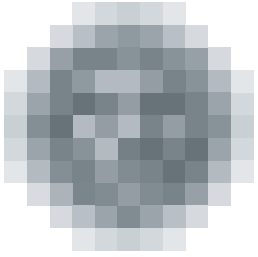
Výroční zpráva 2013



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-6700-4

Ohlédnutí předsedy Úřadu za rokem 2013

Úřad v průběhu roku konstatoval, že kromě přetrvávajících problémů s praxí odpovědných subjektů v oblasti ochrany osobních údajů v souvislosti se zpracováním velkého objemu dat, se některé skutečně staré, a zdálo se vyřešené, problémy vracejí. Poznatky ze zpracování velkého objemu dat přinesly provedené kontroly, které se odehrávaly v souladu s kontrolním plánem, stanoveným pro rok 2013. Z těch staronových problémů jsme se byli nuceni po mnoha letech opět vracet k nepochopitelným snahám pranýřovat dlužníky a vymknout se platnému právnímu řádu.

Při tomto poznání vkládám stále velkou naději v to, že přijímání nových zákonů bude obligatorně provázeno rozvahou o možných dopadech do soukromí a, jak jsem už uvedl v loňské výroční zprávě, předejde se tak situacím, kdy jsou možná úskalí ochrany osobních údajů odhalována až poté, co je právní norma přijata.

Nicméně také poznatky, které přináší nově vznikající judikatura, jsou velmi cenným vkladem pro uplatňování dozorové povinnosti Úřadu pro ochranu osobních údajů – a část výroční zprávy je jí právě proto explicitně věnována.

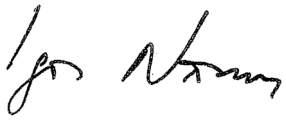
V roce 2013 Úřad plnil svou kompetenci z roku 2012, spojenou s tzv. „data breaches", tj. sledování a postih při narušení bezpečnosti elektronické komunikace; ač nabídl možnost komfortního postupu hlášení pro povinné subjekty – vytvořením elektronického formuláře, který umožňuje snadno podat povinné hlášení Úřadu, musím konstatovat, že tato agenda v práci Úřadu rozhodně nepatří k té nejbohatší.

V souvislosti s aférou sledování občanů Evropské unie a politiků evropských vlád americkou Národní bezpečnostní agenturou (NSA) Úřad plně spolupracuje v rámci evropské struktury s Evropskou komisí, stejně jako v případě zjištěného nedostatečného zabezpečení osobních údajů ve službách poskytovaných společností Google podpořil v rámci tzv. Working Party 29 vznik skupiny, která vedla vyšetřování, jež v několika státech již vyústilo v uložení vysokých sankcí.

Předpoklad, že vznik novelizované evropské právní normy upravující zpracování osobních údajů přinese projasnění v řadě složitých případů, které jsem právě uvedl, zatím uchováváme, přestože se ukazuje, že nové nařízení o ochraně osobních údajů v Evropské unii nevzniká snadno, stejně jako není ještě zdaleka ukončena práce na jeho harmonizaci s modernizovanou Úmluvou č. 108 Rady Evropy. Úřad se aktivně účastní na připomínkovém řízení ke vznikajícímu nařízení, jehož garantem za Českou republiku je Ministerstvo vnitra. Rok 2014 by měl být pro ochranu osobních údajů v Evropě skutečně přelomový: očekáváme totiž, že i připomínky k mechanismu Safe Harbour, regulující předávání osobních údajů mezi Evropou a USA, budou uzavřeny vypořádáním 13 požadavků, jež v zájmu zlepšení ochrany osobních údajů předložila USA evropská komisařka pro spravedlnost Redingová.

Jako v minulých letech jsme i v roce 2013 kladli důraz na vzdělávání mladé generace a diskusi s odbornou veřejností: kulaté stoly, které Úřad pořádal, jsou nadále dobře zavedenou konzultační formou (mezi jinými konzultačními povinnostmi Úřadu).

Ani v roce 2013 Úřad neopustil svou praxi v udržování čilých mezinárodních kontaktů, v jejichž rámci konzultoval problémy, nebo přímo spolupracoval (uvedu jako příklad jen program Leonardo, v jehož rámci spolupracujeme s polskými, chorvatskými a bulharskými kolegy). Je jen přirozené, že kromě každodenních povinností (vždyť jen podnětů za rok přijal Úřad 7428!) je Úřad zapojen do „mezinárodní sítě ochrany osobních údajů", protože jedině v jejím rámci se mohou odehrávat pozitivní posuny v ochraně osobních údajů, potažmo soukromí, potažmo svobodného rozhodování každého občana ve fungující demokracii.



Igor Němec

Obsah

Úřad v číslech 2013

Dotazy a konzultace	dotazy ČR	2994
	zahraničí	15
	konzultace	3013
	státní správě	126
	samosprávě	195
	právnickým osobám	532
	fyzickým osobám podnikajícím	298
	fyzickým osobám	1863
	z celkového počtu konzultací	
	osobní	235
	písemné	2778
Podání a stížnosti	přijaté podněty dle zákona č. 101/2000 Sb.	1336
	stížnosti předané ke kontrole nebo správnímu řízení	139
Nevyžádaná obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	7428
	vyřešených podnětů	5463
	zahájených kontrol	90
	ukončených kontrol	91
	správních rozhodnutí o pokutě	33
	napadeno námitkami	8
	námitkám vyhověno	1
	nevyhověno	5
	převážně vyhověno	0
	převážně nevyhověno	1
Kontroly (vyjma kontrol týkajících se zákona č. 480/2004 Sb.)	zahájeno	90
	ukončeno	74
	předáno jiným státním úřadům	0
	napadeno námitkami	15
	námitkám vyhověno	1
	nevyhověno	11
	převážně vyhověno	3
	převážně nevyhověno	4
	analýzy	11

Správní trestání	správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb.	101
	přestupková řízení podle zákona č. 101/2000 Sb.	18
	správní a přestupkové řízení podle zákona č. 101/2000 Sb. – § 44 a, 45 a	13
	přestupková řízení o porušení zákona č. 159/2006 Sb., o střetu zájmů	0
	rozklady napadená rozhodnutí o porušení zákona	32
	zamítnutých rozkladů	23
	zrušeno a vráceno k novému projednání	3
	zrušených rozhodnutí a zastaveno řízení	2
	změna rozhodnutí	3
Soudní přezkum (Pozn.: * celkem od r. 2001)	podaných žalob k soudu	18 (118*)
	zamítnutých žalob soudem	8
	zrušených rozhodnutí soudem	3
	ukončených/neukončených soudních řízení od roku 2001	74/44
Registrace	přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.)	6570
	zaregistrovaná zpracování	5994
	dosud v řízení	867
	zrušené registrace	97
	oznámení o změně zpracování	878
	řízení podle § 17	85
	zastaveno (nedochází k porušení zákona)	71
	zastaveno z procesních důvodů (např. oznámení vzato zpět)	19
	nepovoleno	7
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	25
	rozhodnutí o povolení předávání	20
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	4
Oznámení podle zákona č. 127/2005 Sb.	došlých oznámení	1
	vyřízených jako opodstatněné	0
	vyřízených jako neopodstatněné	1
Stížnosti podle § 175 správního řádu	přijatých stížností	40
	vyřízených jako důvodné	10
	vyřízených jako částečně důvodné	7
	vyřízených jako bezdůvodné	24

Žádosti podle zákona č. 106/1999 Sb.	přijatých žádostí	79
	zcela vyhověno	47
	částečně vyhověno	22
	odmítnutých žádostí	10
Publikované materiály	Věstník Úřadu (počet částek)	3
	Bulletin Úřadu (počet čísel)	1
Tiskové konference	pravidelné	2
	mimořádné	0
Připomínkované legislativní návrhy		
	zákony	69
	prováděcí předpisy	95
	návrhy nařízení vlády	17
	návrhy vyhlášek	78
	ostatní	60
	zahraniční materiály	25

Kontrolní činnost Úřadu

• KONTROLNÍ PLÁN PRO ROK 2013

Úřad pro ochranu osobních údajů (dále jen „Úřad") se v rámci svých kontrolních aktivit v roce 2013 zaměřil na ty oblasti, které se přímo nebo nepřímo dotýkají každého občana, klienta, zákazníka, účastníka právních vztahů, jejichž součástí je zpracování osobních údajů, a to včetně citlivých. Po zkušenostech z minulého období se inspektoři soustředili na několik vytipovaných oblastí, kde současně provedli své koordinované kontrolní aktivity, tak aby tyto kontroly měly co nejširší dopady jak vůči skupině odpovědných subjektů v postavení správce, případně zpracovatele, tak i z hlediska zájmů společnosti. Současně si však každý z inspektorů vytvořil prostor pro kontrolu zaměřenou dle oblasti, na níž se především specializuje nebo je odborně zaměřen. I když je zřejmé, že obecné povědomí společnosti o nutnosti chránit své osobní údaje před jejich nezákonným zpracováním již existuje, stále přetrvávají některé názory o zbytečnosti obav ze zneužití identity jednotlivce a s tím souvisejícího rizika škody ať majetkového nebo nemajetkového charakteru.

I. OBECNÁ TÉMATA PRO ZAMĚŘENÍ KONTROLNÍ ČINNOSTI INSPEKTORŮ ÚŘADU V ROCE 2013

1. INFORMAČNÍ SYSTÉMY S VELKÝM OBJEMEM DAT

Na rozdíl od minulých let, kdy se v kontrolním plánu oddělovaly kontrolní aktivity inspektorů směřující vůči informačním systémům ve veřejné správě a v oblasti soukromoprávní, jako hlavní obsah plánu roku 2013 byl sledován rozsah jednotlivých informačních systémů, a to jak co do objemu zpracovávaných dat ve vztahu k počtu subjektů údajů, tak i ve vztahu k počtu subjektů zapojených do celého procesu zpracování.

Ukazuje se totiž, že snahy o propojování systémů, původně vytvářených pro určité a předem určené účely, nekončí, a je proto nezbytné sledovat, jakým způsobem zpracování probíhá a jak jsou nastavena pravidla pro stanovení odpovědnosti jednotlivých subjektů.

Takové systémy jsou vytvářeny nejen v oblasti bankovnictví, pojišťovnictví, ale i v oblasti sociální, včetně poskytování sociální péče a služeb. Přitom rovněž rozvoj služeb, tzv. „osobní asistenční služby", kdy jsou propojována data vypovídající o zdravotním stavu klienta s daty o jeho dalších osobních potřebách, musí respektovat práva každého jedince být o rozsahu zpracování informován dříve, než k němu dochází.

S tímto problémem úzce souvisí stále pronikavější uplatňování technologií, kdy se stále zřetelněji prosazují výhradně elektronicky zpracovávané databáze, například pro vedení zdravotnické dokumentace v elektronické podobě (aktuálně podle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování).

V oblasti informačních systémů byly provedeny tyto kontroly:

a. Dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů (dále jen „zákon č. 101/2000 Sb.) se zaměřením na zpracování osobních údajů fyzických osob při **provozování pokladních a odbavovacích systémů provozovaných v lyžařských střediscích**.
   S ohledem na skutečnost, že v průběhu roku 2013 Úřad přijal několik podnětů směřujících na provozovatele lyžařských středisek, která využívají automatizované odbavovací systémy, uskutečnily se kontroly u tří konkrétních provozovatelů lyžařských areálů. Kontroly zpracování osobních údajů byly provedeny ještě v průběhu končící zimní sezóny v zájmu toho, aby jejich případná zjištění a výsledky mohly být zobecněny a aplikovány na veškeré automatizované odbavovací systémy. Podrobné informace o průběhu a výsledcích kontrol lze nalézt v samostatné kapitole. Z kontrolních závěrů inspektorů vyplynulo, že kontrolovaní správci odbavovacích systémů již nařízená opatření k nápravě realizovali a de facto budou již v zimní sezóně 2013/2014 zpracovávat osobní údaje v rozsahu nezbytném pro ochranu svých práv, aniž by současně docházelo k zásahu do soukromého a osobního života jejich zákazníků: Úřadu je známo, že i ostatní provozovatelé lyžařských areálů, u nichž neproběhla kontrola, upravili využívané odbavovací systémy podle pravidel tak, jak bylo Úřadem na základě poznatků z kontrolní činnosti požadováno.

b. Dodržování povinností správce při **zpracování osobních údajů zákazníků energetických obchodních společností** stanovených zákonem č. 101/2000 Sb., se zaměřením na plnění povinnosti správce s ohledem na ustanovení § 5 odst. 4 a § 11 zákona č. 101/2000 Sb. V souladu s kontrolním plánem probíhá kontrola zaměřená na vedení klientské databáze energetické obchodní společnosti. Jejím účelem je sledovat, jak jsou zpracovávány základní kategorie osobních údajů klientů společnosti v návaznosti na plnění smluvních závazků dodavatele energie. Kontrola dosud nebyla ukončena.

c. Dodržování povinností v souvislosti s **provozem nemocničního informačního systému** – ochrana soukromí pacientů, zabezpečení elektronické zdravotnické dokumentace.
   Byly zahájeny dvě kontroly, jejichž záměrem bylo prověřit výměnu informací o pacientech v rámci nemocničního informačního systému z hlediska přístupu oprávněných osob do tohoto systému. Součástí obou kontrol bylo také posouzení analýzy rizik zaměřené na zpřístupňování informací – citlivých osobních údajů v rámci vedení elektronické databáze pacientů využívajících zdravotnické služby kontrolovaného subjektu, a to i s ohledem na změnu

právní úpravy v oblasti vedení zdravotnické dokumentace dle zákona č. 372/2011 Sb., o zdravotních službách. Kontroly dosud probíhají.

d. **Zpracování osobních údajů zákazníků** podle zákona č. 101/2000 Sb., **v souvislosti s nabídkou bankovních služeb** (informovanost zákazníků, zabezpečení osobních údajů, rozsah informací poskytovaných klientům).
Na webových stránkách ČNB se mimo jiné uvádí, že „*bilanční suma bankovního sektoru ČR činila na konci října 4 916 mld. Kč. Dominantní položkou aktivní strany bilance jsou úvěry poskytnuté rezidentům. Objem vkladů rezidentů, jež tvoří nejvýznamnější položku pasiv bankovního sektoru, činil 3 398 mld. Kč.*" Z této zprávy ČNB je zřejmé, že bankovní sektor nezaostává a vyvíjí veškerou podnikatelskou snahu za účelem dosažení zisku, přičemž bez participace klientů je to téměř nemožné. Při uzavírání bankovních obchodů (smlouvy uzavírané bankami při jejich podnikatelské činnosti) je banka povinna postupovat obezřetně, s péčí řádného hospodáře. Podle § 37 odst. 2 zákona č. 21/1992 Sb., o bankách, jsou banky a pobočky zahraničních bank povinny pro účely bankovních obchodů zjišťovat a zpracovávat údaje o osobách, včetně rodného čísla (s výjimkou údajů citlivých). „Řadový spotřebitel", zájemce o produkt banky, který nutně potřebuje získat jistý finanční obnos, je tudíž při jednání s bankou v nerovném postavení; to potřebu kontroly zpracování osobních údajů bankou – zejména v souvislosti s rozsahem zpracovávaných osobních údajů, informovaností klienta a dalších povinností vyplývajících ze zákona č. 101/2000 Sb. – plně odůvodňuje. Dne 26. září 2013 byla dle zákona č. 101/2000 Sb. a zákona č 480/2004 Sb., o některých službách informační společnosti, zahájena kontrola Equa bank a.s., zaměřená na zpracovávání osobních údajů klientů banky využívajících její služby (produkty). Ukončení kontroly lze předpokládat v lednu 2014.

e. Zpracování osobních údajů oprávněných osob v souvislosti s poskytnutím **dávek pěstounské péče** (zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí).
Kontrola zpracování osobních údajů v souvislosti s poskytováním dávek pěstounské péče Úřadu práce ČR – krajskou pobočkou pro hlavní město Prahu, kontaktní pracoviště Praha 2 (dále jen „ÚP ČR") proběhla v březnu až srpnu 2013.
Účel zpracování osobních údajů prováděný uvedeným kontrolovaným subjektem je dán podmínkami pro vedení správního řízení o nároku žadatele na dávky státní sociální podpory podle zákona č. 117/1995 Sb., o státní sociální podpoře, a dále správním řízením o nároku žadatele na dávky pěstounské péče podle zákona č. 359/1999 Sb. Zmocnění pro kontrolovaný subjekt ke shromažďování osobních údajů vyplývá rovněž z uvedených zákonů.
Kontrolou ÚP ČR nebylo zjištěno porušení právních povinností vyplývajících z HLAVY II zákona č. 101/2000 Sb. při zpracování osobních údajů v souvislosti s poskytováním dávek pěstounské péče.

f. Kontrola zpracování osobních údajů zákazníků podle zákona č. 101/2000 Sb. v souvislosti s **nabídkou služeb fitness centra** (provoz kamerového systému, zákaznické karty) byla zaměřena na zpracování osobních údajů klientů (návštěvníků a členů) vyhledávajících služby fitness centra provozovaného společností Pure Health & Fitness, s.r.o. Kontrola byla provedena v době od dubna do září 2013, přičemž kontrolní zjištění byla natolik závažná, že se

promítla jak do kontrolních závěrů (došlo k porušení několika paragrafů zákona č. 101/2000 Sb.), tak do opatření k nápravě (uloženo 11 opatření, přičemž jedno opatření bylo po podaných námitkách rozhodnutím předsedy Úřadu zrušeno). Podstatný a nejzávažnější problém uvedeného fitness centra spočíval v nadbytečnosti shromažďovaných osobních údajů, což představuje do značné míry neoprávněné narušení soukromí klientů.

2. DALŠÍ POLOŽKY V KONTROLNÍM PLÁNU 2013

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

a) Zpracovávání osobních údajů účastníků rekvalifikace v rámci projektů a programů v oblasti státní politiky zaměstnanosti (zákon č. 435/2004 Sb., o zaměstnanosti).

b) Připravenost České republiky na proces migrace – na SIS II.

c) Kontrolu dodržování povinností odpovědných subjektů při sdělování výsledků trestního řízení živnostenským úřadům a nahlížení do trestního spisu (§ 6 odst. 4 zákona č. 455/1991 Sb., živnostenský zákon).

d) Dodržování povinností v režimu zákona č. 101/2000 Sb. při postupech týkajících se zpracování a zpřístupňování informací o žadatelích a příjemcích dotací v souvislosti s aplikací zákona č. 171/2012 Sb., kterým se mění zákon č. 218/2000 Sb., o rozpočtových pravidlech.

e) Podmínky pro zpracování osobních údajů zákazníků v oblasti nabídky zboží a služeb, a to nejen v rámci zákona č. 101/2000 Sb., ale současně i v další oblasti působnosti Úřadu, týkající se některých služeb informační společnosti ve smyslu zákona č. 480/2004 Sb., o některých službách informační společnosti.

f) Dodržování ochrany osobních údajů v procesu zpracování schengenské vízové agendy.

g) Zpracování osobních údajů odpovědným subjektem podle zákona č. 101/2000 Sb. v souvislosti s vyřizováním stížností.

Konkrétně proběhly následující kontroly:

1. Dodržování povinností podle zákona č. 101/2000 Sb. při zpracování a poskytování osobních údajů o žadatelích a příjemcích dotací v rámci **Státního zemědělského intervenčního fondu**.

Státní zemědělský intervenční fond (dále jen „SZIF") je státní instituce, která zprostředkovává českým zemědělcům finanční podporu z Evropské unie a národních zdrojů a zajišťuje následnou kontrolu oprávněnosti užívání dotací. Fond ročně spravuje finance v desítkách miliard korun, přičemž v rámci přidělovaných dotací zpracovává velké objemy dat. Vzhledem k tomu, že SZIF nebyl Úřadem doposud kontrolován, a vzhledem ke zvláštním právním předpisům a směrnicím EU upravujícím povinnosti při zpracování osobních údajů subjektů čerpajících uvedené dotace byla v době od března do října 2013 provedena kontrola zpracování osobních údajů v seznamech příjemců dotací z fondů EU (například Evropského zemědělského záručního fondu – EAGF, Evropského zemědělského fondu pro rozvoj venkova – EAFRD,

Evropského rybářského fondu – EFF) včetně vstupů a výstupů z registrů a evidencí užívaných SZIF, ze-jména Centrálního registru obyvatel. Z kontrolních poznatků vyplynulo, že v souvislosti s rozsudkem Evropského soudního dvora ze dne 9. listopadu 2010, ve věci námitky zveřejňování osobních údajů fyzických osob podnikajících v zemědělství podané dotčenými žalobci Volker und Markus Schecke GbR – C-92/09 a Hartmut Eifert – C-93/09 proti spolkové zemi Hesensko, došlo po konzultaci s evropským inspektorem ochrany osobních údajů ke změně Nařízení komise (ES) č. 259/2008 ze dne 18. března 2008, prováděcím nařízením (EU) č. 410/2011 ze dne 27. dubna 2011, kterým bylo zrušeno zveřejňování jména a příjmení, pokud jsou příjemci dotací fyzické osoby, podle článku 44a nařízení (ES). Ačkoli podle tvrzení SZIF došlo k zastavení zveřejňování osobních údajů fyzických osob v seznamu dotací zveřejněném na internetových stránkách, tak v tomto seznamu bylo možné nalézt údaje týkající se fyzických osob. Kontrolou byla v návaznosti na výše uvedené poznatky uložena jak odpovídající opatření k nápravě, tak i doporučení, kterými by se měl kontrolovaný řídit.

2. Dodržování povinností podle zákona č. 101/2000 Sb. při zpracování a poskytování osobních údajů o žadatelích a příjemcích dotací v rámci **Státního fondu rozvoje bydlení**.

Původní finanční zdroje pro státní podporu bytové politiky byly přidělovány z výtěžků privatizace státních podniků prostřednictvím dnes již zaniklého Fondu národního majetku. Nyní je dotačním garantem fondu bydlení jen Ministerstvo pro místní rozvoj. **Státní fond rozvoje bydlení** (dále jen „SFRB") je garantem plnění koncepce bytové politiky do roku 2020. Jeho cílem je podpora bydlení pro sociálně, zdravotně či jinak znevýhodněné občany. Kontrola byla zahájena v říjnu 2013, s tím že doposud nebyla ukončena a její ukončení se předpokládá v lednu 2014. Předmět kontroly byl vymezen v souvislosti s činností SFRB, jako dodržování povinností správce, případně zpracovatele, stanovených zákonem č. 101/2000 Sb. při zpracování osobních údajů subjektů údajů, tj. zejména osobních údajů žadatelů a příjemců finančních prostředků SFRB nebo zajištěných SFRB, především v souvislosti s jejich použitím: formou úvěru ke krytí částí nákladů spojených s modernizací bytu některými osobami mladšími 36 let (nařízení vlády č. 28/2006 Sb. – úvěr 150, nařízení vlády č. 97/2002 Sb. – úvěr 200, nařízení vlády č. 616/2004 Sb. – úvěr 300); k zajištění úhrady úvěrů formou ručení poskytnutého bance nebo pobočce zahraniční banky ke krytí nákladů spojených s výstavbou nebo s infrastrukturou obce pro výstavbu bytového domu, při kterém vznikne nájemní byt (nařízení vlády č. 370/2004 Sb.); formou dotace ke krytí části nákladů spojených s opravami panelového domu (nařízení vlády č. 63/2006 Sb.); formou dotace ke krytí části nákladů spojených s výstavbou sociálních bytů (nařízení vlády č. 333/2009 Sb.); formou úvěru na podporu výstavby nájemních bytů (nařízení vlády č. 284/2011 Sb.); formou úvěrů na opravy a modernizace domů (nařízení vlády č. 468/2012 Sb.); formou úvěru na úhradu části nákladů spojených s výstavbou bytu fyzickými osobami postiženými povodněmi (nařízení vlády č. 396/2002 Sb.). Kontrola dosud nebyla ukončena.

3. Zpracování osobních údajů odpovědným subjektem podle zákona č. 101/2000 Sb. v souvislosti s vyřizováním stížností v rámci působnosti **České lékařské komory**.

Realizovaná kontrola se zaměřila na ochranu osobních údajů a citlivých údajů stěžovatelů, pacientů a dalších fyzických osob, které jsou zpracovávány ve stížnostních spisech v rámci oprávnění České lékařské komory (dále jen „ČLK") řešit stížnosti na výkon povolání svých členů, včetně výkonu disciplinární pravomoci. Kontrola byla realizována ve dvou okresních sdruženích

ČLK. Dle zákona č. 220/1991 Sb., o České lékařské komoře, České stomatologické komoře a České lékárnické komoře jsou všichni členové těchto samosprávných organizací povinni poskytnout orgánům činným v disciplinárním řízení součinnost nezbytnou k prošetření každé stížnosti, zejména jsou povinni zapůjčit potřebnou zdravotnickou dokumentaci nebo její kopii. Tuto povinnost mají odborní zástupci nestátních zdravotnických zařízení a lékaři ve funkci vedoucích pracovníků ostatních zdravotnických zařízení, přičemž dle interního stavovského předpisu ČLK – disciplinární řád – má právo do disciplinárního spisu nahlížet lékař, proti kterému stížnost směřuje, popřípadě jeho právní zástupce, členové orgánů činných v disciplinárním řízení a pověření právníci ČLK.

V rámci kontroly byl prověřen systém nastavení předávání zdravotnické dokumentace mezi ústředím ČLK a okresním sdružením, systém předávání jednotlivým členům revizní komise, a to jak v listinné, tak i elektronické podobě. Kontrolován byl přijatý technicko-organizační systém uchovávání a zabezpečení osobních a citlivých údajů obsažených ve stížnostních spisech, a to včetně dodržování interních předpisů o spisové a archivační službě. Zkontrolovány byly technicko-organizační předpisy ČLK vztahující se k povinnosti mlčenlivosti členů a zaměstnanců ČLK, zkontrolovány byly předpisy ČLK upravující softwarovou a IT bezpečnost uchovávaných informací.

Kontrolou bylo konstatováno, že v obou kontrolovaných okresních sdruženích ČLK nebylo zjištěno porušení zákona č. 101/2000 Sb. v souvislosti s řešením stížností na výkon povolání svých členů. Více informací o průběhu kontroly lze nalézt v samostatné kapitole věnované kontrolní činnosti inspektorů.

4. **Zpracování osobních údajů účastníků rekvalifikace** v návaznosti na projekty a programy v oblasti státní politiky zaměstnanosti (zákon č. 435/2004 Sb., o zaměstnanosti).

Z kontrolního plánu Úřadu byla provedena kontrola dodržování povinností vyplývajících z ustanovení HLAVY II zákona č. 101/2000 Sb. při zpracování osobních údajů v souvislosti s rekvalifikací uchazečů o zaměstnání a zájemců o zaměstnání podle § 108 a násl. zákona č. 435/2004 Sb., **Úřadem práce České republiky – krajskou pobočkou v Příbrami** (dále jen „ÚP ČR"). Kontrola probíhala od února do června 2013.

Účel zpracování osobních údajů v průběhu rekvalifikace je stanoven zákonem č. 435/2004 Sb., výčet osobních údajů je v rozsahu uvedeném v tiskopisu „Žádost o zprostředkování zaměstnání" a „Žádost o podporu" včetně Základního poučení uchazeče. Data jsou získávána na základě vyplnění „Žádosti o zprostředkování zaměstnání" od samotného klienta a s jeho souhlasem. Data ÚP ČR může získávat též z úřední evidence České (okresní) správy sociálního zabezpečení. Souhlas je součástí „Žádosti o zprostředkování zaměstnání".

ÚP ČR zabezpečuje rekvalifikaci uchazečů a zájemců o zaměstnání a za tímto účelem uzavírá „Dohodu o rekvalifikaci" s rekvalifikačním střediskem. V souvislosti se zajištěním rekvalifikace dochází i k předání identifikačních údajů uchazečů a zájemců o zaměstnání. Předložené písemné dohody uzavírané podle § 108 odst. 7 zákona č. 435/2004 Sb. obsahují závazek rekvalifikačního střediska používat údaje o účastnících rekvalifikace poskytnuté ÚP ČR v souladu se zákonem č. 101/2000 Sb. (*Z tohoto pohledu bylo kontrolou doporučeno doplnit obecný odkaz na zákon č. 101/2000 Sb. v „Dohodě o rekvalifikaci" zárukami rekvalifikačního střediska o přijatém technickém a organizačním zabezpečení ochrany osobních údajů účastníků rekvalifikace podle § 6 zákona č. 101/2000 Sb.*)

Kontrolou ÚP ČR nebylo zjištěno porušení právních povinností vyplývajících z HLAVY II zákona č. 101/2000 Sb. v případě zpracování osobních údajů při realizaci programů rekvalifikací uchazečů o zaměstnání a zájemců o zaměstnání, podle § 108 a násl. zákona č. 435/2004 Sb.

5. Dodržování povinností odpovědného subjektu při zpracování osobních údajů **provozovatele internetového slevového portálu** www.skrz.cz.

Kontrola byla zahájena na základě podnětů doručených Úřadu, současně se záměr Úřadu prověřovat databáze uživatelů slevových portálů stal součástí kontrolního plánu. **Společnost Skrz.cz s.r.o.** působí jako jeden z větších agregátorů slevových portálů a disponuje tak poměrně rozsáhlou databází uživatelů. Záměrem kontroly bylo posouzení dodržování povinností vyplývajících jednak ze zákona č. 101/2000 Sb., a to zejména s ohledem na zabezpečení osobních údajů při zpracování osobních údajů zákazníků i dalších osob v souvislosti s obchodní činností kontrolovaného, a dále též dodržování povinností stanovených zákonem č. 480/2004 Sb., o některých službách informační společnosti týkajících se rozesílání obchodních sdělení pomocí elektronických prostředků. Kontrola doposud probíhá.

6. Dodržování ochrany osobních údajů v procesu zpracování schengenské vízové agendy konzulárním oddělením při českém zastupitelském úřadu. Byla provedena kontrola konzulárních oddělení při českých zastupitelských úřadech v Kyjevě, Rabatu a v Bělehradě. Kontroly, které byly realizovány na základě kontrolního plánu Úřadu, vycházely z doporučení expertní komise pro Schengenské hodnocení členských států na úseku ochrany osobních údajů.

Kontrola dodržování ochrany osobních údajů v procesu zpracování schengenské vízové agendy se zaměřením na dodržování předpisů v oblasti technicko-organizačních opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy byla realizována na **zastupitelském úřadu České republiky v Srbsku**. V rámci kontroly bylo prověřeno zabezpečení osobních údajů žadatelů jak o krátkodobá, tak i dlouhodobá víza, a to včetně využívaných elektronických databází a vnitřních kontrolních mechanismů. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb.

Provedení plánované kontroly **velvyslanectví České republiky v Kyjevě** bylo z důvodu zaneprázdněnosti zastupitelského úřadu v Kyjevě, a to s ohledem na plánovanou návštěvu prezidenta ČR, rozděleno do dvou částí. Kontrola byla zahájena, ale její provedení na místě bylo odloženo na II. čtvrtletí roku 2014.

Kontrola dodržování ochrany osobních údajů v procesu zpracování schengenské vízové agendy se zaměřením na dodržování předpisů v oblasti technicko-organizačních opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy byla realizována na **velvyslanectví České republiky v Maroku (Rabat)**. V rámci kontroly bylo prověřeno zabezpečení osobních údajů žadatelů jak o krátkodobá, tak i dlouhodobá víza, a to včetně Vízového informačního systému, který je používán pro prověřování biometrických údajů žadatelů o vízum. Kontrolou nebylo zjištěno porušení zákona č. 101/2000 Sb.

7. Kontrola připravenosti České republiky na **proces migrace na SIS II**.

Předmětem kontroly je zjistit a ověřit zajištění ochrany osobních údajů Policií České republiky jako správce osobních údajů zpracovávaných v národní součásti Schengenského informačního systému v souvislosti s přechodem ze Schengenského informačního systému (SIS 1+) na

Schengenský informační systém druhé generace (SIS II). Kontrola je zaměřena na postupy Policie ČR a pravidla při zpracování osobních údajů, dále na technické i fyzické zabezpečení ochrany dat v systému a opatření proti neoprávněnému zpracování osobních údajů, uchování a další zpracování osobních údajů v SIS 1+, včetně informací o přístupu k těmto údajům (logům), na zabezpečení osobních údajů ve fázi jejich převodu do databáze SIS II a na nastavení pravidel ochrany osobních údajů v SIS II. Předmětem kontroly je rovněž ověření zpracování osobních údajů konkrétní osoby. Kontrola dosud probíhá.

8. Dodržování povinností odpovědných subjektů při sdělování výsledků trestního řízení **živnostenským úřadům** a nahlížení do trestního spisu (§ 6 odst. 4 zákona č. 455/1991 Sb., živnostenský zákon).

Záměr k provedení šetření vznikl za situace, kdy Úřad obdržel několik stížností, které se týkaly zpracování osobních údajů bývalých živnostníků v živnostenském rejstříku i poté, kdy ukončili živnostenské podnikání. I vzhledem k nekonkrétnosti podmínek právní úpravy proto Úřad tuto věc raději řešil systémově jednáním s gesčním orgánem nežli kontrolou nebo jiným uplatněním dozorových kompetencí.

Pro naplnění tohoto záměru bylo na základě analýzy zahájeno jednání s Ministerstvem průmyslu a obchodu, jehož předmětem byla možnost změny právní úpravy rozsahu údajů, které jsou vedeny ve veřejné části živnostenského rejstříku, zejména se zaměřením na údaje o osobách, jejichž živnostenské oprávnění bylo ukončeno.

Zástupci MPO potvrdili možnosti novelizace živnostenského zákona, mj. i části týkající se živnostenského rejstříku. Nabízí se například možnost historii u bývalých podnikatelů uvádět jen po čtyři roky, tedy po dobu nutnou pro možné vypořádání právních nároků. MPO zvažuje i otázku nezbytnosti uvádění adresy bydliště, kdy se, vzhledem ke zpracování adresy místa podnikání, toto jeví jako nadbytečné. Pokud k takovémuto omezení přístupu dojde, bude však nutno upravit rozdílné režimy přístupu: veřejná část, neveřejná část, do které bude přístup například pouze po prokázání právního zájmu, a další neveřejná část (informace o správních deliktech a rodných číslech), kam lze mít i dle stávající právní úpravy přístup pouze na základě výslovného zákonného zmocnění.

II. KONTROLY Z KONTROLNÍHO PLÁNU 2012 DOKONČENÉ V ROCE 2013

1. V několika posledních letech roste zájem o nakupování prostřednictvím internetových obchodů, které lákají zákazníky nejen na výhodnější ceny, ale i na pohodlí, jež je s tímto nakupováním spojeno. Prodejce je oprávněn zpracovávat údaje nezbytně nutné jak pro plnění smlouvy, tak pro dodržení právní povinnosti vyplývající ze zvláštních zákonů (zákon o účetnictví). S tímto nákupem je v některých případech spojena registrační povinnost zákazníka v příslušném internetovém obchodě, přičemž nezbytnost rozsahu osobních údajů, shromažďovaných prostřednictvím registračního formuláře, není častokrát odůvodněna. I z tohoto důvodu byla v době od září 2012 do ledna 2013 provedena kontrola „internetového obchodu" provozovaného společností **Internet Mall, a.s.** Kontrola byla

zaměřena na zpracování osobních údajů zákazníků/klientů nakupujících přes internetové stránky www.mall.cz. Ve vztahu k povinnostem vztahujícím se ke zpracování osobních údajů zákazníků (souhlas, informační povinnost) nebylo porušení zákona č. 101/2000 Sb. zjištěno. Naopak bylo zjištěno porušení oznamovací povinnosti podle § 16 téhož zákona, kterého se kontrolovaný dopustil. Kontrolovaný ještě v průběhu kontroly své pochybení napravil.

2. V roce 2013 byla z kontrolního plánu 2012 ukončena také **kontrola Ministerstva dopravy**, provedená v době od září 2012 do února 2013, zaměřená na zpracování osobních údajů v souvislosti s vedením centrálního registru vozidel (dále jen „CRV"). I když nebylo v souvislosti s provedenou kontrolou zjištěno porušení zákona č. 101/2000 Sb. ani uložena opatření k nápravě, bylo Úřadem mimo jiné doporučeno navrhnout legislativní změnu zvláštního zákona (§ 5 zákona č. 56/2001 Sb., o podmínkách provozu vozidel na pozemních komunikacích) v působnosti Ministerstva dopravy stanovením jasného a nezpochybnitelného účelu existence CRV v souladu s ustanovením § 4 písm. j) ve spojení s § 5 odst. 1 písm. a) zákona č. 101/2000 Sb.

3. Další kontrola z kontrolního plánu 2012, která byla ukončena v roce 2013, byla **kontrola Ministerstva práce a sociálních věcí**, jakožto subjektu odpovědného za provoz Jednotného informačního systému práce a sociálních věcí. Kontrola byla zahájena v březnu 2012. Kontrola byla zaměřena na dodržování povinností stanovených zákonem č. 101/2000 Sb., zejména tedy na zabezpečení osobních údajů v Jednotném informačním systému práce a sociálních věcí. Více informací o průběhu kontroly lze nalézt v samostatné kapitole věnované kontrolní činnosti inspektorů.

4. Kontrola společnosti **CERD ČR, s.r.o.**, která byla rovněž zahájena již v roce 2012, byla vzhledem k velkému počtu stížností, které Úřad od nespokojených osob obdržel, přesunuta rovněž do roku 2013. Kontrola byla ukončena zjištěním, že kontrolovaný subjekt porušil své povinnosti při zpracování osobních údajů vyplývající ze zákona č. 101/2000 Sb. Více o průběhu a výsledcích kontroly lze nalézt v části věnované kontrolní činnosti inspektorů.

III. KONTROLY ZAHÁJENÉ V ROCE 2013 NA ZÁKLADĚ PODNĚTU PŘEDSEDY

1. V návaznosti na veřejně publikované informace a podnět doručený Úřadu dne 23. července 2013, týkající se přístupu do interního systému **Penzijní společnosti Komerční banky** prostřednictvím internetového bankovnictví Komerční banky a prezentace celého postupu prostřednictvím veřejně dostupného videozáznamu, vznikly důvodné obavy, zda postupem osob odpovědných za zpracování osobních údajů v souvislosti s provozem interního systému Penzijní společnosti Komerční banky nedošlo k porušení povinností správce, případně zpracovatele podle zákona č. 101/2000 Sb. Více informací o této kauze lze nalézt v části kontrolní činnost inspektorů.

• POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

V roce 2013 bylo inspektory Úřadu kromě kontrol z kontrolního plánu provedeno 74 incidenčních kontrol. Jako každý rok se mnoho stížností týkalo zpracování osobních údajů subjektů údajů prostřednictvím záznamů z kamerových systémů, zejména v bytových domech, provedena byla i kontrola kamerových systémů umístěných na pracovišti, dále zpracování osobních údajů zdravotní pojišťovnou v souvislosti se zákonnou možností přeregistrace k jiné zdravotní pojišťovně, kontrola zpracování osobních údajů v databázích dlužníků a zabezpečení informačních systémů. Rozsah oblastí incidenčních kontrol byl velmi široký a níže uvádíme alespoň výběr těch nejvýznamnějších, doplněný o závěry kontrol, které kontrolující inspektoři provedli na základě kontrolního plánu pro rok 2013.

Kromě incidenčních kontrol jsou součástí kontrolní činnosti inspektorů kontroly prováděné na základě kontrolního plánu nebo podnětů předsedy Úřadu. Výsledky těchto kontrol jsou uváděny v části kontrolní plán pro rok 2013.

ČESKÁ LÉKAŘSKÁ KOMORA

Na základě kontrolního plánu Úřadu pro rok 2013 zahájila inspektorka kontrolu České lékařské komory (dále jen „ČLK"), jejímž předmětem byla kontrola dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb., v souvislosti s řešením stížností na výkon povolání svých členů dle § 2 odst. 2 písm. e) zákona č. 220/1991 Sb., o České lékařské komoře, České stomatologické komoře a České lékárnické komoře, a to se zaměřením na činnost okresního sdružení (dále jen „OS") ČLK Děčín, rozšířenou o kontrolu činnosti OS ČLK Most.

Kontrolou bylo zjištěno, že ČLK jako správce osobních údajů pro účely vedení dokumentace ke stížnostem vede disciplinární spis, ve kterém shromažďuje a zpracovává osobní údaje v rozsahu stanoveném v § 6 odst. 2 Stavovského předpisu ČLK č. 4. Disciplinární spis obsahuje jednoznačnou identifikaci lékaře, proti kterému směřuje stížnost, s uvedením jeho titulu, jména, příjmení, data narození a adresy místa poskytování zdravotních služeb a veškeré dostupné identifikační informace o tom, kdo stížnost podal – zejména jeho jméno, příjmení, bydliště, případně jinou adresu pro doručování a další údaje, případně osobní údaje uvedené ve zdravotnické dokumentaci subjektu údajů, ke kterému se stížnost vztahuje.

Dále OS ČLK zpracovává osobní údaje prostřednictvím vedení spisů jednotlivých členů sdružení. Spisy obsahují dokumenty, které jsou podmínkou pro přijetí za člena ČLK (přihláška, vysokoškolský diplom apod.). Spisy členů sdružení jsou vedeny v listinné podobě, a to v rozsahu vyplývajícím z personální a mzdové agendy. Na základě výše uvedených údajů, které OS ČLK zpracovává, jsou subjekty údajů určitelné a lze je přímo identifikovat. ČLK shromažďuje a zpracovává osobní údaje lékařů, stěžovatelů a pacientů, k nimž se vztahuje stížnost, které jsou osobními údaji dle § 4 písm. a) zákona č. 101/2000 Sb. Dále zpracovává citlivé údaje subjektů údajů uvedené ve stížnosti, případně v kopii vyžádané zdravotnické dokumentace, nutné pro řešení problematiky související s výkonem povolání lékaře a poskytování zdravotní péče na území působnosti OS ČLK v souladu s ustanovením § 8 Stavovského předpisu č. 1 – Organizační řád.

Osobní údaje jsou zpracovávány prostřednictvím informačního systému ČLK a prostřednictvím listinné formy disciplinárního spisu, který zakládá sekretářka OS ČLK pro potřeby oprávněných členů revizní komise OS ČLK. V případě vydání rozhodnutí je toto předáno do informačního systému ČLK a dokumenty v listinné formě jsou skartovány. ČLK provádí operace, jimiž zpracovává osobní údaje dle § 4 písm. e) zákona č. 101/2000 Sb.

Archivace a skartace spisových dokumentů se řídí Stavovským předpisem č. 15 – Spisový řád. ČLK uchovává osobní (a citlivé) údaje lékařů – členů sdružení a stěžovatelů, případně pacientů, jichž se stížnost týká v souladu s ustanovením § 5 odst. 1 písm. e) zákona č. 101/2000 Sb.

Kontrolou nebylo prokázáno porušení ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. ČLK zpracovala a dokumentovala přijatá technicko-organizační opatření v souladu s ustanovením § 13 odst. 2 zákona č. 101/2000 Sb. a kontrolou nebylo prokázáno porušení ustanovení § 13 odst. 3 zákona č. 101/2000 Sb. ČLK pořizuje záznamy o všech přístupech a prováděných změnách. Kontrolou nebylo prokázáno porušení ustanovení § 13 odst. 4 zákona č. 101/2000 Sb.

KONTROLA SPOLEČNOSTI ZNANYLEKARZ SP. Z.O.O., PROVOZUJÍCÍ WEBOVÉ STRÁNKY WWW.ZNAMYLEKAR.CZ

Předmětem kontroly bylo dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb. se zaměřením na zpracování osobních údajů subjektů údajů zveřejňovaných na webových stránkách www.znamylekar.cz provozovaných společností ZnanyLekarz Sp.z.o.o. (dále jen „společnost“) se sídlem v Polské republice.

Společnost tím, že na území České republiky zpřístupňuje osobní údaje, které se týkají konkrétních osob vykonávajících svou činnost na území České republiky, zpracovává osobní údaje na území České republiky. Úřad pro ochranu osobních údajů České republiky je věcně a místně příslušný k výkonu dozoru nad zpracováním osobních údajů, ke kterému dochází na území České republiky. Na Úřad se začali obracet čeští lékaři a další zdravotničtí pracovníci (dále jen „zdravotničtí pracovníci“) s tím, že společnost zveřejňuje na webových stránkách www.znamylekar.cz jejich osobní údaje jak v „Základním profilu“ zdravotnického pracovníka, tak zejména v části „Názory a informace“ (diskusní fórum), a to bez jejich souhlasu. Dále uváděli, že Společnost na jejich výzvy k odstranění jejich osobních údajů nereaguje. Úřad na základě těchto stížností zahájil kontrolu společnosti.

V průběhu kontroly bylo zjištěno, že provozovatelem webových stránek, a tedy správcem osobních údajů zveřejňovaných na uvedených stránkách, je výše uvedená společnost a že servery, na nichž jsou data uložena, jsou umístěny ve Francii. Osobní údaje zdravotnických pracovníků může na webové stránky vložit jakýkoliv uživatel, který se u společnosti zaregistruje, stejně tak může vkládat příspěvky a hodnocení k práci konkrétního pracovníka v části „Názory a informace“ (diskusní fórum). Zaregistrovat se může u společnosti i zdravotnický pracovník, a tak vytvořit svůj ověřený profil. Bez provedení registrace je mu však znemožněno jakýmkoliv způsobem reagovat na příspěvky, které k jeho profilu vkládají ostatní uživatelé, ač to provozovatel stránek ve svých podmínkách garantuje.

Kontrolující inspektorka provedla právní posouzení zpracování osobních údajů zdravotnických pracovníků na webových stránkách www.znamylekar.cz, přičemž vycházela z dokumentů, které společnost sama zveřejňuje na svých webových stránkách, v nichž stanovuje pravidla pro zpracování osobních údajů.

Společnost zpracováním (zveřejněním) osobních údajů zdravotnických pracovníků v části „Základní profil" na www.znamylekar.cz neporušuje zákon č. 101/2000 Sb., neboť jejich osobní údaje mohou být zpracovávány (zveřejněny) bez jejich souhlasu na základě výjimky v ustanovení § 5 odst. 2 písm. d) zákona č. 101/2000 Sb., jelikož jejich osobní údaje získává společnost z veřejných zdrojů, tedy především z databáze lékařů zveřejněné na webových stránkách Ústavu zdravotnických informací a statistiky. Osobní údaje zdravotnických pracovníků, které jsou zveřejňovány v části „Názory a informace" (diskusní fórum), u nichž společnost nedisponuje platnou registrací, jsou údaje společností zveřejňovány bez jejich souhlasu, tedy v rozporu s ustanovením § 5 odst. 2 zákona č. 101/2000 Sb.

Dle zjištění kontrolující inspektorky ve čtyřech konkrétních případech zdravotničtí pracovníci provedli registraci u společnosti a na www.znamylekar.cz jsou zveřejňovány jejich osobní údaje v rámci tzv. „Ověřeného profilu". Tito zdravotničtí pracovníci tedy svou registrací poskytli společnosti souhlas se zpracováním svých osobních údajů na www.znamylekar.cz, tedy souhlasili s podmínkami uvedenými v dokumentech společnosti. Následně však všichni čtyři souhlas se zpracováním svých osobních údajů písemně odvolali a toto své rozhodnutí předali písemně společnosti a v souladu se společností uvedenými podmínkami žádali o odstranění záznamů z databáze. Deklarování nesouhlasu se zveřejněním svých osobních údajů, včetně žádosti o odstranění záznamů z databáze, je považováno za odvolání souhlasu se zpracováním osobních údajů a společnost ZnanyLekarz Sp. z.o.o. je povinna takové osobní údaje odstranit nejen v souladu se zákonem, ale i podle vlastních podmínek, které deklaruje.

Kontrolující inspektorka také konstatovala, že pokud se společnost jakožto poskytovatel elektronických služeb dozví o protiprávní povaze některé z uložených informací, je povinna tuto situaci řešit, a to neprodleně, jak vyplývá z § 5 odst. 1 písm. b) zákona č. 480/2004 Sb., o některých službách informační společnosti. Konkrétně musí učinit veškeré kroky k tomu, aby odstranila nebo znepřístupnila informaci protiprávní povahy. V každém případě, když je poskytovatel věrohodně na možný protiprávní charakter uložených informací upozorněn, je povinen tyto údaje alespoň znepřístupnit, tedy blokovat přístup k nim pro všechny uživatele a přezkoumat jejich obsah a námitky proti jejich zveřejnění. Jestliže námitky posoudí jako důvodné či prokazatelné, je povinen dané informace zlikvidovat. Jedinou výjimkou, kdy je provozovatel oprávněn předmětné informace uchovat, je ochrana práv provozovatele a jeho právem chráněných zájmů v navazujících řízeních, ovšem vždy musí zajistit, aby osobní údaje nebyly veřejně dosažitelné. Může se jednat například o uchování údajů pro potřeby orgánů činných v trestním řízení v případě podezření ze spáchání trestného činu, nebo o soudní spor v případě řízení o náhradě škody atd.

Pokud má zdravotnický pracovník zájem řešit věc soudní cestou i poté, co jsou jeho osobní údaje odstraněny, a tak mít možnost prokázat, že zveřejněné údaje, které vložil k jeho profilu jiný uživatel, byly nezákonné povahy a že jejich zveřejněním došlo k porušení osobnostních práv, je společnost povinna zajistit vedení přesných údajů registrovaných osob (uživatelů) tak, aby mu je pro uplatnění občansko-právní žaloby zdravotnickým pracovníkem na jeho žádost mohla předat.

Kontrolující inspektorka zároveň stanovila společnosti opatření k nápravě, a to nezpracovávat na webových stránkách www.znamylekar.cz osobní údaje zdravotnických pracovníků bez jejich souhlasu a zlikvidovat osobní údaje zdravotnických pracovníků zveřejněné na www.znamylekar.cz (tj. osobní údaje zdravotnických pracovníků, kteří podali k Úřadu v uvedené věci stížnost a jejichž údaje jsou uvedeny v kontrolním protokolu), s termínem ihned.

Společnost se ve svém písemném vyjádření, které Úřad obdržel, odvolala na jurisdikci polského Úřadu (dále jen „GIODO") s tím, že tento shledal, že databáze, které společnost spravuje, jsou hlášeny GIODO a kontrola, kterou GIODO provedl, prokázala, že údaje, jež společnost spravuje, jsou zpracovávány náležitě a v souladu s právem. Dle sdělení společnosti byly osobní údaje získány z internetu, kde jsou všeobecně dostupné. Dle názoru společnosti nelze sdělovací prostředek jako internet teritoriálně omezovat.

S ohledem na skutečnost, že Úřadu jsou svěřeny kompetence ústředního správního úřadu pro oblast ochrany osobních údajů v rozsahu stanoveném zákonem č. 101/2000 Sb. v České republice, Úřad nemá možnost uplatnit svoji pravomoc a vymoci opatření k nápravě u subjektu, který spadá pod jurisdikci Polské republiky, a tudíž kontrola mohla být prováděna jen v omezeném rozsahu.

Uvedený postup českého Úřadu, včetně zahájení kontroly společnosti, která má sídlo v zahraničí, ale jako správce osobních údajů provádí zpracování na území České republiky, je bezprecedentní. Právě z toho důvodu je cílem Úřadu takovou problematiku prezentovat a pokud možno vymoci ochranu osobních údajů subjektů údajů (v tomto případě českých lékařů), jejichž osobní údaje jsou na stránkách www.znamylekar.cz společností ZnanyLekarz Sp. z.o. o. v části „Názory a informace" (diskusní fórum) zpracovávány bez souhlasu, tedy v rozporu s českým zákonem. Diskuse evropských ochránců dat k tomuto konkrétnímu případu může napomoci řešit jeden z dosud otevřených problémů (tzv. „one-stop-shop"), diskutovaných v rámci přípravy evropského Nařízení, které nahradí v budoucnu směrnici 95/46/ES.

Výše uvedený postup Úřadu však ani v tuto chvíli nevylučuje, aby se čeští lékaři, jejichž údaje jsou na www.znamylekar.cz zpracovávány bez jejich souhlasu, obrátili na soud v České republice s občansko-právní žalobou na ochranu osobnosti a požadovali po společnosti nejen odstranění jejich osobních údajů z webových stránek, ale i odškodnění.

Úřad stále zastává názor zveřejněný již 15. července 2013 na www.uoou.cz v rubrice Dozorová činnost / Kontrolní činnost inspektorů: Problematika uplatnění práva na ochranu soukromého a rodinného života, v případě, že se provozovatel webového portálu odvolává na právo na svobodu slova a na právo na zveřejňování názoru třetích osob, a přitom se jak provozovatel, tak autor příspěvku schovává za anonymitu internetu, je sice komplikovaná, ale její řešení není nemožné.

KONTROLA ZDRAVOTNÍ POJIŠŤOVNY

Kontrola zdravotní pojišťovny (dále jen „ZP") byla zahájena na základě podnětu, který Úřadu zaslala Policie ČR, které stěžovatelka podala oznámení o přestupku na osobu, která je podezřelá z přestupku dle § 44 odst. 2 písm. e) zákona č. 101/2000 Sb. tím, že v listopadu 2011, jako zpracovatel při zpracování osobních údajů zpracovala osobní údaje bez souhlasu stěžovatelky a sepsala Přihlášku a evidenční list pojištěnce ZP, čímž stěžovatelku bez jejího vědomí přeregistrovala od Všeobecné zdravotní pojišťovny ČR k jiné zdravotní pojišťovně.

Kontrolující inspektorka tedy v červnu 2013 zahájila ve ZP kontrolu, jejímž předmětem byla kontrola dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb. se zaměřením na zpracování osobních údajů pojištěnců ZP v souvislosti s jejich registrací.

Z dokumentů, které Policie ČR zaslala Úřadu jako součást podnětu, vyplývalo, že stěžovatelka je pojištěncem ZP od 1. ledna 2012, její přihlášku ZP obdržela prostřednictvím společnosti, se kterou měla ZP uzavřenu Smlouvu o spolupráci při zprostředkování kontaktů zájemců o změnu

zdravotní pojišťovny. ZP Policii ČR sdělila, že změna zdravotní pojišťovny je považována za svobodnou vůli pojištěnce, kdy jeho vyjádřením je právě vyplnění a podpis Přihlášky a evidenčního listu pojištěnce, a z toho důvodu považuje ZP přihlášku stěžovatelky za doklad splňující podmínky § 11 zákona č. 48/1997 Sb., o veřejném zdravotním pojištění, a na jeho základě byla stěžovatelka zavedena do registru pojištěnců ZP.

Společnost, jež zajišťovala pro ZP přeregistraci klientů, Policii ČR sdělila, že přihlášku stěžovatelky zprostředkoval identifikovaný obchodní zástupce a byla mu ze strany společnosti za toto zprostředkování vyplacena řádná provize/odměna. V úředním záznamu o podání vysvětlení obchodní zástupce uvedl, že Přihlášku a evidenční list stěžovatelky nevypisoval. K této činnosti měl domluvenou další osobu, kterou identifikoval. Dále uvedl, že totožnost stěžovatelky nebyla při sepsání Přihlášky nejspíše nijak ověřena. K tomu osobě, která sepsala Přihlášku a evidenční list, stačila pouze kartička pojištěnce, nebo mohla údaje získat ústním sdělením, jelikož nešlo o žádnou smlouvu, ale pouze o přihlášku. Provizi za přihlášku dle svého sdělení výše jmenovaný obchodní zástupce nedostal, přihlášku převzal od uvedené osoby a po doplnění chybějících údajů ji předal příslušné regionální kanceláři.

Z policejního protokolu o výslechu osoby, která přihlášku vypisovala, vyplynulo, že v listopadu 2011 vypisovala přihlášky kromě stěžovatelky dalších asi pěti lidí. Údaje do přihlášek jí sdělila žena, která jí již dříve zprostředkovávala zájemce o přehlášení. Údaje jí nadiktovala a následně přihlášky odnesla do hotelového domu, aby je nechala podepsat. Totožnost ženy, která si nyní stěžuje, nijak neověřovala. Se sepsáním „fiktivních" přihlášek měla uvedená osoba problémy již v minulosti.

ZP v průběhu kontroly Úřadu sdělila skutečnosti, které již dříve sdělila Policii ČR a doplnila: *„Zaměstnanec ZP, pověřený evidencí Přihlášek pojištěnců, tento formulář řádně zadal dne 20. 12. 2011 do informačního systému ZP. Z předložené Přihlášky pojištěnce pak vyplývá, že pojištěná přešla k ZP od Všeobecné zdravotní pojišťovny. Pojištěná se tak stala pojištěncem ZP ke dni 1. 1. 2012 a v této souvislosti byla dne 22. 12. 2011 obeslána dopisem ZP s průkazem pojištěnce, a to na adresu, která byla ve formuláři Přihláška pojištěnce uvedena jako korespondenční."* V současné době dle sdělení ZP probíhá verifikace osobních údajů pojištěnce prostřednictvím napojení zdravotních pojišťoven na agendu základních registrů, a to prostřednictvím ověření údajů pojištěnce proti údajům evidovaným v Základním registru obyvatel. K napojení zdravotních pojišťoven do základních registrů došlo v průběhu roku 2012. Do té doby používala ZP jako základní možnost kontroly osobních údajů pojištěnce zpětné vazby formou zaslání informačního dopisu s průkazem pojištěnce.

ZP předložila Smlouvu o marketingové spolupráci uzavřenou se společností pro zprostředkování kontaktů zájemců o změnu zdravotní pojišťovny. Podle čl. III je předmětem Smlouvy závazek společnosti jako partnera ZP zajistit pro ZP marketingovou podporu a prezentaci ZP, představování produktů ZP, zodpovídání dotazů ke zdravotnímu pojištění a činnosti ZP, distribuce formulářů – způsoby přiblížení ke klientům a sběr, evidence a předání ZP kontaktních údajů zájemců o pojištění u ZP, a to na Sumáři evidenčních listů.

Dále ZP sdělila, že přihlášky pojištěnců do informačního systému zdravotní pojišťovny zpracovávají pouze zaměstnanci ZP, pro které je zaregistrování pojištěnců, vedení a aktualizace údajů o pojištěncích v registru a informačním systému zdravotní pojišťovny hlavní pracovní náplní. ZP nemá žádné zpracovatelské smlouvy se subjekty, které osobní údaje zpracovávají. Vyjma zaměstnaneckých smluv zaměstnanců ZP, které zakotvují povinnost mlčenlivosti o informacích

zjištěných v rámci vykonávání tohoto zaměstnání, a to nejen v průběhu zaměstnaneckého poměru, ale i po jeho ukončení. Kontrolovaná dále sdělila, že v okamžiku, kdy se dozvěděla o tom, že je Přihláška a evidenční list stěžovatelky fiktivní, projednala s ní vzniklou situaci a dohodla se s ní na jejím setrvání u ZP. ZP zároveň Úřadu v rámci kontroly předložila vnitřní předpisy související s ochranou osobních údajů.

Kontrolující inspektorka posoudila uvedené zpracování osobních údajů a konstatovala, že k neoprávněnému registrování stěžovatelky ke ZP, a tedy k neoprávněnému zpracování jejích osobních údajů ZP došlo. Dopis, který ZP spolu s Evropským průkazem zdravotního pojištění zasílá po přeregistraci klientům, se ZP v případě stěžovatelky vrátil jako nedoručený a ZP následně neprovedla žádné kroky, aby ověřila důvod vrácení poštovní zásilky, neověřila ani správnou identitu stěžovatelky. V registru pojištěnců ZP dále vedla její nepřesné osobní údaje, ač měla dostatek informací, že v daném případě mohlo dojít ke zneužití osobních údajů stěžovatelky při přeregistrování. Vzhledem k nečinnosti ZP lze konstatovat, že nepostupovala v souladu s třetí větou ustanovení § 5 odst. 1 písm. c) zákona č. 101/2000 Sb., kdy jako správce osobních údajů s ohledem na důvodné podezření na možné zneužití osobních údajů k přeregistraci nepřijala přiměřená opatření, zejména zpracování osobních údajů stěžovatelky neblokovala. V registru klientů pojišťovny ZP dále vedla nepřesné osobní údaje stěžovatelky a její přeregistraci považovala za platnou.

Z kontroly vyplynulo, že ZP neměla nastaveny takové mechanismy, které by v případě, že k přeregistraci pojištěnců nedochází prostřednictvím osobního kontaktu s pracovníkem na přepážce pobočky pojišťovny, a tudíž za dostatečného ověření identity žadatele o přeregistraci, indikovaly, že došlo k předložení „fiktivní" Přihlášky a evidenčního listu pojištěnce. ZP neměla vůči společnosti, se kterou měla uzavřenu zpracovatelskou smlouvu, nastaveny žádné kontrolní mechanismy tak, aby zajistila jako správce osobních údajů klientů (pojištěnců) a potencionálních klientů jejich shromažďování a zpracovávání v souladu se zákonem č. 101/2000 Sb. Povinnost registrovat pojištěnce ve smyslu zákona č. 48/1997 Sb., o veřejném zdravotním pojištění Úřad tímto nezpochybňuje, přesto však platí povinnosti správce osobních údajů, tedy ZP, vyplývající z ustanovení § 5 odst. 1 písm. c) zákona č. 101/2000 Sb., tj. zpracovávat přesné osobní údaje. ZP tím, že na základě „fiktivní" Přihlášky a evidenčního listu pojištěnce, která jí byla předložena spolu se Sumářem evidenčních listů externí společností, a tím, že zpracovávala nepřesné osobní údaje stěžovatelky v určitém vymezeném období, porušila povinnost správce osobních údajů § 5 odst. 1 písm. c) zákona č. 101/2000 Sb.

Dále kontrolující inspektorka konstatovala, že smlouva, kterou měla ZP uzavřenu se společností, jež pro ni zajišťovala přeregistraci klientů, obsahovala pouze prohlášení ZP o přenesení odpovědnosti na zpracovatele, ale neobsahovala žádnou záruku zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů. ZP tedy nesplnila povinnost správce osobních údajů stanovenou § 6 zákona č. 101/2000 Sb., neboť bez prověření, jaké má její zpracovatel přijaté technicko-organizační zabezpečení, v rozporu s povinnostmi uvedenými v zákoně, přenesla svoji odpovědnost na jinou osobu. Smyslem ustanovení § 6 zákona č. 101/2000 Sb. je, že správce se nemůže své odpovědnosti zajistit ochranu osobních údajů, které zpracovává, zbavit.

ZP na základě smlouvy, jejímž předmětem byla marketingová spolupráce, tj. spolupráce při zprostředkování kontaktů zájemců o změnu zdravotní pojišťovny, uskutečnila přeregistraci pojištěnců a v průběhu kontroly se pokusila přenést odpovědnost na svého smluvního partnera, přičemž bez prověření předložených návrhů zájemců o přeregistraci je automaticky

přeregistrovala do vlastního kmene pojištěnců. ZP po převzetí přihlášky, která je běžně využívána jako evidenční list pojištěnce, proplatila smluvní odměnu zprostředkovateli a provedla přeregistraci pojištěnce jak ve svém systému, tak v centrálním registru pojištěnců VZP ČR. V souladu s vnitřními předpisy byl novému pojištěnci vyhotoven nový průkaz evropského pojištěnce, který mu byl s průvodním dopisem zaslán. V rámci tohoto procesu ale pojišťovna neměla přijata opatření pro případ, že by odeslaný dopis s evropským průkazem nebyl doručen a byl ZP vrácen. Důsledkem popsaného systému zpracování přihlášek zájemců o přeregistraci byla nečinnost ZP, a v kontrolovaném případě tak proto zasáhla do práv stěžovatelky. Nastavený systém zpracování přihlášek zájemců o přeregistraci by ve své podstatě mohl být hodnocen jako automatizované zpracování osobních údajů, jehož výsledkem je vydání rozhodnutí o registraci bez ověření s důsledkem zásahu do práv a právem chráněných zájmů subjektu údajů.

V návaznosti na výše uváděné kontrolní zjištění kontrolující inspektorka v kontrolním protokolu uložila opatření k nápravě, která musí být přijata v termínu do dvou měsíců – tedy musí být nastavena taková technicko-organizační opatření, aby osobní údaje klientů byly vedeny v souladu s ustanovením § 5 odst. 1 písm. c) zákona č. 101/2000 Sb.

KAMEROVÉ SYSTÉMY NA PRACOVIŠTI

Předmětem kontroly, kterou kontrolující inspektorka zahájila v provozovně kontrolované společnosti (dále jen „kontrolovaný"), která se zabývá zámečnickými pracemi a nástrojařstvím, bylo dodržování povinností stanovených zákonem č. 101/2000 Sb. vztahujícími se na zpracování osobních údajů prostřednictvím kamerového systému se záznamem, provozovaného v provozovně kontrolovaného. „Zástupci" zaměstnanců kontrolovaného zaslali Úřadu podnět ke kontrole, ve kterém poukazovali na porušování soukromí zaměstnanců kontrolovaného užíváním kamerového systému instalovaného na pracovišti, dále uvedli, že umístění kamer a sledování zaměstnanců nemá za cíl vyšší bezpečnost na pracovištích, že záznamy jsou využívány výhradně k šikaně zaměstnanců (telefonáty „Kde jste teď byl?" – „Na WC" apod.) a k zastrašování jak stávajících, tak nově příchozích zaměstnanců. Současně iniciátoři podnětu upozornili, že pracoviště kontrolovaného nejsou zařazena do kategorie rizikových pracovišť. V této souvislosti odkázali na Listinu základních práv a svobod, zákon č. 101/2000 Sb., zákon č. 40/1964 Sb., občanský zákoník i § 316 odst. 2 zákona č. 262/2006 Sb., zákoník práce. Dále pak uvedli, že záběry z kamerového systému jsou sledovány vybranými osobami přímo ve firmě, ale i ze soukromých prostor. V průběhu kontroly bylo zjištěno, že předmětem činnosti kontrolovaného je výroba strojírenských výrobků, jejich dílů a příslušenství, opravy a údržba; konstruování výrobků, nářadí, racionalizační návrhy, práce a služby v oblasti kovovýroby, obchodní činnost v okruhu působnosti a zaměření firmy a nákladní silniční motorová doprava. Kontrolovaný zajišťuje vstup do areálu provozovny oprávněným osobám pouze prostřednictvím čipových karet, přičemž oprávnění ke vstupu do stavebně oddělených prostor je řešeno rozdílnými úrovněmi oprávnění. Vstoupit do areálu provozovny návštěvám je umožněno pouze v přítomnosti oprávněných vedoucích zaměstnanců. Kontrolovaný nemá zajištěn režim ochrany vstupu do areálu prostřednictvím fyzické ostrahy (vrátnice). Vstupní prostory jsou označeny informačními tabulkami obsahujícími informace o provozu kamerového systému. Stejné informační tabulky jsou umístěny v blízkosti každé instalované kamery.

Kontrolou bylo zjištěno, že se jedná o průmyslovou výrobu v areálu kontrolovaného, který je celý oplocen a skládá se z několika budov. Kontrolovaný zaměstnává přibližně 80 zaměstnanců,

kteří pracují převážně ve vlastní výrobě, a to v třísměnném (nepřetržitém) provozu. Předmětem činnosti kontrolovaného je strojírenská výroba převážně malosériového charakteru, což v praxi znamená, že určitý zaměstnanec nemusí nutně pracovat kontinuálně (i v rámci jedné směny) na jednom stroji, jeho pracoviště se může měnit v závislosti na technologických postupech při opracování určitého výrobku nebo na okamžitých výrobních požadavcích. Až na malé výjimky není výroba robotizována, takže zaměstnanci v rámci výrobního procesu pracují na několika strojích. Zaměstnanec kromě vlastní obsluhy stroje se může, resp. musí pohybovat v určeném okolí stroje, například od úložiště materiálu (polotovarů) k opracování až k úložišti opracovaných dílů. V případě zneužití strojů nebo ztráty materiálu uloženého v dílnách nelze tedy s ohledem na výše popsaný technologický postup určit konkrétního viníka.

Kontrolovaný rozhodl o instalaci a provozování kamerového systému na základě předchozích negativních zkušeností s krádežemi a neoprávněným používáním strojového zařízení ze strany zaměstnanců, neboť s ohledem na charakter provozu a výroby nelze zajistit ochranu zařízení, vybavení a materiálu jiným, levnějším a vhodnějším způsobem. Nejméně v jednom případě krádeže materiálu bylo podáno trestní oznámení Policii ČR. Rozhodnutí o instalaci kamerového systému bylo přijato po zjištění, že viníkem krádeže materiálu byl zaměstnanec kontrolovaného. Rozhodnutí o instalaci kamerového systému předcházelo odmítnutí návrhu vedení kontrolovaného vůči zaměstnancům na zavedení společné hmotné zodpovědnosti. Dle zástupců kontrolovaného se zaměstnanci většinově přiklonili k provozu kamerového systému. Zaměstnanci současně žádali zabezpečení parkoviště, na kterém mají zaparkována vozidla, po dobu pracovního procesu. Pozemek, na kterém je parkoviště umístěno, je ve vlastnictví kontrolovaného.

Důvodem, respektive účelem pro instalaci a následný provoz kamerového systému se záznamem je podle kontrolovaného ochrana majetku, ochrana před krádežemi, ochrana před zneužíváním technických zařízení a ochrana před neoprávněným jednáním zaměstnanců.

Zkušební provoz byl zahájen v březnu 2013, a to postupně, jak byly jednotlivé kamery (celkem 16) instalovány. O rozhodnutí instalace a provozu kamerového systému byli zaměstnanci informováni prostřednictvím svých vedoucích, dále prostřednictvím informačních tabulek a prostřednictvím Směrnice o provozu kamerového systému, která je vedoucím přístupna na intranetu kontrolovaného. Ovládání softwaru a přístup k pořízeným záznamům mají na základě přidělených přístupových oprávnění oba jednatelé kontrolovaného a dále správce systému na úrovni administrátora. Kamerový systém je instalován (provozován) v samostatné IT síti, včetně samostatných rozvodů. Přístup je však možný přes webové rozhraní i prostřednictvím informačního systému kontrolovaného, včetně dálkového přístupu.

Do systému je přístup umožněn na základě přístupového jména (přihlášení login) a hesla. Další podmínkou pro přihlášení je znalost IP adresy a vyhrazeného komunikačního portu. Přes webové rozhraní se ovládají funkce a nastavení videorekordéru včetně pořizování kopií (exportů) uložených záznamů. Od doby zahájení zkušebního provozu nebyla ani v jednom případě pořízena kopie záznamu, protože nedošlo k žádné krádeži ani k mimořádné události.

Kamerovým systémem jsou monitorovány např. docházkový terminál – kamera je umístěna nad vchodovými dveřmi spojovací chodby a zaznamenává průchod osob spojovacím prostorem, dvůr – kamera je umístěna v prvním patře a snímá vnitřní prostor mezi několika objekty areálu kontrolovaného a zaznamenává pohyb osob mezi objekty a zde parkující vozidla, dvůr za obrobnou – kamera je umístěna pod přístřeškem a sleduje prostor oploceného dvora (sklad materiálu) s výjezdem na státní komunikaci a manipulační prostor s přístupem do výrobny – obrobny, skladový

prostor s nakládkou a vykládkou materiálu a výrobků, prostor haly, v jejíž zadní části jsou lisy (nejedná se o detailní sledování konkrétního pracoviště), obrobna, parkoviště, které využívají zaměstnanci a návštěvy kontrolovaného a kam zajíždí autobus, který zde má zastávku.

Ke kameře označené jako docházkový terminál zástupce kontrolovaného sdělil, že namísto finančně náročné fyzické ochrany a kontroly docházky do zaměstnání zvolil kontrolovaný podstatně lacinější elektronickou kontrolu docházky. Z důvodu kontroly případného zneužití nepřenosnosti čipové karty (zapůjčení čipové karty neoprávněné osobě nebo umožnění průchodu neoprávněné osobě současně s oprávněnou osobou, což se v minulosti již stalo a v důsledku toho byly odcizeny kromě železného odpadu i již hotové výrobky, které byly ke škodě kontrolovaného následně odevzdány do sběrných surovin), jsou vstupy do areálu kontrolovaného monitorovány kamerovým systémem. V případě mimořádné události je pak záznam vyhodnocen a případně předán orgánům činným v trestním řízení.

Kamerový systém není provozován v režimu on-line. Přístup k záznamům z kamerového systému je omezen pouze na oprávněné osoby, záznamové zařízení i přístup k němu mají jen určení pracovníci (jednatelé kontrolovaného a IT specialista), přičemž každý přístup ke kamerovým záznamům je logován. Kamerový systém je provozován v samostatné IT síti, přístup oprávněným osobám je umožněn přes webové rozhraní prostřednictvím informačního systému kontrolovaného, a to včetně dálkového přístupu. Přístup k záznamům je zabezpečen heslem, loginem a znalostí IP adresy vyhrazeného komunikačního portu. Od uvedení kamerového systému do provozu nebyl nikomu zpřístupněn jakýkoliv záznam z kamerového systému, neboť již v areálu kontrolovaného nedošlo k žádné krádeži majetku ani mimořádné události. Z kontroly elektronických přístupů k pořízeným záznamům (logování) vyplývá, že od doby instalace kamerového systému do doby ústního jednání a místního šetření nedošlo ani k jednomu přístupu k pořízeným záznamům.

Na základě ustanovení § 29 odst. 1 písm. a) zákona č. 101/2000 Sb. *„provádí Úřad dozor nad dodržováním povinností stanovených tímto zákonem při zpracování osobních údajů"*, zákon č. 262/2006 Sb., zákoník práce ukládá ustanovením § 316 odst. 2 zaměstnavatelům povinnost: *„Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměst-navatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměst-navatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci."*

Tím, že kontrolovaný provádí primárně sledování jakožto prevenci zneužívání strojního a technického zařízení kontrolovaného a ochranu materiálu, a pořízené záznamy mají být využívány výhradně za účelem objasnění případného excesu, přičemž o provádění kontroly tímto způsobem zaměstnavatel své zaměstnance předem informuje, nedochází k narušování soukromí zaměstnance. Kontrolující inspektorka vyhodnotila, že uvedeným zpracováním nedochází k porušení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Dále bylo zjištěno, že kontrolovaný v souvislosti s provozem kamerového systému se záznamem porušil informační povinnost správce osobních údajů (dle § 11 odst. 1 zákona č. 101/2000 Sb.), neboť neinformoval subjekty údajů o jejich právu na přístup k vlastním osobním údajům, jakož i o dalších právech stanovených § 21 zákona č. 101/2000 Sb., ani že neinformuje třetí osoby prostřednictvím informačních tabulek neinformoval o tom, kdo je správcem osobních údajů.

Kontrolovanému byla v návaznosti na kontrolní zjištění uložena opatření k nápravě: splnit informační povinnost dle § 11 odst. 1 zákona č. 101/2000 Sb. a doplnit informaci o tom, kdo a za jakým účelem zpracovává osobní údaje prostřednictvím kamerového systému; doplnit také vnitřní předpisy – informovat o právu subjektu údajů na přístup k osobním údajům, o právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona č. 101/2000 Sb.

KAMEROVÝ SYSTÉM V MÍSTĚ BYDLIŠTĚ A PROVOZOVNĚ AUTOOPRAVNY

Kontrolující inspektorka zahájila na základě podnětu kontrolu dodržování povinností stanovených správci osobních údajů zákonem č. 101/2000 Sb. kontrolované společnosti (dále jen „kontrolovaný“) se zaměřením na zpracování osobních údajů prostřednictvím kamerového systému se záznamem, provozovaného na dvou místech: v prostorách bytového domu a v místě podnikání – autoservisu. Dle stěžovatele byl první kamerový systém instalován na adrese bydliště kontrolovaného a s jeho pomocí údajně sleduje vstup do restaurace, kterou provozuje bývalá manželka kontrolovaného. Důvodem instalace kamerového systému měla být ochrana soukromého majetku – vozidla kontrolovaného. Druhý kamerový systém byl dle stěžovatele instalován na plášti provozovny autoservisu. Stěžovatel v podání uvedl, že kontrolovaný pořízené záběry z kamerového systému ukazuje kamarádům a také kontroluje pohyb osob kolem uvedené restaurace.

V rámci analýzy podnětu byly osloveny orgány činné v trestním řízení a další orgány státní správy, zda jim nejsou známy nějaké okolnosti, za kterých byly použity či využity záznamy z kamerového systému provozovaného kontrolovaným. Došlo k prohlídce předmětných údajně sledovaných prostor s cílem ověřit, zda se na udávaných místech nacházejí kamery, které by mohly být součástí kamerového systému se záznamem.

Kontrolou bylo zjištěno, že na místech popsaných stěžovatelem se skutečně nacházejí kamery, které by mohly být součástí kamerového systému se záznamem.

K prvnímu kamerovému systému, který byl instalován v bydlišti kontrolovaného, s jehož pomocí údajně kontrolovaný sledoval vstup do restaurace, kterou provozovala jeho bývalá manželka, kontrolovaný sdělil, že nemovitost na uvedené adrese spoluvlastní a „*kamery má instalovány kolem oken svého bytu. Kamery nejsou zapojeny do záznamového zařízení a mají funkci pouze preventivní – odstrašující, a to ve vztahu právě ke stěžovateli. Bývalá žena kontrolovaného navázala se stěžovatelem bližší kontakt a kontrolovaný jej podezírá, že záměrně poškozuje jeho majetek a vozidlo, které parkuje před domem. Kamery také slouží k tomu, pokud by opět došlo k poškozování jeho vozidla, aby mohl bezprostředně reagovat a zavolat orgány činné v trestním řízení.*“ Z výše uvedeného tvrzení, které kontrolovaný uvedl mimo jiné i při místním šetření, vyplývalo, že kamerový systém v místě jeho bydliště není provozován se záznamem, a nejsou proto zpracovávány osobní údaje ve smyslu zákona č. 101/2000 Sb. Z uvedeného důvodu jeho šetření nepříslušelo věcně Úřadu.

K druhému kamerovému systému, který byl umístěn v provozovně autoservisu, právní zástupce kontrolovaného sdělil, že kontrolovaný podniká na základě živnostenského zákona a dále že „*se jedná o autoopravnu a na svůj objekt, který patří do jeho vlastnictví, umístil 4 kamery, které snímají prostor, respektive pozemky, které jsou spojeny s tímto servisem a jež patří do vlastnictví mého mandanta, a jiný prostor nesnímají. Systém je založen na pohybových čidlech a opět z důvodů zcela stejných, kdy došlo zejména v době, kdy se rozváděl se svojí*

manželkou, k vykrádání tohoto servisu, tak si umístil tyto kamery, aby zejména v době, kdy není přítomen, měl možnost orgánům činným v trestním řízení pomoci odhalovat trestnou činnost."

Kontrolující inspektorka místním šetřením zjistila, že se v provozovně autoservisu nachází celkem osm kamer, v době šetření bylo sedm kamer funkčních. Kamerový systém byl provozován v nepřetržitém provozu, vlastní záznam byl aktivován při detekci pohybu v zorném poli kamery, kamery snímaly barevný obraz a měly infračervené přisvícení pro noční vidění. Digitální videorekordér uchovával záznamy 14 dní a pak byly automaticky přepsány novým záznamem. Záznamové zařízení bylo uloženo v otevřené skříni umístěné v samostatné kanceláři kontrolovaného. Záznamové zařízení bylo propojeno na monitor, který v běžném režimu on-line zobrazoval aktuální pohled kamer. Do samotné kanceláře měl přístup jen kontrolovaný, ostatní osoby pouze s jeho doprovodem (např. syn kontrolovaného, který mu občas pomáhal s opravami vozidel). Přístup k záznamům v záznamovém zařízení byl umožněn na základě přístupového jména a přístupového hesla, které určil a znal pouze kontrolovaný.

Žádné směrnice či podobné písemnosti k provozování a zabezpečení kamerového systému kontrolovaný nevypracoval, neboť nikdo jiný než on sám neměl k zařízení přístup. Zařízení si kontrolovaný instaloval a zprovoznil sám, až do doby kontroly nevyužil žádných služeb externí společnosti k údržbě či opravě kamerového systému. Na oknech provozovny, směřujících k silnici a mimo přístupovou cestu do provozovny, byla umístěna nálepka s textem „Objekt je monitorován kamerovým systémem" s piktogramem kamery. Kontrolovaný jinou informaci o zpracování osobních údajů prostřednictvím kamerového systému neposkytoval. Kontrolovaný sdělil, že jej zatím nikdo nevyzval, aby mu ukázal jeho zpracovávané osobní údaje, popřípadě aby je vymazal. Kontrolovaný v průběhu kontroly přislíbil, že na informační nálepku doplní svůj kontakt. Důvodem instalace kamerového systému se záznamovým zařízením bylo několikeré vloupání do provozovny autoservisu a poškozování majetku, zejména vandalismem, z čehož kontrolovaný podezíral stěžovatele. Od instalace kamerového systému již k žádnému vandalismu nedošlo, a proto nikomu záznamy z kamerového systému nepředával. Náhledem záznamu z kamerového systému a při on-line přenosu během místního šetření kontrolující inspektorka zjistila, že kvalita obrazu je dostatečná k identifikaci snímaných osob.

Šetřením bylo dále zjištěno, že kontrolovaný nehovořil pravdu, když tvrdil, že přilehlé parkoviště, které sledovaly kamery č. 1 a č. 2, má ve svém pronájmu od obce. Kontrolující inspektorka zjistila, že jeho nájemní smlouva k parkovišti byla ukončena k datu 31. prosince 2011, a tedy dvě kamery kamerového systému sledovaly veřejné prostranství v majetku obce a dále i soukromý dům, jehož obyvatelé využívají stejné parkoviště jako zákazníci kontrolovaného. Kontrolovaný ve svém vyjádření před ukončením kontroly uvedl, že zjedná nápravu nedostatků zjištěných při místním šetření. Dosud nastavené uchování osobních údajů z kamerového systému po dobu třinácti dní bylo odbornou firmou přenastaveno tak, že záznam kamerového systému je nyní uchováván z vybraných kamer, ve smyslu ustanovení § 5 odst. 1 písm. e) zákona č. 101/2000 Sb., po dobu 24 hodin. Dále kontrolovaný změnil režim nastavení a snímání záznamu jednotlivých kamer v kamerovém systému. Kamery snímající veřejné prostranství – parkoviště – jsou provozovány pouze v režimu on-line, bez záznamu, tedy mimo režim zákona č. 101/2000 Sb. Kontrolovaný splnil informační povinnost tím, že informaci na okenních nálepkách doplnil ve smyslu ustanovení § 11 odst. 1 zákona č. 101/2000 Sb., který ukládá správci povinnost *„informovat subjekt údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být*

osobní údaje zpřístupněny, včetně informace pro subjekt údajů o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21 zákona č. 101/2000 Sb."

Kontrolující inspektorka v rámci právního hodnocení konstatovala, že i přes skutečnost, že parkoviště využívá značná část klientů kontrolovaného, který může argumentovat tím, že chrání majetek svých zákazníků, je nezbytné konstatovat, že uvedené parkoviště není vyhrazeno pouze pro činnost kontrolovaného. Kontrolovaný tím, že uchovává záznamy pořízené z celého prostoru parkoviště prostřednictvím kamerového systému, porušil povinnost správce osobních údajů zpracovávat osobní údaje pouze se souhlasem subjektu údajů podle § 5 odst. 2 zákona č. 101/2000 Sb. Před ukončením kontroly kontrolovaný zjednal nápravu. Kontrolující inspektorka kontrolovanému uložila ještě opatření k nápravě, a to doplnit registraci u Úřadu ve lhůtě sedmi dnů od nabytí právní moci kontrolního protokolu, neboť nezajistil nejméně od začátku května 2013 do místního šetření dne 6. srpna 2013 oznamovací povinnost vůči Úřadu, stanovenou ustanovením § 16 odst. 1 zákona č. 101/2000 Sb., čímž porušil ustanovení § 16 odst. 1 zákona č. 101/2000 Sb.

sKARTA (KARTA SOCIÁLNÍCH SYSTÉMŮ)

Dle kontrolního plánu Úřadu na rok 2012 byla v listopadu 2012 zahájena kontrola Ministerstva práce a sociálních věcí (dále jen „ministerstvo") jakožto správce Jednotného informačního systému práce a sociálních věcí (dále jen „JIS"), která byla ukončena v lednu 2013. Kontrola byla zaměřena na zpracování osobních údajů oprávněných osob a příjemců dávek v souvislosti s vydáváním karty sociálních systémů.

Úřad obdržel také několik podnětů, v nichž bylo vysloveno podezření z porušení zákona č. 101/2000 Sb., a to z důvodu neoprávněného předávání dat oprávněných osob a příjemců dávek České spořitelně, a.s. (dále jen „ČS, a.s.").

Při posuzování nezbytnosti předávání osobních údajů oprávněných osob a příjemců dávek ČS, a.s., bylo třeba vycházet z níže uvedené právní úpravy.

Ministerstvo je správcem JIS podle § 4a odst. 1 zákona č. 73/2011 Sb., o Úřadu práce, jehož součástí jsou veškeré údaje z informačních systémů o dávkách státní sociální podpory, sociálně-právní ochrany dětí, pomoci v hmotné nouzi, o příspěvku na péči, o dávkách pro osoby se zdravotním postižením a v oblasti státní politiky zaměstnanosti a je správcem osobních údajů i ve smyslu § 4 písm. j) zákona č. 101/2000 Sb. Ze zvláštního právního předpisu může správce JIS, tedy ministerstvo, pověřit správou evidence údajů o výplatách dávek pouze Českou správu sociálního zabezpečení (dále jen „ČSSZ").

Podle § 4b zákona č. 73/2011 Sb. náleží v rámci JIS oprávněným osobám a příjemcům dávek vedeným v tomto systému karta sociálních systémů. Karta sociálních systémů je veřejnou listinou a slouží k identifikaci osob uvedených v JIS pro účely informačních systémů o dávkách státní sociální podpory, sociálně-právní ochrany dětí, pomoci v hmotné nouzi, o příspěvku na péči, o dávkách pro osoby se zdravotním postižením a v oblasti státní politiky zaměstnanosti. Karta může mít dále funkce elektronicky čitelného identifikačního dokladu ve vztahu k JIS, průkazu osoby se zdravotním postižením a funkci platební podle zákona 329/2011 Sb., o poskytování dávek osobám se zdravotním postižením.

Kontrolou bylo zjištěno, že vydání sKarty probíhá v úzké součinnosti s ČS, a.s., a to na základě uzavřené smlouvy. Podle § 6 zákona č. 101/2000 Sb. „*pokud zmocnění nevyplývá z právního*

předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů."

Ministerstvo uzavřelo na základě uvedeného § 6 zákona č. 101/2000 Sb. smlouvu s ČS, a.s. jako zpracovatelem a předávalo jí na základě této smlouvy osobní údaje oprávněných osob a příjemců dávek. Předmětem smlouvy bylo stanoveno zajištění administrace výplaty nepojistných dávek a dávek z oblasti státní politiky zaměstnanosti a provozování karty sociálních systémů. Rozsah předávaných osobních údajů byl zcela identický s výčtem uváděným zákonem č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu. Tento zákon však určuje základní pravidla pro platební styk mezi bankovní institucí a klientem při smluvním soukromoprávním vztahu, který nevyplývá ze zákonné úpravy dávek uvedených v § 4a zákona č. 73/2011 Sb.

Podle čl. 2 odst. 3 ústavního zákona č. 1/1993 Sb., Ústavy České republiky „*státní moc slouží všem občanům a lze jí uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Každý může činit, co není zákonem zakázáno, a nikdo nesmí být nucen činit, co zákon neukládá.*" Podle čl. 3 Ústavy je součástí ústavního pořádku Listina základních práv a svobod.

Dle Ústavy a Listiny základních práv a svobod lze státní moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Zákon č. 73/2011 Sb. jako zvláštní právní předpis upravuje vydání sKarty jako veřejné listiny, identifikační funkci sKarty a stanoví další funkce sKarty, které může mít. Zvláštní právní předpis, v souvislosti s vydáváním sKarty, neupravuje zmocnění ministerstva k předání osobních údajů oprávněných osob a příjemců dávek ČS, a.s. k zajištění plnění povinností ČS, a.s. dle předmětu smlouvy. Takové zmocnění je upraveno v § 4a zákona č. 73/2011 Sb. v souvislosti s pověřením správou evidence údajů o výplatách dávek jen pro ČSSZ, nikoliv pro ČS, a.s. Ze smlouvy však jednoznačně vyplývá, že oprávněné osoby a příjemci dávek se musejí stát majiteli účtu (klienty) u ČS, a.s. Taková povinnost ve vztahu k ČS, a.s. pro oprávněné osoby a příjemce dávek nevyplývá ze zvláštního právního předpisu (zákona č. 73/2011 Sb. a zákonů upravujících způsob výplaty jednotlivých dávek uvedených v § 4a zákona č. 73/2011 Sb.) a ani oprávnění či povinnost ministerstva předávat osobní údaje těchto osob ČS, a.s.

Až ze smlouvy uzavřené mezi ministerstvem a ČS a.s. vyplývá povinnost ministerstva předávat osobní údaje oprávněných osob a příjemců dávek ČS, a.s. v souvislosti s předmětem smlouvy a při převzetí sKarty povinnost oprávněných osob a příjemců dávek uzavřít smluvní vztah s ČS, a.s. a souhlasit se Smluvními podmínkami za účelem otevření a vedení platebního účtu, na který je následně poukazována dávka. V důsledku tohoto postupu fakticky vzniká ČS, a.s. databáze osobních údajů držitelů sKaret a majitelů účtů oprávněných osob a příjemců dávek bez zákonného důvodu. Absence zákonného důvodu (zmocnění) k předání osobních údajů oprávněných osob a příjemců dávek při výkonu veřejné správy nemůže tak být zhojena Smlouvou o zpracování osobních údajů se zpracovatelem podle § 6 zákona č. 101/2000 Sb. Takovým zákonným důvodem pro předání osobních údajů nemůže být ani zákon č. 253/2008 Sb., neboť nezbytnost předání osobních údajů podle něj vyplývá až z předmětu samotné Smlouvy a právního vztahu mezi oprávněnými osobami a příjemci dávek a ČS, a.s., nikoliv ze zvláštních právních předpisů, které upravují vydávání karty a způsob výplaty dávek.

Podle § 13 odst. 1 zákona č. 101/2000 Sb. „*jsou správce a zpracovatel povinni 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. Tato povinnost platí i po ukončení zpracování osobních údajů."

Jelikož ministerstvo nebylo zvláštním zákonem zmocněno k předání osobních údajů oprávněných osob a příjemců dávek ČS, a.s. v souvislosti s sKartou sociálních systémů (§ 4a a 4b zákona č. 73/2011 Sb.), docházelo k předávání osobních údajů ČS, a.s. jako neoprávněné osobě bez právního důvodu. Tím ministerstvo porušilo svou povinnost při zabezpečení osobních údajů dle § 13 odst. 1 zákona č. 101/2000 Sb., tedy zabránit, aby nedošlo k neoprávněnému přístupu k osobním údajům.

Kontrolující inspektorka uložila ministerstvu, aby odstranilo závadný stav ve stanovené lhůtě.

KONTROLA DODRŽOVÁNÍ POVINNOSTÍ PŘI ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ V JEDNOTNÉM INFORMAČNÍM SYSTÉMU PRÁCE A SOCIÁLNÍCH VĚCÍ

Problémy, které vznikly kolem vyplácení nepojistných sociálních dávek v lednu 2012 v souvislosti s přechodem na nové agendové systémy, vyvolaly značný mediální ohlas, k němuž výrazně přispělo i prohlášení informatiků Úřadů práce, v němž vyjádřili, mimo jiné, pochyby o zabezpečení dat. Databáze Ministerstva práce a sociálních věcí (dále jen „ministerstvo") spravují ekonomická, zdravotnická a sociální data více než poloviny české populace. Z pohledu zákona č. 101/2000 Sb. jde převážně o citlivá data. Vzápětí po zveřejnění zmíněného prohlášení obdržel Úřad sedm podnětů od fyzických i právnických osob, na jejichž základě zahájil v březnu 2012 kontrolu u správce osobních údajů, jímž je ministerstvo.

Při úvodním jednání byl na ministerstvu předán kontrolní dotazník, jehož součástí byly otázky týkající se opatření přijatých k zabezpečení ochrany osobních údajů podle § 6 zákona č. 101/2000 Sb., tj. smluvní zajištění vztahu mezi správcem a zpracovatelem, dále § 13, zejména v oblasti automatizovaného zpracování osobních údajů a § 14 a § 15 téhož zákona, které se týkají povinností zaměstnanců správce nebo zpracovatele při ochraně osobních údajů.

V průběhu kontroly byla osobou poskytující součinnost předána kontrolujícímu inspektorovi kopie e-mailového pokynu z ledna 2012, v němž byli zaměstnanci informováni, že *„nemají-li přiřazenou roli, mohou bez problému pracovat na principu tzv. zdvojené či násobené identity, tj. na jedno ‚jméno a heslo' se může přihlásit více osob*." Uvedený e-mail je podepsán statutárními zástupci správce (náměstek ministra) a zpracovatele (náměstek Generálního ředitelství Úřadu práce). Že se takto mohlo postupovat, potvrzuje rovněž dopis náměstka ministryně práce a sociálních věcí datovaný v prosinci 2012: *„Kontrolovaný subjekt nepopírá tu skutečnost, že pod jednou identitou mohly do systému vstupovat dvě osoby."*

Je nutno konstatovat, že uvedené opatření odporuje mimo jiné i internímu předpisu ministerstva, konkrétně Příkazu ministra č. 28/2007, kde v příloze 1 (Provozní řád informačního systému úřadu MPSV) je v odst. 11 explicitně stanoveno *„Sdílení přístupových účtů několika zaměstnanci je zakázáno*." Rozhodně však odporuje znění zákona č. 101/2000 Sb., který v ustanovení § 13 odst. 4 stanoví, že *„v oblasti automatizovaného zpracování osobních údajů je správce nebo zpracovatel v rámci opatření podle odstavce 1 povinen také* a) *zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby*, b) *zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob,*

a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, c) *pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány, a* d) *zabránit neoprávněnému přístupu k datovým nosičům.*"

Problémem celého jednotného informačního systému (JIS) bylo, že fungoval od začátku bez logování přístupu oprávněných osob. V období leden až únor 2012, tj. v počáteční fázi, fungoval dokonce i bez individuálních přístupových oprávnění zaměstnanců. Avšak i poté, co byli všichni zaměstnanci vybaveni osobními přístupovými kartami, bylo možno zjistit pouze to, že někdo údaje obsažené v aplikaci zpracovával. Nebylo možno zjistit, zda došlo k neoprávněnému nahlížení či stahování osobních údajů mimo aplikace.

Po ukončení kontroly byla v návaznosti na kontrolní zjištění ministerstva, jako správci osobních údajů, uložena dvě nápravná opatření, a to s okamžitou platností zrušit e-mailový pokyn vybízející zaměstnance k používání sdílené identity a zajistit u dodavatele aplikací zavedení logování všech přístupů do JIS.

SYSTÉM EURODAC (ELEKTRONICKÁ DATABÁZE OTISKŮ PRSTŮ ŽADATELŮ O AZYL)

V listopadu 2012 byla zahájena kontrola systému Evropské unie EURODAC. Jedná se o elektronickou databázi otisků prstů žadatelů o azyl v některém ze členských států Evropské unie. Správcem tohoto systému v České republice je ministerstvo vnitra (dále jen „ministerstvo"), resp. Odbor azylové a migrační politiky ministerstva. Provedení kontroly vycházelo z kontrolního plánu Úřadu na rok 2013 a bylo realizováno na základě doporučení expertní komise pro schengenské hodnocení členských států v oblasti ochrany osobních údajů.

Kontrola se zaměřila především na zjištění, jakým způsobem, a zda vůbec, správce systému dohlíží na aktualizaci a přesnost zpracovávaných osobních a citlivých údajů ve smyslu § 5 odst. 1 písm. c) zákona č. 101/2000 Sb. a dále na kontrolu bezpečnostních opatření a ochranu osobních údajů ve smyslu § 13 téhož zákona.

Cizinci, který projeví zájem o mezinárodní ochranu, jsou odebrány otisky prstů k prověření v tzv. Dublinském systému. Dublinský systém má za cíl eliminovat jev nazývaný „asylum shopping", tedy předcházet situacím, kdy cizinci podávají současně či postupně v několika členských státech EU žádost o azyl a tyto státy současně či postupně vedou řízení o udělení azylu a rozhodují ve věci této žádosti. Smyslem systému je tedy určit bezprostředně po podání žádosti o azyl pouze jeden členský stát, který bude podanou žádost posuzovat a ve věci rozhodne.

Odběrová místa otisků prstů s přímým vstupem do systému EURODAC jsou v České republice pouze tři: středisko pro azylanty v Zastávce u Brna, zařízení pro zajištění cizinců Jezová- Bělá a Letiště Václava Havla v Praze. Otisky jsou vloženy do EURODACu a zároveň jsou elektronicky přeposlány na Dublinské středisko na Ministerstvu vnitra. Zde jsou na speciálním počítači převedeny do centrálního systému EURODAC, aby byla zjištěna případná shoda (tzv. „HIT"), podezření, že cizinec požádal o azyl v jiném státě EU. V případě tohoto podezření se otisky přepošlou elektronicky do Kriminalistického ústavu Policie ČR se všemi otisky, které jsou podezřelé ze shody, a experti otisky porovnají a označí ten, který je s vloženým otiskem shodný. Dále následuje korespondence mezi zainteresovanými členskými státy EU, která vyústí v deportaci cizince do země, ve které požádal již dříve o azyl. Do systému EURODAC se vkládají otisky prstů žadatelů o azyl starších 14 let, které jsou v systému uchovávány po dobu

deseti let; pouze v případě, kdy cizinec získá státní příslušnost daného státu, by jeho otisky prstů měly být ze systému vymazány. Cizinec je před daktyloskopováním písemně poučen, že má právo na výmaz těch údajů o jeho osobě, které byly do systému EURODAC zaslány neoprávněně, dále je informován, že se může také obrátit se žádostí o výmaz či opravu nesprávných údajů přímo na Úřad. Kontrolou deseti náhodně vybraných záznamů dle evidenčních čísel si kontrolující inspektorka ověřila oprávněnost uchování všech kontrolovaných údajů v systému EURODAC. Dále jsou vkládány do systému EURODAC otisky prstů každého cizince staršího 14 let zadrženého v souvislosti s neoprávněným překročením hranice, což ovšem nastává v ČR pouze na letišti – jiné hranice se zeměmi, které nejsou v Evropské unii, ČR nemá.

Kontrolující inspektorka kontrolou nezjistila porušení zákona č. 101/2000 Sb. ministerstvu však bylo ve vztahu k výše citovanému zákonu doporučeno v případě, že cizinec získá české občanství, spolupracovat s odborem všeobecné správy ministerstva, oddělením státního občanství a matrik. Toto oddělení přímo uděluje české občanství, tedy tato informace se může bezodkladně doručit na odbor azylové a migrační politiky ministerstva, který následně uloží Kriminalistickému ústavu Policie ČR vymazání údajů držitele českého občanství ze systému EURODAC. V případě, že žadatel získá občanství jiného členského státu EU, doporučuje inspektorka vyvinout mezinárodní iniciativu pro výměnu těchto informací, které jsou nezbytné pro uchování přesných a úplných informací v systému EURODAC. V závěru kontrolního protokolu inspektorka ministerstvu doporučila, aby ve spolupráci s Policejním prezídiem ČR přijalo takový systém vnitřní kontroly oprávněnosti přístupů do EURODACu, aby byly dodrženy podmínky § 13 zákona č. 101/2000 Sb. (logování).

PROVOZOVÁNÍ POKLADNÍCH A ODBAVOVACÍCH SYSTÉMŮ V LYŽAŘSKÝCH STŘEDISCÍCH

V rámci kontrolního plánu Úřadu na rok 2013 proběhla kontrola ve třech zimních lyžařských střediscích, v nichž při odbavování lyžařů používají fotografickou techniku, která zachycuje konkrétního lyžaře při průchodu turniketem.

Kontrolou bylo zjištěno, že kontrolované společnosti provozují kontrolní systém, který se skládá z turniketů vybavených fotografickým přístrojem, laserovým čidlem pro kontrolu výšky a PC jednotky s monitorem. Jako účel provozu uvedeného systému společnosti uvádějí ochranu před neoprávněným užíváním jízdenek (skipasů), zejména sezónních, protože je využívají osoby odlišné od oprávněného držitele jízdenky, čímž provozovatelům vznikají značné finanční škody. Prostřednictvím kontrolního systému jsou kontrolovány dětské jízdenky, a to bez dalšího zpracování osobních údajů, sezónní jízdenky vydané na konkrétního držitele, a to za využití zpracování osobních údajů, a ostatní jízdenky bez zpracování osobních údajů. Při nákupu sezónní jízdenky jsou od kupujícího shromažďovány osobní údaje v rozsahu: sken fotografie, jméno a příjmení. Údaje se ukládají v rámci softwarové aplikace v databázi, kterou spravuje kontrolovaná společnost, s rozlišením podle typu a čísla jízdenky.

Při průchodu turniketem je pořízena fotografie držitele sezónní jízdenky, která je automaticky přiřazena v databázi ke konkrétní jízdence, a to včetně informace o datu a hodině odbavení. V databázi jsou shromažďovány fotografie, včetně data a hodiny odbavení, a to po celou dobu platnosti sezónní jízdenky. Odbavovací systém dále využívá automatickou kontrolu výšky odbavované osoby s informací, zda je využívána dětská jízdenka. V tomto případě je porovnávána pouze informace o typu jízdenky s výškou odbavované osoby v aktuálním čase. Informace

uložené v databázi systému jsou ukládány po celou dobu sezóny. Po jejím ukončení jsou všechny informace ručně smazány – likvidovány.

Společnosti zpracovávají osobní údaje svých klientů v rozsahu jméno, příjmení a fotografie držitelů sezónních jízdenek po dobu platnosti jízdenek, maximálně do konce lyžařské sezóny (cca 4 až 5 měsíců). Důvodem uvedené délky zpracování osobních údajů jsou reklamace klientů, stížnosti klientů a možnost zneužití jízdenek v průběhu sezóny neoprávněnou osobou. Kontrolní systém je technicky nastaven tak, že použití sezónní jízdenky neoprávněnou osobou lze zjistit zpětně.

Kontrolním závěrem bylo konstatováno, že doba zpracování fotografií držitelů jízdenek a dalších osobních údajů je přiměřená výše uvedeným důvodům. Společnosti proto neporušily § 5 odst. 1 písm. e) zákona č. 101/2000 Sb. Fotografie držitelů jízdenek a další související osobní údaje jsou společnostmi likvidovány do konce lyžařské sezóny.

Dle § 5 odst. 2 zákona č. 101/2000 Sb. „*může správce zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu může zpracovávat osobní údaje pouze za předpokladu, že je splněna některá z výjimek tohoto ustanovení uvedených v § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb.*"

Dle výjimky uvedené v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. „*může správce zpracovávat osobní údaje bez souhlasu subjektu údajů, 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 fotografií držitelů sezónních jízdenek provádějí společnosti za účelem ochrany svého majetku, tedy za účelem ochrany svých práv a právem chráněných zájmů. Pomocí kontrolního systému společnosti sledují oprávněnost jednotlivých uživatelů jízdenek k využívání lyžařského areálu, jehož jsou společnosti provozovatelem. Zpracování fotografií a dalších osobních údajů uživatelů jízdenek nebylo shledáno takovým zásahem do práv subjektů údajů, aby byl narušen jejich soukromý a osobní život. Vzhledem k účelu shromažďování fotografií, kterým je ochrana majetku společností, spatřuje kontrolní orgán toto zpracování v daném případě jako proporcionální, s konstatováním, že zásah do soukromí dotčených osob je minimální.

Kontrolující inspektor tak celý případ uzavřel s tím, že kontrolované společnosti v souvislosti s pořizováním fotografií při prodeji jízdenek neporušují ustanovení § 5 odst. 2 zákona č. 101/2000 Sb., jelikož se na uvedené zpracování vztahuje výjimka uvedená v § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.

Kontrolou společností bylo však dále zjištěno, že společnosti porušují § 11 odst. 1 zákona č. 101/2000 Sb., který ukládá správci povinnost „*informovat subjekt údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, 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.*" Provedenou kontrolou bylo zjištěno, že klienti společností nejsou informováni ve smyslu § 11 odst. 1 zákona č. 101/2000 Sb. o tom, v jakém rozsahu a pro jaký účel jsou osobní údaje zpracovávány, kdo je správcem osobních údajů a také scházejí informace týkající se poučení subjektů údajů o jejich právech dle § 21 zákona č. 101/2000 Sb. v souvislosti se zpracováním jejich osobních údajů.

Podle § 16 odst. 1 zákona č. 101/2000 Sb. „*ten, kdo hodlá jako správce zpracovávat osobní údaje nebo měnit registrované zpracování podle tohoto zákona, s výjimkou zpracování uvedených*

v § 18, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováním osobních údajů." Kontrolou bylo zjištěno, že společnosti ke dni zahájení kontroly neoznámily Úřadu, že zpracovávají osobní údaje, a tím porušily výše uvedený paragraf. Tato dvě porušení zákona č. 101/2000 Sb. byla vyřešena uložením nápravných opatření kontrolovaným společnostem v jednotlivých kontrolních protokolech.

CENTRÁLNÍ REGISTR DLUŽNÍKŮ – CERD

V roce 2013 se Úřad zaměřil také na provozovatele databází dlužníků CERD. Důvodem bylo nejen množství stížností a podnětů, ale i zájem veřejnosti a médií.

V období od února 2012 do března 2013 byla na základě mnoha podnětů zaslaných Úřadu kontrolujícím inspektorem provedena kontrola dodržování povinností stanovených zákonem č. 101/2000 Sb. při zpracování osobních údajů subjektů údajů v souvislosti s poskytováním služeb nabízených na webových stránkách www.cerd.cz a www.centralniregistrdluzniku.cz ve společnosti CERD ČR, s.r.o. (dále jen „kontrolovaný").

Kontrolou bylo zjištěno, že kontrolovaný je pouze zpracovatelem – správce osobních údajů sídlí na území USA. Kontrolující inspektor konstatoval, že došlo k porušení povinností při zpracování osobních údajů vyplývajících z § 5 odst. 1 písm. d) a § 21 odst. 1 zákona č. 101/2000 Sb. V souladu s § 40 odst. 1 zákona č. 101/2000 Sb., po zvážení kontrolních zjištění, byla kontrolovanému subjektu uložena nápravná opatření, včetně povinnosti informovat Úřad o jejich splnění.

Současně kontrolní protokol obsahoval doporučení kontrolovanému, která by měla zlepšit srozumitelnost nabízených služeb a předejít případným dalším podnětům adresovaným Úřadu. Stížnosti se především týkají zveřejňování nepravdivých nebo neúplných a nepřesných osobních údajů. Špatná je také komunikace uvedeného zpracovatele: Subjekty údajů se nemohou domoci likvidace neoprávněně zpracovávaných či nepřesných osobních údajů.

S ohledem na skutečnost, že Úřadu jsou zákonem svěřeny kompetence pro zpracování osobních údajů prováděné na území České republiky a dále tam, kde lze v souladu s mezinárodním právem prosadit právní řád ČR a zajistit evropské standardy ochrany osobních údajů, Úřad nemá možnost uplatnit svoji pravomoc a vymoci opatření k nápravě u subjektu, který spadá pod jurisdikci USA, a tudíž kontrola mohla být prováděna jen v omezeném rozsahu.

KB PENZIJNÍ SPOLEČNOST, A.S.

V polovině roku 2013 proběhla médii informace o úniku osobních údajů z databází Komerční banky, a.s. (nejednalo se o osobní údaje z databáze Komerční banky, ale o osobní údaje z databáze KB Penzijní společnosti, a.s.). Z reportáže podložené videonahrávkou bylo patrné, že za určitých okolností je možné mít přístup k obsahu databáze.

V období od července do září 2013 byla kontrolujícím inspektorem provedena, na základě podnětu zaslaného stěžovatelem, kontrola dodržování povinností stanovených zákonem č. 101/2000 Sb. v KB Penzijní společnosti, a.s. (dále jen „kontrolovaný") v souvislosti se zabezpečením osobních údajů subjektů údajů (klientů, zájemců apod.) kontrolovaného, neboť bylo zjištěno, že šlo o klienty této společnosti.

Kontrolou bylo zjištěno porušení povinnosti vyplývající z ustanovení § 13 odst. 1 zákona č. 101/2000 Sb. Vzhledem k tomu, že kontrolovaný již v průběhu kontroly uvedl, že do chybné aplikace doplnil kontrolní mechanismy, které zabezpečují správnou autorizaci uživatele tak, aby

nedošlo k vygenerování chybného linku, čímž zabezpečil ověření přístupu na stránku v aplikaci, nebyla uložena nápravná opatření.

Případ je flagrantní ukázkou rizika moderní komunikace založené na používání internetu. Nejednalo se o hackerský útok na bezpečnostní systémy banky. Šlo o chybu v aplikaci, která měla nepovoleným vstupům do systému zabránit. Kontrolovaným provedené kontrolní testy chybu neodhalily a systém mohl fungovat mnohem déle, kdyby klient nebyl banku na problém upozornil.

Ze zjištění kontrolujícího inspektora vyplynulo, že se správci osobních údajů nepodařilo dostatečně zabezpečit uchovávané osobní údaje. Software, který měl data chránit, obsahoval chybu a umožnil únik informací.

S ohledem na výše uvedené kontrolující inspektor konstatoval, že považuje za oprávněný požadavek povinnost interního vyhodnocování rizik správcem osobních údajů.

PURE HEALTH & FITNESS, S.R.O.

V roce 2013 byla do kontrolního plánu Úřadu zahrnuta kontrola společnosti Pure Health & Fitness, s.r.o. (dále jen „kontrolovaný"), která provozuje fitness centrum. Podobná fitness centra navštěvují tisíce klientů, kteří obvykle využívají nabízených služeb pravidelně, a tedy v rámci dlouhodobějších nabídek. Některá fitness centra tyto balíčky služeb podmiňují členstvím v jejich klubu, čímž dochází při registraci klientů ke zpracovávání osobních údajů.

Kontrola v uvedeném fitness centru probíhala od dubna do září 2013. Předmětem kontroly bylo dodržování povinností vyplývajících ze zákona č. 101/2000 Sb. v souvislosti s veškerým zpracováním osobních údajů klientů centra, a to i prostřednictvím kamerového systému.

Kontrolou bylo zjištěno porušení mnoha povinností vyplývajících z § 5 odst. 1 písm. d) a e) a odst. 2, § 11 odst. 1 a 2, § 13 odst. 1, 3 a 4, § 16 odst. 1 a § 20 odst. 1 zákona č. 101/2000 Sb. Kontrolovanému bylo uloženo deset nápravných opatření, která kontrolovanému ukládala mj. upravit papírovou přihlášku ke členství v klubu PURE, změnit *Směrnici pro zpracování osobních údajů pro členy klubu PURE*, upravit technicko-organizační opatření týkající se uchování záznamů z kamerového systému nebo zlepšit způsoby informování klientů o instalaci kamerového systému v tělocvičnách. Z kontrolních zjištění vyplynulo velké podcenění problematiky ochrany soukromí ze strany kontrolovaného provozovatele fitness. Vzhledem k počtu klientů kontrolované společnosti se jednalo o poměrně závažná zjištění.

Při celkovém hodnocení této kauzy je ale třeba konstatovat neopatrnost i ze strany subjektů údajů, protože poskytovaly i nepovinné údaje bez jakékoli snahy o získání informace o účelu zpracování těchto dat. Úřad se proto této problematice hodlá věnovat také v příštím období.

VIDEOZÁZNAMY Z JEDNÁNÍ ZASTUPITELSTVA MĚSTA ZPŘÍSTUPNĚNÉ PROSTŘEDNICTVÍM WEBOVÝCH STRÁNEK MĚSTA

Kontrolující inspektor provedl kontrolu statutárního města (dále jen „kontrolovaný"), jejímž předmětem bylo dodržování povinností stanovených v HLAVĚ II zákona č. 101/2000 Sb., se zaměřením na ochranu osobních údajů zpracovávaných prostřednictvím videozáznamů z jednání zastupitelstva kontrolovaného ve funkčním období 2010–2014 zpřístupněných prostřednictvím webových stránek kontrolovaného. Kontrola byla provedena na základě podnětu zaslaného občanem města, kde bylo poukázáno na porušení zákona č.101/2000 Sb.

Při místním šetření a ústním jednání u kontrolovaného bylo zjištěno, že usnesením městské rady bylo schváleno Programové prohlášení, v němž bylo mimo jiné uvedeno, že se rada města rozhodla otevřít radnici lidem, resp. že radnice bude sledovat trend maximální otevřenosti města. K tomu byla schválena smlouva mezi kontrolovaným a soukromou televizní společností o výrobě a zajištění televizního a internetového vysílání pořadu „U nás ve městě"; smlouva obsahuje podmínky využití práv k pořadu a k pořízení záznamů z jednání zastupitelstva města i využití práv k nim, jakož i podmínky výroby a zajištění televizního a internetového vysílání pořadu „Městský expres". Účelem a předmětem uzavíraných smluv kontrolovaného s dodavatelskou společností bylo mimo jiné pořízení nesestříhaných záznamů z jednání zastupitelstva kontrolovaného, poskytnutí práv k užití těchto záznamů kontrolovaným a jejich umístění na webové stránky kontrolovaného nejpozději do 48 hodin od ukončení každého jednání zastupitelstva. Smlouvy uzavřené kontrolovaným s dodavatelem však neobsahovaly žádná ujednání o zárukách o technickém a organizačním zabezpečení ochrany osobních údajů. Záznamy z jednání zastupitelstev pak byly zveřejňovány na webových stránkách, resp. tato webová stránka obsahovala odkaz, jehož prostřednictvím byl otevírán konkrétní audiovizuální záznam. Kamera pořizující záznamy z jednání zastupitelstev snímala prostory, ve kterých se nacházejí místa pro sezení vedení kontrolovaného a část zastupitelů kontrolovaného a pultík s mikrofonem. Kamera byla umístěna staticky, probíhalo pouze přibližování a oddalování obrazu.

Souhlasy subjektů údajů, konkrétně osob, které nejsou osobami veřejně činnými ani občany uplatňujícími svá politická práva, nebyly kontrolovaným získávány. Na záznamech jednání zastupitelstva kontrolovaného nebyly nalezeny žádné osoby, které by nebyly osobami veřejně činnými ani občany uplatňujícími svá politická práva. Při jednání zastupitelstva kontrolovaného nebyla sdělována osobou řídící schůzi zastupitelstva žádná informace o tom, že bude pořizován videozáznam průběhu jednání, jehož záznam bude následně zveřejněn prostřednictvím webových stránek. Kontrolovaný měl u všech vchodů do prostor, odkud byly pořizovány videozáznamy jednání zastupitelstev, umístěny tabulky pouze s upozorněním: *„Z tohoto jednání zastupitelstva se pořizuje audiovizuální záznam, který bude umístěn na webových stránkách."* Tento stav se změnil po konzultaci s kontrolujícími na jednání zastupitelstva v červnu 2013, kdy byli všichni přítomní osobou řídící schůzi zastupitelstva řádně poučeni.

Při posouzení zjištěných skutečností dle zákona č. 101/2000 Sb. se ukázalo, že zveřejněné záznamy jednání zastupitelstva kontrolovaného obsahovaly informace týkající se identifikovaných nebo identifikovatelných fyzických osob, zveřejněné záznamy tedy obsahovaly osobní údaje ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. Účel a prostředky zpracování osobních údajů určil kontrolovaný, v souladu s § 4 písm. j) zákona č. 101/2000 Sb. byl kontrolovaný správcem osobních údajů. V souladu s § 5 odst. 1 písm. e) zákona č. 101/2000 Sb. je správce povinen uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Do vydání kontrolního protokolu byly dostupné všechny videozáznamy z jednání zastupitelstva kontrolovaného pouze z volebního období 2010–2014, konkrétně tedy do června 2013. Ve vztahu k účelu je možné považovat za adekvátní dobu zveřejnění záznamů dobu trvání funkčního období zastupitelstva. Kontrolovaný dodržel povinnost stanovenou v § 5 odst. 1 písm. e) zákona č. 101/2000 Sb.

V souladu s § 5 odst. 2 zákona č. 101/2000 Sb. může správce osobních údajů zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat jen v případech uvedených v § 5 odst. 2 písm. a) až g) téhož zákona.

V případě zastupitelů, úředníků obce a dalších úředních osob se aplikuje znění § 5 odst. 2 písm. f) zákona č. 101/2000 Sb., kde je uvedeno, že správce může zpracovávat osobní údaje bez souhlasu subjektu údajů *„pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o jeho funkčním nebo pracovním zařazení.*"

Rozdílná situace nastává u fyzických osob, které nespadají do výše uvedených skupin subjektů údajů. V tomto případě není možné neomezené zveřejnění těchto osobních údajů, a je tedy třeba tyto osobní údaje před zveřejněním záznamu anonymizovat. Avšak tyto osoby nebyly na videozáznamech jednání zastupitelstva kontrolovaného zjištěny. Kontrolou tak nebylo shledáno porušení povinnosti vyplývající z § 5 odst. 2 zákona č. 101/2000 Sb.

Ustanovení § 6 zákona č. 101/2000 Sb. uvádí, že *„pokud zmocnění nevyplývá z právního předpisu, musí správce se zpracovatelem uzavřít smlouvu o zpracování osobních údajů. Smlouva musí mít písemnou formu. Musí v ní být zejména výslovně uvedeno, v jakém rozsahu, za jakým účelem a na jakou dobu se uzavírá, a musí obsahovat záruky zpracovatele o technickém a organizačním zabezpečení ochrany osobních údajů*." Smlouvy uzavřené kontrolovaným se soukromou televizní společností o výrobě a zajištění televizního a internetového vysílání pořadu „U nás ve městě" a využití práv k němu a pořízení záznamů z jednání zastupitelstva města a využití práv k nim resp. o výrobě a zajištění televizního a internetového vysílání pořadu „Městský expres" a využití práv k němu a pořízení záznamů z jednání zastupitelstva města a využití práv k nim nejsou smlouvami o zpracování osobních údajů. Není však vyloučeno, aby příslušná ustanovení byla začleněna do smluv komplexněji s upravujícími vztahy mezi příslušnými subjekty (např. smlouvy jmenované výše).

Smlouvy splňují požadavky obecných náležitostí pro právní úkon dle zákona č. 40/1964 Sb., občanský zákoník, dále jsou v písemné formě, jsou uzavřeny na konkrétní dobu, je uvedeno, v jakém rozsahu a za jakým účelem, avšak neobsahují žádná ujednání o zárukách o technickém a organizačním zabezpečení ochrany osobních údajů. Kontrolující inspektor dospěl k závěru, že kontrolovaný porušil § 6 zákona č. 101/2000 Sb. tím, že smlouvy uzavřené se soukromou televizní společností neobsahovaly náležitosti, které jsou zákonem č. 101/2000 Sb. vyžadovány, konkrétně záruky o technickém a organizačním zabezpečení.

V období od září 2011 do června 2013 kontrolovaný poskytoval subjektům údajů informace o zpracování jejich osobních údajů v rozsahu vyvěšených cedulí s upozorněním: *„Z tohoto jednání zastupitelstva se pořizuje audiovizuální záznam, který bude umístěn na webových stránkách,*" což byla dle kontrolujícího inspektora nedostatečná forma poučení subjektů údajů dle § 11 odst. 1 zákona č. 101/2000 Sb. V uvedeném poučení chyběla informace o rozsahu zpracování osobních údajů, informace, pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny. Dále chyběla informace o přístupu k osobním údajům, o právu na opravu osobních údajů i o dalších právech stanovených v § 21 zákona č. 101/2000 Sb. Tento stav se změnil na jednání zastupitelstva v červnu 2013, kde byli všichni přítomní osobou řídící schůzi zastupitelstva kontrolovaného řádně poučeni ve smyslu § 11 odst. 1 zákona č. 101/2000 Sb. Kontrolovaný porušil informační povinnost vyplývající z ustanovení § 11 odst. 1 zákona č. 101/2000 Sb., a to konkrétně v období od září 2011 do června 2013.

Kontrolovaný měl zpracovány interní normy „Směrnici o anonymizaci údajů v materiálech projednaných a rozhodnutých zastupitelstvem statutárního města zveřejňovaných na webových

stránkách statutárního města", dále „Směrnici o bezpečnosti informací" a také „Směrnici vymezující kompetence při poskytování informací" či „Pravidla pro přijímání a vyřizování petic a stížností". Všechny tyto normy obsahovaly rozpracovaná ustanovení vztahující se k ochraně osobních údajů, resp. to byla faktická provedení (zdokumentování) technicko-organizačních opatření k zajištění ochrany osobních údajů, avšak tato ustanovení se nevztahovala ke zpracování osobních údajů prostřednictvím pořízených a následně i zveřejněných videozáznamů jednání zastupitelstva kontrolovaného. Jelikož sám kontrolovaný toto zpracování neprováděl, mohl tato ustanovení provést do smluv uzavíraných se zpracovateli, resp. mohl iniciovat vznik příslušné normy, která by obsahovala část týkající se ochrany osobních údajů obsažených ve videozáznamech jednání zastupitelstva kontrolovaného a která by byla pro smluvní televizní společnost závazná.

Kontrolovaný porušil svou povinnost dle § 13 odst. 2 zákona č. 101/2000 Sb., neboť jako správce osobních údajů nezpracoval a nezdokumentoval technicko-organizační opatření k zajištění ochrany osobních údajů obsažených ve videozáznamech jednání zastupitelstva. Kontrolovaný zpracování osobních údajů prostřednictvím pořizování a zveřejňování videozáznamů jednání zastupitelstva kontrolovaného za účelem informování veřejnosti neoznámil Úřadu. Vzhledem k tomu, že se na kontrolovaného nevztahují výjimky uvedené v § 18 zákona č. 101/2000 Sb. kontrolovaný porušil § 16 odst. 1 zákona č. 101/2000 Sb.

Výše uvedená kontrola byla běžná, jakých inspektoři Úřadu provedli v důsledku stížností občanů více. Jiný na ní byl přístup vedení a zástupců kontrolovaného. Přesto, že za porušení zákona č. 101/2000 Sb. byl kontrolovaný sankcionován, představitelé města výsledek kontroly reflektovali pro budoucí praxi. Otevřenost jednání městského zastupitelstva občanům města hájili, ale místo stížností na Úřad a zákon č. 101/2000 Sb., – což je při jednáních Úřadu se samosprávnými orgány bohužel běžné – uznali, že systém informování občanů musí uvést do souladu se zákonem č.101/2000 Sb., a dali najevo odhodlání zjištěné nedostatky okamžitě ve spolupráci s Úřadem řešit. Úřad jim při jejich řešení poskytl metodickou pomoc. Prakticky ještě před vydáním kontrolního protokolu, ve spolupráci s Úřadem, uvedl kontrolovaný všechny smlouvy i interní dokumenty do souladu se zákonem č. 101/2000 Sb.

• VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ

Po letech nárůstu stížností a podnětů se v roce 2013 jejich počet ustálil. Jejich poměrně vysoký počet vypovídá o tom, že lidé si již zvykli se prostřednictvím Úřadu domáhat práva na ochranu soukromí, do kterého ochrana osobních údajů spadá. Ke vzrůstajícímu povědomí o ochraně osobních údajů přispívá i konzultační činnost Úřadu.

Statistika stížností vyřízených v roce 2013

Celkem	1336
z toho:	
předáno ke kontrole	81
předáno na zahájení správního řízení	58
postoupeno příslušným orgánům	21
odloženo jako nedůvodné	1176

Stížnosti a podněty se jako obvykle v předcházejících letech týkaly ve velké míře provozování kamerových systémů. Zejména pak kamerových systémů v bytových domech (ať už družstevních nebo ve správě společenství vlastníků jednotek) a umístění kamer na nemovitostech ve vlastnictví jedné osoby či více spolumajitelů, nejčastěji rodinných domů. Problematice kamerových systémů v bytových domech se Úřad soustavně věnuje a důsledně vyžaduje ze strany správců a zpracovatelů plnění zákonem č. 101/2000 Sb. stanovených povinností, jako je legalita pořizovaného záznamu, dostatečné zabezpečení v souladu s § 13 zákona č. 101/2000 Sb. Naopak u kamer nainstalovaných u rodinných domů, kdy se soused domnívá, že kamera zabírá i jeho pozemek, nebo mu je zasahováno do jeho práva na soukromí jiným způsobem (např. pořizováním fotografií), jde dle názoru Úřadu primárně o věc soukromoprávní (občanskoprávní), tj. je nutné tyto soukromoprávní spory, v případě, že nedojde mezi zúčastněnými stranami k dohodě, řešit na prvém místě soudní cestou. Je třeba zdůraznit, že Úřad, resp. kontrolující inspektor a jeho tým, nemají právo vstupovat do obydlí, pokud neslouží zároveň k výkonu podnikatelské činnosti, tudíž často nemají možnost zdokumentovat a doložit skutečný stav věci, na niž obdržel Úřad stížnost, a relevantně uzavřít kontrolu.

V roce 2013 pokračoval mírný nárůst stížností a podnětů v oblasti informačních technologií. Tento nárůst započal v předchozích letech s rozšířením počtu uživatelů sociálních sítí, resp. internetu obecně. Uživatelé internetu si již uvědomují, že na internetu zanechávají digitální stopu, a to zejména v případě, že využívají sociální sítě, na nichž sdílejí svůj uživatelský obsah, včetně fotografií, a nad šířením informací o sobě ztrácejí kontrolu. V případě nalezených rozporů se zákonem č. 101/2000 Sb. naráží Úřad na bariéru, kterou je územní působnost samotného zákona č. 101/2000 Sb., který se vztahuje pouze na správce osobních údajů usazené na území České republiky anebo na zpracování, ke kterému na území České republiky dochází. Nelze tak reálně postihovat správce nebo zpracovatele osobních údajů, kteří zpracovávají osobní

údaje v zahraničí (např. správce usídlený ve Spojených státech amerických) s dopadem na české občany. Uplatnění zákonem svěřených pravomocí ze strany Úřadu tak není v těchto případech reálně možné a ustanovení 3 odst. 5 zákona č. 101/2000 Sb., které umožňuje použití právního řádu České republiky přednostně na základě mezinárodního práva veřejného, i když správce není usazen na území České republiky, nemohlo být doposud aplikováno, vzhledem k absenci příslušné mezinárodní smlouvy.

Jako další podstatnou oblast stížnostní agendy v roce 2013 můžeme označit i problematiku týkající se negativních registrů např. dlužníků nebo osob s finančními nebo majetkovými závazky. Této problematice se Úřad dlouhodobě věnuje a bude i nadále věnovat tak, aby zpracování osobních údajů v negativních registrech probíhalo v souladu se zákonem č. 101/2000 Sb.

Častým předmětem stížností a podnětů občanů je požadování kopií občanských průkazů (na nebezpečí zasílání kopií občanských průkazů Úřad veřejnost upozornil a setkal se se značnou odezvou v podobě dotazů i stížností), případně jiných dokumentů, a to ze strany finančních společností nebo zaměstnavatelů, využívání rodných čísel, kdy se nejčastěji jedná o jejich neoprávněné využívání formou zveřejňování. Opomenout nelze ani četné stížnosti týkající se zveřejňování osobních údajů obcemi.

Mezi nejčastější porušení zákona č. 101/2000 Sb. správci nebo zpracovateli osobních údajů dlouhodobě patří zpracování osobních údajů bez právního titulu, jejich zpracování k jinému účelu, než pro který byly shromážděny (což se často týká právě samosprávy), a nepřijetí adekvátních opatření k zabezpečení osobních údajů ve smyslu § 13 zákona č. 101/2000 Sb. Mezi další častá pochybení lze zařadit neposkytnutí informací nebo vysvětlení subjektu údajů o zpracování jeho osobních údajů na jeho písemnou žádost. Zejména právo na vysvětlení dle ustanovení § 21 zákona č. 101/2000 Sb. je dle poznatků Úřadu správci i zpracovateli osobních údajů podceňováno. Přitom žádost o vysvětlení by měla být pro správce nebo zpracovatele impulzem pro ověření, zda dochází ke zpracování osobních údajů subjektu údajů v souladu se zákonem č. 101/2000 Sb., eventuálně k přijetí adekvátních opatření, například likvidaci osobních údajů subjektu údajů a jeho informování o přijatých krocích učiněných k nápravě stavu, na nějž si stěžoval. Odezvou na žádost subjektů údajů o vysvětlení lze často rychle a efektivně odstranit bagatelní nedodržení zákona č. 101/2000 Sb. ze strany správce osobních údajů.

V roce 2013 se Úřad jako i v předešlých letech zabýval poskytováním konzultací a odpovědí na dotazy subjektů údajů, občanů, právnických osob a státních institucí. Dotazy jsou Úřadu zasílány nejčastěji elektronickými zprávami (e-mailem, poštovní datovou zprávou) a předávány telefonicky, přičemž zejména počet písemných dotazů každoročně narůstá. Problematiku ochrany osobních údajů lze konzultovat na základě vyžádání i osobně v prostorách Úřadu; využívají toho jak občané, tak instituce a velké obchodní společnosti, které se snaží klást vysoký důraz na ochranu osobních údajů, jež zpracovávají.

Nejčastější byly i v roce 2013 dotazy týkající se provozování kamerových systémů, nakládání s rodnými čísly, autentizace zaměstnanců při vstupu do zaměstnání, evidence pracovní doby, předávání osobních údajů do zahraničí, zveřejňování osobních údajů na internetu, zasílání obchodních sdělení.

Jako nový trend lze v roce 2013 hodnotit zakládání interních protikorupčních linek a s tím spojených dotazů na možnost upozornit v rámci společnosti na nekalé, nezákonné nebo neetické praktiky na pracovišti, které se dějí s velkou pravděpodobností se souhlasem nadřízeného. Na rozdíl od mnoha zemí neexistuje v České republice speciální právní úprava upravující

tzv. whistleblowing. Na zpracování osobních údajů, k němuž touto formou dochází, je proto třeba uplatnit obecný zákon, jímž je zákon č. 101/2000 Sb. K této problematice pořádal Úřad kulatý stůl za účasti nadnárodních společností poskytujících služby spojené s tzv. whistleblowingem.

Z poskytnutých významných konzultací státním institucím v roce 2013 lze zmínit Českou obchodní inspekci a Ministerstvo dopravy. V rámci konzultace Úřad doporučil v prvním případě České obchodní inspekci způsob zveřejňování pravomocně uložených pokut, který nebude při zpracování osobních údajů představovat zásah do práva na ochranu soukromí podnikajících fyzických osob oproti původně zamýšlenému záměru České obchodní inspekce plošně zveřejňovat. V druhém případě bylo konzultováno ověřování funkčnosti Centrálního registru vozidel.

• POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

ZVEŘEJŇOVÁNÍ OSOBNÍCH ÚDAJŮ DLUŽNÍKŮ

Úřad se už od začátku své existence věnoval problematice zveřejňování osobních údajů dlužníků, jak je zřejmé i z toho, že právě této právní otázky se týkalo již stanovisko č. 1/2001 – Zveřejňování jmen dlužníků.

Za dobu 12 let, které od vydání tohoto stanoviska uběhly, se přitom na právních předpisech ani názoru Úřadu nic nezměnilo. Důvody, proč je zveřejňování osobních údajů dlužníků z hlediska zákona č. 101/2000 Sb. neakceptovatelné, lze shrnout závěrem uvedeného stanoviska: *Zveřejňování osobních údajů v souvislosti se vznikem pohledávek považuje Úřad za nepřípustné zasahování 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*.

Z hlediska Úřadu se jedná o nátlakové jednání, kterým je porušováno i ustanovení článku 10 odst. 1 až 3 Listiny základních práv a svobod, podle něhož má každý právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno, každý má právo na ochranu před zasahováním do soukromého a rodinného života a každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Právní řád poskytuje nepochybně dostatečné prostředky k ochraně práv v případě, kdy věřiteli skutečně nebudou ze strany zákazníků/klientů konkrétní pohledávky uhrazeny, a to včetně následného výkonu případného soudního rozhodnutí; mezi tyto prostředky však zveřejňování seznamu dlužníků nepatří.

Prodávající či poskytovatel služby zpracovává osobní údaje svých zákazníků za účelem uskutečnění obchodu či poskytování svých služeb a s tím souvisejících činností, včetně vymáhání případných pohledávek. Zveřejnění osobních údajů je ovšem třeba již bez jakýchkoli pochybností považovat za jiný účel zpracování ve smyslu § 5 odst. 1 písm. f) zákona č. 101/2000 Sb. (správce je povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny), ke kterému není oprávněn.

V praxi Úřadu se toto téma po prvních letech jeho činnosti dostalo poněkud do pozadí. Zdálo se, že tato praxe není mezi soukromoprávními subjekty nijak rozšířená a pro vymáhání pohledávek jsou využívány standardní nástroje, které právní řád věřitelům dává.

V roce 2013 se však objevilo několik případů (zejména v souvislosti s provozováním internetových obchodů), které by, jak se zdá, mohly znamenat návrat k těmto postupům věřitelů. Zda existuje nějaký reálný důvod (například zvýšený počet dlužníků, obtížnější vymáhání pohledávek soudní cestou apod.), proč k tomu dochází, přitom není příliš jasné. Je však nezbytné znovu na nezákonnost takového jednání upozornit a osoby, které zamýšlejí takový postup, před jeho riziky varovat.

V případě, že správce zveřejní osobní údaje svých dlužníků (pravidelně se přitom jedná o situaci, kdy existence dluhu není podložena žádným soudním rozhodnutím, ale pouze jednostranným tvrzením správce; i pokud by však existence pohledávky byla potvrzena soudem, je třeba zdůraznit, že taková situace neopravňuje věřitele rozhodnutí či informace z něj vyplývající, jedná-li se o osobní údaje, zveřejnit), vystavuje se nejen nebezpečí řízení o správním deliktu podle zákona č. 101/2000 Sb., ale též občanskoprávní žaloby těch osob, do jejichž práva

na soukromí zveřejněním údajů zasáhl. Oba tyto postupy mohou probíhat samostatně, ale nic nebrání tomu, aby se dotčený subjekt údajů obrátil na Úřad a současně se svých práv domáhal občanskoprávní cestou.

Jedna ze základních skutečností, kterou je třeba v souvislosti s touto problematikou opakovaně zmínit, je to, že osobním údajem nejsou jen jméno, příjmení, příp. adresa či datum narození, ale též informace, že osoba je dlužníkem (ať už skutečným či domnělým), komu dluží a jakou částku [srov. definice osobního údaje v § 4 písm. a) zákona č. 101/2000 Sb., podle které je osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů].

Při vedení správního řízení a v jeho závěru při určování výše sankce Úřad přihlíží v souladu s § 46 odst. 2 zákona č. 101/2000 Sb. zejména k závažnosti, způsobu, době trvání a následkům protiprávního jednání a k okolnostem, za nichž bylo protiprávní jednání spácháno. V praxi se v případech zveřejňování osobních údajů dlužníků posoudí, kolik osob bylo jednáním dotčeno, jaký rozsah jejich údajů byl zveřejněn, jak dlouho byly údaje zveřejněny, zda bylo zveřejněno ve spojení s osobními údaji též nějaké hanlivé označení (např. zloděj) i to, jak vysoký měl být dluh (za závažnější z hlediska okolností, za kterých byl správní delikt spáchán, je třeba považovat, jsou-li zveřejňovány dlužné částky v řádech stokorun než v řádech sta tisíců). Z hlediska způsobu zveřejnění je zřejmě nejzávažnějším zveřejněním zveřejnění prostřednictvím internetu neomezenému okruhu osob, ale lze uvažovat i o způsobech jiných (Úřad se setkal např. s výlepem desítek plakátů v místě bydliště údajného dlužníka).

Závěrem je třeba zdůraznit, že uložení sankce ve správním řízení neznamená, že je možné osobní údaje zveřejněné prostřednictvím internetu ponechat na webových stránkách veřejně přístupné i nadále s poukazem na to, že správce již byl za toto jednání potrestán. V daném případě se totiž jedná o správní delikt trvající. Podle rozsudku Nejvyššího správního soudu čj. 5 A 164/2002-44 ze dne 22. února 2005 je trvajícím jiným správním deliktem takový správní delikt, jímž pachatel vyvolá protiprávní stav, který posléze udržuje, popřípadě jímž udržuje protiprávní stav, aniž jej vyvolal. Jednání, jímž pachatel udržuje protiprávní stav, závadný z hlediska správního práva, tvoří jeden skutek a jeden správní delikt až do okamžiku ukončení deliktního jednání, tj. až do okamžiku odstranění protiprávního stavu. V případě, že je ve věci zahájeno správní řízení a delikt trvá dále, nejedná se však z hlediska totožnosti skutku o skutek shodný, nýbrž o skutek nový, za který lze uložit další sankci.

ZVEŘEJŇOVÁNÍ INFORMACÍ O OSOBÁCH PODEZŘELÝCH ZE SPÁCHÁNÍ PŘESTUPKU

Velmi sporným tématem z hlediska veřejnosti se stal v roce 2013 případ obce, která na svých webových stránkách začala zveřejňovat osobní údaje osob podezřelých ze spáchání přestupku. Docházelo tím ve svém důsledku k vytváření specifického typu černé listiny, tzv. blacklistu. Tento pojem je používán pro seznamy subjektů či objektů (např. fyzická osoba, podnikatel, IP adresa počítače, e-mailová adresa), kterým byla uložena nějaká restrikce či sankce (např. jim nebude povolen vstup do určitého státu, nemohou se ucházet o veřejnou zakázku, není povoleno od nich přijímat e-maily nebo nemohou vkládat příspěvky do diskusí).

Úřad ve vedeném řízení předně konstatoval, že žádný právní předpis neobsahuje podmínky zveřejňování osobních údajů podezřelých ze spáchání přestupků projednávaných obcí, a proto se na daný postup vztahuje obecná úprava zpracování osobních údajů obsažená v zákoně

č. 101/2000 Sb. Obec je tedy, jakožto správce osobních údajů, podle § 5 odst. 1 písm. f) zákona č. 101/2000 Sb.povinna nakládat s osobními údaji pouze v souladu s účelem, pro který byly shromážděny; zpracovávat osobní údaje k jinému účelu lze, jen pokud k tomu dal subjekt údajů předem souhlas, případně pokud se na takové zpracování vztahuje některá z výjimek dle § 5 odst. 2 písm. a) až g) zákona č. 101/2000 Sb. Současně je také správce povinen dbát práva na ochranu soukromého a osobního života subjektů údajů. Zveřejněním osobních údajů prostřednictvím webových stránek byl účel zpracování z níže uvedených důvodů zjevně překročen.

Účelem zpracování osobních údajů podezřelých ze spáchání přestupků je totiž zjevně evidence těchto přestupků a jejich předání k vyřízení městu, se kterým má uzavřenu příslušnou veřejnoprávní smlouvu o jejich projednání. O všech těchto krocích je obec povinna vést evidenci dle zákona č. 499/2004 Sb., o archivnictví a spisové službě. Je přitom nutné považovat postupy související s projednáváním přestupků za systematickou činnost upravenou zákonem, přičemž obec je povinna shromažďovat informace o pachatelích přestupků, případně o osobách podezřelých ze spáchání přestupků, a jedná se tedy o zpracování osobních údajů ve smyslu definice uvedené v § 4 písm. e) zákona č. 101/2000 Sb., na které se tento zákon plně vztahuje, a to bez ohledu na to, zda obec přestupky projednává sama, nebo věc k přestupkovému řízení předává jiné obci.

Ke zveřejňování osobních údajů o pachatelích přestupků, natož o osobách ze spáchání přestupku pouze podezřelých, lze uvést, že státní moc lze dle článku 2 odst. 3 Ústavy České republiky uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. Možnost zveřejnit osobní údaje pachatele přestupku dříve vyplývala z § 26 odst. 1 písm. b) zákona č. 60/1961 Sb., o úkolech národních výborů při zajišťování socialistického pořádku, a to formou uložení opatření tzv. veřejné důtky. Také věcný záměr zákona o odpovědnosti za přestupky a řízení o nich (zákon o přestupcích) předpokládá, že za přestupek bude možné uložit správní trest zveřejnění rozhodnutí o přestupku. Z odůvodnění tohoto záměru však jednoznačně vyplývá, že tento správní trest by nebylo možné uložit fyzické osobě z důvodu ochrany jejích osobních údajů. V obou výše uvedených případech se však jedná o zveřejnění informací o spáchání přestupků, o nichž již bylo pravomocně rozhodnuto. Současný zákon č. 200/1990 Sb., o přestupcích, však zveřejňování informací o pachatelích přestupků neumožňuje, neboť řízení i jeho výsledek jsou neveřejné.

V konkrétním projednávaném případě se přitom v době zveřejnění prozatím nejednalo ani o osoby obviněné z přestupku (dosud proti nim nebylo zahájeno řízení), a i pokud by tyto osoby byly uznány vinnými ze spáchání přestupku, ani tehdy, jak je popsáno výše, zákon zveřejnění takové informace neumožňuje.

Nelze akceptovat ani tvrzení, že tento postup je snahou o transparentnost činnosti obce, protože i při zveřejňování informací o vynakládání veřejných prostředků, se kterými hospodaří, je obec povinna postupovat v souladu se všemi právními předpisy, a to včetně zákona č. 101/2000 Sb. Za účelem zajištění transparentnosti je možno zveřejnit počty oznámených přestupků, případně částky vynaložené na jejich projednání příslušným městem, nikoliv však osobní údaje (údajných) pachatelů.

Je možné ještě dodat, že zveřejněním osobních údajů na internetu dochází k vytvoření tzv. elektronické stopy, která se pojí se subjektem údajů a které je obtížné, ne-li nemožné, se zcela zbavit. K informacím zveřejněným na internetu má navíc přístup neomezený okruh osob a jejich šíření je velmi snadné a rychlé.

• POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

Řada rozhodnutí Úřadu je předmětem soudního přezkumu. Pokud jde o konkrétní poznatky z předmětné soudní praxe za rok 2013, lze poukázat na několik dále uvedených významných rozsudků týkajících se zejména provozování kamerových systémů a zveřejňování osobních údajů.

DOHLED ZAJIŠŤOVANÝ POMOCÍ VIDEOKAMER, KDY DOCHÁZÍ K POŘIZOVÁNÍ ZÁZNAMŮ A NÁSLEDNÉ IDENTIFIKACI OSOB ZACHYCENÝCH NA ZÁZNAMECH V PŘÍPADECH, KTERÉ URČÍ SPRÁVCE OSOBNÍCH ÚDAJŮ, JE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ, A TO I TEHDY, POKUD BY NĚKTERÉ NATOČENÉ OSOBY NEBYLY V PRAXI IDENTIFIKOVATELNÉ

Nejvyšší správní soud v rozsudku čj. 5 As 158/2012-49 ze dne 23. srpna 2013 především obecně uvedl, že účelem dohledu pomocí videokamer je právě identifikace osob zachycených na záznamu ve všech případech, kdy to správce pokládá za nezbytné. Celý systém jako takový se proto musí považovat za zpracovávání údajů o identifikovatelných osobách, i když například některé osoby zachycené na záznamu v praxi identifikovatelné být nemusí. Podle názoru Nejvyššího správního soudu tedy dochází ke shromažďování a zpracování osobních údajů i za situace, kdy k jedinému identifikátoru – podobizně – nejsou připojovány doplňující informace, nicméně lze je dodatečně zjistit (např. datum konání semináře, meetingu, jeho pořadatele, seznam účastníků apod.); rovněž tak i z účelu pořizování záznamu lze dovodit, že důvod pořízení záznamu – ochrana právem chráněných zájmů – takovéto ztotožnění předpokládá. Navíc nelze zpochybnit, že doplňující informace ohledně některých osob, například zaměstnanců či ubytovaných osob, mívá správce osobních údajů přímo k dispozici. Nejvyšší správní soud dále podotkl, že značná část informací, jež jsou shromažďovány prostřednictvím kamerového sledování, se týká identifikovaných nebo identifikovatelných osob, které jsou filmovány při svém pohybu na veřejnosti nebo na veřejně přístupných místech. Takovéto osoby sice mohou očekávat menší stupeň soukromí, nejsou však plně zbaveny svých práv a svobod, jež se mj. týkají jejich soukromého života.

Co se týče kamerového sledování v hotelových prostorách, Nejvyšší správní soud především výslovně odmítl argumenty, poukazuje-li se jimi například na vysoký standard hotelu, resp. uvádí-li se, že se jedná o hotel, který poskytuje služby nejvyšší úrovně a z toho se následně dovozuje legitimita nastaveného kamerového systému. Nejvyšší správní soud předmětným rozsudkem deklaroval názor, podle něhož k vysoké úrovni poskytovaných služeb mimo jiné patří i vysoký standard v oblasti ochrany soukromí jejich příjemců, tj. hostů. Právě schopnost zajistit vedle všech ostatních standardních služeb i vysokou míru soukromí (diskrétnosti) je znakem vysoké úrovně, resp. nadstandardnosti.

Ohledně legality kamerových systémů v hotelových zařízeních Nejvyšší správní soud označil za v podstatě jedinou aplikovatelnou výjimku, kdy není třeba souhlasu subjektu údajů, tu, která je obsažena v ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb. V této souvislosti však bylo konstatováno, že k instalaci kamerových systémů, s ohledem na jejich povahu a zásah do osobní integrity osob, je možné přistoupit až tehdy, pokud už veškeré méně invazivní prostředky selhaly anebo by nebyly schopny naplnit vytyčený účel, který je sledován. Je zcela nepochybné,

že kamerový systém ve srovnání s jinými prostředky (např. personálními, mechanickými), které mohou dosáhnout naplnění stanovených účelů, zasahuje základní lidská práva, a to právo na soukromí a na soukromý rodinný život, která jsou garantována čl. 10 Listiny základních práv a svobod a čl. 8 Evropské úmluvy o ochraně lidských práv a základních svobod, a tudíž i do lidské důstojnosti, z které tato práva vyplývají.

Aby mohla být dána přednost ochraně jiného lidského práva nebo svobody před ochranou soukromí, musí se jednat o takovou situaci, kdy jinak si rovná základní práva a svobody jsou v konfliktu a je třeba důkladně zvážit, zda v té které konkrétní situaci je zájem chráněný jiným základním právem a svobodou natolik závažný a natolik ohrožen, že lze svolit k zásahu do soukromí, a tedy částečně či úplně omezit základní lidské právo na soukromí nebo soukromý a rodinný život, a tedy i lidskou důstojnost. Má-li být připuštěn kamerový systém, jakožto prostředek k dosažení určitého účelu, kterým byla v daném případě ochrana bezpečnosti osob a majetku vlastníka objektu a hotelových hostů a dalších návštěvníků, je třeba posoudit zejména to, zda tento kamerový systém zasahuje do základních práv a svobod, zda v tom kterém případě kamerovým systémem chráněné základní právo a svoboda převáží nad ochranou soukromí, zda tento prostředek je jediný možný a nejvhodnější pro ochranu daného zájmu, resp. zda neexistuje jiný prostředek, který by stanoveného účelu byl rovněž schopen dosáhnout, a to buď bez zásahu do základního práva na soukromí, nebo s menší mírou. Současně je třeba posoudit i míru proporcionality, tedy uvážit, zda porušení hodnoty, do které tento prostředek zasahuje – zde do práva na soukromí, respektive lidské důstojnosti a svobody – je přiměřené, tedy zda právo na soukromí zasluhuje menší míru ochrany než hodnota, která má být ochráněna, konkrétně ochrana osob a majetku.

Kamerové sledování tudíž z obecného pohledu může sloužit řadě různých účelů, které lze seskupit do několika hlavních kategorií: 1) ochrana jednotlivců, 2) ochrana majetku, 3) veřejný zájem, 4) odhalování, prevence a stíhání trestné činnosti, 5) získávání důkazů, 6) jiné legitimní zájmy. Klíčovou otázkou je však opět nezbytnost takovéhoto využití kamerového systému, tedy zda lze či nelze ochránit práva a právem chráněné zájmy jiným způsobem, a to v návaznosti na druhou podmínku ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb., tedy zda takové zpracování osobních údajů není v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Je třeba konstatovat, že každé zpracování osobních údajů víceméně představuje zásah do soukromí jednotlivce. Aby tento zásah a celé zpracování bylo legální, je třeba, aby správce osobních údajů ve všech případech, kdy je to možné, posoudil všechny možné případné způsoby zpracování a zvolil ten, který do soukromí subjektů údajů zasáhne v nejmenší míře.

V konkrétním případě bylo shledáno, že v denních hodinách byli v recepci hotelu standardně přítomni dva až tři pracovníci, ve vstupní hale hotelu jeden až dva vrátní a jeden až dva organizační pracovníci; v nočních hodinách byl v recepci a vstupní hale přítomen jeden noční recepční; v lobby baru byli po celou otevírací dobu (11.00 hod. – 01.00 hod.) přítomni tři zaměstnanci; u vjezdu do garáží bylo stanoviště soukromé bezpečnostní služby; toto místo současně sloužilo jako služební vchod pro zaměstnance hotelu, přičemž služba zde byla nepřetržitá. Kamerový systém skládající se z 16 kamer přitom monitoroval mimo jiné rovněž vstupní halu a recepci, vchody do výtahů, restaurace, lobby bar, v nichž byli sledováni klienti ubytovaní v hotelu, hosté restaurací a rovněž zaměstnanci hotelu; dále byly monitorovány provozní a technické prostory hotelu – vjezd do garáží, služební vchod, nákladová rampa, přístupy do skladů

– zde byli sledováni zaměstnanci hotelu a mohli být přitom sledováni i hosté hotelu při vstupu do garáže. Monitorovací systém snímal nadto i chodník a vozovku před hotelem, kde kromě hostů vstupujících do hotelu byly sledovány i veškeré procházející osoby. Z uvedeného bylo zjevné, že stěžovatel měl dostatek jiných prostředků k zabezpečení ochrany svého majetku, jakož i bezpečnosti ubytovaných osob a hostů hotelu, a kamerový systém tudíž nesplnil žádnou výše uvedenou základní podmínku legality.

Předmětný rozsudek se také zabýval podmínkami pro řádné udělení konkludentního, tedy nikoliv výslovného, souhlasu subjektu údajů. Uvedl, že takovýto souhlas je sice možný, ale pouze za podmínky, kdy je tento souhlas dán aktivním jednáním, které je nezpochybnitelné; takové jednání potom ovšem musí být kdykoli později správcem osobních údajů, který nese důkazní břemeno, prokazatelné. Tyto podmínky tedy ve většině případů vylučují pouhé konkludentní udělení souhlasu subjektem údajů tím, že skutečnost, že prostor je monitorován, dotčené osoby mlčky akceptují a strpí. Tak tomu fakticky je i v případě, kdy by souhlas měl být de facto dáván již tím, že hosté do hotelu vstoupí a ubytují se v něm. Lze připustit, že případný souhlas může být dán jednáním subjektu údajů – konkrétně tím, že po přečtení informační tabulky vstoupí do snímané oblasti, tento případný konkludentní souhlas však rozhodně není nezpochybnitelný (např. subjekt údajů tabulku přehlédne) a rovněž není prokazatelný, resp. je určitá možnost prokazatelnosti pouze po dobu uchovávání záznamů. Informační tabulky s textem: „pozor, objekt střežen kamerou", velikosti cca 10 x 10 cm, které byly umístěny u hlavního vchodu do budovy (vstup pro handicapované) a vchodu do baru ze vstupní hotelové haly, by tak například musely být umístěny před vstupem do každého snímaného prostoru, nikoli pouze v místě hlavního vstupu, resp. vchodu do baru. Je třeba brát v potaz také to, že rozsah poskytovaných informací, tedy zejména pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období, takto nebyl správcem subjektů údajů poskytnut v dostatečné míře a nelze dovodit možnost, že si dotčený subjekt údajů bude předmětné informace sám dedukovat z logiky věci.

ÚZEMNĚ SPRÁVNÍ CELEK SE ZŘÍZENOU OBECNÍ POLICIÍ NENÍ OPRÁVNĚN KE ZŘÍZENÍ KAMEROVÉHO SYSTÉMU, KTERÝ BY BYL V PŘÍPADĚ SOUKROMÉHO SUBJEKTU PRAVDĚPODOBNĚ NEPŘÍPUSTNÝ; V TÉTO SOUVISLOSTI SE NELZE ODVOLÁVAT NA TO, ŽE SOUČÁSTÍ PŘÍSLUŠNÉHO ÚZEMNĚ SPRÁVNÍHO CELKU JE OBECNÍ POLICIE, PRO KTEROU VŠAK TAKOVÝTO KAMEROVÝ SYSTÉM NEBYL ZŘÍZEN

Nejvyšší správní soud svým rozsudkem čj. 4 As 75/2012-28 ze dne 25. září 2013 uvedl, že obec jako celek se nemůže dovolávat toho, že na její část (tedy obecní policii) dopadá speciální právní regulace a dovozovat z toho obecné oprávnění nakládat s osobními údaji pro sebe jako pro celek (tj. bez omezení pouze na obecní policii). Opačný výklad by ve vztahu ke státním orgánům obecně vedl ke zcela absurdnímu závěru v tom smyslu, že by každý státní orgán coby součást státu jako právního subjektu tvrdil, že jím shromažďované údaje v podobě záznamů z kamerového systému slouží pro účely Policie České republiky, jež nemá samostatnou právní subjektivitu a je naopak součástí téže entity jako dotčený státní orgán a jíž je zákonem stanovena povinnost pečovat o veřejný pořádek a vnitřní bezpečnost.

Podle uvedeného rozsudku obecní policie sice nemá samostatnou právní subjektivitu a z právních úkonů obecní policie je vázána příslušná obec, je však třeba poukázat na to, že v posuzované věci není rozhodné to, kdo má či nemá právní subjektivitu, ale jde o příslušný právní režim a faktické nastavení kamerového systému. V posuzované věci přitom bylo zjevné, že přístup ke kamerovému systému měla nejen obecní policie, ale i zaměstnanci městského úřadu. Pokud tedy měl být vytvořen kamerový systém k ochraně veřejného pořádku, života a zdraví, majetku a dalších práv a právem chráněných zájmů osob, měl plně odpovídat zákonu č. 553/1991 Sb., o obecní policii; kamerový systém by pak rovněž pouze obecní policie spravovala a měla k němu přístup. Jestliže tak nebylo postupováno a vytvořil se určitý „hybrid" mezi „kamerovým systémem obecní policie" a „běžným kamerovým systémem, který je určen ke střežení majetku, kontrole zaměstnanců a klientů úřadu", nelze hovořit o tom, že bylo postupováno v souladu se zákonem.

Dále Nejvyšší správní soud dospěl k závěru, že legalitu předmětného kamerového systému nelze založit ani aplikací ustanovení § 3 odst. 6 písm. c) zákona č. 101/2000 Sb., jelikož nebyly splněny podmínky obsažené v posledně citovaném ustanovení, které určují, že se musí jednat o zpracování osobních údajů nezbytných pro plnění povinností správce stanovených zvláštními zákony k zajištění veřejného pořádku a vnitřní bezpečnosti.

Územně samosprávnému celku totiž není žádným právním předpisem stanovena povinnost spočívající v zajištění veřejného pořádku a vnitřní bezpečnosti. Ustanovení § 35 odst. 2 zákona č. 128/2000 Sb., o obcích sice hovoří o ochraně veřejného pořádku, ale pouze v tom smyslu, že ochrana veřejného pořádku patří do samostatné působnosti obce. Zákon č. 128/2000 Sb. však v žádném svém ustanovení neurčuje, že ochrana veřejného pořádku je povinností obce, ale v tomto směru pouze stanoví, že obce se mohou otázkou veřejného pořádku zabývat, tj. že tato problematika patří do jejich věcné působnosti, a to konkrétně do samostatné působnosti. Věcná působnost správního orgánu tak určuje pouze okruh věcí, kterými se správní orgán může zabývat. Otázka, jaké prostředky má správní orgán k působení na jemu svěřenou problematiku, tj. jakou má pravomoc a zda musí svou pravomoc i vykonávat, je od věcné působnosti správního orgánu věcí odlišnou.

ZVEŘEJŇOVÁNÍ OSOBNÍCH ÚDAJŮ TĚCH, KDO SE NA OBEC OBRÁTILI SE SVÝM PODNĚTEM NEBO VÝZVOU, MUSÍ BÝT ZALOŽENO ŘÁDNÝM PRÁVNÍM TITULEM, KTERÝ NELZE DOVOZOVAT ZE SAMOTNÉHO AKTU PŘEDMĚTNÉHO PODÁNÍ

Rozsudkem čj. 6 A 120/2012-54 ze dne 23. srpna 2013 Městský soud v Praze především judikoval, že zveřejnění osobních údajů na internetových stránkách obce není nutné k vyřízení obsahu výzvy, tedy k naplnění samotného účelu, pro nějž byly osobní údaje shromážděny. Výzva jako taková není souhlasem se zveřejněním zde obsažených osobních údajů na úřední desce, resp. internetových stránkách, lze ji chápat pouze jako souhlas se zpracováním těchto osobních údajů v rámci projednání předmětného podání.

Speciálně pak bylo připomenuto, že takovéto zveřejnění není v souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb. ve spojení s ustanovením § 93 odst. 1 zákona č. 128/2000 Sb., o obcích, popřípadě ustanovením § 103 odst. 4 písm. e) zákona č. 128/2000 Sb. Ani jedno z citovaných ustanovení téhož zákona totiž nevede k závěru, že ke splnění povinností uvedených v těchto ustanoveních je nutné výzvu subjektů údajů zveřejnit, nadto v plném znění. Ustanovení § 93

odst. 1 zákona č. 128/2000 Sb. vyžaduje toliko informaci o navrženém programu připravovaného zasedání zastupitelstva. Pokud jedním z bodů programu má být určitá výzva, nepochybně postačí uvést pouze její předmět a základní identifikaci osob (například pouze jménem a příjmením), jichž se tento program týká. Ke splnění účelu informace rozhodně není nutné uveřejnit výzvu jako celek, zejména veškeré osobní údaje v ní obsažené (tak především rodná čísla či přesnou adresu bydliště). Již vůbec pak nelze dovodit povinnost zveřejnit informaci obdobného rozsahu z ustanovení § 103 odst. 4 písm. e) zákona č. 128/2000 Sb., podle něhož starosta obce odpovídá za informování veřejnosti o činnosti obce.

Zveřejnění nelze neodůvodnit ani ustanovením § 5 odst. 2 písm. d) zákona č. 101/2000 Sb., jelikož za zveřejnění osobních údajů podle § 4 písm. l) zákona č. 101/2000 Sb. rozhodně nelze označit skutečnost, že subjekt údajů v daném čase a na daném místě poskytne své osobní údaje omezenému okruhu dalších osob, aniž by byly zveřejněny prostřednictvím sdělovacích prostředků nebo jako součást veřejného seznamu. Nejedná se v daném případě ani o zpřístupnění jiným veřejným sdělením, jelikož za veřejné sdělení lze považovat pouze takové sdělení, které má potenci zasáhnout blíže neurčený okruh recipientů v místě i čase. Tak tomu ovšem v případě zasedání zastupitelstva obce není – jakkoliv je zasedání zastupitelstva obce veřejné, v okamžiku svého konání zahrnuje místem i časem omezený okruh účastníků.

Dále se Městský soud v Praze zabýval aplikací ustanovení § 8b odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, podle něhož povinný subjekt poskytne základní osobní údaje o osobě, které poskytl veřejné prostředky, přičemž základními osobními údaji se rozumí podle § 8b odst. 3 zákona č. 106/1999 Sb. jméno, příjmení, rok narození, obec, kde má příjemce trvalý pobyt, výše, účel a podmínky poskytnutých veřejných prostředků. Toto ustanovení podle názoru Městského soudu v Praze představuje výjimku z obecného pravidla zakotveného v ustanovení § 8a zákona č. 106/1999 Sb., podle něhož informace týkající se osobnosti, projevů osobní povahy, soukromí fyzické osoby a osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy upravujícími jejich ochranu. Zásadně je tedy třeba i při poskytování informací podle zákona č. 106/1999 Sb. postupovat v souladu s pravidly stanovenými zákonem č. 101/2000 Sb. Pokud jde o případnou aplikaci zvláštního režimu ustanovení § 8b zákona č. 106/1999 Sb., bylo zdůrazněno, že samo neukládá povinnost takovou informaci zveřejnit. Zveřejnění na základě ustanovení § 5 odst. 3 zákona č. 106/1999 Sb. primárně vyžaduje vyhovění příslušné žádosti.

• REGISTRACE

V roce 2013 bylo podáno celkem 6570 oznámení o zpracování osobních údajů a pokračoval tak trend jejich každoročního nárůstu. V letošním roce se jednalo o 13% nárůst oproti roku minulému. Oznámených žádostí o doplnění bylo v tomto roce celkem 877, což je pouze o málo více než v roce loňském. Ve druhé polovině roku 2012 se Registr zpracování osobních údajů připojil k systému základních registrů a dílčí změny adresních a identifikačních údajů jednotlivých subjektů se do něj promítají prostřednictvím automatických aktualizací údajů ze základních registrů. Není tedy již nutné provádět tyto změny prostřednictvím oznámení o změně zpracování. Vedle posuzování přijatých registračních oznámení vydává Úřad rozhodnutí o zrušení registrace podle § 17a odst. 2 zákona č. 101/2000 Sb. V letošním roce bylo zrušeno celkem 97 zpracování na žádost správce, nejčastěji z důvodů zániku či sloučení společnosti, zrušení podnikatelské činnosti nebo ukončení zpracování osobních údajů. Jednalo se o nárůst 20 %. Informace o zrušených registracích Úřad zveřejňuje ve Věstníku.

Vzhledem k tomu, že v řadě oznámených zpracování osobních údajů neumožňovaly zaslané údaje dostatečné posouzení zpracování osobních údajů nebo zaslaná oznámení byla neúplná, musel Úřad registrační řízení přerušit a zaslat oznamovateli výzvu k doplnění oznámení podle § 16 zákona č. 101/2000 Sb. Z celkového počtu 6570 došlých oznámení o zpracování osobních údajů bylo nutné v 867 případech řízení přerušit. V 63 % případů se přerušení týkalo oznámení zpracování prostřednictvím kamerových systémů, v 11 % zpracování citlivých údajů a zbylých 26 % připadalo na jiné důvody.

V případě, že na základě doplnění oznámení vznikla důvodná obava, že by zamýšleným zpracováním osobních údajů mohlo dojít k porušení zákona č. 101/2000 Sb., bylo takové oznámení předáno k zahájení správního řízení, což se stalo v 91 případech (tj u 1,4 % oznámení). Celkem v 8 případech pak zahájení zpracování nebylo v rámci správního řízení podle § 17 zákona č. 101/2000 Sb. povoleno (tj. v 0,1 % oznámení).

Nejčastěji oznamovaným druhem zpracování, podobně jako v letech minulých, bylo zpracování osobních údajů prostřednictvím kamerových systémů (cca 19 % ze všech podaných oznámení). Celkem je v registru zpracování osobních údajů zapsáno 10 995 subjektů, které podaly oznámení o zpracování osobních údajů kamerovými systémy. V roce 2013 podalo oznámení 2373 subjektů, což je nárůst oproti roku 2012 o 20 %.

Tabulka 1

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

Rok	Počet subjektů	Rok	Počet subjektů
do 2005	32	2010	1268
2006	386	2011	1505
2007	890	2012	1887
2008	1399	2013	2373
2009	1255	**Celkem**	**10 995**

Při zodpovídání dotazů se pracovníci registračního odboru Úřadu setkávali často s problematikou zpracování osobních údajů v rámci internetových obchodů, možnostmi umístění kamer v určitých prostorách, nezbytností souhlasu se zpracováním osobních údajů prostřednictvím kamerového systému, žádostmi o pomoc při vyplňování oznámení o zpracování osobních údajů, rušením registrovaného oznámení o zpracování osobních údajů a žádostmi o informace o stavu oznámení o zpracování osobních údajů. Velkou měrou jsou zastoupeny dotazy a konzultace týkající se předávání osobních údajů do zahraničí, zejména v rámci nadnárodních korporací.

Registrační odbor ve spolupráci s dalšími útvary Úřadu v roce 2013 připravil Metodiku pro splnění některých povinností ukládaných zákonem o ochraně osobních údajů při provozování internetových obchodů. Měla by pomoci subjektům provozujícím internetové obchody při plnění povinností vůči Úřadu a dalších povinností stanovených zákonem č. 101/2000 Sb. Metodika bude zájemcům k dispozici v elektronické podobě na webových stránkách Úřadu.

Do českého právního řádu byla v roce 2012 zákonem č. 468/2011 Sb., kterým se mění zákon č. 127/2005 Sb., o elektronických komunikacích transponována Směrnice Evropského parlamentu a Rady 2007/66/ES. Úprava se mimo jiné týkala problematiky narušení bezpečnosti osobních údajů. V souvislosti s následným přijetím Nařízení komise (EU) č. 611/2013 o opatřeních vztahujících se na oznámení o narušení bezpečnosti osobních údajů podle směrnice Evropského parlamentu a Rady 2002/58/ES o soukromí a elektronických komunikacích, které je přímo aplikovatelné, bylo nutno upravit webové stránky Úřadu v rubrice „Oznámení podle zákona č. 127/2005 Sb.", a to včetně formuláře určeného k plnění oznamovací povinnosti, upřesnit některé pojmy a upravit postup pro oznamovatele.

V roce 2013 obdržel Úřad jediné podání týkající se narušení bezpečnosti osobních údajů, které však bylo podáno subjektem, na nějž se oznamovací povinnost podle tohoto zákona nevztahuje.

Oznamována jsou ve velké míře zpracování pro účely reklamní a marketingové činnosti, realitní činnosti, poradenské činnosti v oblasti společenských věd a rozvoje osobnosti, kulturní, rekreační, sportovní a společenské aktivity, poskytování služeb osobního charakteru, pořádání odborných kurzů, školení a jiných vzdělávacích akcí, mimoškolní výchova a vzdělávání, vytváření databází klientů, dodavatelů, přepravců, obchodních partnerů apod.

Z registrační činnosti lze vysledovat, že pokračují tendence zaměstnavatelů monitorovat své zaměstnance na pracovišti prostřednictvím nejrůznějších dostupných technologií. Nejsou to pouze kamerové systémy, i když ty jsou nejčastějším prostředkem. Jedná se rovněž o používání speciálních počítačových systémů, které monitorují, jakým způsobem zaměstnanci využívají výpočetní techniku na svém pracovišti, například prostřednictvím monitorování pohybu zaměstnance na internetu či využívání různých softwarových programů. Jako účel takového zpracování je nejčastěji uváděno efektivní využívání pracovní doby a kontrola využívání, resp. zneužívání svěřené výpočetní techniky. V rámci registračních řízení jsou tak oznamovatelé opakovaně upozorňováni, že plošné monitorování a zpracování obsahu korespondence zaměstnanců v rámci pracovních e-mailů je z hlediska zákona č. 101/2000 Sb. nepřípustné, podobně jako plošné odposlouchávání a zpracovávání obsahu telefonních hovorů. Podobně je nutné v rámci registračních řízení upozorňovat na rizika spojená se sledováním zaměstnanců prostřednictvím geolokačních zařízení, umožňujících zjistit místo, kde se zaměstnanec nachází, prostřednictvím mobilního zařízení. Často se totiž jedná o služební mobil, který zaměstnavatel poskytne zaměstnanci s již instalovaným softwarem umožňujícím lokalizaci. Zaměstnance je tak možné vystopovat i v mimopracovní době, pokud má služební mobil u sebe.

Velké procento oznamovaných zpracování trvale souvisí s využíváním věrnostních karet. Účelem zpracování je obecně možnost čerpání různých slev a výhod na nákupy prováděné držitelem karty, který uvede své jméno, adresu, případně další kontaktní údaje, pokud má zájem dostávat sdělení o marketingových akcích. Správci osobních údajů v registračních oznámeních deklarují, že se tak děje se souhlasem subjektu údajů.

Poměrně hojně se vyskytovala oznámení, která souvisejí s tzv. whistleblowingem, a to výhradně v souvislosti se zákonem SOX (Sarbanes-Oxley Act). Oznámení se tedy týkala pouze společností majetkově ovládanými subjekty, které spadají pod tento zákon, a mají tedy povinnost systém whistleblowingu v rámci svého podniku zavést. Taková oznámení jsou úzce spjata s problematikou mezinárodních přenosů osobních údajů. Zákon SOX byl přijat Kongresem USA v roce 2002 v reakci na různé finanční a účetní nesrovnalosti při řízení některých významných podniků. Institut oznamování (whistleblowing) představuje určitý doplňkový mechanismus umožňující zaměstnancům interně, v rámci podniku, oznamovat protiprávní jednání s využitím zvláštního informačního kanálu. Na základě dosavadních poznatků Úřadu lze konstatovat, že způsob fungování systému whistleblowing se liší případ od případu (někdy se jedná o systém pro oznamování, kdy dceřiná společnost pouze umožní zaměstnancům přístup do systému oznamování, aniž by se sama jakkoliv podílela na vyšetřovacích postupech. Vyšetřování je zcela v režii mateřské společnosti. Dalším modelem je situace, kdy vyšetřování vede jen dceřiná společnost a výsledky šetření pouze oznámí mateřské společnosti, nebo je to kombinace obojího). Nejčastější účel zpracování je definován takto: řešení a vyšetření hlášení o výskytu podezřelých okolností (whistleblowing reports, whistleblowing hotline) předložených jednotlivci v souvislosti s obavami týkajícími se etického chování či pravidel chování společnosti. Společnost tak dává jednotlivcům možnost nahlásit své obavy ohledně případného výskytu finančního podvodu, úplatkářství, nevhodného chování nebo omylů či chyb ve finančním účetnictví, interních účetních postupech či v oblasti auditu nebo jiných záležitostí majících vliv na životně důležité zájmy společnosti. Při naplnění tohoto účelu může docházet k poměrně velkému rozsahu zpracovávaných osobních údajů (nebo také nemusí, existují různé modely dle významu a velikosti společnosti). Kromě identifikačních údajů také například okolnosti nahlášené situace, jak k ní došlo, jak se o tom osoba dozvěděla, ale také osobní údaje o třetích osobách, například informace o osobách, které o tom mohou vědět či podat bližší informace, dokumentace obsahující osobní údaje třetích osob.

Český právní řád dosud neobsahuje žádnou výslovnou úpravu whistleblowingu, existují pouze dva návrhy „zákona o whistleblowingu". Z toho důvodu se Úřad zabýval problémem ochrany osobních údajů v souvislosti s whistleblowingem pouze okrajově. V roce 2013 se na PF UK v Praze uskutečnila mezinárodní konference na téma whistleblowingu, na které vystoupil se svým příspěvkem i zástupce Úřadu.

• PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Při dodržení obecných zásad zákonného zpracování osobních údajů vyplývajících ze zákona č. 101/2000 Sb. mohou správci osobních údajů bez předchozího povolení Úřadu předávat osobní údaje nejen do členských států Evropské unie, resp. Evropského hospodářského prostoru včetně Švýcarska, ale také do třetích zemí s přiměřenou úrovní ochrany osobních údajů. Pro předávání do třetích zemí s nepřiměřenou úrovní ochrany osobních údajů je nutné Úřad předem požádat o povolení, pokud takové předávání není ošetřeno smlouvou, jejíž nedílnou součástí jsou standardní smluvní doložky podle rozhodnutí Evropské komise.

Mezi tyto třetí země se řadí státy, u nichž byla adekvátní úroveň ochrany osobních údajů konstatována Rozhodnutím Evropské komise (Argentina, Uruguay, Nový Zéland, Izrael, Švýcarsko, Faerské ostrovy, ostrovy Guernsey, Jersey a Man, a v případě komerční sféry Kanada), a dále také státy, které ratifikovaly Úmluvu č. 108 Rady Evropy o ochraně osob se zřetelem na automatizované zpracování osobních dat z roku 1981 (Albánie, Andorra, Arménie, Ázerbájdžán, Bosna a Hercegovina, Černá Hora, Gruzie, Island, Lichtenštejnsko, Makedonie, Moldavsko, Monako, Norsko, Rusko, Srbsko, Švýcarsko a Ukrajina). Právní předpisy těchto zemí zaručují dostatečnou ochranu osobních údajů odpovídající všem požadavkům směrnice Evropského parlamentu a Rady 95/46/ES, a tedy také zákona č. 101/2000 Sb.

Předání osobních údajů do všech ostatních zemí, tzn. do třetích zemí s nepřiměřenou úrovní ochrany osobních údajů, je pak možné pouze tehdy, pokud vývozce osobních údajů v konkrétním případě zaručí odpovídající úroveň ochrany jím předávaných osobních údajů. K vytvoření takovýchto garancí mohou vývozci údajů využít standardní smluvní doložky podle rozhodnutí Evropské komise; v případě amerických dovozců osobních údajů je za dostatečnou záruku považována jejich účast v programu Safe Harbor (dále jen „Bezpečný přístav"), definovaném rovněž rozhodnutím Evropské komise.

Třetím, v praxi stále častěji užívaným nástrojem k vytvoření odpovídající garance, a to zvláště ze strany velkých nadnárodních korporací, jsou závazná vnitropodniková pravidla (Binding Corporate Rules – dále jen „BCR"), která byla schválena ze strany některého z unijních úřadů pro ochranu osobních údajů jakožto vedoucího dozorového orgánu 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.

Na rozdíl od standardních smluvních doložek a účasti v programu Bezpečný přístav je v případě schválených BCR před započetím předávání osobních údajů do zahraničí nutné požádat Úřad o povolení k předání osobních údajů do třetích zemí podle § 27 odst. 4 zákona č. 101/2000 Sb., přičemž právním titulem, na jehož základě budou osobní údaje předávány, bude ustanovení § 27 odst. 3 písm. b) zákona č. 101/2000 Sb.

V povolovacím řízení Úřad zkoumá konkrétní okolnosti předání z České republiky do třetích zemí, zvláště pak zdroj, rozsah a kategorie předávaných osobních údajů, příjemce předávaných osobních údajů, včetně výčtu cílových zemí, účel předání a dobu zpracování. Kromě přiložení českého znění příslušných BCR a rozhodnutí o jejich schválení ze strany vedoucího dozorového

orgánu je proto nezbytné tyto okolnosti v žádosti podrobně uvést. Není možné odkazovat na text samotných BCR, protože BCR popisují toky dat v rámci nadnárodní korporace, zatímco v žádosti o povolení k předání osobních údajů do třetích zemí jde o konkrétní osobní údaje, které budou předány do třetích zemí z České republiky a jejichž rozsah, účel předání i další okolnosti mohou, nebo by měly být proto definovány přesněji, a to tak, aby bylo jasné, že všechny požadavky zákona č. 101/2000 Sb. jsou naplněny.

O tom, že se BCR stávají běžným instrumentem, kterým nadnárodní korporace zajišťují přiměřenou úroveň ochrany osobních údajů zpracovávaných a předávaných v rámci nadnárodní korporace po celém světě, svědčí i statistika vydaných povolení za rok 2013.

Úřad přijal za rok 2013 celkem 24 žádostí o povolení k předání osobních údajů do třetích zemí. Ve čtyřech případech Úřad věc odložil, a to vždy z důvodu, že žadatel omezil předání pouze na státy Evropské unie nebo na jiné bezpečné země.

Z dvaceti vydaných povolení bylo letos poprvé nejčastějším právním titulem, na jehož základě Úřad povolení vydal, ustanovení § 27 odst. 3 písm. b) zákona č. 101/2000 Sb., neboť žadatel vytvořil ve třetí zemi dostatečné zvláštní záruky ochrany osobních údajů, a to právě prostřednictvím schválených BCR. Stalo se tak v sedmi případech. Šestkrát bylo právním titulem povolení ustanovení § 27 odst. 3 písm. a) zákona č. 101/2000 Sb., tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů. Pětkrát bylo právním titulem povolení ustanovení § 27 odst. 3 písm. e) zákona č. 101/2000 Sb., tedy předání údajů nezbytných pro jednání o uzavření nebo změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů. Zbývající dvě povolení byla vydána na základě ustanovení § 27 odst. 3 písm. c) zákona č. 101/2000 Sb., kdy šlo o předání osobních údajů, které jsou na základě zvláštního zákona součástí datových souborů veřejně přístupných nebo přístupných tomu, kdo prokáže právní zájem.

Geograficky šlo i v roce 2013 především o předání osobních údajů do Spojených států amerických, Indie a oblasti jihovýchodní Asie a Pacifiku (Jižní Korea, Japonsko, Čína, Hongkong, Singapur), v jednom případě do Kazachstánu. V případech předání osobních údajů probíhajících na základě BCR zpravidla dochází k předání osobních údajů prostřednictvím jejich zpřístupnění pobočkám skupiny usazeným obvykle ve větším počtu zemí, ba často takřka po celém světě.

V sedmi případech vydal Úřad povolení k předání osobních údajů na základě BCR. Jednalo se o tzv. závazná vnitropodniková pravidla pro správce (Binding Corporate Rules for Controllers, dále jen „BCR-C“). Takto jsou nyní označována klasická BCR, která byla a jsou nadále určená pro nadnárodní správce osobních údajů, kteří při své činnosti shromažďují, předávají a zpracovávají osobní údaje k vlastním účelům v rámci celé nadnárodní korporace. Schvalovací procedura těchto BCR-C ze strany některého z unijních úřadů pro ochranu osobních údajů jakožto vedoucího dozorové autority nadále probíhá na základě výše zmíněných dokumentů Pracovní skupiny pro ochranu dat podle článku 29 (Working party 29), konkrétně WP 74, WP 107, WP 108, WP 133, WP 153, WP 154 a WP 155.

Vedle klasických BCR-C jsou nyní nově definována závazná vnitropodniková pravidla pro zpracovatele (Binding Corporate Rules for Processors, dále jen „BCR-P“). Ta jsou určena pro velké nadnárodní zpracovatele osobních údajů, typicky poskytovatele cloudových služeb, kteří provádějí zpracování osobních údajů pro velká množství správců osobních údajů. Analogicky jako u klasických BCR-C je i pro BCR-P nutné projít schvalovací procedurou ze strany některého

z unijních úřadů pro ochranu osobních údajů jakožto vedoucího dozorového orgánu, přičemž tato procedura, její náležitosti a průběh jsou definovány Pracovní skupinou pro ochranu dat podle článku 29 (Working party 29) v pracovních dokumentech WP 195, WP 195a a WP 204.

Stejně jako u klasických BCR-C je i v případě BCR-P nutné před započetím předávání osobních údajů do zahraničí požádat český Úřad o povolení k předání osobních údajů do třetích zemí podle § 27 odst. 4 zákona č. 101/2000 Sb. O povolení přitom však nežádá vlastní nadnárodní zpracovatel, ale jednotliví správci osobních údajů, kteří se rozhodli využít jeho zpracovatelských, obvykle cloudových služeb. Je třeba upozornit, že správce osobních údajů, který se rozhodne zpracovávat osobní údaje v nadnárodním cloudu, je i v takovém případě nadále plně zodpovědný za zpracování osobních údajů a že o povolení k předání osobních údajů do třetích zemí musí samozřejmě požádat i v tomto případě předtím, než zahájí předání v souladu s ustanovením § 27 odst. 4 zákona č. 101/2000 Sb.

V souvislosti se zveřejněním informací o programu PRISM, v jehož rámci americká Národní bezpečnostní agentura (National Security Agency, NSA) shromažďuje obrovská množství osobních údajů ze všech typů elektronických komunikací, mj. prostřednictvím vynucení systémového přístupu do systémů amerických poskytovatelů služeb elektronických komunikací a služeb informační společnosti a jiných subjektů, vzniká otázka, zda instituty bezpečného přístavu, standardních smluvních doložek a závazných vnitropodnikových pravidel jsou skutečně schopny zajistit efektivní ochranu osobních údajů ve třetích zemích. Konkrétně v případě předávání osobních údajů do USA na základě programu Bezpečného přístavu. Otázkou bezpečnosti předávaných osobních údajů z EU do USA se zabývala rovněž Evropská komise ve svém Sdělení Evropskému Parlamentu a Radě – Obnovení důvěry v toky údajů mezi EU a USA z 27. 11. 2013. Ze Sdělení Komise mj. vyplývá, že ze zjištění ad-hoc pracovní skupiny EU-USA je také jasné, že občané EU nemají v rámci programu PRISM a dalších obdobných programů sledování stejná práva a procesní ochranu jako Američané. To vyvolává pochybnosti ohledně úrovně ochrany, kterou systém Bezpečného přístavu poskytuje. Podle Sdělení Komise mnoho společností zapsaných na seznamu Bezpečného přístavu jeho zásady v praxi nedodržuje. Dalším vážným nešvarem je fakt, že Bezpečný přístav také funguje jako cesta pro předávání osobních údajů občanů EU z EU do USA společnostmi, které jsou povinny vydávat údaje zpravodajským službám Spojených států podle programů Spojených států pro shromažďování zpravodajských informací. Komise došla k názoru, že je nezbytné provést kompletní inventuru fungování Bezpečného přístavu, přijmout do léta 2014 nápravná opatření, která by měla být co nejdříve uplatněna. Pochybnosti ohledně programu Bezpečného přístavu, coby nástroje pro bezpečné předávání osobních údajů z EU do USA, sdílí rovněž Úřad, a proto i nadále doporučuje správcům (vývozcům údajů) před samotným předáním ověřit, zda je certifikace příslušné společnosti stále platná, zda a jakým způsobem jsou fyzické osoby informovány o vnitřních postupech pro vyřizování stížností, případně zda jsou „privacy policy" příslušné společnosti veřejně přístupné například prostřednictvím webových stránek. V případě zjištěných nedostatků při uplatňování principů Bezpečného přístavu je namístě o tom informovat Úřad.

Článek 13 (1), případně čl. 26 (1d) směrnice 95/46/ES, stejně jako § 3 odst. 6 zákona č. 101/2000 Sb. předpokládá, že zpracování osobních údajů bezpečnostními složkami států za vyjmenovanými účely spojenými se základními funkcemi států bude probíhat ve zvláštním volnějším režimu, který umožní správcům osobních údajů v jednotlivých zákonem definovaných a odůvodněných případech předat relevantní informace bez konfliktu s evropskou úpravou

ochrany osobních údajů. Avšak pod takto definované výjimky rozhodně nelze podřadit systémový přístup Národní bezpečnostní agentury do systémů privátních správců či zpracovatelů osobních údajů a jejich hromadné shromažďování bez ohledu na to, zda subjekty údajů jsou podezřelými osobami, rozpracovanými bezpečnostními složkami státu. Je to svým způsobem analogický případ k vynucenému předávání údajů jmenné evidence cestujících (Passanger Name Record Data, PNR data) leteckými společnostmi bezpečnostním složkám Spojených států amerických po 11. září 2001.

Takové zpracování osobních údajů je rozhodně v rozporu s evropskými zásadami ochrany osobních údajů a příslušní dovozci osobních údajů ve třetí zemi jsou povinni podle znění příslušných klauzulí programu Bezpečný přístav, standardních smluvních doložek i závazných vnitropodnikových pravidel oznámit tuto skutečnost jako překážku, která jim brání plnit jejich povinnosti, a to vývozcům osobních údajů a příslušným dozorovým úřadům. Vývozci osobních údajů a dozorové úřady jsou přitom oprávněni v takovém případě zastavit předání osobních údajů do třetí země.

V rámci své povolovací činnosti Úřad řešil v roce 2013 rovněž žádosti o povolení předání předběžné informace o cestujících (Advance Passenger Information Data, API data) leteckých společností do Spojených arabských emirátů a do Jižní Koreje. Podobně jako v dřívějších případech dospěl Úřad k názoru, že v posuzovaném případě bude naplněna podmínka § 27 odst. 3 písm. e) zákona č. 101/2000 Sb., tzn. že předání bude nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů. Úřad vzal přitom v úvahu také článek 13 Úmluvy o mezinárodním civilním letectví, sjednané 7. prosince 1944 (Chicagská úmluva), publikované pod č. 147/1947 Sb., podle které musí dopravce respektovat zákony a nařízení smluvního státu, které se týkají vstupu a výstupu cestujících na území tohoto státu. V této souvislosti ve svém rozhodování Úřad zohlednil skutečnost, že letecké společnosti hodlají předávat osobní údaje svých cestujících pouze v omezeném rozsahu osobních údajů, které jsou de facto součástí cestovního dokladu a letenky; a tedy nikoliv prostřednictvím svých rezervačních a odbavovacích systémů, jak je tomu v případech předání údajů jmenné evidence cestujících (Passanger Name Record Data, PNR data). V roce 2013 byla Úřadu doručena ze strany leteckého přepravce žádost o povolení k předání PNR dat do Korejské republiky. V této věci Úřad dosud nerozhodl.

• SCHENGENSKÁ SPOLUPRÁCE

V souladu se závazky České republiky v oblasti mezinárodní spolupráce v bezpečnostní oblasti Úřad efektivně pokračoval v ustálené praxi, výměně poznatků a zkušeností týkajících se ochrany osobních údajů.

Zástupci Úřadu se stejně jako v předešlých letech i v roce 2013 účastnili pravidelných jednání a aktivit společných dozorových orgánů pro dohled nad rozsáhlými informačními systémy, jakými jsou především Schengenský informační systém, Vízový informační systém, Celní informační systém či EURODAC, který zpracovává především otisky prstů žadatelů o azyl. V souvislosti s přechodem na Schengenský informační systém druhé generace v dubnu 2013 byla ukončena činnost Společného dozorového orgánu pro SIS Evropské rady, který byl nahrazen Koordinační skupinou pro dohled nad systémem SIS II, zřízenou v rámci Úřadu evropského inspektora pro ochranu údajů, přičemž jednání této skupiny se v druhé polovině roku 2013 rovněž účastnil zástupce českého Úřadu. Bezpečnostní aspekty přechodu na nový informační systém SIS II na vnitrostátní úrovni Úřad rovněž prověřil kontrolou, která však nebyla ke konci roku 2013 pravomocně ukončena.

V roce 2013 Úřad obdržel 63 podnětů týkajících se vízové politiky České republiky, především žádosti o informace týkající se vízového řízení, žádosti o schůzky či další podněty, z kterých většina byla učiněna v anglickém jazyce, ale také v češtině, francouzštině, rumunštině, ruštině apod., přičemž na všechny Úřad odpověděl. Vzhledem k tomu, že Úřad není kompetentní podávat informace v oblasti vízové politiky České republiky, byli žadatelé odkazováni na příslušný zastupitelský úřad České republiky a na související informace a kontakty zveřejněné na webových stránkách Ministerstva zahraničních věcí, přičemž jim byla rovněž vysvětlena role Úřadu jako dozorového orgánu pro oblast ochrany osobních údajů.

Na základě uvedeného lze konstatovat, že žadatelé o víza či o související informace se v řadě případů mylně domnívají, že Úřadu jsou svěřeny pravomoci v rámci vízové politiky České republiky. Úřad je však kompetentní pouze v případě, že jsou v některém z rozsáhlých informačních systémů provozovaných v rámci schengenského prostoru osobní údaje zpracovávány neoprávněně, tedy pokud byly do určitého systému vloženy nebo jsou nadále zpracovávány v rozporu s právními předpisy, anebo jsou zpracovávány nesprávné nebo nepřesné údaje subjektu údajů, kterým může být například i žadatel o víza, jehož žádost byla zamítnuta právě z důvodu záznamu v Schengenském informačním systému (SIS). V takovém případě je subjekt údajů, vzhledem k tomu, že v České republice se uplatňuje tzv. přímý přístup k osobním údajům, oprávněn podat žádost primárně správci informačního systému, kterým je v případě SIS Policejní prezidium České republiky. V případě, že subjekt údajů kontaktuje primárně Úřad, je jeho žádost obvykle postoupena Policejnímu prezidiu České republiky. Pokud pak Policie České republiky neposkytne subjektu údajů uspokojivou odpověď nebo do 60 dnů neodpoví vůbec, je subjekt údajů oprávněn podat na Úřad stížnost na neoprávněné zpracování svých osobních údajů a tehdy mohou být uplatněny dozorové kompetence Úřadu. Příslušné formuláře i všechny informace týkající se výkonu práva na ochranu osobních údajů v oblasti schengenské spolupráce jsou zveřejněny na webových stránkách Úřadu společně s příslušnými formuláři žádostí a stížnosti.

V roce 2013 bylo Úřadu zasláno celkem 9 žádostí týkajících se zpracování osobních údajů v SIS. Jednalo se o žádosti o poskytnutí informace o zpracování osobních údajů žadatele

v národní součásti SIS ČR a žádosti o opravu či výmaz zde zpracovávaných osobních údajů. Některé žádosti byly také podány v souvislosti se zamítavým rozhodnutím v rámci vízového řízení anebo řízení o povolení k pobytu v České republice. Žádosti byly vzhledem k výše uvedenému postoupeny k vyřízení správci SIS, tedy Policejnímu prezidiu Policie ČR, o čemž byli všichni žadatelé Úřadem vyrozuměni. Úřad také poskytl několik telefonických konzultací a osobní konzultaci týkající se záznamu v SIS vloženého jiným členským státem, přičemž tato žádost byla v souladu s právními předpisy Evropské unie postoupena dozorovému úřadu odpovědného členského státu. Jedna stížnost ve věci zpracování osobních údajů v SIS byla postoupena ke kontrole inspektorovi Úřadu. Kontrola nebyla v roce 2013 ještě ukončena.

Legislativní činnost

Novou nosnou agendou v legislativní oblasti bylo v roce 2013 **zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů** (Data Protection Impact Assessment, dále jen „**DPIA**"), zavedené v roce 2012 do legislativních pravidel vlády. Po mnoha letech překotné legislativní činnosti, která mnohdy příliš nezohledňovala specifika práce s informacemi a ochrany soukromí, se v ČR v podobě DPIA konečně objevil nástroj, který připomíná gestorům přípravy právních předpisů nutnost zabývat se implementací pravidel ochrany soukromí již v návrhu záměrů a koncepcí. A to nikoliv obecnými proklamacemi o ochraně údajů s odkazem na zákon č. 101/2000 Sb., ale popisem a vyhodnocením konkrétních dopadů navrhovaných legislativních řešení v oblastech stávajících a zamýšlených zpracování osobních údajů.

V působnosti ani kapacitních možnostech Úřadu není sledovat přípravu a rozvoj všech informačních systémů, v rámci připomínkového řízení k legislativním návrhům se však snažil v těch případech, kdy mu byly materiály předloženy, postihnout klíčové aspekty zamýšleného zpracování osobních údajů a navrhnout schémata, jak k vypracování DPIA přistoupit. Pro mnohé navrhovatele právních předpisů tudíž bylo v roce 2013 mnohdy překvapením zjištění, že smyslem DPIA není vyhodnotit soulad se zákonem č. 101/2000 Sb. (ten se rozumí sám sebou, stejně jako soulad s mnoha dalšími relevantními předpisy), nýbrž povinnost explicitně konstatovat, zda navrhované úpravy zakládají nějaké nové zpracování osobních údajů; a pokud ano, pak zdůvodnit jeho nezbytnost a uvést jeho základní parametry: potřebný účel zpracování, kategorie zpracovávaných osobních údajů a klíčové části zpracování, zejména výstupy ze zpracování a lhůty pro uchování osobních údajů, se specifiky a pravidly pro dnes tolik populární zveřejňování a zpřístupňování údajů na internetu.

S ohledem na DPIA není možno akceptovat návrhy právních regulací poplatné informačním systémům, které nebyly poptány v souladu se zásadami pro práci s informacemi a ochranu soukromí (**Privacy by Design**). Praxe přitom ukazuje, že řada novel právních předpisů přijímaných v Parlamentu postrádá kvalitní odůvodnění procesů zacházení s daty, proto nezbývá než doufat, že na základě povinné DPIA začne probíhat debata o nakládání s údaji občanů v dostatečném časovém předstihu, nejlépe při zpracování věcného záměru zákonů, která poskytne jasné podklady i pro rozhodující část legislativního procesu – přijímání zákonů v Parlamentu.

Na nutnost vypracování DPIA Úřad upozorňoval zejména v případech **rejstříků (registrů, evidencí) s osobními údaji**, které veřejné úřady vedou. Právní úprava vedení řady rejstříků je stále mnohdy velmi nekonkrétní, v zákonech je často pouze obecné zmocnění k vedení rejstříku a zbývající problematika je upravena v podzákonných předpisech nebo interních směrnicích správce rejstříku, které nejsou běžně přístupné subjektu údajů. Jen omezeně lze přitom přihlédnout k novému zákonu o veřejných rejstřících právnických a fyzických osob, týkajícímu se několika vybraných databází.

Podle judikatury Ústavního soudu (např. nález sp. zn. Pl. ÚS 24/10 ze dne 22. března 2011 nebo nález sp. zn. Pl. ÚS 24/11 ze dne 20. prosince 2011), jakož i Evropského soudu pro lidská práva (např. rozsudky *Leander v. Švédsko* ze dne 26. března 1987 nebo *Amann v. Švýcarsko* ze dne 16. února 2000) je za zásah do základního práva na soukromí považováno už samo shromažďování a uchovávání osobních údajů, přičemž není rozhodné, zda zároveň dochází k jejich dalšímu zpracovávání. Samotné shromažďování osobních údajů v rejstřících vedených státní správou nebo samosprávou, zpravidla bez souhlasu daného člověka, je tedy zásahem do práva na soukromí. Pravidla pro takový zásah by pak měla být dostatečně konkrétně upravena v zákoně. Nezbytnost zákonné úpravy vedení rejstříků vyplývá přímo i z ústavních předpisů. V souladu s čl. 2 odst. 3 Ústavy lze státní moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon. V souladu s čl. 2 odst. 2 Listiny základních práv a svobod lze státní moc uplatňovat jen v případech a v mezích stanovených zákonem, a to způsobem, který zákon stanoví. V souladu s čl. 4 odst. 2 Listiny lze meze základních práv a svobod za podmínek stanovených Listinou upravit pouze zákonem.

Úřad v záležitostech rejstříků poskytoval v roce 2013 v rámci připomínkového řízení návodnou metodiku pro tvorbu legislativní úpravy konkrétního rejstříku a požadoval, aby předkladatel návrhu právního předpisu vždy ujasnil, zda bude navrhovaný rejstřík veřejně přístupný nebo nikoli. Úřad také mnohdy doporučoval, aby byl rejstřík rozdělen na veřejnou a neveřejnou část, spolu s určením, která část informací v něm obsažených bude volně přístupná. Přitom upozorňoval na povinnost jasně vyjádřit účel, pro který mají být osobní údaje dostupné, a na povinnost stanovit taková pravidla, aby údaje nebyly prezentovány v nepřesné či neaktualizované podobě. Příkladem navrhovaných zlepšení rejstříku jsou požadavky Úřadu adresované Ministerstvu průmyslu a obchodu, týkající se **živnostenského rejstříku**. Úřad v rámci návrhu na přesnější rozdělení tohoto rejstříku na veřejnou a neveřejnou část požadoval přehodnocení právní úpravy s ohledem na prokázaný právní zájem využívání údajů o podnikatelích, tj. podstatné zpřesnění zveřejňování údajů o zániku živností, zejména aby údaje o bývalých živnostnících byly po uplynutí většího časového odstupu zpřístupňovány pouze po prokázání právního zájmu individuálního žadatele. Dále Úřad doporučil zamezit zveřejňování údajů dotýkajících se více soukromí podnikatelů než jejich podnikatelské činnosti – v případech, kdy živnostník uvádí místo podnikání anebo adresu provozovny odlišné od místa bydliště či pobytu, není již nezbytné bydliště a pobyt zpřístupňovat ve veřejné části rejstříku; dále v případě, že se místo bydliště či pobytu shoduje s místem podnikání nebo adresou provozovny, nejeví se jako nezbytné uvádět informaci o tom, že se jedná rovněž o adresu bydliště daného podnikatele.

Absencí DPIA se často vyznačují i **nelegislativní agendy**, jejichž příkladem byla Národní strategie pro zdraví 2020, předložená Úřadu k připomínkám Ministerstvem zdravotnictví. Materiál v podobě ze závěru roku 2013 pouze odkazoval na zákon o zdravotních službách i existující Národní zdravotní informační systém (NZIS). Úřad upozornil na nedostatečnost vysvětlování složité

věci zahrnující zpracování citlivých údajů občanů pouze odkazy na zmiňovaný zákon. Za přijatelné řešení by Úřad považoval postup s odkazem na jiný materiál obsahující jistý přehled o tom, jak konkrétně, z jakých zdrojů a k jakým účelům (konkrétním agendám, programům, výstupům) jsou vybrané údaje používány. Takovým materiálem by mohl být transparentní dokument – kupř. politika zpracování osobních údajů zejména v rámci NZISu.

Úřad v roce 2013 Ministerstvo zdravotnictví opakovaně upozornil, že ustanovení zákona o zdravotních službách nebyla řádně odůvodněna a ve schválené podobě nedávají jasné záruky pro zákonné zpracování osobních údajů – ani nejsou navázána na základní povinnosti uvedené v zákoně č. 101/2000 Sb. (zejména: přesně definované účely zpracování, řádný zákonný titul pro konkrétní použití osobních údajů, odůvodněná přiměřená doba uchovávání). Bez popisu bližších pravidel může být opakovaně vznášena otázka pochybnosti o účelnosti celého NZIS a transparentnosti a věrohodnosti výstupů z něj.

V návaznosti na svou účast ve veřejné diskusi k přípravě návrhu **zákona o kybernetické bezpečnosti** Úřad prosadil připomínky poukazující na skutečnost, že nezbytnou zákonnou podmínkou nakládání s evidencí podle tohoto zákona bude i vedení elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly údaje shromážděné podle tohoto zákona zpracovány, včetně toho, jak dlouho a pro jaký účel byly uchovávány (nevyjímaje protokoly o likvidaci). Dokumentaci zpracování údajů používaných v boji proti kybernetickému zločinu považuje za účinné a technologicky přiměřené opatření k zabezpečení ochrany osobních údajů stanovené v § 13 zákona č. 101/2000 Sb., které vytváří podmínky pro případný dozor a vymahatelnost zákonné povinnosti zachovávat mlčenlivost.

Úřad se rovněž několikrát vyjadřoval ke zpracováním zaváděným přímo **aplikovatelnými předpisy EU** (nařízení). V případě úpravy evropských strukturálních fondů a vykazování informací o podpořených osobách bylo nemilým překvapením zjištění, že zcela chybí konkrétní pravidla pro související a evropským předpisem vyžadované zpracování citlivých údajů. V této věci Úřad odmítl stručnou novelu zákona č. 101/2000 Sb. a ve spolupráci s Ministerstvem pro místní rozvoj a dalšími ministerstvy se podílí na přípravě detailnějšího materiálu, který bude řešit zásadní otázky zpracování, včetně práce s údaji na straně příjemců dotací.

V oblasti připravované legislativy dotýkající se postavení Úřadu nedošlo v roce 2013 oproti dřívějším letům k významnějšímu posunu. V rámci opatření navazujících na přijetí kontrolního zákona, podle něhož bude Úřad od počátku roku postupovat, byl finalizován a Parlamentu předložen **návrh novely zákona o ochraně osobních údajů**. S ohledem na nové vládní zadání zabývat se souhrnně pouze otázkami bezprostředně se vztahujícími ke kontrolnímu řádu byla oproti staršímu verzím návrhu z textu vypuštěna ambiciózní část, týkající se postavení kolegia inspektorů. Postupy inspektorů v rámci kolegia (kupř. projednání námitek proti protokolu o kontrole) budou tedy jako v minulosti upraveny v rámci Úřadu vnitřními předpisy.

U jedné z největších politických priorit ČR, **zavedení systému státní služby**, vzali gestoři její přípravy na vědomí postavení nezávislých správních úřadů, tedy i Úřadu. Zatím však nedošlo k řešení širších problémů s tím souvisejích, na něž Úřad v roce 2013 upozornil. Ukázkovým případem je věc platové regulace a s tím souvisejících zohledňování počtu odsloužených let – praxe namísto osobního rozvoje (diskriminace podle věku). Zásadní otázkou navazující na téma státní služby bude pak v roce 2014 vztah nezávislých regulačních a dozorových úřadů k vládě, kupř. k ministerstvu s kompetencí pro agendu lidských práv, za situace, kdy vláda vytváří politiku k právě reformovanému evropskému právnímu rámci ochrany osobních údajů.

Styky se zahraničím a mezinárodní spolupráce

Stejně jako v předchozích letech věnoval i v roce 2013 v zahraničních agendách Úřad značnou pozornost **projednávání nového evropského právního rámce ochrany soukromí**, které probíhá téměř nepřetržitě již od ledna 2012. Vedle 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 se jedná především o 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").

Práce spojená s GDPR je obsáhlá, podobně jako byla v prvních letech 21. století příprava směrnice 2006/123/ES o službách na vnitřním trhu. K agendě GDPR se v roce 2013 konalo 18 schůzí bruselské skupiny pro výměnu informací a ochranu osobních údajů (DAPIX) a 2 schůze „přátel předsednictví" (v porovnání s rokem 2012, kdy se konalo jen 8 schůzí DAPIX). Vypracování stanovisek a pozic ČR k agendám obou připravovaných předpisů má ve své výlučné gesci Ministerstvo vnitra. Úřad připomínkoval návrhy instrukcí jak pro schůze skupiny DAPIX, tak i pro schůze „přátel předsednictví" k jednotlivým etapám projednávání GDPR. Celkem 11 schůzí DAPIX proběhlo za irského předsednictví, zbytek, včetně obou „přátel předsednictví", za litevského předsednictví EU. GDPR bylo rovněž předmětem pozornosti dalších orgánů a dne 14. února 2013 bylo dokončeno jeho první přezkoumání v Radě JHA (Justice and Home Affairs), druhé přezkoumání bylo zahájeno 12. března 2013. V Evropském parlamentu jeho gesční výbor pro občanské svobody, spravedlnost a vnitřní záležitosti (LIBE) schválil pozměňovací návrhy ke GDPR, celkem rozhodoval o 3133 pozměňovacích návrzích.

V souvislosti s přípravou GDPR dále Úřad upozornil na nutnost aktualizace a revize překladu terminologie GDPR do češtiny. S ohledem na rozsah prací, kdy dokončení GDPR bude v roce 2014 úkolem až nových orgánů EU, považoval Úřad za negativní fakt, že dosud nebyla aktualizována rámcová pozice ČR k GDPR.

Připomínky k agendě GDPR Úřad rovněž uplatnil prostřednictvím poradního orgánu Evropské komise **Pracovní skupiny pro ochranu osobních údajů**

(WP29), v jehož vedení působí předseda Úřadu. Zaměstnanci Úřadu se účastnili prací v pěti podskupinách WP29, které v roce 2013 připravovaly stanoviska nejen k výše uvedenému nařízení i směrnici, ale i k dalším otázkám, jako jsou například aktuální témata cookies a „chytrých" zařízení a přípravy na implementaci inovované evropské směrnice o opakovaném použití informací veřejného sektoru. Úřad se již tradičně účastnil i zvláštních kontrolních skupin. Příkladem je Společný kontrolní orgán Europolu, jehož činnost mj. zahrnovala kontroly v sídle Europolu v Haagu, posuzováním příkazů k založení analytických souborů a posuzováním návrhů čtyř dohod o vztazích Europolu se třetími státy; ad hoc pracovní skupina připravila dvě stanoviska k návrhu nařízení o Europolu, na které navázaly mj. přijaté pozměňovací návrhy výboru LIBE a stanovisko WP29. Obdobně zástupci Úřadu působili ve společných kontrolních orgánech k některým mezinárodním informačním systémům, především se jedná o Schengenský informační systém, Vízový informační systém, Celní informační systém či systém EURODAC.

Práce výboru k Úmluvě o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva 108) Rady Evropy (T-PD) se účastnila ve funkci místopředsedkyně tisková mluvčí Úřadu. V roce 2013 uvedený orgán dokončil práce na modernizované Úmluvě 108 a postoupil ji ad hoc vytvořenému výboru (CAHDATA), který se v současné době zabývá harmonizací Úmluvy 108 s nařízením připravovaným v rámci prací GDPR Evropskou komisí. Výbor v průběhu roku 2013 připravil komentáře k modernizované Úmluvě a připomínkoval doporučení k osobním údajům využívaným pro práci policie (včetně dotazníku rozeslanému jednotlivým úřadům pro ochranu osobních údajů členských států Rady Evropy) a expertní podklady ke strategii Rady ministrů ve vztahu k internetu a k novelizaci doporučení RE k zaměstnaneckým, zdravotnickým a biometrickým údajům.

V oblasti mezinárodní projektové spolupráce v minulém roce Úřad pokračoval v programu **Leonardo da Vinci Partnerství**. Jeho cílem je poskytnout zaměstnancům (i zaměstnavatelům) praktickou informaci o jejich právech a povinnostech při zpracování osobních údajů v souvislosti se zaměstnáváním (oficiální název akce zní „Zvýšení povědomí o ochraně dat mezi zaměstnanci pracujícími v EU"). Řešitelský tým složený z odborníků z bulharského, českého, chorvatského a polského dozorového orgánu ochrany dat dokončuje text podrobné příručky, která srozumitelně pojednává o hlavních aspektech ochrany osobních údajů a soukromí na pracovišti a jehož konečná verze bude představena v roce 2014. V rámci projektu připravují zúčastněné úřady také propagační akce, které rovněž proběhnou v roce 2014.

Experti Úřadu v zahraničních agendách dále v roce 2013 přednášeli v rámci **studijní návštěvy** kolegů z moldavského úřadu s názvem „Ochrana osobních údajů v tištěných a audiovizuálních médiích", dále v rámci expertní podpory moldavského úřadu pro ochranu osobních údajů na téma cloud computingu a ochraně dat, na konferenci European Data Forum 2013 v Dublinu na téma „Další využití informací veřejného sektoru a ochrana osobních údajů", na mezinárodní konferenci o ochraně dat v Moskvě na téma „Osobní údaje a mobilní komunikace a aplikace" a na **konferenci úřadů pro ochranu osobních údajů ze zemí střední a východní Evropy** v Bělehradě na několik témat: nezávislosti dozorových úřadů, inspekce v oblasti automatizovaného zpracování osobních dat a povinnosti zaměstnavatelů v oblasti elektronické kontroly na pracovišti.

Novou dynamickou agendou se zahraničním prvkem byla v roce 2013 spolupráce na **vyjádřeních k předběžným otázkám** (za Českou republiku), které jsou řešeny **před Soudním dvorem EU** a vztahují se k problematice ochrany osobních údajů. Úřad se začal pravidelně

účastnit měsíčních zasedání Výboru vládního zmocněnce pro zastupování České republiky před Soudním dvorem EU, která se konají na Ministerstvu zahraničí. Zatímco v minulých letech Úřad komentoval tři až čtyři předběžné otázky za rok, v posledním období počet předběžných otázek vztahujících se k problematice ochrany osobních údajů tak vzrostl, že Úřad nyní sleduje dvě až tři předběžné otázky za měsíc.

Úřad se v rámci této agendy zabýval zejména těmito problematikami: sdělování informací poplatkové dlužnici, které jsou o ní vedeny v základním rejstříku správních orgánů obce (C-486/12 X), práce soukromých detektivů (rozhodnutí C-473/12 IPI v. Geoffrey Englebert), evidence výkazů práce (rozhodnutí C-342/12 Worten v. Act), povinnost mlčenlivosti ve spojení s vnitrostátními úřady, které vykonávají dohled nad finančními službami (C-140/13 Altmann), přístup k přípravným dokumentům v rámci žádosti o azyl. Více případů se týkalo oblasti elektronických komunikací (zejm. C-293/12 Digital Rights Ireland a C-594/12 Seitlinger).

Zásadní povahy je předběžná otázka C-131/12 Google v. Costeja, k níž se ČR na základě rozhodnutí odpovědných ministerstev nevyjádřila, týkající se **práva být zapomenut** ve vztahu k informacím, které jsou umístěny na internetu, s významem jak pro stávající praxi zpracování osobních údajů, tak diskusi ohledně nového evropského nařízení (GDPR).

Bezprostředně se Úřadu dotýká řízení o předběžné otázce C-212/13 Ryneš. Jádrem věci je nainstalování průmyslové kamery, zabírající mj. veřejné prostranství, na rodinný dům, který byl předmětem útoků neznámých osob (zejména opakované rozbíjení oken). V souvislosti s uvedeným Úřad udělil pokutu za porušení pravidel pro zpracování osobních údajů v souvislosti se zabíráním veřejného prostoru kamerou a shromažďováním záznamů bez registrace požadované zákonem č. 101/2000 Sb. Předmětem posouzení Soudním dvorem EU je to, zda lze **provozování kamerového systému** umístěného na rodinném domě za účelem ochrany majetku, zdraví a života majitelů domu podřadit pod zpracování osobních údajů prováděné fyzickou osobou pro výkon výlučně osobních či domácích činností ve smyslu čl. 3 odst. 2 směrnice 95/46/ES, třebaže takový systém zabírá též veřejné prostranství. Úřad v písemné fázi zaslal Soudnímu dvoru EU vyjádření v pozici účastníka řízení.

Odlišný postoj než ministerstva formulující postoj ČR zastával Úřad v případu předběžné otázky C-293/12 Digital Rights Ireland, která se týkala problematiky elektronických komunikací a **data retention** (dle směrnice č. 2006/24/ES). ČR se v písemné fázi řízení nevyjádřila a stanovisko navrhované Úřadem tak nebylo Soudnímu dvoru EU zasláno. V závěru roku 2013 vydal generální advokát Pedro Cruz Villalón stanovisko, v němž vyjádřil názor shodný s vyjádřením Úřadu. Podle generálního advokáta by směrnice č. 2006/24/ES měla stanovit základní zásady, na jejichž základě by byly vymezeny minimální záruky upravující přístup ke shromážděným a uchovávaným údajům a jejich využívání. S ohledem na to generální advokát navrhuje, aby byly pozastaveny účinky určení neplatnosti směrnice až do doby, než unijní zákonodárce přijme opatření nezbytná k nápravě.

Úřad, sdělovací prostředky a komunikační nástroje

Každodenní servis poskytovaný médiím v roce 2013 vycházel vstříc dotazům novinářů a poskytoval odpovědi v co nejkratší lhůtě, ve většině případů v rozmezí jednoho pracovního dne. O aktuální agendě Úřadu informovaly i nadále webové stránky Úřadu, především na domácí stránce v rubrice „Novinky". Dotaz novinářů, který současně obsahoval faktické upozornění na prohřešky proti zákonu č. 101/2000 Sb. či indikoval přímo jeho porušení, se stal součástí spisové dokumentace jako podnět k šetření prováděnému Úřadem. Dá se tedy říci, že se projevilo, že i mediální scéna je na ochranu osobních údajů značně citlivá. Nicméně bylo možné zaznamenat také mediální zpochybňování postupu Úřadu. Přístup médií k aplikaci práva na ochranu soukromí a práva na přístup k informacím občas napomáhal devalvaci ochrany osobních údajů.

Tisková konference pořádaná u příležitosti Dne ochrany osobních údajů v lednu 2013 měla kromě připomínky tohoto základního lidského práva také bilanční charakter – obsah konference je trvale dokumentován tiskovou zprávou umístěnou na www.uoou.cz / Tiskové zprávy a konference, jak je ostatně u tiskových konferencí Úřadu tradiční. Tiskové konference přivádějí na Úřad standardně novináře z tištěných médií – deníků i odborně zaměřeného tisku – agenturní novináře, zástupce hlavních rozhlasových i televizních stanic. Výstupy z tiskových konferencí se jako obvykle objevily již v ranním rozhovoru s předsedou Úřadu v rozhlase i v poledním zpravodajství v den konání konference. Zatímco každý den se v denním zpravodajství objeví jedna až pět zpráv týkajících se podstatnějším způsobem ochrany osobních údajů, po tiskové konferenci v prosinci 2013 vyšlo 22 zpráv (nepočítaje krátké rozhlasové vstupy věnované tiskové konferenci prostřednictvím rozhovorů s předsedou Úřadu).

Je tudíž zřejmé, že toto zjištění hovoří ve prospěch pořádání bilančních tiskových konferencí a že každodenní informování pouze prostřednictvím webových stránek a zveřejňování ad hoc tiskových zpráv se neukázalo jako dostatečné.

Přehled nejsledovanějších případů i nejzávažnější problematiky je soustavně dostupný na webových stránkách Úřadu v rubrikách „Tiskové zprávy a konference“ a „Názory Úřadu“.

ŠÍŘENÍ ZNALOSTÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Úřad každoroční připomínku Dne ochrany osobních údajů 28. ledna využil k vyhlášení 7. ročníku soutěže pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“. Poznatky ze zaměření soutěže na přístup mladých lidí k využívání sociálních sítí – zejména Facebooku – ukázaly, že zájem o ochranu soukromí na internetu je u mládeže minimální a že nevěnuje pozornost ani minimálním zárukám, které sociální sítě pro ochranu osobních údajů nabízejí. Přitom příspěvky řady odborníků, kteří se pro Informační bulletin Úřadu otázkám mládeže a sociálních sítí věnovali, ukázaly hlubokou znalost problematiky, která ale nenachází, jak se jeví, dostatečná konkrétní řešení, např. ve školní výuce. Přesto lze s jistotou říci, že pokud se digitální gramotnost nestane součástí vzdělávacího procesu, včetně poznatků o ochraně osobních údajů a soukromí, jejich nahlížení v kontextu základních lidských práv a určujících hodnot pro svobodu jedince a občana, nelze předpokládat jakékoliv zlepšení přístupu mladé generace k sociálním sítím. Je zřejmé, že k tomuto poznatku dospívají i další evropské úřady pro ochranu osobních údajů a přijetí „Usnesení o digitálním vzdělávání“ na celosvětové konferenci komisařů ochrany osobních údajů v roce 2013 ve Varšavě je toho dokladem. V rámci svých možností Úřad podpořil společnost Europe Generation a vydání Studentského diáře, v němž publikoval základní informaci o zabezpečení osobních údajů na Facebooku. Studentský diář distribuovala společnost Europe Generation spolu s Informačním bulletinem Úřadu, který byl touto cestou nabídnut pedagogům spolu s letákem – základními informacemi o ochraně osobních údajů.

Značný byl i v roce 2013 rozsah přednáškové činnosti zaměstnanců Úřadu. Ochrana osobních údajů jako speciální právní úprava byla předmětem 33 přednášek pro státní instituce, samosprávu a podnikatelské subjekty.

Jako nová forma komunikace s odbornou veřejností se v práci Úřadu ustálilo pořádání kulatých stolů. Zástupci oborů, po nichž je vyžadováno plnění povinností ukládaných zákonem č. 101/2000 Sb., tak dostávají přímo příležitost klást otázky přítomným expertům plynoucí z jejich každodenní praxe a pro Úřad je tak dána možnost vysvětlovat své aplikační přístupy k dozoru nad dodržováním zákona č. 101/2000 Sb. V roce 2013 byly kulaté stoly věnovány tématům „Moderní trendy zabezpečovací techniky z pohledu zákona o ochraně osobních údajů“ a následně „Aktuální otázky ochrany osobních údajů ve vztahu k prevenci a vyšetřování podvodů ve společnostech“. Spolupořadatelem byla v prvním případě Asociace technických služeb Grémium Alarm (AGA), v druhém případě kancelář bnt attorneys-at-law s.r.o.

KNIHOVNA A PUBLIKACE ÚŘADU

Knihovna plní úlohu zázemí pro pracovníky Úřadu a poskytuje na individuální vyžádání též přístup odborné veřejnosti. Využívají ji studenti pro své seminární a diplomové práce dotýkající se ochrany osobních údajů. Tyto práce se povětšinou jakožto dar stávají součástí uvedené vysoce

specializované knihovny. Fond knihovny se rozrostl v roce 2013 o 37 nových titulů a rovněž o materiály z konferencí, jichž se účastnili zaměstnanci Úřadu.

V roce 2013 Úřad publikoval částky 64 až 66 svého Věstníku. Stanoviska Úřadu a jeho právní výklady jsou v této podobě určeny široké (především odborné) veřejnosti, 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. Od roku 2014 se Úřad rozhodl přejít na výhradně elektronické publikování svého Věstníku.

V roce 2013 vyšlo již výše zmíněné číslo Informačního bulletinu, které soustředilo značně širokou škálu pohledu na úskalí, kterým mladá generace čelí na sociálních sítích. Rozšíření na školy dává možnost pedagogům nahlédnout problém sociálních sítí z hlediska nejen výchovného, ale také psychologického, sociologického i z hlediska bezpečnostního.

Úřad poskytl v předcházejících letech ve spolupráci s partnerskými úřady v Polsku a Maďarsku přehled o ochraně osobních údajů zaměřený na podnikatele. Publikace vyšla za podpory z evropského programu Leonardo da Vinci. To našlo své pokračování v přípravě obdobné publikace připravované i v průběhu roku 2013 ve spolupráci s polskými, chorvatskými a bulharskými kolegy – tentokrát je publikace zaměřena na zaměstnance a ochranu jejich soukromí na pracovišti.

WEBOVÉ STRÁNKY ÚŘADU

Úřad se rozhodl vytvořit nové webové stránky, které poskytnou komplexnější vyhledávací možnosti. Začalo se na nich pracovat poté, co Úřad prostřednictvím diskusního fóra ověřil názory a potřeby uživatelů stránek a jako dodavatel byla vybrána společnost Webhouse. Kromě komfortnějšího prostorového členění stránky musí umožnit odborné i laické veřejnosti získat okamžitě soubor dokumentů zabývajících se konkrétním tématem ochrany osobních údajů. Dávají také možnost vyhledávat dokumenty dle jednotlivých aplikovaných paragrafů zákona č. 101/2000 Sb. a soustřeďovat je do jediného přehledu. Pro interní potřeby Úřadu zavádějí účelné využití redakčního a publikačního systému. Uvedeny do provozu budou v lednu 2014.

Informační systém ORG

Zákon č. 111/2009 Sb., o základních registrech, přinesl Úřadu úkol zajistit bezpečnou identifikaci občanů v systému Základních registrů prostřednictvím zdrojových a agendových identifikátorů fyzických osob.

Výsledkem tohoto požadavku je vytvoření a provoz Informačního systému ORG, který vytváří a překládá agendové identifikátory z jedné agendy do agendy druhé a vede jejich seznam.

Základní registry obsahují mimo jiné referenční údaje o občanech, právnických osobách, podnikajících fyzických osobách a orgánech veřejné moci a zjednodušují a urychlují tak komunikaci občanů s úřady.

V roce 2013 se Systému základních registrů, který je svou rozsáhlostí v Evropě ojedinělý, dostalo významného ocenění. Česká asociace manažerů informačních technologií CACIO dne 20. února 2013 vyhlásila Základní registry veřejné správy nejlepším IT projektem roku 2012. Hodnotící komise ocenila nejen přínos projektu z pohledu informačních a komunikačních technologií, ale především skutečnost, že realizace tohoto IT projektu znamená významný přínos pro běžné občany.

„Základní registry v tuto chvíli propojují na 2000 informačních systémů veřejné správy. To dělá z projektu dosud největší realizovanou kooperaci v oblasti veřejné správy. Už samotné hladké spuštění v červenci 2012 byl úspěch. Jde však o úspěch, který je pouhým základem pro další propojování datových fondů v Česku," okomentoval ocenění v červenci 2013 hlavní architekt eGovernmentu Ondřej Felix.

Na Informační systém Základních registrů na konci roku 2013 však již bylo napojeno 2700 informačních systémů veřejné správy, přes které mají koncoví uživatelé přístup k datům v základních registrech. Celý systém základních registrů běží v rutinním provozu 24 hodin denně, 7 dní v týdnu. Šíři záběru systému základních registrů představuje registrace téměř 400 agend.

Zaměstnanci Úřadu pracující v útvaru ORG se ve spolupráci s dodavatelem systému (TESCO SW) starají o bezpečný chod Informačního systému ORG (dále „IS ORG") a udržují ho v nepřetržitém provozu a tím zabezpečují vysoké nároky na trvalou dostupnost služeb. Zabezpečují administraci hardwarových prvků v datových centrech. Podílejí se na rozvoji systému a zavádění nových

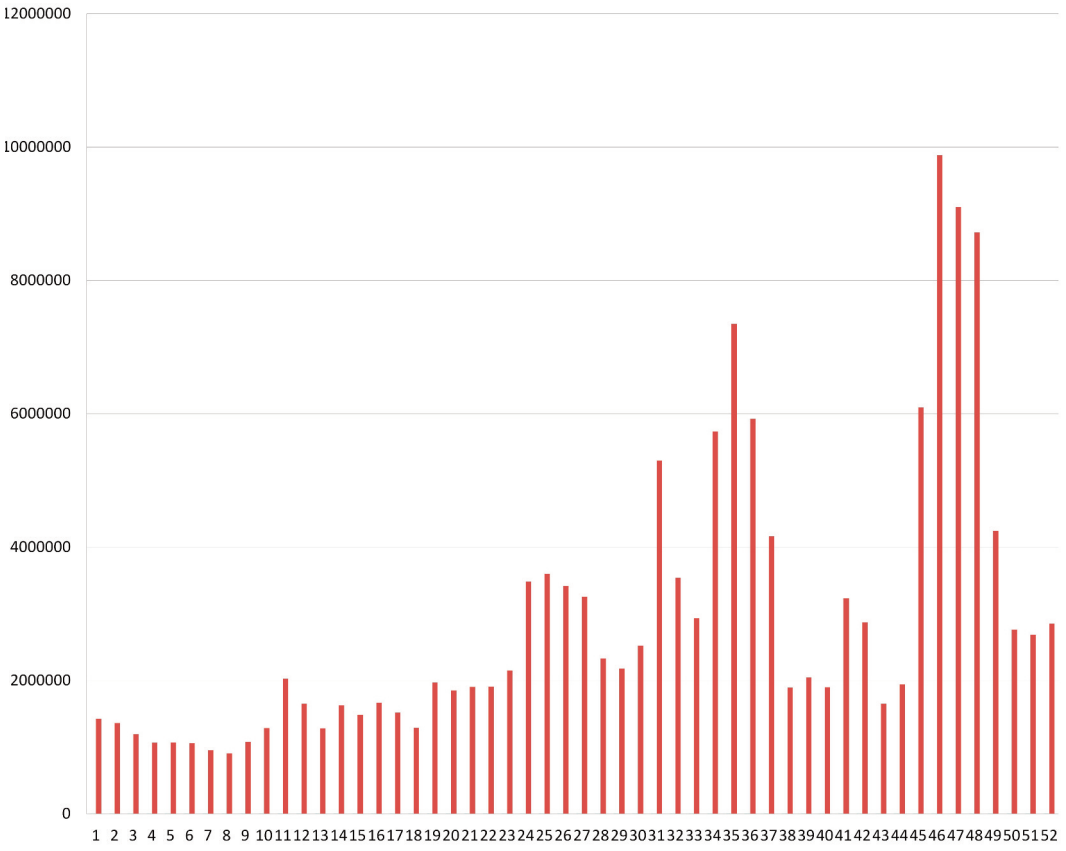
agendových skupin. Pracovníci IS ORG pravidelně vytvářejí reporty o chodu IS ORG a naplnění registru ORG daty. Tyto reporty předávají Správě základních registrů (dále „SZR").

Probíhají pravidelná školení zaměstnanců, spravujících IS ORG, pracovníky firmy TESCO SW a pracovníky SZR.

Provoz IS ORG je dokladován aplikací Service Desk, provozovanou SZR. Zde jsou zaznamenány všechny provozní požadavky a události související s provozem a rozšiřováním systému.

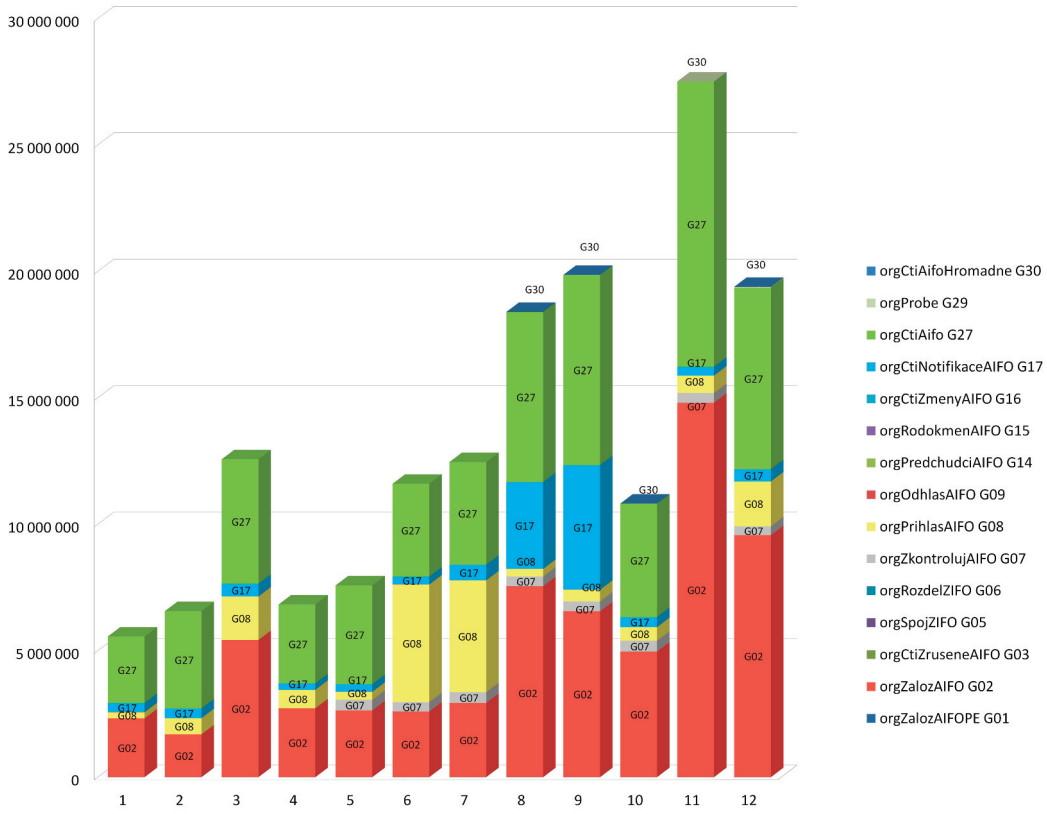
Od 1. července 2012 pracuje IS ORG v rutinním provozu a stále pozvolna narůstá počet zpracovaných transakcí. Výrazný vzestup počtu transakcí ovlivnila letošní příprava voleb. V tomto období vzrostl počet transakcí v IS ORG na trojnásobek oproti běžnému provozu. Základní registry byly využity pro vytváření volebních seznamů jednotlivých volebních okrsků. V září to bylo zhruba 20 milionů transakcí. Nejvytíženější byl systém 2. září 2013, kdy zpracoval 2 720 950 transakcí. Průměrně se měsíčně zpracuje 13 262 758 transakcí.

Týdenní počet transakcí – rok 2013



Týdenní počet transakcí IS ORG v průběhu roku.

Souhrnná měsíční statistika pro všechny AIS – rok 2013



Podrobná statistika transakcí v průběhu jednotlivých měsíců.

Pravidelně probíhá (naposled na podzim 2013) test DRP (Disaster Recovery Plan) – havarijní plán obnovy. Při testu DRP je ve spolupráci s ostatními registry a SZR odstaveno primární datové centrum a provoz systému základních registrů se přepne do sekundární lokality. Určitou dobu probíhá provoz ze sekundární lokality a následně dojde ke zpětnému přepnutí provozu do primárního datového centra. Přepnutí IS ORG oběma směry probíhalo v roce 2013 bez problémů, bez jakéhokoliv narušení funkčnosti a bezpečnosti systému a samozřejmě bez ztráty dat. Test potvrdil bezpečnost provozu i v případě, že by došlo k výpadku jednoho datového centra.

V roce 2013 probíhal audit projektu „Informační systém ORG v systému základních registrů" auditním orgánem Ministerstva financí. Výsledek tohoto auditu není ještě znám.

I v tomto roce se ředitelka Odboru základních identifikátorů věnovala publicitě Informačního systému základních registrů, a to hlavně na přednáškách a pracovních setkáních se zástupci obcí s rozšířenou působností (ORP). Hovořila o využívání základních registrů a zkušeností za rok ostrého provozu v Jihlavě, Plzni a Olomouci.

Přednášku „Zkušenosti z provozu systému ORG v rámci základních registrů" přednesla na mezinárodní vědecké konferenci Security and Protection of Information 2013 pořádané ve dnech 22.–24. května 2013 v Brně.

O zkušenostech z ročního provozu IS ORG přednášela i na konferenci IIR eGovernment.

Projekt „Optimalizace procesů ÚOOÚ“

Úřad zakončil třetí rok realizace projektu „Optimalizace procesů ÚOOÚ“, jehož cílem bylo zvýšit kvalitu a efektivitu 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 byl 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 a optimalizaci provozních, ekonomických a personálních procesů.

V rámci provozních procesů byla navržena SW podpora řízení provozních služeb – elektronizace procesů (helpdesk). Jednalo se především o zajištění autoprovozu, technických služeb a IT požadavků. Součástí optimalizace byla také úprava interní řídící kontroly.

Projekt byl ukončen 31. 8. 2013. Do projektu byli 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. Výstupy projektu byly v červnu 2013 prezentovány zástupcům státní správy z řad Českého telekomunikačního úřadu, Ministerstva financí, Národního archivu, Úřadu pro zastupování státu ve věcech majetkových, Archivu bezpečnostních složek. Jednotlivé prezentace byly zaměřeny na účastníky z oboru ekonomického, IT, personálního či na vedoucí pracovníky.

Personální obsazení Úřadu

Počet funkčních míst je Úřadu určen státním rozpočtem a je od roku 2010 stanoven na 102.

Fluktuace zaměstnanců v roce 2013 se pohybovala kolem 10 %, stejně jako v předchozím roce. Pracovní poměr uzavřelo 10 nových zaměstnanců a 9 zaměstnanců pracovní poměr ukončilo. Z toho čtyři zaměstnanci odešli do starobního důchodu, dvě zaměstnankyně na mateřskou dovolenou, jednomu inspektorovi skončilo desetileté funkční období, a proto na jeho pracovní místo byl prezidentem republiky jmenován nový inspektor.

Ke dni 1. 1. 2013 bylo v Úřadu ve stavu 99 zaměstnanců, ke dni 31. 12. 2013 byl jejich počet 100.

Průměrný evidenční přepočtený počet zaměstnanců za rok 2013 byl 99.

Úřad zaměstnával i další zaměstnance na základě uzavřených dohod o pracích konaných mimo pracovní poměr. Tito zaměstnanci převážně vykonávali odborné úzce specializované a nárazové činnosti. V roce 2013 Úřad uzavřel celkem 35 dohod o pracovní činnosti a provedení práce.

Věková struktura zaměstnanců (viz tabulka) zůstala téměř shodná jako v předchozím roce. Nejpočetnější skupinu tvořili zaměstnanci ve věku od 51 do 60 let (37 %), v roce 2012 to bylo 37,11 %.

Struktura vzdělání (viz tabulka) zůstala také téměř shodná jako v předchozím roce. Nejvyšší počet zaměstnanců Úřadu měl vysokoškolské vzdělání (63 %), a to především v oboru práva a IT, v roce 2012 to bylo 62,89 %.

Vzdělání zaměstnanců odpovídá stanoveným předpokladům a odborným požadavkům na jejich pracovní místa. Úřad umožňuje a zabezpečuje odborný rozvoj svých zaměstnanců. Zajišťuje jim prohlubování odborné kvalifikace a v případě potřeby Úřadu i její zvýšení. Umožňuje zaměstnancům navštěvovat jazykové kurzy a jazykové znalosti uplatnit při výkonu práce. Absolventům středních a vysokých škol umožňuje absolvovat odbornou praxi a tím podporovat jejich zájem o problematiku ochrany osobních údajů a vychovávat si tak nové zaměstnance.

Členění zaměstnanců ÚOOÚ podle věku a pohlaví – stav k 31. prosinci 2013

Celý soubor	muži	ženy	celkem	%
do 20 let	0,00	0,00	0,00	0,00
od 21 do 30 let	4,00	11,00	15,00	15,00
od 31 do 40 let	8,00	9,00	17,00	17,00
od 41 do 50 let	8,00	6,00	14,00	14,00
od 51 do 60 let	15,00	22,00	37,00	37,00
61 a více	13,00	4,00	17,00	17,00
Celkem	**48,00**	**52,00**	**100,00**	**100,00**

Členění zaměstnanců ÚOOÚ podle vzdělání a pohlaví – stav k 31. prosinci 2013

Celý soubor	muži	ženy	celkem	%
C – Základní	0	1	1	1,00
H – Střední odborné + VL	1	0	1	1,00
J – Střední odborné	0	1	1	1,00
K – Úplné střední všeobecné	2	7	9	9,00
L – Úplné střední odborné + VL	1	1	2	2,00
M – Úplné střední odborné	5	15	20	20,00
N – Vyšší odborné vzdělání	0	1	1	1,00
R – Bakalářské	0	2	2	2,00
T – Vysokoškolské	39	24	63	63,00
Celkem	**48**	**52**	**100**	**100**

Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 504/2012 Sb., o státním rozpočtu České republiky na rok 2013.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

	v tisících Kč
Souhrnné ukazatele	
Příjmy celkem	11 881,33
Výdaje celkem	128 731,47
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	11 881,33
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	4 380,07
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	7 501,26
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	128 731,47
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	43 787,90
Povinné pojistné placené zaměstnavatelem*)	14 805,25
Převod fondu kulturních a sociálních potřeb	425,13
Platy zaměstnanců v pracovním poměru	34 246,50
Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	8 135,00
Výdaje spolufinancované z rozpočtu Evropské unie bez SZP celkem	1 871,00
v tom: ze státního rozpočtu	265,98
podíl rozpočtu Evropské unie	1 605,02
Výdaje vedené v informačním systému program. financování EDS/SMVS celkem	17 644,03

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

1. Příjmy

Příjmy pro rok 2013 byly schváleným rozpočtem stanoveny ve výši 571 tisíc Kč, a to v souvislosti s projektem spolufinancovaným z rozpočtu EU – projektem OP LZZ „Optimalizace řídících procesů ÚOOÚ".

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů – byl naplněn částkou 11 881,33 tisíc Kč.

Jednalo se zejména o refundace zahraničních cest zaměstnanců Úřadu Europolem 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., a jiných zákonů, o náhrady nákladů řízení, o úroky z finančních prostředků uložených na bankovních účtech, o 100% refundace výdajů týkajících se komunitárního programu Leonardo da Vinci „Zvýšení povědomí o ochraně osobních údajů mezi zaměstnanci pracujícími v EU", o refundace všech výdajů projektu TAIEX, o příjmy vztahující se k roku 2012 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2012).

Úroky z finančních prostředků uložené na účtech u ČNB činily 0,01 tisíc Kč.

Přijaté sankční platby byly ve výši 6 464,48 tisíc Kč, neinvestiční dotace z EU ve výši 4 380,07 tisíc Kč, pojistné náhrady ve výši 0,52 tisíc Kč, přijaté nekap. příspěvky a náhrady týkající se minulých let ve výši 210,27 tis. Kč, převody z ostatních vlastních fondů ve výši 795,98 tisíc Kč a příjmy z prodeje ostatního hmotného dlouhodobého majetku ve výši 30,00 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

2. Výdaje

Čerpání běžných výdajů ve výši 128 731,47 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 2013 2 160,19 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 1 871,00 tisíc 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 a náhrady v době nemoci, ve výši 59 105,29 tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. 12. 2013 byl 100 zaměstnanců.

4. Výdaje vedené v informačním systému programového financování Ministerstva financí – 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 17 644,03 tisíc Kč.

V podprogramu 143V01100 „Pořízení, obnova a provozování ICT ÚOOÚ" bylo v roce 2013 čerpáno celkem 16 672,57 tisíc Kč v ***investičních a neinvestičních*** *systémově určených výdajích SR* na následující akce:

	v tis. Kč
akci 143V011000037 „Prodloužení smlouvy Enterprise na používání produktů Microsoft"	1 842,04
akci 143V011000046 „Datové centrum"	1 098,21
akci 143V011000047 „Registr – vytvoření vazby na ISZR"	319,49
akci 143V01100P005 „Provozování ICT v roce 2013"	12,56
akci 143V011000048 „IS ÚOOÚ – Úprava modulu NOS – II. etapa"	72,92
akci 143V011000049 „Optimalizace dostupnosti řešení IS ORG"	9 606,77
akci 143V011000050 „NOS – vytvoření vazby na ISZR"	231,28
akci 143V011000051 „Výroba a implementace webové služby – Hromadný překlad AIFO"	907,50
akci 143V011000052 „Technologická a techn. obnova akt. části datové sítě LAN"	742,62
akci 143V011000053 „Rozšíření spisové služby GINIS"	65,95
akci 143V011000027 „Optimalizace procesů ÚOOÚ"	1 773,23

V podprogramu 143V01200 „Reprodukce majetku ÚOOÚ" bylo v roce 2013 čerpáno celkem 971,46 tisíc Kč v ***investičních a neinvestičních*** *systémově určených výdajích SR* na následující akce:

akci 143V012000019 „Pořízení osobního vozidla – 2013"	459,96
akci 143V01200P008 „Údržba zařízení budovy a DHM – rok 2013"	511,50

Přehled čerpání rozpočtu v roce 2013

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2013 v tis. Kč	Konečný rozpočet 2013 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2013 v tis. Kč	Skutečný konečný rozpočet v %
4118	Neinvestiční převody z Národního fondu	571,00	571,00	4 282,29	749,96
4135	Převody z rez. fondů OSS	0,00	0,00	72,21	
4153	Neinvestiční transfery přijaté od EU	0,00	0,00	25,57	
2141, 2211, 2212, 2322, 2324, 3113, 4132	Ostatní nedaňové příjmy	0,00	0,00	7 501,26	

	PŘÍJMY CELKEM	571,00	571,00	**11 881,33**	**2 080,79**
501	Platy	42 409	42 421,50	42 381,50	99,91
5011	Platy zaměstnanců	34 244	34 256,50	34 246,50	99,97
5014	Platy zaměst. odvozov. od platů úst. činitelů	8 165	8 165,00	8 135,00	99,63
502	Ostatní platby za provedenou práci	2 055	2 056,40	1 406,40	68,39
5021	Ostatní osobní výdaje	1 755	1 756,40	1 406,40	68,39
5024	Odstupné	300	300,00	0,00	0,00
503	Povin. pojist. plac. zaměstnavatelem	15 118	15 122,25	14 805,25	97,90
5031	Povin. pojist. na sociál. zabezp.	11 116	11 119,12	10 864,12	97,71
5032	Povin. pojist. na veřej. zdr. pojišt.	4 002	4 003,13	3 941,13	98,45
513	Nákup materiálu	1 788	1 838,00	1 361,04	74,05
514	Úroky a ost. fin. výdaje	15	15,00	11,07	73,77
515	Nákup vody, paliv a energie	2 430	2 645,00	2 160,19	81,67
516	Nákup služeb	71 957	65 304,18	46 059,70	70,53
517	Ostatní nákupy	4 882	5 014,50	2 322,01	46,31
5171	Opravy a udržování	1 714	1 714,00	524,07	30,58
5173	Cestovné	2 300	2 372,21	1 404,05	59,19
518	Poskyt. zálohy, jistiny	0	350,00	0,00	0,00
519	Výdaje souvis. s neinv. nákupy	2 269	2 621,93	2 316,66	88,36
5342	Převody do FKSP	424	427,13	425,13	99,53
536	Ost. neinv. transf. jin. veřej. rozp.	17	54,50	48,78	81,51
542	Náhrady plac. obyvatelstvu	300	300,00	87,01	29,00
5424	Náhrady v době nemoci	300	300,00	87,01	29,00
	Běžné výdaje celkem	**143 664**	**138 170,39**	**113 384,74**	**82,06**
611	Pořízení dlouh. nehmot. majetku	4 200	5 114,30	5 114,06	100,00
612	Pořízení dlouh. hmot. majetku	11 200	10 285,70	10 232,67	99,48
	Kapitálové výdaje celkem	**15 400**	**15 400,00**	**15 346,73**	**99,65**
	VÝDAJE CELKEM	**159 064**	**153 570,39**	**128 731,47**	**83,83**

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 12. 2013.

Přehled výdajů na projekty spolufinancované z rozpočtu EU v roce 2013

v tis. Kč

Název projektu	Schválený rozpočet 2013	Konečný rozpočet 2013	Skutečnost dle účetních výkazů k 31. 12. 2013	Skutečnost/ /konečný rozpočet v %
„Optimalizace procesů ÚOOÚ“	672	1 830,55	1 773,22	96,86
Leonardo da Vinci „Zvýšení povědomí o ochraně osobních údajů mezi zaměstnanci pracujícími v EU“		72,21	72,21	100,00
TAIEX		25,57	25,57	100,00
Celkem za projekty spolufinancované z EU	672	1 928,33	1 871,00	97,02

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

V roce 2013 Úřad obdržel celkem 79 žádostí o informace. V porovnání s předchozím rokem se tak jedná o téměř stoprocentní nárůst, stejně tak jako v roce 2012 oproti roku 2011. Trend ve zvyšování zájmu veřejnosti o informace týkající se činnosti Úřadu je tak zjevný.

Z celkového počtu žádostí o informace Úřad v roce 2013 zcela vyhověl 47, ve 22 případech žádost o informace odmítl částečně a 10 žádostí o informace odmítl zcela. Mezi nejčastější důvody pro částečné nebo celkové odmítnutí žádosti o informace byla ochrana osobních údajů, které byly mezi požadovanými informacemi obsaženy, ochrana informací získaných při kontrole, které jsou chráněny zákonem uloženou povinností mlčenlivosti, či ta skutečnost, že žádost směřovala k poskytnutí informací, jimiž Úřad nedisponoval.

Rozhodnutí o částečném nebo úplném odmítnutí žádosti o informace byla celkem ve 4 případech napadena rozkladem, přičemž odvolací orgán, předseda Úřadu, rozkladu vyhověl v jednom případě a orgánu prvého stupně uložil požadované informace poskytnout v plné šíři. Postup při vyřizování žádosti o informace byl ve dvou případech rovněž napaden stížností podle § 16 a zákona o svobodném přístupu k informacím. Důvodem pro obě stížnosti byla skutečnost, že žadateli byly informace poskytnuty v jiném formátu, než který požadoval, konkrétně řečeno v případě, kdy žádost byla částečně odmítnuta a žadateli bylo zasíláno jak rozhodnutí o částečném odmítnutí žádosti, tak ty informace, kterých se rozhodnutí netýkalo, nebyly mu informace poskytnuty elektronicky na jím uvedenou e-mailovou adresu, ale byly mu spolu s rozhodnutím poslány klasickou poštou. Předseda Úřadu oběma stížnostem vyhověl a uložil prvoinstančnímu orgánu, aby i v případě, kdy rozhodnutí o částečném odmítnutí žádosti o informace zasílá klasickou poštou, žadateli, který o to požádá, dané informace poskytl na jeho

e-mailovou adresu. V dalších případech již bylo tímto způsobem standardně postupováno. Postup Úřadu při vyřizování žádostí o informace podle zákona o svobodném přístupu k informacím nebyl ani v roce 2013 předmětem soudního přezkumu, Úřadu tak nevznikly žádné související náklady.

Obsahově žádosti o informace nejčastěji směřovaly k rozhodovací praxi Úřadu. Žadatelé požadovali buď kontrolní závěry či správní rozhodnutí týkající se určité kategorie správců údajů či určité činnosti, nebo více informací v případě řízení, které Úřad zahájil z moci úřední na základě jejich předchozího podnětu. Významná část žádostí o informace se týkala hospodaření Úřadu, a to především v oblasti softwarového a hardwarového vybavení, v oblasti personální či mzdové.

Vyřizování stížností podle § 175 správního řádu

I v roce 2013 Úřad řešil stížnosti podle § 175 správního řádu. Dotčené osoby se na základě tohoto ustanovení mají právo obracet na správní orgán se stížností v případě, pokud se domnívají, že správní orgán postupoval nesprávně, nebo když došlo k nevhodnému chování úředních osob. Institut stížnosti podle § 175 správního řádu slouží k ochraně práv dotčených osob, pokud jim zákon neposkytuje jiný prostředek ochrany, čímž se myslí především odvolání a další řádné či mimořádné opravné prostředky.

V roce 2013 Úřad vyřídil celkem 41 podnětů, které byly vyhodnoceny a následně řešeny jako stížnost podle § 175 správního řádu. Z tohoto celkového počtu stížností bylo 10 posouzeno jako důvodné a 7 stížností jako částečně důvodné. Zbylých 24 stížností bylo shledáno bezdůvodnými. Celkový počet stížností v porovnání s předchozími roky tak neustále narůstá, byť se jedná o nárůst mírný.

V převážné většině stížností byl vyjádřen nesouhlas s vyřízením předchozího podnětu, který stěžovatel zaslal Úřadu a ve kterém bylo uvedeno podezření na porušení zákona č. 101/2000 Sb. V deseti případech bylo po prošetření stížnosti konstatováno, že při posuzování předchozího podnětu stěžovatele Úřad nepostupoval správně. V těchto případech byly stížnosti postoupeny buď inspektorovi Úřadu k provedení kontroly, nebo Odboru správních činností k zahájení správního řízení pro podezření ze spáchání správního deliktu či přestupku. V devíti případech se stěžovatel obrátil na Úřad se stížností proti kontrolním závěrům inspektorů Úřadu či postupu při vedení kontroly na základě podnětu, kdy tři stížnosti byly v tomto případě posouzeny jako částečně důvodné. Jedna stížnost směřovala proti postupu Registračního odboru při registračním řízení; v tomto případě nebylo shledáno porušení zákona. Příslušný útvar Úřadu byl ve všech případech o vyřízení stížnosti informován s tím, že pokud byl jeho postup shledán, byť částečně, nesprávným, byl vyzván k tomu, aby přijal opatření, která by zabránila v budoucnu opakování napadeného postupu.

Z celkového počtu 41 stížností nesměřovala ani jedna stížnost proti nevhodnému chování úředních osob. Tato skutečnost je vzhledem k množství podnětů, které Úřad během jednoho roku obdrží, velice dobrým zjištěním a je důkazem, že Úřad při vyřizování přijatých podnětů, provádění kontrolní činnosti i vedení správního řízení komunikuje s veřejností korektně a v souladu s principy dobré správy.

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2013
Úřad pro ochranu osobních údajů
Pplk. Sochora 27, 170 00 Praha 7
E-mail: posta@uoou.cz
Internetová adresa: www.uoou.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 2014 na svých webových stránkách.

Editor: PhDr. Hana Štěpánková, telefon 234 665 286
Redakční zpracování: PhDr. David Pavlát
Grafické řešení: Eva Lufferová
Jazyková korektura: Mgr. Eva Strnadová
Tisk: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno
Pro Úřad pro ochranu osobních údajů vydalo Nakladatelství MU Brno, 2014

ISBN 978-80-210-6700-4