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci (povinné pojistné placené zaměstnavatelem)*	44 292,01
Převod fondu kulturních a sociálních potřeb	15 624,07
Platy zaměstnanců v pracovním poměru	424,76
Platy zaměstnanců v prac. poměru odvozané od platů ústav. činitelů	34 335,36
Výdaje spolufinancované z rozpočtu Evropské unie bez SZP celkem	8 165,00
v tom: ze státního rozpočtu	104 626,45
podíl rozpočtu Evropské unie	15 657,92
Výdaje vedené v informačním systému program. financování celkem	88 968,52
	110 695,59

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

1. PŘÍJMY

Příjmy pro rok 2012 byly schváleným rozpočtem stanoveny ve výši 22 942 tisíc Kč, a to v souvislosti s projekty spolufinancovanými z rozpočtu EU – IOP „Informační systém ORG v systému základních registrů“ a projektem OP LZZ „Optimalizace řídicích procesů ÚOOÚ“.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů byl naplněn částkou 89 566,00 tisíc Kč.

Jednalo se zejména o refundace zahraničních cest zaměstnanců Úřadu Evropelem a Evropskou komisí, o sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti, o sankce uložené podle zákona č. 101/2000 Sb., o ochraně osobních údajů a jiných zákonů, o náhrady nákladů řízení, o úroky z finančních prostředků uložených na bankovních účtech, o refundace výdajů týkající se komunitárního programu Leonardo da Vinci „Zvýšení povědomí o ochraně osobních údajů mezi zaměstnanci pracujícími v EU“, o refundace výdajů projektu Technické pomoci Makedonie, o příjmy vztahující se k roku 2011 (odvod zůstatku depozitního účtu po vyplacení platů a přidělu do FKSP za prosinec 2011).

Úroky z finančních prostředků uložené na účtech u ČNB činily 0,24 tisíc Kč.

Přijaté sankční platby byly ve výši 3 775,78 tisíc Kč, investiční a neinvestiční dotace z EU ve výši 84 991,88 tisíc Kč, pojistné náhrady ve výši 36,44 tisíc Kč, přijaté nekap. příspěvky a náhrady týkající se minulých let, včetně převodů z ostatních vlastních fondů ve výši 61,66 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

2. OSTATNÍ BĚŽNÉ VÝDAJE

Čerpání běžných výdajů ve výši 42 805,90 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. Dále se zde promítly i výdaje spojené s provozováním informačního systému ORG v systému základních registrů, který byl spuštěn do provozu 1. 7. 2012.

Výdaje za vodu, plyn, el. energii a PHM činily v roce 2012 2 003,45 tisíc Kč.

Výše uvedené částky odpovídají požadavku na účelný a hospodárný provoz Úřadu.

Jsou zde rovněž zahrnuty běžné výdaje na projekty, spolufinancované z rozpočtu EU v celkové výši 10 403,72 tis. Kč.

3. PLATY ZAMĚSTNANCŮ A OSTATNÍ PLATBY ZA PROVEDENOU PRÁCI, VČ. SOUVISEJÍCÍCH VÝDAJŮ

Čerpání rozpočtu na platy zaměstnanců, ostatních výdajů za provedenou práci a souvisejících výdajů, vč. projektů, ve výši 60 340,84 tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. 12. 2012 byl 97 zaměstnanců.

4. VÝDAJE VEDENÉ V INFORMAČNÍM SYSTÉMU PROGRAMOVÉHO FINANCOVÁNÍ MINISTERSTVA FINANČÍ – EDS/SMVS

V souladu se schválenou dokumentací programu 143V01 „Rozvoj a obnova materiálně-technické základny Úřadu pro ochranu osobních údajů – od r. 2007“ bylo celkem vyčerpáno 110 695,59 tisíc Kč.

V podprogramu 143V01100 „Pořízení, obnova a provozování ICT ÚOOÚ“ bylo v roce 2012 čerpáno celkem 109 840,49 tis. Kč v *investičních* systémově určených výdajích SR na následující akce:

	v tis. Kč
akci 143V011000037 „Prodloužení smlouvy Enterprise na používání produktů Microsoft“	1 680,67
akci 143V011000040 „Prodloužení platnosti licencí AVG“	165,08
akci 143V011000041 „Úprava modulu NOS“	98,15
akci 143V011000042 „Nový modul Data Breaches“	70,60
akci 143V011000043 „Upgrade int. služ. serveru a zajišť. jeho provozu...“	271,02
akci 143V011000044 „Rozšíření spisové služby GINIS a napojení na ISZR“	258,00
akci 143V011000045 „Doplnění funkcionality IS ORG...“	144,00
akci 143V011000019 „Základní registry-ORG“ projekt IOP	100 131,25
akci 143V011000027 „Optimalizace procesů ÚOOÚ“ projekt OP LZZ	4 254,91
akci 143V011000046 „Datové centrum“	2 616,81
akci 143V011000047 „Registr – vytvoření vazby na ISZR“	150,00

V podprogramu 143V01200 „Reprodukce majetku ÚOOÚ“ bylo v roce 2012 čerpáno celkem 855,10 tis. Kč v *investičních* systémově určených výdajích SR na následující akce:

akci 143V012000015 „Pořízení osobního vozidla“	553,31
akci 143V012000016 „Úprava silových el. rozvodů v objektu Úřad“	86,70
akci 143V012000017 „Stavební úprava místnosti 021“	145,30
akci 143V012000018 „Instalace bezpečnostních dveří – místnost 021“	69,79

Přehled čerpání rozpočtu v roce 2012

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2012 v tis. Kč	Konečný rozpočet 2012 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2012 v tis. Kč	Skut./konečný rozpočet v %
4118	Neinvestiční převody z Národního fondu	9 786	9 786	4 766,98	48,71
4135	Převody z RF	0	0	240,29	0,00
2141, 2211, 2212, 2322, 2324, 4132,	Ostatní nedaňové příjmy	0	0	4 574,12	0,00
	Investiční převody z Národního fondu	13 156	13 156	79 984,60	607,97
	PŘÍJMY CELKEM	22 942	22 942	89 566,00	390,40
Platy		42 409	42 500,36	42 500,36	100,0
5011	Platy zaměstnanců	34 244	34 335,36	34 335,36	100,00
5014	Platy zaměst. odvozov. od platů úst. činitelů	8 165	8 165,00	8 165,00	100,00
502	Ostatní platby za provedenou práci	4 608	4 608,00	1 791,65	38,88
5021	Ostatní osobní výdaje	4 308	4 308,00	1 735,00	40,27
5024	Odstupné	300	300,00	56,65	18,88
503	Povin. pojist. plac. zaměstnavatelem	15 875	15 906,06	15 624,06	98,23
5031	Povin. pojist. na sociál. zabezp.	11 672	11 694,84	11 487,84	98,23
5032	Povin. pojist. na veřej. zdr. pojišť.	4 203	4 211,22	4 136,22	98,22
513	Nákup materiálu	4 502	4 049,91	1 707,53	42,16
514	Úroky a ost. fin. výdaje	15	15,02	8,34	55,53
515	Nákup vody, paliv a energie	2 623	2 723,00	2 003,45	73,58
516	Nákup služeb	44 523	47 731,67	32 921,59	68,97
517	Ostatní nákupy	6 507	5 502,93	3 409,47	61,96

5171	Opravy a udržování	3 100	1 979,00	1 228,87	62,10
5173	Cestovné	2 200	2 316,93	1 698,80	73,32
519	Výdaje souvis. s neinv. nákupy	2 383	2 436,00	2 161,00	88,71
5342	Převody FKSP	424	424,76	424,76	100,00
536	Ost. neinv. transf. jin. veřej. rozp.	12	498,00	491,55	98,71
542	Náhrady plac. obyvatelstvu	300	300,00	102,98	34,33
5424	Náhrady v době nemoci	300	300,00	102,98	34,33
	Běžné výdaje celkem	124 181	126 695,72	103 146,73	81,41
611	Pořízení dlouh. nehmot. majetku	17 9778	72 538,54	56 982,04	78,55
612	Pořízení dlouh. hmot. majetku	4 060	43 599,00	43 426,93	99,61
	Kapitálové výdaje celkem	22 038	116 137,54	100 408,97	86,46
	VÝDAJE CELKEM	146 219	242 833,58	203 555,71	83,83

Číselné údaje jsou použity z výkazů zpracovaných ke dni 30. 12. 2012.

Přehled výdajů na projekty spolufinancované z rozpočtu EU v roce 2012

Název projektu	Schválený rozpočet 2012	Konečný rozpočet 2012	Skutečnost dle účetních výkazů k 31. 12. 2012	v tis. Kč
				Skutečnost/ konečný rozpočet v %
„Informační systém ORG v systému základních registruů – projekt IOP	21 120	120 652,06	100 131,25	82,99
„Optimalizace procesů Ú00Ú“	5 870,00	8 138,91	4 254,91	52,27
Leonardo da Vinci „Zvyšování povědomí o ochraně osobních údajů mezi zaměstnanci pracujícími v EU“		72,63	72,63	100,00
Technická pomoc „Makedonie“		167,66	167,66	100,00
Celkem za projekty spolufinancované z EU	26 990	129 031,26	104 626,45	81,08

Poskytování informací podle zákona č.106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Úřad v roce 2012 obdržel celkem dvaadvacet žádostí o poskytnutí informace podle zákona o svobodném přístupu k informacím. V porovnání s předešlým rokem se jedná o téměř dvojnásobný nárůst.

Z celkového počtu žádostí o informace Úřad v roce 2012 zcela vyhověl dvaceti devíti z nich, v deseti případech žádost o informace odmítl částečně a ve třech případech žádost odmítl zcela. Nejčastějším důvodem odmítnutí nebo částečného odmítnutí žádosti o informace byla ochrana osobních údajů. Úřad rovněž odmítl žádost o informace z důvodu ochrany obchodního tajemství třetích osob, z důvodu ochrany utajovaných informací a v jednom případě rovněž proto, že žadatel požadoval poskytnutí informací, jimiž Úřad nedisponuje a není povinen disponovat.

Rozhodnutí o částečném nebo úplném odmítnutí žádosti o informace byla celkem v osmi případech napadena rozkladem, přičemž odvolací orgán, předseda Úřadu, rozkladu vyhověl ve dvou případech. Postup Úřadu při vyřizování žádosti o informace byl ve dvou případech rovněž napaden stížností podle § 16a zákona o svobodném přístupu k informacím. Důvodem byla skutečnost, že žadatelé nebyly poskytnuty všechny jím požadované informace a že o těch, které mu poskytnuty nebyly, nebylo vydáno příslušné rozhodnutí o odmítnutí žádosti o informace. V jednom případě bylo pochybení napraveno prvoinstančním orgánem, který požadované informace poskytl v plném rozsahu postupem podle § 16a odst. 5 zákona, v druhém případě o stížnosti rozhodl předseda Úřadu, a to tak, že jí vyhověl a požadované informace sám poskytl.

Žadatelé nejčastěji požadovali informace týkající se výkonu dozorové činnosti Úřadu, například určité správní rozhodnutí či kontrolní závěr, nebo naopak rozhodnutí či vyjádření Úřadu týkající se určité oblasti zpracování osobních údajů. Další významnou část žádostí o informace pak tvořily žádosti týkající se hospodaření Úřadu.



Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2012

Úřad pro ochranu osobních údajů

Pplk. Sochora 27, 170 00 Praha 7

E-mail: posta@uouu.cz

Internetová adresa: www.uouu.cz

Na základě povinnosti, kterou mu ukládá zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, § 29 písm. d) a § 36, zveřejnil Úřad pro ochranu osobních údajů tuto výroční zprávu v únoru 2013 na svých webových stránkách.

Editor: PhDr. Hana Štěpánková, telefon 234 665 286

Redakční zpracování: PhDr. David Pavlát

Grafické řešení: Eva Lufferová

Jazyková korektura: Andrea Sklenářová a Mgr. Eva Strnadová

Tisk: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno

Pro Úřad pro ochranu osobních údajů vydalo Nakladatelství MU Brno, 2013

ISBN 978-80-210-6179-8