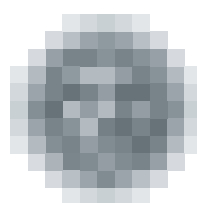


VÝROČNÍ ZPRÁVA

2010



úřad pro ochranu
osobních údajů
the office for personal
data protection

Ohlédnutí předsedy Úřadu za rokem 2010



Rok 2010 byl pro Úřad význačný jednak mezinárodním uznáním, kterého se mu dostalo tím, že se stal pořadatelem celoevropské Konference evropských komisařů ochrany dat a soukromí, jednak i tím, že otevřel druhé desetiletí svého působení, jímž posiluje základní lidské právo na ochranu soukromí v České republice.

V práci Úřadu není mnoho času na to se zastavovat a hledět zpět, zato nové úkoly, které stojí před ním, udávají rytmus jeho života. Nicméně pro jednání zmíněné mezinárodní konference jsme po zralé úvaze zvolili jako motto slogan „Hodnotit minulost, myslet na budoucnost“.

Předkládaná výroční zpráva je samozřejmě vždy svého druhu hodnocením uplynulého roku: podrobný přehled o kontrolní činnosti Úřadu, jeho správním rozhodování a přispění v oblasti legislativního procesu, rozsahu i obsahu přijímaných stížností dávají ale také tušit, v čem je třeba myslet na budoucnost. Není toho skutečně málo a čtenář této výroční zprávy si jistě utvoří svou představu. Několik věcí bych ale rád zdůraznil.

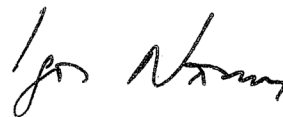
Už v loňské výroční zprávě jsem konstatoval, že je zřejmé, jak se zintenzivnilo povědomí i znalost zákona o ochraně osobních údajů. V důsledku toho ovšem na jedné straně narůstá množství dotazů, o jejichž zodpovězení občané žádají; na straně druhé instituce, firmy a společnosti nejen zákon o ochraně osobních údajů znají, ale také využívají daleko umněji. Ve vztahu ke stížnostem to pro Úřad znamená, že musí soustředit svou konzultační činnost ryze na kompetenci ukládanou mu zákonem o ochraně osobních údajů a v přesahujících ji žádostech odkazovat občany na příslušné jiné právní normy. Ukazuje se totiž, že jinak už nelze stále narůstající stížnostní a konzultační agendu časově ani personálně zvládnout. V souvislosti s uvedeným využíváním zákona o ochraně osobních údajů dospíváme k poznání, že nabývá na naléhavosti otázka společenské odpovědnosti institucí a firem, zejména při jejich požadování souhlasu se zpracováním osobních údajů subjektů údajů.

Nepochybně zázemím pro řešení uvedeného problému se stane řada českých právních norem, k nimž se Úřad v uplynulém roce vyjádřil; na stole našich legislativců však jsou i další závažné právní dokumenty, k nimž bude své připomínky z hlediska ochrany osobních údajů Úřad uplatňovat. Na jeho rozhodování budou mít bezpochyby vliv i zásadní mezinárodní právní normy – směrnice Evropského parlamentu a Rady 95/46/ES a Úmluva 108 Rady Evropy –, které za velmi aktivní účasti českého Úřadu procházejí novelizací. V tomto ohledu mohu takřkajíc přijít s informací od pramene, vzhledem k tomu, že jsem v uplynulém roce byl zvolen do funkce místopředsedy poradního orgánu pro ochranu osobních údajů Evropské komise, pracovní skupiny WP29.

Stranou naší pozornosti nezůstávalo a nebude zůstat ani šíření znalostí o ochraně osobních údajů – už tradičně mezi mladou generací, ale také na základě v roce 2010 získaných zkušeností bližší spolupráce s různými institucemi, o nichž rovněž vydáváme počet na následujících stránkách.

Rád bych ještě zdůraznil: Z detailů a jednotlivých zkušeností, o nichž výroční zpráva za poslední roční období předkládá informace, dovozujeme další směřování v ochraně osobních údajů, které je stále indikátorem kvality vyspělých demokracií. A pokud nedojde k naprosté změně paradigmatu civilizace, v níž je soukromí základní hodnotou a ukazatelem svobody každého občana, pak se bude ochrana osobních údajů i nadále vyvíjet tak, aby dokázala z právního hlediska dokonaleji reflektovat nové technologie i technické nástroje, které by občanům měly sloužit, aniž by se staly božstvem a ovládly jejich životy.

Takovému vyvoji přispěje i český Úřad. Nepochybuji o tom, protože znám kvality jeho pracovníků i atmosféru, v níž pracujeme. V tomto smyslu nemohu než zopakovat, co už jsem nejednou řekl: Jsme jeden tým. Na tom faktu se nezměnilo nic ani s příchodem dvou nových inspektorů, kteří zaujali místo po těch, jimž vypršel desetiletý mandát. Do příštího roku hledím s nadějí, že v pozitivním klimatu Úřadu nedojde ke změně ani volbou dalších pěti inspektorů, o níž v příštím roce rozhodne Senát Parlamentu ČR a prezident České republiky.



Igor Němec

OBSAH

ÚŘAD V ČÍSLECH 2010	8
KONTROLNÍ ČINNOST ÚŘADU	10
■ KONTROLNÍ PLÁN PRO ROK 2010	10
I. Obecná témata pro zaměření kontrolní činnosti inspektorů Úřadu	10
1. Informační systémy veřejné správy	10
2. Informační systémy v oblasti soukromoprávní	10
3. Informační systémy v oblasti justice	11
4. Dodržování podmínek při předávání osobních údajů do třetích zemí	11
5. Ochrana osobních údajů subjektu údajů v krizových situacích	11
II. Plánované a kontrolně ukončené aktivity vyplývající z kontrolního plánu pro rok 2010	11
1. Kontrola Krajského státního zastupitelství v Hradci Králové	11
2. Kontrola subjektu Královéhradecký kraj	12
3. Kontrola zpracování osobních údajů hotelových hostů	13
4. Kontrola zpracování osobních údajů v informačních systémech Pražské správy sociálního zabezpečení	14
III. Kontrolní a dozorová činnost 2010 – její podmínky a zobecňující závěry	16
■ POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI	18
Osobní údaje v rezortu zdravotnictví	18
Opencard	22
Matriky studentů, zveřejňování údajů studentů vysokých škol	23
Matrika studentů	26
Obsah e-mailové schránky	27
Zpracování osobních údajů prostřednictvím kamerových systémů	28

Nebankovní subjekty	32
Kontrola společenství vlastníků bytů	35
Aplikace zákona o ochraně osobních údajů v kynologii	36
Nevyžádaná obchodní sdělení	37
■ VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ	39
■ POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ	41
Povaha řízení podle § 17 zákona o ochraně osobních údajů	41
Několik poznámek k pojmu osobní údaj	42
Několik poznámek k povinnosti zpracovávat pouze přesná data	42
Zpracování osobních údajů v souvislosti s vrácením kreditu z předplacené telefonní karty	43
Služba Street View	44
■ REGISTRACE	46
Povaha registrace při další činnosti Úřadu	46
Okruhy zpracování řešené v rámci registračního řízení	47
■ PŘEDÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ	49
LEGISLATIVNÍ ČINNOST	52
STYKY SE ZAHRANIČÍM A MEZINÁRODNÍ SPOLUPRÁCE	56
ÚŘAD, SDĚLOVACÍ PROSTŘEDKY A KOMUNIKAČNÍ NÁSTROJE	59
Kontakty s médii	59
Webové stránky Úřadu	60
Šíření znalostí o ochraně osobních údajů	60
Knihovna a publikace Úřadu	61
SPOLUPRÁCE S INSTITUCEMI	62
Spolupráce s Americkou obchodní komorou	62
Spolupráce s Českým telekomunikačním úřadem	62
Spolupráce s Českou poštou	62
Spolupráce se Svazem měst a obcí	63

INFORMAČNÍ SYSTÉM ORG	64
PERSONÁLNÍ OBSAZENÍ ÚŘADU	66
HOSPODAŘENÍ ÚŘADU	67
POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ	73

ÚŘAD V ČÍSLECH 2010

Dotazy a konzultace	dotazy ČR	2 451
	zahraničí	91
	konzultace	
	státní správě	75
	samosprávě	142
	právníkům osobám	317
	fyzickým osobám podnikajícím	219
	fyzickým osobám	1 371
Podání a stížnosti	přijaté podněty dle zákona o ochraně osobních údajů	1 039
	stížnosti předané ke kontrole	161
Nevyžádaná obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	2 834
	vyřešených podnětů	1 525
	zahájených kontrol	163
	ukončených kontrol	144
	správních rozhodnutí o pokutě	96
Kontroly (vyjma kontrol týkajících se zákona č. 480/2004 Sb.)	zahájeno	106
	ukončeno	106
	předáno jiným státním úřadům	2
	napadeno námitkami	17
	námitkám vyhověno	0
	nevyhověno	8
	převážně vyhověno	3
	převážně nevyhověno	5
Správní trestání (Pozn.: * z toho k § 17)	správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb.	113
	přestupková řízení podle zákona č. 101/2000 Sb.	38
	správní a přestupková řízení podle zákona č. 101/2000 Sb. – § 44a, 45a	5
	přestupková řízení podle zákona č. 159/2006 Sb., o střetu zájmů	0
	rozklady napadená rozhodnutí o porušení zákona	46
		(2*)
	zamítnutých rozkladů	23
	zrušeno a vráceno k novému projednání	9
	zrušených rozhodnutí a zastaveno řízení	6
	změna rozhodnutí	7
Soudní přezkum (Pozn.: ** celkem od r. 2001)	podaných žalob k soudu	18 (81**)
	zamítnutých žalob soudem	7
	zrušených rozhodnutí soudem	6

	postoupení k vydání rozhodnutí (podle § 21 zákona č. 101/2000 Sb.)	0
	ukončených/neukončených soudních řízení	3/15 (39/42**)
Registrace	přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.)	4 037
	zaregistrovaná zpracování	3 576
	dosud v řízení	742
	zrušené registrace	119
	oznámení o změně zpracování	906
	řízení podle § 17 (zákon č. 101/2000 Sb.)	
	zastaveno (nedochází k porušení zákona)	64
	zastaveno z procesních důvodů (např. oznámení vzato zpět)	6
	nepovoleno	3
Povolení k předávání osobních údajů do zahraničí	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	22
	přijatých rozhodnutí o povolení předávání	18
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	2
Stížnosti podle § 175 správního řádu	přijatých stížností	34
	vyřízených jako důvodné	5
	vyřízených jako částečně důvodné	3
	vyřízených jako bezdůvodné	25
Stížnosti a jiné podněty na postup Úřadu, které nebyly řešeny podle § 175 správního řádu	došlých podnětů	0
	vyřízených jako oprávněné	
	vyřízených jako neoprávněné	
Žádosti podle zákona č. 106/1999 Sb.	přijatých žádostí	20
	vyřízených žádostí	15
	odmítnutých žádostí	4
Publikované materiály	Věstník Úřadu (počet částek)	3
	Bulletin Úřadu (počet čísel)	1
Tiskové konference	pravidelné	2
	mimořádné	0
Připomínkované legislativní návrhy	zákony	59
	prováděcí předpisy	0
	návrhy nařízení vlády	21
	návrhy vyhlášek	64
	ostatní	58
	zahraniční materiály	39

KONTROLNÍ ČINNOST ÚŘADU

Úřad pro ochranu osobních údajů (dále v celé výroční zprávě jen „Úřad“), který byl primárně zřízen jako nezávislý dozorový orgán podle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále v celé výroční zprávě jen „zákon o ochraně osobních údajů“), provádí kontrolní činnost na základě kontrolního plánu a na základě podnětů a stížností osob, které se na něj přímo obracejí a ve svých podáních upozorňují na porušování povinností odpovědných osob.

■ KONTROLNÍ PLÁN PRO ROK 2010

I. OBECNÁ TÉMATA PRO ZAMĚŘENÍ KONTROLNÍ ČINNOSTI INSPEKTORŮ ÚŘADU

1. INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

V návaznosti na dosud provedená kontrolní zjištění se kontrolní aktivity inspektorů i v roce 2010 zaměřovaly na dodržování povinností při zpracovávání osobních údajů v oblasti veřejné správy. Tyto záměry se týkaly jak státní správy (například dopravní informační systém, informační systém vytipované zdravotní pojišťovny, fungování důchodového systému, respektive státní správy v oblasti důchodového zabezpečení), tak, a to zejména, oblasti samosprávy (vytipován byl krajský a městský úřad), kde vždy s nástupem nových úředníků dochází ve zpracovávání osobních údajů k problémům – ochrana osobních údajů je přehlížena a podceňována, preferováno je například právo na přístup k informacím, nedbá se na povinnosti ochrany osobních údajů, které jsou součástí spisové dokumentace apod.

2. INFORMAČNÍ SYSTÉMY V OBLASTI SOUKROMOPRÁVNÍ

I když ve srovnání se systémy veřejnoprávními nejsou systémy soukromoprávní tak rozsáhlé a propojené, i zde se očekával další rozvoj technologií, podporujících zpřístupňování informací, a to zejména v oblasti, kde fyzická osoba – subjekt údajů vystupuje jako spotřebitel, klient, pacient apod. Nezbytným se proto ukázalo sledování dalšího vývoje právní úpravy a realizace již schválených právních podmínek pro provoz velkých registrů a databází, jako je například zpracovávání osobních údajů

v souvislosti s provozem datových schránek fyzických osob Českou poštou. V návaznosti na možnou kontrolu systému důchodového zabezpečení bylo záměrem kontrolního plánu prověřit zpracovávání osobních údajů v oblasti pojišťovnictví. Na základě aktuálních poznatků o způsobu používání RFID technologií při komunikaci prostřednictvím elektronických karet se kontrolující zaměřili na další typ městské nebo studentské karty.

3. INFORMAČNÍ SYSTÉMY V OBLASTI JUSTICE

V návaznosti na dosavadní vývoj informačních systémů e-justice se stále objevují některé otázky a problémy týkající se zpřístupňování a výměny dat, které jsou v těchto registrech zpracovávány. Nejde jen o oblast soudnictví. Úřad se zaměřil také na další související problémy, které se týkají práv a povinností při zpracovávání osobních údajů všech subjektů, které v této oblasti působí. Zajisté základní právní úprava vytváří dostatečné právní záruky pro to, aby nedocházelo k excesům, přesto je třeba zmapovat oblast zejména s ohledem na dodržování povinností podle § 13 zákona o ochraně osobních údajů.

4. DODRŽOVÁNÍ PODMÍNEK PŘI PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO TŘETÍCH ZEMÍ

Stejně jako v roce minulém se Úřad i v roce 2010 zabýval aktuálními problémy praktického naplňování podmínek pro tok dat mimo území České republiky a EU. Často jsou totiž deklarována pravidla, tzv. „Binding corporate rules“, ale následná kontrola dodržování těchto pravidel ze strany odpovědného subjektu zatím nebyla předmětem kontroly. Tento záměr Úřadu byl o to obtížnější, že zde bude muset být navázána spolupráce s dalším úřadem nebo subjektem, který je garantem pro naplnění obecně platných povinností na území jiného státu.

5. OCHRANA OSOBNÍCH ÚDAJŮ SUBJEKTU ÚDAJŮ V KRIZOVÝCH SITUACÍCH

Po zkušenostech z minulého období se ukázalo jako potřebné i do budoucna sledovat způsob zpracovávání osobních údajů osob v obtížných životních nebo krizových situacích. Lidé jsou často pod tlakem momentální situace a nemohou nebo se nedokážou ubránit intenzivnímu zásahu do soukromí. I když právní úprava přinesla významné změny zejména ve prospěch soukromí nezletilých osob, je třeba mít neustále na mysli, že je třeba ve vztahu k uvedeným okolnostem kontrolní působnost Úřadu uplatňovat i preventivně.

II. PLÁNOVANÉ A KONTROLNĚ UKONČENÉ AKTIVITY VYPLÝVAJÍCÍ Z KONTROLNÍHO PLÁNU PRO ROK 2010

1. KONTROLA KRAJSKÉHO STÁTNÍHO ZASTUPITELSTVÍ V HRADCI KRÁLOVÉ

V termínu stanoveném kontrolním plánem byla provedena kontrola v Krajském státním zastupitelství v Hradci Králové. Bylo prověřeno dodržování všech relevantních povinností stanovených zákonem o ochraně osobních údajů a zákonem č. 133/2000 Sb., k jejichž kontrole je Úřad příslušný při zpracování osobních údajů osob zúčastněných na trestním řízení.

Tyto údaje Krajské státní zastupitelství zjišťuje z dokumentů, nebo vytváří vlastní činností, vkládá do rejstříků a evidenčních pomůcek, uchovává a dále používá; používání zahrnuje ověřování aktuálních hodnot. Tyto operace jsou organizačně uspořádány podle ustanovení věcně příslušných předpisů a jsou založeny na vedení spisové dokumentace a na automatizovaném zpracování v interním systému ISYZ; operace zahrnují používání osobních údajů vně vedení příslušné aplikace. ISYZ – Informační systém pro státní zastupitelství – je počítačový informační systém pro vedení evidencí stanovených státnímu zastupitelství právním předpisem, tj. i všech rejstříků a vybraných evidenčních pomůcek. Obsah ISYZ je dán kancelářským řádem. Systém zahrnuje propojení na informační

system evidence obyvatel. Pro zjišťování již zpracovaných osobních údajů je stanoven přesný postup. Rovněž Centrální evidence stíhaných osob (dále jen „CESO“) je elektronickým datovým souborem osobních údajů. V CESO se evidují vybrané údaje z trestního řízení včetně osobních údajů obviněných nebo podezřelých. CESO je centrálně spravovanou databází s třívrstvou architekturou. Databázový server spravuje Nejvyšší státní zastupitelství České republiky. V obvodu působnosti Krajského státního zastupitelství je přístup do CESO výlučně přes ISYZ; databáze CESO potřebné údaje samočinně přebírá. Krajské státní zastupitelství má přístup do CESO pouze pro povolené vkládání dat a dotazů nezbytných pro výkon působnosti státního zastupitelství. Tato zjištění platí pro všechna státní zastupitelství v České republice.

V prověřovaném vzorku záznamů CESO nebyly u Krajského státního zastupitelství v Hradci Králové zjištěny žádné známky navozující pochybnost o důsledném dodržování parametrů stanovených zákonem o ochraně osobních údajů. Ke všem auditním záznamům existuje odpovídající spisová dokumentace a u všech byl proveden záznam do spisu podepsaný oprávněným uživatelem. Obecná opatření k zabezpečení osobních údajů jsou stanovena především v normativních dokumentech; na kancelářský řád navazují aplikačně zaměřené dokumenty, které zavádějí specifická bezpečnostní opatření pro jednotlivé datové soubory, a to buď na rezortní úrovni (pokyny obecné povahy nejvyššího státního zástupce), nebo na úrovni krajského státního zastupitelství (pokyny krajské státní zástupkyně). Krajská státní zástupkyně mj. rozhodla o provádění kontroly záznamů přenášených z ISYZ do CESO.

2. KONTROLA SUBJEKTU KRÁLOVÉHRADECKÝ KRAJ

V termínu stanoveném kontrolním plánem byla provedena kontrola v Královéhradeckém kraji. Prověřována byla zpracování osobních údajů při výkonu státní správy v přenesené působnosti a při výkonu samostatné působnosti kraje, tedy údajů účastníků správních řízení, jejich vazebních osob a dalších dotčených osob, získávaných přímo od subjektu údajů prostřednictvím formulářů nebo z korespondence, stejně jako takové údaje získávané z informačního systému evidence obyvatel nebo jiného seznamu vedeného pro úřední potřebu a zpracování osobních údajů zaměstnanců Královéhradeckého kraje a osob vstupujících do objektu Královéhradeckého kraje. Rovněž tato kontrola sledovala dodržování všech relevantních povinností stanovených zákonem o ochraně osobních údajů a zákonem o evidenci obyvatel. Bylo při ní přímo použito sedmnáct dalších předpisů upravujících zpracování osobních údajů, např. správní řád, zákon o archivnictví a spisové službě, zákon o lesích a zákoník práce.

Královéhradecký kraj zpracovává osobní údaje formou elektronických datových souborů v jednácti síťových aplikacích v lokální počítačové síti a čtyřech aplikacích provozovaných samostatně. K jednotlivým aplikacím jsou – s výjimkou technických systémů určených ke sledování objektu – současně vedeny listinné datové soubory nebo listinná spisová dokumentace. Ve dvojí roli působí kraj při zpracování osobních údajů informačního systému evidence obyvatel: Jednak podle § 3 zákona o evidenci obyvatel zapisuje do informačního systému evidence obyvatel údaje o fyzických osobách, které nabyly nebo pozbyly státní občanství, jednak je uživatelem údajů z tohoto systému o občanech přihlášených k trvalému pobytu ve správním obvodu kraje. Využívání bylo prověřeno za použití spisové dokumentace krajského úřadu a auditních záznamů pořizovaných Ministerstvem vnitra. Nebyl zjištěn žádný dotaz poukazující na nesplnění podmínky použití pouze ve věcech, které jsou evidovány u Krajského úřadu Královéhradeckého kraje. Při zpracování osobních údajů pro jednotlivé účely a podle jednotlivých zvláštních zákonů byly zjištěny nedostatky pouze při zabezpečení osobních údajů.

V rámci automatizovaného zpracování osobních údajů bylo u Královéhradeckého kraje zjištěno pořizování *ad hoc* elektronických záznamů, které umožňují určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zpracovány v úplnosti ke třem aplikacím, pouze pro evidenci přístupu a ke změnám ve zpracovávaných osobních údajích ve dvou dalších aplikacích používaných shodně ke zpracování osobních údajů vlastních zaměstnanců, pouze pro evidenci přístupu ve dvou drobnějších aplikacích a nejsou pořizovány u devíti identifikovaných samostatných, nebo relativně samostatných zpracování osobních údajů prováděných za specifickým účelem.

Pro posouzení postupu Královéhradeckého kraje podle tohoto ustanovení zákona o ochraně osobních údajů se na zjištěný stav pohlíží tak, že požadované záznamy jsou pořízeny i tehdy, pokud je pořídilo Ministerstvo vnitra (ISEO) za součinnosti kontrolovaného spočívající ve vedení údajů ve spisu. Obsah spisu, počínaje spisovým přehledem a konče vloženým tiskovým výstupem nebo rukopisným záznamem o lustraci, jednoznačně vypovídají o účelu vyhledávání – pokud ten není zřejmý ze záznamu samotného, je doplněn provozní údaj, který o účelu vyhledávání v užším smyslu slova vypovídá. Pro tyto záznamy je rozhodné, že kontrolovaný zajistil řádné dokumentování prověřovaného zpracování a učinil tak s vědomím, že zpracování osobních údajů v ISEO je auditováno. Prověřování není pracovně náročné a umožňuje prověřit důvod vyhledávání v ISEO ve všech případech bez opětovného zadání identického dotazu.

Pouze u aplikace Katastr nemovitostí lze s přihlédnutím k veřejné dostupnosti těchto údajů od auditování přístupu upustit. U zbývajících třinácti aplikací je třeba přihlédnout k dostupnosti listinné části zpracování; pro dvě aplikace se s ohledem na konkrétní podmínky Královéhradeckého kraje záznamy podle ustanovení § 13 odst. 4 písm. c) zákona o ochraně osobních údajů považují společně se záznamy k dalším třem systémům za pořizované v míře splňující požadavky zákona. Zjištěný stav byl vyhodnocen jako porušení povinnosti kontrolovaného podle ustanovení § 13 odst. 1 a odst. 4 písm. c) zákona o ochraně osobních údajů.

Krajský úřad zveřejňuje informace podle § 18 odst. 2 zákona o ochraně osobních údajů; informace zveřejněné ke dni zahájení kontroly nebyly veřejně dostupné v rozsahu vyplývajícím ze zákona, chyběly jakékoli informace o docházkovém a přístupovém systému. Povinnost nebyla použita na kamerový systém, který Královéhradecký kraj předem oznámil Úřadu podle § 16 zákona o ochraně osobních údajů.

K nápravě zjištěných nedostatků byla uložena tři opatření; správní řízení nebylo do konce roku 2010 zahájeno.

3. KONTROLA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ HOTELOVÝCH HOSTŮ

Kontrola se zaměřila na zpracování osobních údajů hostů v kontextu ustanovení § 101 zákona č. 326/1999 Sb., o pobytu cizinců na území České republiky, které ukládá povinnost ubytovateli vést evidenční knihu a uchovávat ji po dobu 6 let od posledního zápisu; a dále v souladu s odst. 1 tohoto ustanovení, v němž je uveden rozsah osobních údajů, které se do evidenční knihy zapisují: jméno a příjmení ubytovaného cizince, den, měsíc a rok narození, státní občanství, číslo cestovního dokladu, počátek a konec ubytování.

V případě, že se jedná o lázeňský nebo rekreační pobyt v lázeňských místech a v místech soustředěného turistického ruchu za účelem léčení nebo rekreace, či o poplatek z ubytovací kapacity, je-li vybírán, podle zákona č. 565/1990 Sb., o místních poplatcích, je ubytovatel povinen vést v písemné podobě evidenční knihu, do které zapisuje dobu ubytování, účel pobytu (účel a doba se neeviduje v knize u poplatku z ubytovací kapacity), jméno, příjmení, adresu místa trvalého pobytu nebo místa trvalého bydliště v zahraničí a číslo občanského průkazu nebo cestovního dokladu fyzické osoby, které ubytování poskytl. Zápisy do evidenční knihy musí být vedeny přehledně a srozumitelně. Tyto zápisy musí být uspořádány chronologicky. Evidenční knihu ubytovatel uchovává po dobu 6 let od provedení posledního zápisu.

V případě, že se nejedná o lázeňská nebo rekreační místa, je nutné vyjít pouze ze smluvního vztahu. Pro vznik smlouvy je nutné jednoznačně identifikovat smluvní stranu – hosta. Z uvedených osobních údajů uvedených v knize hosta vede k jednoznačné identifikaci jméno, příjmení a číslo občanského průkazu. Ostatní údaje (datum narození) nejsou tudíž nezbytné a neměly by být součástí údajů, zpracovávaných pro účely identifikace hosta pro případ trestného činu či přečinu zjištěného po odchodu hosta. Pro účely klientely stálých hostů jsou tyto údaje dostačující. Tento způsob je z hlediska ochrany osobních údajů vyhovující, protože číslo občanského průkazu je sice jednoznačně identifikující, ale pouze v součinnosti s policií.

K nadbytečnosti čísla občanského průkazu by došlo tehdy, pokud by byl český občan – host identifikován adresou svého trvalého bydliště (obec, jméno ulice a číslo popisné), což nebyl případ kontrolovaného subjektu. Identifikaci v tomto případě by pak tvořilo jméno a příjmení, datum narození a trvalé bydliště.

Pokud jde o dobu, po kterou mohou být údaje v případě českých občanů v knize hostů uchovávány – a když na ubytovatele nedopadá jeden ze dvou výše uvedených poplatků podle zákona č. 565/1990 Sb., o místních poplatcích – je zde určující občanský zákoník, který v ustanovení § 101 stanovuje obecnou tříletou promlčecí dobu pro výkon práva. Tato doba by neměla být v případě tuzemců překračována, výjimkou jsou pouze případy, kdy je zahájeno řízení, jehož účastníky jsou Společnost a host.

Mnohem problematičtější se ovšem jeví zpracovávání osobních údajů doprovázejících osob, tj. osob, které sice mají v úmyslu bydlet v hotelu, ale smlouva na pronájem jejich pokoje je uzavřena s někým jiným, neboť není jasný účel tohoto zpracování. Uváděný důvod, že hotel má právo vědět, kdo u hosta přespává, se nezdá být dostatečným právním důvodem zpracovávání těchto osobních údajů.

Podle ustanovení § 5 odst. 2 zákona o ochraně osobních údajů lze zpracovávat osobní údaje pouze se souhlasem nebo na základě zákonné výjimky, přičemž pro doprovázející osoby výjimka neexistuje. Lze tudíž použít pouze titul souhlasu, ten ovšem musí být dobrovolný, a tudíž jím nemůže být podmíněna služba ubytování. Pokud by se už tyto údaje se souhlasem zpracovávaly, je doba jejich uchovávání jiná, neboť se nejedná o osoby, se kterými byla uzavřena nějaká smlouva, ale pouze o osoby, které v hotelu přespaly. Tudíž by údaje o nich měly být při odchodu a kontrole pokoje vymazány.

Na základě výsledků kontroly hotelu byla uspořádána schůzka se společností HORES PLUS, s. r. o., která jako jeden z majoritních dodavatelů zajišťuje software pro zpracování osobních údajů hostů v hotelech; při jednání bylo mj. domluveno, aby:

System vyžadoval jako povinné vyplnění pouze těchto údajů: jméno (Novák), datum příjezdu a odjezdu, státní příslušnost, počet pokojů. Pro další osoby, které neplatí za ubytování, systém umožňuje jejich evidenci pouze označením +1 a státní příslušností.

Osobní údaje jsou nejdříve systémem zpracovány při rezervaci, následně dochází při ubytování k rozšíření rozsahu zaznamenávaných osobních údajů, při odjezdu hosta se údaje překlápí do „Banky hostů“ a archivu. Do Banky hostů by měly být osobní údaje hostů předávány pouze s jejich souhlasem. Osobní údaje hostů by neměly být zpracovávány ani v archivu déle než 6 let od poslední návštěvy.

Bylo zavedeno logování přístupu oprávněných osob nejen do archivu, ale také do Banky hostů, speciálně do položky vlastnosti, neboť do této položky by mělo být vstupováno pouze tehdy, pokud si host stěžoval nebo naopak projevil znovu zájem o ubytování.

Pro využití databáze pro marketing lze používat dle ustanovení § 5 odst. 5 zákona o ochraně osobních údajů pouze jméno, příjmení a adresu, ostatní osobní údaje pouze se souhlasem hosta. Statistiky dle vlastností by měly být dělány pouze hromadně, tj. pomocí programů, k profilování jednotlivých hostů bez jejich souhlasu není zákonný podklad.

4. KONTROLA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V INFORMAČNÍM SYSTÉMU PRAŽSKÉ SPRÁVY SOCIÁLNÍHO ZABEZPEČENÍ

Jedna z kontrol se týkala dodržování povinností vyplývajících z ustanovení Hlavy II zákona o ochraně osobních údajů územním pracovištěm Pražské správy sociálního zabezpečení (dále jen „ÚP PSSZ“) při zpracování osobních údajů pojištěnců nemocenského pojištění. Účel a rozsah zpracování osobních údajů určuje zákon č. 187/2006 Sb., o nemocenském pojištění, OSSZ při provádění pojištění zaměstnaných osob a osob samostatně výdělečně činných plní úkoly stanovené tímto zákonem orgánů nemocenského pojištění, pokud nejde o úkoly, které plní česká správa sociálního zabezpečení. Úkoly okresních správ sociálního zabezpečení stanoví § 84 tohoto zákona. Způsoby zpracování osobních údajů, druhy operací k dosažení stanoveného účelu závazně určuje Česká správa sociálního zabezpečení. Podle § 120 odst. 4 zákona č. 187/2006 Sb. mohou orgány nemocenského pojištění vést evidenci o fyzických osobách pro účely tohoto zákona podle jejich rodných čísel. Výčet osobních údajů tento

zákon stanoví v § 122. ÚP PSSZ využívá datovou základnu informačních systémů pojištění. Data jsou průběžně shromažďována z titulu plnění úkolů ČSSZ a okresních správ sociálního zabezpečení jako orgánů nemocenského pojištění podle §§ 84 a 85 a násl. zákona č. 187/2006 Sb., a to v rozsahu věcné a místní příslušnosti podle §§ 82 a 83.

Zákon č. 187/2006 Sb. upravuje nemocenské pojištění pro případ dočasné pracovní neschopnosti, nařízené karantény, těhotenství a mateřství a ošetřování člena domácnosti nebo péče o něj a organizaci a provádění pojištění. Prováděním pojištění se rozumí též posuzování zdravotního stavu pro účely pojištění (§ 1 odst. 1). Podle § 120 a násl. tohoto zákona údaje shromažďované orgány nemocenského pojištění pro účely provádění pojištění tvoří datovou základnu informačních systémů pojištění. Jednotlivé orgány jsou oprávněny shromažďovat údaje v rozsahu nezbytně nutném pro plnění jejich úkolů v oblasti pojištění, a to včetně údajů o jednotlivých pojištěncích. Informačními systémy pojištění jsou registry pojištěnců a registry zaměstnavatelů, které jsou informačními systémy veřejné správy podle zák. č. 365/2000 Sb. Informační systémy nejsou veřejně přístupné. Přístup do informačních systémů mají orgány nemocenského pojištění a orgány provádějící důchodové pojištění, a to i způsobem umožňujícím dálkový přístup. Registr pojištěnců obsahuje o pojištěncích údaje uvedené § 122 odst. 3, písm. a) – x) zákona o nemocenském pojištění (např. jméno a současné příjmení, rodné a všechna další příjmení předcházející současnému příjmení, datum a místo narození a datum úmrtí pojištěnce, pohlaví, rodné číslo, státní občanství, adresu trvalého pobytu, vznik a zánik pojištění a dobu přerušování pojištění, údaje o dávkách a o době trvání pracovní neschopnosti atd.). Posuzování zdravotního stavu pro účely pojištění upravuje část čtvrtá tohoto zákona, která dále zahrnuje posuzování zdravotního stavu pojištěnců a dalších osob pro účely pojištění, posuzování dočasné pracovní neschopnosti, pracovní schopnosti po uplynutí podpůrní doby, zdravotního stavu pro účely poskytování peněžité pomoci v mateřství, ošetrovného a vyrovnávacího příspěvku v těhotenství a mateřství. Okresní správa sociálního zabezpečení tak zpracovává osobní údaje nezbytné pro dodržení jeho právní povinnosti dle zákona o nemocenském pojištění.

ÚP PSSZ jako správce osobních údajů má přijata potřebná opatření pro zabezpečení osobních údajů ve smyslu § 13 zákona o ochraně osobních údajů. Pro územní pracoviště PSSZ jsou závazné kromě zákonné úpravy interní směrnice ČSSZ a PSSZ. Zásadním vnitřním předpisem pro oblast IS je směrnice Bezpečnostní politika informací, která stanoví povinnosti zaměstnanců a vedoucích pracovníků v rámci dodržování bezpečnosti informací, a dále směrnice o bezpečnostní politice a technickoorganizačních opatřeních k ochraně osobních údajů v systémech organizačních jednotek ČSSZ, která vymezuje odpovědnost za provoz informačních a komunikačních technologií (IKT) v IS územních organizačních jednotek, stanovuje bezpečnostní politiku IS organizačních jednotek ČSSZ a pracoviště serverů stanovuje režimovým pracovištěm, stanovuje technickoorganizační opatření k zajištění ochrany osobních údajů v IS a povinnosti správce sítě, operátora výpočetní techniky, administrátora výpočetní techniky na územních organizačních jednotkách a uživatelů územních organizačních jednotek při ochraně osobních údajů. Oprávněným uživatelem IS územních organizačních jednotek ČSSZ je osoba s platným přístupem k IS, který byl udělen se souhlasem příslušného nadřízeného pracovníka.

Je stanovena odpovědnost za dodržování konfigurace technického a programového vybavení, zajištění antivirové ochrany, správný chod zařízení kryptografické ochrany při přenosu dat počítačovou sítí. Přijatá technickoorganizační opatření k zajištění ochrany osobních údajů jsou předmětem periodických prověrek. Jsou upraveny povinnosti uživatelů informačních systémů, včetně povinnosti mlčenlivosti a povinnosti zabezpečit, aby nedošlo k neoprávněnému přístupu k aplikacím IS. Upraveno je zabezpečení režimových pracovišť s umístěním serverů. Pro podmínky PSSZ byl vydán prováděcí pokyn ředitele PSSZ. Vydání bezpečnostní politiky informačního systému PSSZ a přijetí technickoorganizačních opatření k zajištění ochrany osobních údajů, který obsahově odpovídá uvedeným směrnicím ředitele odboru bezpečnostní politiky ČSSZ. Spisový a skartační řád a spisový a skartační plán upravuje manipulaci s došlými dokumenty, základní evidenci a rozsah osobních údajů v nich, třídění dokumentů a jejich předávání příslušným organizačním útvarům, vyřizování dokumentů, vnitřní

oběh dokumentů a jejich odesílání, zabezpečení spisů a jejich předávání do spisovny a skartování spisů. Směrnice ředitelky ČSSZ „Certifikační politika pro vydávání zaměstnaneckých certifikátů ČSSZ“ stanoví závazné postupy pro žadatele o vydání zaměstnavatelské čipové karty, postup při vydávání těchto karet a přiřazování certifikátů, povinnosti držitelů zaměstnavatelského certifikátu. Jednotlivé fáze přístupu k IS tak podléhají autentizaci a autorizaci, vložení hesel a zadání přístupových kódů. Zaměstnanci mají podle zastávané pozice dle pracovní smlouvy individuálně přiznaná oprávnění k přístupům do informačního systému. Prováděcí pokyn ředitele PSSZ „Zabezpečení kanceláří, ochrana prostor a režim vstupu osob“ byl vydán k zajištění bezpečnostních požadavků, zajištění vlastního provozu objektů PSSZ a k ochraně zpracovávaných dat.

Na základě kontrolních zjištění bylo v kontrolním protokolu konstatováno, že ÚP PSSZ při zpracování osobních údajů fyzických osob (subjektů údajů), pojištěnců nemocenského pojištění, postupuje v souladu s ustanoveními § 13 až § 15 zákona o ochraně osobních údajů.

III. KONTROLNÍ A DOZOROVÁ ČINNOST 2010 – JEJÍ PODMÍNKY A ZOBECŇUJÍCÍ ZÁVĚRY

V roce 2010 došlo k ukončení činnosti dvou inspektorů, kterým vypršel jejich desetiletý mandát. Na jejich místa jmenoval prezident republiky nové inspektory, kteří tak znovu doplnili kolegium inspektorů na plný počet. Kontinuita výkonu kontrolní činnosti Úřadu tím nebyla narušena.

Stěžejním úkolem v rámci dozorové činnosti je provádění státních kontrol, a proto jsou na tuto oblast kladeny stále větší nároky, a to zejména na kvalitu jednotlivých procesních úkonů. Úřad na základě jak soudního rozhodování, tak na základě poznatků z vlastního námitkového nebo rozkladového řízení upravil některé procesní postupy tak, aby byla prohloubena průkaznost důkazů zajišťovaných v rámci kontrolního řízení a zároveň byla posílena práva kontrolovaných subjektů již v průběhu kontroly.

Z průběhu prováděných kontrol vyplývá poznatek, že na jedné straně se zvyšuje právní vědomí a znalosti ochrany osobních údajů, a na straně druhé, v návaznosti na rozšiřující se možnosti využívání nových technologií – se zvyšuje počet osob, které vůbec netuší, že prostřednictvím moderních technologií zpracovávají osobní údaje a zasahují tím do soukromí fyzických osob.

Stoupající trend zájmu o ochranu osobních údajů je zřejmý zejména u veřejných institucí a u velkých společností, zejména v oblasti bankovníctví, pojišťovnictví nebo i velkých telekomunikačních společností. Stále častěji jsou společnosti zastupovány poradci, kteří se specializují na ochranu osobních údajů.

Bohužel se ovšem zvyšuje podíl nejen fyzických, ale i právnických osob, které se kontrole vyhýbají, nebo ji jakýmkoliv způsobem zdržují: Především tím, že nepřebírají poštovní zásilky zasílané jak poštou, tak datovými schránkami a vyhýbají se kontaktu s kontrolujícími. Stále častěji se Úřad setkává s tím, že kontrolované subjekty využívají fiktivní adresy, na kterých buď nikdo nesídlí, nebo neodpovídají skutečnému stavu. V některých případech se kontrolující setkali i s tím, že na jednání se dostavil zástupce kontrolované společnosti, který nebyl ani pověřen, ani oprávněn za společnost vystupovat. Za zdržovací taktikou se často skrývá snaha dosáhnout promlčení subjektivní lhůty pro následné správní řízení. Jsou využívány instituty námitek podjatosti a žádosti o odložení nařízených jednání z rozličných důvodů. S tímto se kontrolující musí vyrovnat.

Specifické je provádění kontrol v oblasti internetu, kde jsou kontrolující limitováni kompetencemi podle zákona o elektronických komunikacích, dle něhož nemá Úřad možnost zjistit od provozovatelů elektronických komunikací provozní a lokalizační údaje podezřelého subjektu, schovávajícího se za anonymitu webového prostředí, nebo přímo zneužívajícího internet jakožto celosvětový anonymní prostředek; podezřelý subjekt nezákonně informace často umísťuje na zahraniční servery, kde není možné nejen dohledat adekvátní informace k danému subjektu z výše uvedených důvodů, ale ani postihnout podle českého právního řádu.

Jediným účinným nástrojem, který mají kontrolující k dispozici, je možnost uložení pořádkové pokuty za neposkytnutí součinnosti, kde je horní hranice stanovena do výše 25 000 Kč. Tuto pokutu lze ukládat opakovaně, ovšem v kontrolách v rámci elektronických komunikací do maximální souhrnné výše 200 000 Kč. Navíc častým výsledkem takových řízení je následná urychlená likvidace společností a zakládání společností nových, se stejným personálním složením. Rok 2010 ale rovněž potvrdil i pokračující trend v přístupu stěžovatelů, kteří často neakceptují informace o výsledcích kontrolních zjištění a zpochybňují výsledky kontroly, jež konstatuje jiné skutečnosti, než uvádějí stěžovatelé ve svých podnětech. Z toho plynou stížnosti na postupy kontrolních pracovníků, které jsou ve své podstatě stížnostmi na výsledky kontrolních zjištění. V tomto kontextu je třeba také říci, že se stále zvyšuje počet stěžovatelů, kteří využívají Úřad k řešení svých soukromoprávních problémů či sporů – podezření z nakládání s osobními údaji je v těchto případech pouze zástupným problémem. Ovšem již pouhé prověřování takových podnětů, kdy velice často musí být konstatováno, že se netýkají zákona o ochraně osobních údajů, je časově náročné.

Závěrem této části je třeba konstatovat, že i přes úsporná rozpočtová opatření nedošlo v roce 2010 k žádnému snížení počtu zaměstnanců, kteří se na kontrole podílejí, a dále je třeba uvést, že až na výjimečné případy se průměrná délka prováděných kontrol zkrátila.

POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

OSOBNÍ ÚDAJE V REZORTU ZDRAVOTNICTVÍ

V souvislosti s registrací nových správců osobních údajů ve zdravotnictví nezaznamenal Úřad žádné výrazné problémy. Průběžně jsou řešeny otázky týkající se rozšiřování stávajících registrací velkých nemocnic a zdravotních pojišťoven. Jedná se především o rozšiřování preventivní péče, která je zajišťována zdravotnickými subjekty ve spolupráci se subjekty obchodními (např. elektronické zdravotní knížky apod.).

Na celkový počet přijatých dotazů, podnětů a stížností měla velký vliv medializovaná kauza centrálního úložiště elektronických receptů Státního ústavu pro kontrolu léčiv (dále jen „SÚKL“), včetně následné iniciativy SÚKL vynutit si pouhou změnou interního pokynu SÚKL zaslání informací do centrálního úložiště elektronických receptů. Takovou změnu však umožňuje pouze zákon, Úřad proto musel opětovně reagovat na stížnosti soukromých lékáren, Svazu pacientů i jednotlivých lékařů, lékárníků a pacientů. Následně došlo k poměrně ostré výměně stanovisek Úřadu s Ministerstvem zdravotnictví ČR. Na základě jednání byl učiněn společný závěr, že příslušná legislativa, zejména prováděcí vyhlášky a další rezortní předpisy, nejsou z pohledu ochrany zpracovávaných osobních údajů a citlivých údajů dostačující, a je nezbytné, aby došlo k jednotné a zcela jasné změně právních předpisů.

Úřad dále zaznamenal stále se zvyšující počet stížností pacientů na nesprávné zacházení s jejich údaji ve zdravotnické dokumentaci a s tím související nezabezpečené předávání informací o zdravotním stavu mezi jednotlivými zdravotnickými zařízeními při poskytování zdravotní péče. Úřad dospěl k závěru, že oblast ochrany osobních údajů a citlivých údajů, zpracovávaných v rámci rezortu zdravotnictví, je podceňována, a to nejen kvůli roztržitosti právních předpisů, ale vede k tomu i nedostatečná spolupráce jednotlivých orgánů a institucí, které se podílejí na zajišťování zdravotní péče. Lze pochopit, že k podcenění ochrany osobních údajů dochází při praktickém výkonu zdravotnické péče, zejména tam, kde dochází k bezprostřednímu ohrožení života a zdraví pacientů. Ale nelze akceptovat stávající přehlížení a neřešení problémů související se systémovým přístupem rezortu k ochraně soukromí pacientů. Přitom je nezbytné zdůraznit, že až na jednotlivé excesy svévolného jednání zdravotnických pracovníků je obecně v rezortu zdravotnictví respektován a správně chápán institut souhlasu subjektu údajů se zpracováním osobních údajů. Méně je však přijímán požadavek na legalitu účelu zpracování osobních údajů, tedy zohlednění toho, zda je záměr zpracování osobních údajů a citlivých údajů v souladu s oprávněním činnosti příslušných subjektů. Na tomto principu jsou založeny například celonárodní projekty, jako je program elektronických zdravotních knížek IZIP, Karta života či projekt ACORD.

Ke zpracování osobních údajů a citlivých údajů však dochází také v rámci spolupráce jednotlivých nemocnic. Například Pardubický kraj konzultoval s Úřadem projekt, jehož cílem by byla možnost vytvoření centrálního úložiště zdravotnických informací pacientů v rámci celého kraje. V souvislosti s poskytováním konzultací bylo zjištěno podceňování důsledné anonymizace osobních údajů, například v souvislosti s prováděním klinického i neklinického hodnocení léčiv a léčivých přípravků, vědeckého výzkumu, ale i při vyúčtování cest lékařů za pacienty zdravotním pojišťovám.

Kromě standardních stížností na ztráty či neoprávněné nakládání se zdravotnickou dokumentací se Úřad v roce 2010 nově setkal s nedůvěrou odpovědných osob reprezentujících zdravotnická zařízení k datovým schránkám. Ve svých vyjádřeních Úřad konstatoval, že odpovědným rezortem je Ministerstvo vnitra ČR a že z pohledu ochrany osobních údajů nebyly zjištěny takové skutečnosti, které by znemožňovaly využívání datových schránek pro komunikaci mezi zdravotnickými zařízeními, včetně zaslání dokumentů obsahujících citlivé osobní údaje.

Novou problematikou, řešenou Úřadem, bylo zpracování osobních údajů v oblasti osobní dozimetrie a dalších systémů radiační ochrany. Úřad poskytoval rozsáhlé konzultace subjektu, který na základě příslušného povolení Státního úřadu pro jadernou bezpečnost zajišťuje pro více pracovišť vybavených zdroji ionizujícího záření vedení databází, propojování a zpracování informací o osobách z jednotlivých pracovišť, a to jak zdravotnických, tak i nezdravotnických. Obdobné konzultace byly poskytnuty Generálnímu ředitelství hasičského záchranného sboru, zejména k rozsahu zpracovávaných informací v databázích osob vystavených v rámci služebního zákroku ionizujícím záření.

V roce 2010 uskutečnili inspektoři Úřadu v oblasti zdravotnictví řadu kontrol, a to jak na základě plánu kontrol, tak i na základě stížností a podnětů.

V rámci kontroly provedené na základě kontrolního plánu bylo prověřeno nakládání se zdravotnickou dokumentací převzatou od zdravotnických zařízení zrušených bez nástupců při výkonu působnosti krajského úřadu podle § 67b odst. 16 zákona č. 20/1966 Sb., o péči o zdraví lidu. Inspektorka Úřadu konstatovala, že zjištěný stav svědčí o bezvadném postupu orgánu veřejné správy. Zdravotní dokumentace tvořená převážně ambulantními kartami byla řádně uložena, a pokud si některou z karet vyžádá lékař, je předání dokumentace pacienta zaprotokolováno.

Inspektor Úřadu provedl kontrolu u lékařky, která nedodržela povinnosti při předávání zdravotnické dokumentace. Jednalo se o následnou kontrolu poté, co stěžovatelka se svou stížností neuspěla u příslušného krajského odboru zdravotnictví a sociální péče a u příslušné oblastní České lékařské komory. Kontrolou bylo zjištěno, že dětská lékařka, sídlící v jednom statutárním městě, při předávání zdravotnické dokumentace novému lékaři využila přepravní službu, která na základě smlouvy převáží zdravotnické laboratorní vzorky mezi krajskou nemocnicí a jednotlivými lékaři. Zdravotní dokumentaci ponechala na místě, odkud si běžně přebíral zásilky pracovník firmy zajišťující jejich převoz, aniž požadovala potvrzení o převzetí. Kontrolou bylo zjištěno, že zásilková společnost má uzavřenu smlouvu pouze s krajskou nemocnicí, a to na převoz zdravotnického materiálu a laboratorních vzorků. Krajská nemocnice dále uzavřela smlouvy o využívání nemocniční laboratoře s jednotlivými zdravotnickými zařízeními ve městě. Běžnou praxí se stalo využívání převozní služby i pro předávání lékařské korespondence mezi všemi lékaři ve městě.

Příslušný odbor krajského úřadu pro zdravotnictví a sociální péči stížnost odložil s konstatováním, že v daném případě lékařka neporušila svoji povinnost, neboť zdravotnickou dokumentaci pacientky řádně předala. Rovněž příslušné oblastní sdružení lékařské komory odmítlo řešit stížnost s odůvodněním, že lékařka neporušila žádný zdravotnický předpis. V daném případě však došlo k nedodržení povinnosti uložené správci osobních údajů přijmout taková technicko-organizační opatření, aby nemohlo dojít ani k nahodilé ztrátě osobních údajů. Zdravotnická dokumentace, kterou na základě zákona o péči o zdraví lidu vede ošetřující lékař, obsahuje nejen osobní údaje pacienta, ale zejména citlivé údaje vypovídající o zdravotním stavu konkrétní fyzické osoby. Na toto zpracování osobních údajů a citlivých údajů se plně vztahuje povinnost, uložená lékaři zákonem o ochraně osobních údajů, spočívající v povinnosti přijmout taková technicko-organizační opatření, aby nemohlo dojít ani k nahodilé ztrátě osobních údajů. I když příslušný zdravotnický zákon (zákon o péči o zdraví lidu), který upravuje povinnosti nakládání se zdravotnickou dokumentací, neukládá lékařům a ostatním zdravotnickým pracovníkům povinnost zabezpečit zdravotnickou dokumentaci před ztrátou, odcizením či jiným poškozením, odkazuje právě na obecnou povinnost upravenou v zákoně o ochraně osobních údajů. Úřad nejen konstatoval, že lékařka tuto povinnost nedodržela, ale v následném správním řízení uložil lékařce za porušení této povinnosti pokutu.

Na základě stížností několika patientek uskutečnil inspektor Úřadu šetření na jedné pražské poliklinice. Stěžovatelky uvedly, že na gynekologické ambulanci je umístěno pracoviště zdravotní sestry přímo v čekárně, a tedy pacientky jsou před vyšetřením lékařem v ordinaci nuceny sdělovat před ostatními pacientkami sestře nejen své osobní kontaktní údaje, ale i informace o svém zdravotním stavu. Šetřením bylo zjištěno, že k této praxi se vedoucí gynekologické ambulance rozhodl z důvodu postupné stavební rekonstrukce proto, aby nemusel omezovat provoz. V tomto případě tedy došlo jak k neetickému jednání ze strany všech zaměstnanců lékařské ambulance, tak i porušení ochrany

soukromí pacientek. Základním problémem se však ukázala skutečnost, že i když se pacientkám tento postup nelíbil, nechaly si jednání zdravotnického personálu líbit, protože měly strach svůj nesouhlas s takovým postupem projevit.

Inspektor Úřadu převzal stížnost zasloupanou ředitelem sociálního zařízení, které se stará o těžce postižené pacienty. Obsahem stížnosti byla skutečnost, že oblastní pobočka zdravotní pojišťovny provádí v sociálním zařízení kontrolu a v rámci této kontroly zkopírovala kompletní zdravotnickou dokumentaci tří pacientů-klientů sociálního zařízení v rozsahu 680 stránek a tyto kopie si odvezla. Dle stěžovatele tím došlo k neoprávněnému shromažďování a zpracování osobních údajů a citlivých údajů pacientů, a to v rozporu se zákony upravujícími dozorovou činnost VZP, se zákonem o péči o zdraví lidu, který upravuje nakládání se zdravotnickou dokumentací, a zákonem o veřejném zdravotním pojištění. V rámci kontroly bylo zjištěno, že sociální zařízení je současně smluvním zdravotnickým zařízením VZP, ve kterém jsou na základě příslušného zákonného zmocnění revizní lékaři oprávněni kontrolovat využívání zdravotní péče hrazené ze zdravotního pojištění, a to včetně pořizování si kopií zdravotnické dokumentace i zařazení pořizovaných fotokopií do spisu prováděného šetření. V opačném případě by tak bylo VZP, resp. i dalším zdravotním pojišťovnám znemožněno kontrolovat a posuzovat odůvodněnost léčebného procesu, předepisování léčivých přípravků, prostředků zdravotnické techniky a porovnání vynaložených nákladů se skutečností a rozsahu a druhu zdravotní péče odpovídající zdravotnímu stavu pojištěnce.

Dále byla provedena kontrola jedné středočeské nemocnice, a to na základě podnětu, který Úřadu předala jedna zdravotní pojišťovna. Předmětem kontroly bylo podezření, že v rámci vymáhání náhrady škody vzniklé při léčbě poškozené pacientky byly předloženy informace pořízené neoprávněně z nemocničního informačního systému. Kontrolou bylo zjištěno, že žena, po které pojišťovna vymáhala úhradu léčebných nákladů, použila informace z nemocničního informačního systému obsahující osobní údaje a citlivé údaje poškozené pacientky. Dále bylo zjištěno, že tato žena současně pracuje v příslušné nemocnici na úseku, který komunikuje s jednotlivými zdravotními pojišťovnami za nemocnici, a že si v rozporu s obecnou povinností nakládání se zdravotnickou dokumentací podle zákona o péči o zdraví lidu a obecnou povinností upravenou zákonem o ochraně osobních údajů vyhledala a následně vytiskla informace ze zdravotní dokumentace. V rámci kontroly byla posuzována i otázka, jakým způsobem zabezpečila nemocnice ochranu informací uložených v nemocničním informačním systému. Nemocnice nebyla schopna zpětně vyhledat a doložit informace o osobách, které nahlížely prostřednictvím IT systému do databáze pacientů a do jednotlivých zdravotnických dokumentací. Proto bylo konstatováno, že nemocnice nesplnila povinnost uloženou jí zákonem o ochraně osobních údajů, a to aby v oblasti automatizovaného zpracování osobních údajů zajistila přístup pouze osobám, které jej využívají na základě svého oprávnění, a aby takové oprávněné osoby měly přístup pouze k osobním údajům odpovídajícím stanoveným oprávněním. Kontrolou bylo rovněž zjištěno, že nemocnice jako provozovatel nemocničního informačního systému nezajistila logování, čímž porušila povinnost uloženou zákonem o ochraně osobních údajů, a tím tedy umožnila zneužití osobních údajů bez možnosti jejich následného dohledání, čímž současně jako správce osobních údajů nesplnila povinnost uloženou zákonem o ochraně osobních údajů – přijmout taková technicko-organizační 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. V tomto konkrétním případě kontrolovaná nemocnice tento nedostatek napravila již v průběhu kontroly.

Velice často se na Úřad obracují občané se stížnostmi, že jim bez jejich vědomí byla změněna registrace u praktického lékaře nebo došlo ke změně jejich zdravotní pojišťovny.

Právo pacienta na změnu praktického lékaře, resp. praktického lékaře pro děti a dorost upravuje příslušné ustanovení zákona o péči o zdraví lidu, přičemž samotnou změnu při převzetí lékaře do péče řeší zákon o veřejném zdravotním pojištění. Konkrétní postup nejen pacienta a lékaře upravují příslušné podzákonné předpisy rezortu zdravotnictví. Se změnou registrujícího lékaře úzce souvisí

i povinnost VZP vést centrální registr pacientů a navazující povinnost příslušné zdravotní pojišťovny evidovat nejen změnu lékaře, ale hradit za pacienta registrujícímu lékaři tzv. kapitační platbu.

V rámci kontroly prováděné v jednom nestátním zdravotnickém zařízení provozujícím síť poboček praktických lékařů v ČR bylo zjištěno, že zde došlo k zaregistrování nové pacientky, a to včetně zaslání povinné informace VZP. Tato registrace byla ovšem provedena bez vědomí stěžovatelky, která se o změně dozvěděla až při návštěvě své praktické lékařky. V daném případě bylo konstatováno, že k přeregistrování došlo chybou lékaře – zaměstnance kontrolovaného zařízení, který omylem vyplnil elektronický registrační formulář a na základě této skutečnosti byl celý registrační proces, včetně změny zápisu v registru VZP a změny zasílání kapitačních plateb, proveden zcela automatizovaně, bez jakékoliv kontroly. Teprve po zásahu pacientky došlo k okamžité nápravě a vrácení registrace do původního stavu. Kontrolou bylo zjištěno, že pacient, který žádá o změnu praktického lékaře, vyplňuje tzv. registrační list, na kterém se uvádějí jeho osobní údaje v rozsahu jméno, příjmení, adresa, číslo pojištěnce (rodné číslo), datum podání registračního listu a identifikace nového zdravotnického zařízení, resp. nového praktického lékaře a podpis pacienta. Na základě takto vyplněného registračního listu provádí nový registrující lékař změnu v centrální evidenci VZP prostřednictvím dálkového elektronického přístupu, přičemž má za povinnost registrační list uschovat ve svém zařízení. Takto upravený postup a rozsah vyžadovaných osobních údajů je často zneužíván, protože údaje lze získat například z obchodního nebo živnostenského rejstříku. K rozlišení, zda registrační list podal skutečně pacient, slouží pouze podpis, který však nemá nový registrující lékař s čím porovnat.

Ze zkušeností z předchozích kontrol, které Úřad uskutečnil, vyplývá, že tento postup je často zneužíván, a to z různých důvodů. Shodné zkušenosti má i Policie ČR. Tím, že VZP nebo příslušná zdravotní pojišťovna pacienta obdrží změnu pouze prostřednictvím dálkové elektronické informace, *de facto* nemůže zjistit, zda nedošlo k neoprávněnému zápisu. Stávající situaci navrhuje Úřad řešit tak, aby jednotlivé zdravotní pojišťovny provedly zápis změny registrace pacienta při převzetí do péče registrujícím lékařem až poté, bude-li splněna povinnost uložená lékařům vyhláškou Ministerstva zdravotnictví ČR č. 3/12010 Sb., která ukládá praktickému lékaři, resp. praktickému lékaři pro děti a dorost, aby provedl komplexní vyšetření podle vyhlášky, kterou se vydává seznam zdravotních úkonů. Je zcela logické, že v převážné většině dochází k žádosti o zaregistrování u nového lékaře současně s jeho návštěvou a požadavkem o poskytnutí konkrétní péče. Dodržování této jednoduché povinnosti by výrazně pomohlo zamezit neoprávněným změnám registrujícího lékaře bez vědomí pacientů.

V rámci své dozorové činnosti se Úřad zabýval řešením podnětů na jednotlivá pochybení lékařů a zdravotnických pracovníků nelékařských profesí souvisejících převážně s pochybením při nakládání se zdravotnickou dokumentací, resp. s informacemi vypovídajícími o zdravotním stavu konkrétního pacienta. Například Úřad vedl správní řízení s lékařkou, které se ztratilo z ordinace přenosný nosič informací (flash-disk), na kterém měla nahranou záložní kopii všech zdravotních dokumentací svých pacientů. V rámci řízení se prokázalo, že tento nosič měla volně přístupný v neuzamčené skříňce v ordinaci. I přestože nebylo prokázáno, že by došlo ke zneužití osobních údajů, které takto byly uloženy, lékařka byla pokutována, neboť porušila povinnost přijmout takové technicko-organizační opatření, aby nedošlo ani k nahodilé ztrátě osobních údajů.

Úřad se v rámci správního řízení rovněž zabýval jednáním lékaře, který na článek publikovaný v novinách a obsahující kritiku nemocnice, v níž pracoval, reagoval písemnou odpovědí, která obsahovala informace o zdravotním stavu konkrétního pacienta včetně způsobu léčby. Tento článek následně přečetl na zastupitelstvu města a současně identifikoval svého pacienta. Svou obhajobou však lékař porušil povinnost, již zákon ukládá zaměstnancům správce, kteří v rámci plnění svých pracovních povinností přicházejí do styku s osobními údaji, a to povinnost zachovávat mlčenlivost o osobních údajích, přičemž tato povinnost mlčenlivosti trvá i po ukončení zaměstnaneckého poměru nebo příslušných prací. Za toto jednání Úřad lékaře pokutoval, neboť porušil obecnou povinnost mlčenlivosti, kterou má uloženou zákonem o ochraně osobních údajů.

Úřad se také zabýval podněty, jejichž obsahem bylo podezření na neoprávněné nakládání s osobními údaji v souvislosti s předáváním občanských průkazů zemřelých pacientů v nemocnici. I když

občanský průkaz obsahuje osobní údaje svého držitele, v těchto případech byly stížnosti postupovány příslušným matričním úřadům, kterým je dle zákona o občanských průkazech svěřena dozorová kompetence nakládání s občanskými průkazy. Shodný postup Úřad uplatňuje i v souvislosti s šetřením relativně častých nálezů zdravotní dokumentace. Za takových okolností je nezbytná součinnost nejen mezi policejními orgány a Úřadem, ale zejména s příslušnými krajskými odbory zdravotnictví.

OPENCARD

Na začátku roku 2010 dokončil inspektor Úřadu kontrolní šetření vedené s Hlavním městem Prahou ve věci vydání Karty Pražana, tzv. Opencard, a to včetně sepsání kontrolního protokolu se stanovenými nápravnými opatřeními, vyplývajícími ze zjištěných nedostatků. Se závěry kontrolního protokolu a navrženými nápravnými opatřeními zástupci Hlavního města Prahy nesouhlasili a v souladu s právem kontrolovaného vyjádřit své stanovisko vyvolali řadu jednání s cílem změnit navržená nápravná opatření. Vzhledem k značnému časovému zdržení byl kontrolní protokol závěrem června 2010 s konečnou platností předán. Hlavní město Praha proti kontrolnímu protokolu podalo řádné námítky. Současně však sdělilo, že souhlasí s uloženými nápravnými opatřeními.

Předseda Úřadu rozhodl o námítkách podaných Hlavním městem Prahou vůči kontrolnímu protokolu. Potvrdil kontrolní zjištění, že při zpracování osobních údajů v souvislosti s vydáváním Karty Pražana – Opencard došlo k porušení zákona o ochraně osobních údajů. Konkrétně potvrdil, že Hlavní město Praha nedostatečným způsobem informovalo zájemce o vydání Opencard o parametrech budoucího zpracování jejich osobních údajů za situace, kdy pro takové zpracování není nezbytné vyžadovat souhlas uživatele karty. Současně potvrdil nápravná opatření uložená kontrolujícím inspektorem, aby každému stávajícímu držiteli karty bylo zpětně umožněno vyjádřit svůj souhlas nebo nesouhlas se zpracováním jeho osobních údajů, aniž by mu bylo omezeno využívání všech služeb souvisejících s projektem „Opencard“. Dále potvrdil uložené nápravné opatření, aby všem novým zájemcům o vydání Karty Pražana – Opencard bylo umožněno vyjádřit svůj svobodný souhlas se zpracováním osobních údajů již při podání žádosti.

Současně předseda Úřadu ve svém Rozhodnutí o námítkách potvrdil další uložené opatření, spočívající ve splnění řádné informační povinnosti o zpracování osobních údajů dle zákona o ochraně osobních údajů.

Smyslem nápravných opatření, která jsou v souladu s dosavadní kontrolní a rozhodovací činností Úřadu, je umožnit všem zájemcům, kteří nedají svůj svobodný souhlas se zpracováním svých osobních údajů, využívat Opencard v plném rozsahu. Hlavní město Praha tento závěr akceptovalo, ale současně požádalo o prodloužení lhůty ke splnění nápravných opatření do konce června roku 2011.

Po uplynutí této lhůty bude Hlavní město Praha, na základě žádosti žadatele o vydání karty, shromažďovat osobní údaje výhradně za účelem vytištění jeho osobních údajů na kartu, a to včetně fotografie žadatele. Po vydání karty následně osobní údaje zlikviduje a nebude dále zpracovávat. Stávajícím držitelům Opencard umožní Hlavní město Praha zpětně vyjádřit svůj souhlas či nesouhlas se zpracováním osobních údajů.

Kromě účelu vydání karty Opencard může Hlavní město Praha zpracovávat osobní údaje držitelů karty s jeho výslovným souhlasem z důvodu snadnějšího vydání náhradní Opencard v případě ztráty či odcizení.

MATRIKY STUDENTŮ, ZVEŘEJŇOVÁNÍ ÚDAJŮ STUDENTŮ VYSOKÝCH ŠKOL

Jednou z mediálních kauz, která byla základem stížnosti doručené Úřadu v roce 2010, byli „rychlo-studenti“ Právnické fakulty Západočeské univerzity v Plzni. Stěžovatelka v souvislosti se svým studiem na Západočeské univerzitě v Plzni napadla zveřejnění svých osobních údajů v deníku MF DNES ze dne 23. ledna 2010. Zveřejněny byly její osobní údaje v rozsahu fotografie, jméno, příjmení, dřívější veřejná funkce, současné zaměstnání, studium na Právnické fakultě Západočeské univerzity v Plzni od do, předchozí studium a její reakce na tyto údaje. Ve stejném rozsahu byly uvedeny osobní údaje dalších osmi osob a u tří osob nebyla zveřejněna fotografie. V jiných článcích byly uvedeny osobní údaje dalších třinácti osob v rozsahu jméno, příjmení, celková délka studia na Právnické fakultě, bývalá veřejná funkce, současné zaměstnání, doba studia od do a vyjádření k údajům o studiu. Celkem byly zveřejněny osobní údaje dvaceti pěti lidí. Ze zveřejněných informací je zřejmé, že autoři vycházeli ze záznamů o studiu vedených na základě zákona.

Údaje vypovídající o vysokoškolském studiu, které byly zveřejněny, prokazatelně pocházely z matriky studentů vedené Západočeskou univerzitou podle § 88 zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů (dále jen „zákon o vysokých školách“).

Univerzita tyto údaje prvotně zpracovává v interním automatizovaném informačním systému a dvakrát ročně předává na základě zákona a prováděcích pokynů Ministerstvu školství, mládeže a tělovýchovy (dále jen „Ministerstvo“), pro něž databázi sdružených údajů z jednotlivých matrik („databáze SIMS“) zpracovává na základě smlouvy Masarykova univerzita v Brně. Ministerstvo je správcem databáze SIMS a na zpracování údajů z ní se samo také podílí.

Na základě stížnosti byly proto provedeny dvě kontroly dodržování povinností stanovených zákonem o ochraně osobních údajů – v Západočeské univerzitě v Plzni a na Ministerstvu – a na jejich základě poté vedena tři správní řízení. V jedné z kontrol byly podány námitky. Všechny kontroly byly v roce 2010 pravomocně ukončeny.

Západočeská univerzita i Ministerstvo zpracovávají osobní údaje studentů na základě povinností a oprávnění daných zákonem o vysokých školách. Jako správci osobních údajů ve smyslu ustanovení § 4 písm. j) zákona o ochraně osobních údajů je tak mohly zpracovávat bez souhlasu subjektů údajů podle § 5 odst. 2 písm. a) tohoto zákona, neboť prováděly zpracování nezbytné pro dodržení právní povinnosti správce.

V matrice studentů a sdružených údajích – databázi SIMS – mají být zapsáni všichni studenti studující na některé vysoké škole v České republice po 1. lednu 1999. Jako seznam vedený pro úřední potřebu na základě zákona jsou matrika a doklady o rozhodných událostech archiváliemi. Vysoká škola sdělí příslušný údaj z matriky tomu, kdo osvědčil právní zájem. Sdružené údaje matrik využívá Ministerstvo při výkonu své role ústředního orgánu státní správy.

Kontrolované osoby byly mj. povinny podle § 13 odst. 1 zákona o ochraně osobních údajů přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení nebo ztrátě, k neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů a podle § 13 odst. 4 písm. c) zákona o ochraně osobních údajů pořizovat elektronické záznamy, které by umožnily určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje v informačním systému univerzity a databázi SIMS vyhledávány a použity jinak než k aktualizaci. Rozsah a forma dokumentování použití osobních údajů z informačního systému univerzity i v databázi SIMS neumožnily zjistit za použití prostředků dostupných pro kontrolu, že by někdo v Západočeské univerzitě nebo na Ministerstvu porušil svoji povinnost podle ustanovení § 15 odst. 1 zákona o ochraně osobních údajů (tj. povinnost zaměstnanců správce nebo zpracovatele, jiné fyzické osoby, které zpracovávají osobní údaje na základě smlouvy se správcem nebo zpracovatelem, a dalších osob, které v rámci plnění zákonem o ochraně osobních údajů stanovených oprávnění a povinností přicházejí do styku s osobními údaji, zachovávat mlčenlivost o osobních údajích a o bezpečnostních opatřeních, jejichž zveřejnění by

ohrozilo zabezpečení osobních údajů). Zjištěn byl pouze zdrojový soubor zveřejněných osobních údajů o studiu na Právnické fakultě Západočeské univerzity v Plzni, který vznikl výběrem z údajů matriky studentů – databáze SIMS, a užší okruh lidí, kteří prvotně měli po určitou dobu k souboru „rychlostudentů“ přístup.

Pro zjištění zdroje úniku osobních údajů studentů bylo neúspěšně využito i oprávnění dané v § 39 odst. 1 zákona o ochraně osobních údajů (ukládá povinnost součinnosti). Zástupce vydavatelství MAFRA, a. s., vydavatele deníku Mladá fronta DNES, sdělil s odvoláním na ustanovení § 16 zákona č. 46/2000 Sb., o právech a povinnostech při vydávání periodického tisku a o změně některých dalších zákonů (tiskový zákon), ve znění pozdějších předpisů, že informace o původu či obsahu informací zveřejněných v periodickém tisku /.../ nebudou poskytnuty.

Kontrolami nebylo zjištěno, že by k úniku osobních údajů studentů, které spravovaly kontrolované osoby, došlo vinou konkrétních osob. Bylo nicméně zjištěno, že ze strany kontrolovaných subjektů nebyly dostatečně plněny jejich povinnosti stanovené v § 13 odst. 1 (jak byly výše odcitovány) a v odst. 4 písm. c) zákona o ochraně osobních údajů. U Ministerstva bylo i po námitkách shledáno porušení povinnosti uložené v § 5 odst. 1 písm. c) zákona o ochraně osobních údajů tím, že neprověřovalo úplnost dat vkládaných do databáze SIMS a současně neprovádělo kontrolní opatření ke zjištění přesnosti zpracovávaných osobních údajů studentů. V důsledku toho nebyla databáze SIMS s to sloužit jako prostředek dosažení účelů sledovaných zpracováním, prováděným na základě zvláštního zákona.

Ve správním řízení byly uloženy pokuty všem třem institucím jako subjektům odpovědným za zpracování osobních údajů, z něhož v důsledku neodpovídajících a nedostatečně účinných bezpečnostních opatření byly nezjištěnou osobou dále předány informace o studentech práv na Západočeské univerzitě. Spolehlivě proto nemohl být zjištěn ani skutečný rozsah zpřístupnění takových údajů. S původním zdrojem informací o studiu – Západočeskou univerzitou v Plzni – a s Ministerstvem bylo vedeno a ukončeno správní řízení také pro porušení povinnosti podle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů (zpracovávat pouze přesné osobní údaje). Západočeská univerzita tuto povinnost porušila tím, že při vkládání údajů o studentech a jejich studiu do matriky studentů – databáze SIMS, zpracovávaných ve vnitřním informačním systému, nezavedla formálně logické kontroly přípustnosti určitých hodnot údajů v datových polích. V důsledku toho zapsala do svého informačního systému a do databáze SIMS předala údaje, že stěžovatelka absolvovala pětiletý studijní program formou prezenčního studia, a to zároveň s údajem o délce studia nedosahujícím hodnoty 1,5 roku, ačkoli v daném případě nebylo ani uznáno žádné předchozí studium. Stejně postupovala nejméně u 21 dalších studentů, a to přinejmenším v období od 1. září 2006 do 4. května 2010.

Zjištěná pochybení jsou však jen okrajovými jevy celé kauzy zveřejnění osobních údajů studentů Západočeské univerzity v Plzni v tisku, a provedené kontroly tak nemohly dát odpovědi na všechny vznesené otázky. Ačkoli jádro společenského problému spočívá v jiných činnostech univerzity a vysokého školství v České republice, stěžovatelka postihla zjevný nedostatek ve zpracování osobních údajů, které je s formalizovaným vysokoškolským studiem spojeno takřkajíc z podstaty.

Zřejmě pod vlivem medializované kauzy Západočeské univerzity řešil Úřad v roce 2010 celou řadu podání a poskytoval konzultace k novele zákona o vysokých školách, konkrétně k povinnosti vysokých škol zveřejňovat s účinností od 1. ledna 2006 údaje vyjmenované v ustanovení § 47 b citovaného zákona – disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a záznamu o průběhu a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou škola spravuje. Z hlediska zákona o ochraně osobních údajů je jednoznačně aplikovatelný § 5 odst. 2 písm. a) umožňující zpracovávat osobní údaje v rozsahu předpokládaném zvláštním zákonem i bez souhlasu subjektu údajů – studenta. Navíc zákon o vysokých školách konstatuje, že autor příslušné práce jejím předložením souhlasí s jejím zveřejněním ve stanoveném rozsahu bez ohledu na výsledek obhajoby.

Jedním z cílů této novely zřejmě bylo umožnit potenciálním zaměstnavatelům kvalifikovanější výběr vhodných uchazečů. Iniciativy zaměstnavatelů zjišťovat si u vysokých škol, zda je zájemce o zaměstnání jejich absolventem, případně podrobnosti o průběhu studia, nemohly být s ohledem na

dosavadní dikci zákona vyřizovány. Povinnost doložit nejvyšší stupeň dosaženého vzdělání jako jeden ze základních kvalifikačních předpokladů ležela zcela na žadateli o zaměstnání. Argumenty některých zaměstnavatelů, že v této souvislosti dochází k podvodnému jednání, je nutno považovat za irrelevantní. Takové skutečnosti mohly zakládat trestnou činnost, např. padělání a pozměňování úřední listiny, nemohou však být důvodem k porušení povinností uložených správcům a zpracovatelům osobních údajů zákonem. V tomto směru Úřad odpovídal vysokým školám i dalším institucím na dotazy a žádosti o stanovisko k dané problematice.

Prakticky současně s případem nestandardního studia na Právnické fakultě vedl Úřad se Západočeskou univerzitou správní řízení ve věci jiného zveřejňování osobních údajů studentů. Nejpozději ke dni 28. ledna 2010 univerzita zveřejnila prostřednictvím veřejně přístupných internetových stránek Právnické fakulty www.fpr.juristic.cz seznam 169 studentů 2. ročníku v akademickém roce 2009/2010 přihlášených ke státní zkoušce a seznam 204 studentů 5. ročníku v akademickém roce 2009/2010 přihlášených na závěrečnou státní soubornou zkoušku (trestní právo, správní právo); tyto seznamy obsahovaly osobní údaje studentů v rozsahu jméno, příjmení, osobní číslo, datum a čas konání zkoušky. Úřad konstatoval, že skutečnost, že jsou zveřejněny průběh a vyhlášení výsledků státních zkoušek, které jsou veřejné, ještě neznamená, že je možné zveřejnit prostřednictvím internetu seznam konkrétních studentů zařazených k jednotlivým termínům konání těchto státních zkoušek. Veřejnost státních zkoušek ještě neznamená, že by s ní byla spojena právní povinnost ve smyslu § 5 odst. 1 písm. a) zákona o ochraně osobních údajů zveřejnit předem seznam účastníků této zkoušky. Pokud univerzita zveřejňuje osobní údaje za účelem pozvání studentů ke zkoušce a jejich informování o termínu a čase zkoušky, nemá veřejnost či neveřejnost zkoušky s tímto účelem zpracování žádnou souvislost.

Za porušení povinnosti stanovené v § 13 odst. 1 zákona o ochraně osobních údajů – přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů a spáchání správního deliktu – byla Západočeské univerzitě v Plzni uložena pokuta. Splnění povinnosti přijmout dostatečná opatření směřující k tomu, aby osobní údaje nebyly vystaveny riziku neoprávněného zpracování či využití, předpokládá, že správce důsledně zváží veškerá rizika, která jsou s prováděným zpracováním osobních údajů spojena, a přijme odpovídající opatření k jejich vyloučení. Zveřejnění seznamů studentů za účelem jejich řádného pozvání ke státní závěrečné zkoušce bylo nepochybně jednáním v rozporu s těmito požadavky zákona, jelikož k údajům zveřejněným prostřednictvím internetových stránek měl přístup neomezený okruh osob. Tyto seznamy byly dále zveřejněny i po datech konání jednotlivých státních závěrečných zkoušek.

Také Univerzita Karlova v Praze zveřejnila v souvislosti se zpracováním osobních údajů studentů údaje, o nichž tak zákon nestanoví, a aniž získala předchozí souhlas studentů. Ode dne 9. září 2009 byly osobní údaje studentů 2. lékařské fakulty Univerzity Karlovy zveřejněny na internetových stránkách fakulty (www.lf2.cuni.cz) jako seznam 170 studentů 1. ročníku studijního oboru Všeobecné lékařství v rozsahu jméno, příjmení a datum narození a jejich zařazení do okruhů pro akademický rok 2009/2010. Konstatováno bylo porušení povinnosti podle § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, a k jinému účelu jen v mezích ustanovení § 3 odst. 6 zákona o ochraně osobních údajů, nebo pokud k tomu dal subjekt údajů předem souhlas. Předem stanovený účel zpracování, jímž je vedení matriky studentů a organizační zajištění studia, byl zveřejněním osobních údajů studentů překročen. Na postup školy není možné aplikovat žádnou z výjimek stanovených v § 3 odst. 6 zákona o ochraně osobních údajů. Univerzita navíc disponuje veřejně nepřístupným informačním systémem, prostřednictvím kterého informuje studenty o záležitostech týkajících se jejich studia; studenti do něho mají přístup prostřednictvím přihlašovacího jména a hesla.

Vysoká škola ekonomická v Praze zveřejnila na svých internetových stránkách <http://nf.vse.cz/cze/nfvse/o-fakulte/disciplinari-komise> zápisy z 18 jednání disciplinární komise Národohospodářské fakulty VŠE v době od 23. února 2004 do 28. ledna 2010, které obsahovaly osobní údaje 89 studentů Národohospodářské fakulty v rozsahu jméno, příjmení, popis skutku a druh doporučeného

disciplinárního trestu, aniž by disponovala souhlasem studentů se zveřejněním. Úřad konstatoval také v tomto případě porušení povinnosti stanovené v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tedy povinnosti zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny, a k jinému účelu jen v mezích ustanovení § 3 odst. 6 tohoto zákona, nebo pokud k tomu dal subjekt údajů předem souhlas. Úřad shledal, že jednání disciplinární komise je neveřejné, a má za to, že i na průběh disciplinárního řízení vedeného veřejnou vysokou školou je nutné uplatnit principy vyjádřené v § 2 až 8 správního řádu. Při stanovení sankce bylo jako k přitěžující okolnosti přihlédnuto ke skutečnosti, že došlo k užití osobních údajů v rozporu se zákonem o ochraně osobních údajů u 89 subjektů údajů, a dále ke skutečností, že osobní údaje byly prostřednictvím internetu zpřístupněny širokému okruhu osob a že byly zpřístupněny informace o disciplinárních trestech, jejichž zveřejnění lze považovat za citelnější zásah do soukromí subjektů údajů. Dále správní orgán zohlednil fakt, že zápisy byly na internetových stránkách zveřejněny nepřetržitě, což u nejstarších zápisů činí až šest let.

Ve všech šesti případech, které byly pravomocně uzavřeny, byla uložena sankce při dolní hranici zákonné sazby a pokuty byly uhrazeny. Z devíti opatření k nápravě uložených ve dvou kontrolách Úřadu bylo šest splněno ve lhůtě stanovené inspektorkou, pro zbývající opatření, která směřují k zajištění vybraných technických a organizačních podmínek, byla příslušnému správci stanovena delší lhůta.

Se zveřejňováním údajů studentů vysokých škol volně souvisí poskytování informací o zletilých studentech rodičům. Úřad i v tomto případě při své rozhodovací činnosti a při zodpovídání dotazů vychází ze zákona o vysokých školách, který upravuje mimo jiné v § 88 matriku studentů. V dané souvislosti je pro rozhodnutí o možnosti rodičů získat informace o průběhu vysokoškolského studia stěžejním ustanovení odst. 5 citovaného paragrafu, že „vysoká škola sdělí tomu, kdo osvědčil právní zájem, příslušný údaj z matriky studentů“. Právní zájem lze samozřejmě spojovat např. s uplatňováním slevy na snížení daňového základu na vyživované studenty do dosažení příslušného věku, zpravidla 26 let. Pro tento účel ovšem rodič podle názoru Úřadu vystačí s řádně doloženou informací, že došlo k zápisu do vyššího ročníku. Další podrobnosti by pak bylo nutno považovat jako pro daný účel nadbytečné.

MATRIKA STUDENTŮ

Na základě stížnosti byla provedena kontrola Matriky studentů, jejímž správcem je Ministerstvo školství, mládeže a tělovýchovy (dále jen „Ministerstvo“) a zpracovává ji Ministerstvem řízený Ústav pro informace ve vzdělávání.

Každá škola a školské zařízení zpracovávají osobní údaje žáků a studentů, kteří je navštěvují, v Matrice žáků a studentů (dále jen „studentů“). Některé osobní údaje z těchto matrik jsou předávány do centrální matriky studentů, kde jsou žáci a studenti vedeni pod svými rodnými čísly, tudíž nejde o anonymizované údaje, ale jedná se o údaje osobní. Toto zpracování je prováděno na základě ustanovení § 28 zákona č. 561/2004 Sb., o předškolním, základním, středním, vyšším odborném a jiném vzdělání (dále jen „školský zákon“), ve znění pozdějších předpisů a Vyhlášky č. 364/2005 Sb., o vedení dokumentace škol a školských zařízení a o předávání údajů z dokumentace škol a školských zařízení a ze školní matriky ve znění pozdějších předpisů (dále jen „Vyhláška o dokumentaci škol“).

Údaje se tzv. anonymizují a studenti vystupují pod jinými kódy, ovšem tak, že lze každý rok přidávat další informace a výsledně vznikají časové řady všech studentů v trvání 9–13 let, které vypovídají o studijní trase každého českého studenta. Tím vzniká vlastně registr studentů, který dle názoru Úřadu nelze podřadit pod ustanovení § 28 školského zákona: *Ministerstvo, popřípadě jím zřízená organizace, sdružuje pro statistické účely a plnění dalších povinností podle tohoto zákona údaje z dokumentace škol a školských zařízení a ze školních matrik.* Ministerstvo se domnívá, že další povinnosti zahrnují zpracování těchto časových řad, které slouží pro účely mapování průchodnosti vzdělávací soustavy. Naopak Úřad se domnívá, že pro zpracování pro statistické účely lze osobní údaje

shromáždit každý rok, statisticky zpracovat a zlikvidovat. V žádném případě takto definovaný účel nestačí pro vytvoření registru všech studentů.

Matrika studentů zpracovává také údaje o *zdravotní způsobilosti ke vzdělávání a o zdravotních obtížích, které by mohly mít vliv na průběh vzdělání*. Tyto údaje lze ovšem dle zákona zpracovávat pouze anonymně. Způsob zpracování, který zvolilo Ministerstvo – tj. že každý žák byl jednou charakterizován rodným číslem a informacemi o studiu a podruhé kódem, informacemi o studiu a informacemi o zdravotních obtížích – nebyl anonymní.

OBSAH E-MAILOVÉ SCHRÁNKY

Na Úřad přišla stížnost bývalého rektora jedné vysoké školy, že po jmenování nového rektora mu byla znepřístupněna e-mailová schránka, kterou měl pod svým jménem na škole zřízenou, a naopak, byla zpřístupněna novému vedení školy. Inspektorka zahájila kontrolu a zjistila, že ještě po devíti měsících stále adresa existuje a do došlé pošty má přístup nový rektor s odůvodněním, že se nejednalo o soukromou adresu, ale o adresu rektora školy, tudíž bylo třeba v případě např. urgencye ověřit, zda do schránky bývalého rektora nedošla důležitá pošta určená vysoké škole, a ne osobě bývalého rektora.

Kontrolující posoudili případ následovně:

Vysoká škola oprávněně zpracovává osobní údaje svých zaměstnanců včetně technického zabezpečení e-mailové korespondence, tudíž je správcem osobních údajů (§ 4 písm. j) zákona o ochraně osobních údajů) svých zaměstnanců včetně rektora.

Vzhledem k tomu, že bývalý rektor nepoužíval dvě různé e-mailové schránky, z nichž jedna by se týkala pouze korespondence s ním jakožto s rektorem Vysoké školy a druhá by obsahovala korespondenci s jeho osobou jakožto s učitelem nebo kolegou, je třeba považovat veškerou korespondenci v e-mailové schránce za jeho osobní, k níž má mít přístup pouze on, přestože k tomu je používán server školy. To, že jde o osobní schránku, je také zřejmé z toho, že ke své e-mailové poště má přístup pouze zaměstnanec po přihlášení svým jménem a heslem.

Proto ve chvíli, kdy bývalý rektor přestal být rektorem a v daném případě i zaměstnancem Vysoké školy, měla být jeho e-mailová schránka zrušena. Neexistuje žádný důvod, aby tato schránka ještě po devíti měsících existovala a přitom k ní neměl bývalý rektor přístup. Pokud e-mailová schránka neexistuje, protože v instituci již nepůsobí osoba, která je adresátem, tato informace by měla být automaticky odesílateli sdělena a ten musí činit další kroky adekvátní tomuto poznatku.

Podle ustanovení § 5 odst. 2 zákona o ochraně osobních údajů smí správce zpracovávat osobní údaje pouze se souhlasem subjektu údajů nebo podle výjimek uvedených v tomto odstavci. Pokud se jedná o zaměstnance, jsou jeho osobní údaje zpracovávány také v souladu se zákony týkajícími se vztahu zaměstnavatele a zaměstnance. V případě, že bývalý rektor už nebyl zaměstnancem Vysoké školy, neměl kontrolovaný žádný právní důvod pro zpracování jeho osobních údajů v podobě e-mailové pošty. V době kontroly, tj. více než devět měsíců po odvolání z postu rektora a po ukončení jeho pracovního poměru, nezískal zaměstnavatel souhlas bývalého rektora se zpracováním jeho osobních údajů v podobě e-mailové schránky a dopisů, které v ní byly uloženy. Tudíž kontrolovaný porušil ustanovení § 5 odst. 2 zákona o ochraně osobních údajů, neboť zpracovával osobní údaje bývalého rektora, tj. obsah jeho e-mailové schránky, bez jeho souhlasu.

Problém, který škola viděla v nebezpečí z prodlení v případě korespondence adresované bývalému rektorovi, bylo třeba řešit jiným způsobem – kupříkladu zrušením osobní e-mailové schránky, automatickou informativní odpovědí, žádostí o zaslání na adresu nového rektora. V žádném případě nebyla Vysoká škola oprávněna prohlížet soukromou poštu svého bývalého zaměstnance.

Ustanovení § 13 odst. 1 zákona o ochraně osobních údajů stanoví povinnost správce *přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému*

zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů. Přístup do e-mailové schránky bývalého rektora bez jeho souhlasu nebyl oprávněným přístupem, jednalo se tudíž o porušení povinnosti při zabezpečení osobních údajů (§ 13 zákona o ochraně osobních údajů).

Je třeba zohlednit rovněž čl. 13 Listiny základních práv a svobod, která je součástí Ústavy ČR: *Nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí nebo zasílaných poštou anebo jiným způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.* Nelze si zajisté představit, že by normální dopis, adresovaný jmenovitě bývalému rektorovi, byl na adresu Vysoké školy, kontrolovaný otevřen.

Kontrolující tudíž konstatovali porušení § 5 odst. 2 zákona o ochraně osobních údajů, neboť Vysoká škola zpracovávala některé osobní údaje (obsah e-mailové schránky) bývalého zaměstnance bez jeho souhlasu, a § 13 odst. 1 zákona o ochraně osobních údajů, neboť umožnila přístup do e-mailové schránky bývalého rektora osobě postrádající oprávnění pro tento přístup.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PROSTŘEDNICTVÍM KAMEROVÝCH SYSTÉMŮ

I přes skutečnost, že v současné době nás kamery sledují téměř na každém kroku, eviduje Úřad v registru zpracování osobních údajů přibližně 6 000 registrací kamerových systémů, což je dle odhadu Úřadu pouze nepatrná část z těch v České republice používaných. V roce 2010 dokonce došlo ke snížení počtu registrovaných subjektů.

Prostřednictvím nově podaných registrací kamerových systémů bylo zjištěno, že se zvyšuje podíl osob, které se samy na provozu kamerových systémů nepodílejí, ale zajišťují si tuto činnost prostřednictvím specializovaných firem. Počet takových subjektů vzrostl od roku 2006 o téměř 50 %. Dochází tedy k možnosti kumulace shromažďovaných informací u několika málo specializovaných firem, zejména bezpečnostních agentur. I z tohoto důvodu byl v rámci registrace kladen značný důraz na doložení plnění povinností o zabezpečení osobních údajů.

V rámci předkládaných oznámení o zpracování osobních údajů se opakovaně vyskytovaly problémy související s monitorováním zaměstnanců, monitorováním zákazníků a klientů, a to v čekárnách, jednacích a konferenčních místnostech. Tento trend jde napříč jak veřejným, tak soukromým sektorem. Záměr instalovat a provozovat kamerové systémy mají školy, hotelové společnosti, restaurace, fitness centra, koupaliště, nemocnice, obce a města. Přestože Úřad dlouhodobě ve svých stanoviscích a rozhodnutích sděluje podmínky, za kterých lze kamerové systémy provozovat, objevují se v nových registračních oznámeních stále stejné problémy. Jedná se zejména o samotné naplnění stanoveného účelu, tedy konkrétně umístění a nastavení jednotlivých kamer a doby uchovávání záznamů; právě doba uchovávání v řadě případů značně přesahovala lhůtu, kterou Úřad obecně považuje za přiměřenou (3 dny). Na základě výzvy Úřadu došlo téměř ve všech případech podávaného oznámení k opravě a redukci podávaného oznámení.

Jedním z častých problémů, který je nutné v rámci registračního řízení řešit, zůstává obecná informace, že prostřednictvím kamerového systému jsou zpracovávány citlivé údaje, zejména biometrické. Výjimkou jsou pouze kamerové systémy využívající novou technologii, jejichž prostřednictvím lze ověřovat a autentizovat konkrétní fyzickou osobu pomocí některých z biometrických charakteristik (vyhledávání dle obličejových markant, charakteristiky chůze apod.).

Opakujícím se nedostatkem při registraci je to, že správci kamerových systémů v bytových domech předkládají svá oznámení o zahájení zpracování osobních údajů bez souhlasu všech a nahrazují ho buď jen souhlasem majitele, resp. členů představenstva, nebo pouze zástupce jednotlivých bytů (např. členů společenství, členů družstva).

Stále stoupající trend má počet přijatých oznámení fyzických osob, zejména vlastníků nemovitostí, které jsou užívány výhradně pro bydlení, tedy pro soukromé účely. V těchto případech nevzniká povinnost registrace, neboť se jedná o zpracování osobních údajů určených pro vlastní potřebu.

Nově jsou ve větším počtu zaznamenávány žádosti o registraci kamerových systémů se současným nahráváním audiozáznamu. Převážná většina provozovatelů uvádí, že účelem tohoto monitorování je ochrana majetku, identifikace pachatele, zloděje, vandala. Na základě upozornění Úřadu o nepřiměřeném, neproporcionálním zásahu do soukromí všech dotčených osob převážná většina těchto provozovatelů změnila nastavení systémů a audiozáznamy nepořizuje. Jedná se o klasický případ: Dostupnost technologie vede správce k postoji „když to existuje, proč bychom to nevyužili“.

Úřad věnuje mnoho sil poskytování konzultací a odpovídání na stále se zvyšující počet dotazů a stížností. Ze statistiky odboru pro styk s veřejností vyplývá, že více než jedna pětina podání se týkala provozování kamerových systémů na pracovištích. Úřad pokračoval i v roce 2010 ve spolupráci se Státním úřadem inspekce práce v Opavě. Na 20 stížností a podnětů obsahujících důvodné podezření z porušení § 316 zákoníku práce bylo postoupeno uvedenému úřadu nebo přímo příslušným oblastním inspektorátům práce. Z vyhodnocení zpětné vazby lze konstatovat, že od počátečního váhavého přístupu je zřejmý posun k rutinnímu řešení problémů ve věcné působnosti těchto orgánů. Ve zbylých případech bylo stěžovatelům doporučeno své podání doplnit, konkretizovat a adresovat příslušnému oblastnímu inspektorátu práce.

Značná část podání, celá pětina, směřovala vůči provozování kamerových systémů fyzickými osobami za účelem ochrany majetku, v drtivé většině vlastněných nemovitostí. Až na výjimky nebylo z obsahu podání zjištěno překročení osobní potřeby ve smyslu ustanovení § 3 odst. 3 zákona o ochraně osobních údajů, např. zveřejnění pořízených záznamů nebo jejich využití pro jiný účel, a proto byly stížnosti odkládány jako nedůvodné, neboť neumožňovaly Úřadu uplatnit jeho dozorové kompetence. Podávajícím osobám bylo vysvětleno, že popsaná činnost může být v rozporu s občanským zákoníkem, a bylo jim doporučeno řešit věc občanskoprávní žalobou.

Na základě plánu kontrol a oprávněných přijatých podnětů uskutečnili v roce 2010 inspektoři Úřadu 25 kontrol se zaměřením na zpracování osobních údajů prostřednictvím kamerových systémů. Kontrolování byli správci osobních údajů, kteří provozovali kamerové systémy z různých důvodů a v různých prostorách a zařízeních.

Pro velkou část subjektů údajů je dlouhodobě citlivým tématem provozování kamerových systémů v bytových domech, což vnímají jako velký zásah do svého soukromí. Úřad zaujal k této problematice již v roce 2008 poměrně přísné stanovisko doporučující příslušným správcům osobních údajů disponovat souhlasem všech osob v bytovém domě bydlících. Své postoje Úřad prosazoval i prostřednictvím Asociace bytových družstev. Důvodné podezření na porušování zákona o ochraně osobních údajů při provozování kamerových systémů se záznamovým zařízením v bytových domech tvořilo největší část ze 13 případů předaných ke kontrole.

Na základě konkrétních stížností bylo provedeno několik kontrol v bytových domech. Výsledky těchto kontrol lze shrnout do poznatků, které Úřad zohlednil ve svém stanovisku ke zpracování osobních údajů prostřednictvím kamerových systémů v bytových domech. Základním problémem však zůstává disproporce preventivního účinku umístěných kamer oproti skutečně získávaným informacím v případě jednotlivých excesů. Inspektoři Úřadu se při kontrolách bytových domů často setkávají s nepochopením potřeby vyváženosti mezi ochranou majetku a ochranou soukromí ubytovaných osob. Souhlas jednotlivých obyvatel domů je často nahrazován souhlasem vedení družstva nebo společenství vlastníků; častým prohřeškem je nezabezpečený přístup k záznamové jednotce, využívání pořízených záznamů k vyřizování si různých sousedských sporů.

V jednom případě si předseda společenství bytových jednotek pořizoval každodenní poznámky o chování nájemníků a ty pak následně zveřejňoval na nástěnce ve vstupu do domu. Kamerové systémy tak často suplují nedobré vzájemné vztahy mezi lidmi. Úřad zaznamenal, že výše uvedený rozpor se projevil i v tom, že tyto subjekty se neztotožňují ani s kontrolními závěry, ani s rozhodnutími ze správního řízení a v téměř stoprocentním počtu podávají odvolání formou opravného prostředku,

ve třech případech byly proti rozhodnutím předsedy Úřadu o rozkladu podány soudní žaloby, přestože na webových stránkách Úřadu jsou zveřejněny rozsudky soudů z předcházejících žalob ve věci narušování soukromí v bytových domech, které potvrzují rozhodnutí Úřadu.

Za nový jev v roce 2010 lze považovat masivní snahu o nasazování kamerových systémů v prostředcích městské hromadné dopravy, vlakové a autobusové přepravy. Úřad je v tomto směru velmi obezřetný a důsledně individuálně posuzuje každý případ *ad hoc* za využití všech zákonných prostředků, zejména zahájení řízení z vlastního podnětu ve smyslu § 17 zákona o ochraně osobních údajů v případě, kdy existuje důvodná obava z porušování citovaného zákona. Cílem není *a priori* bránit využití kamerových systémů k ochraně života a zdraví cestujících i zaměstnanců nebo ochraně majetku, ale korigovat a nepřipustit nepřiměřené zásahy do soukromí přepravovaných osob.

V rámci kontrolního plánu Úřadu byl prověřen rozsáhlý technický kamerový systém jednoho krajského úřadu. Kamerový systém využíval 60 jednotlivých kamer. Kontrolující inspektorka prověřila jak umístění jednotlivých kamer, tak i zabezpečení přístupu k pořízeným záznamům. Zjistila, že záznamová jednotka je umístěna na pracovišti bezpečnostního ředitele, sídlícího v zabezpečené části objektu (stupeň „D“). Rovněž se zaměřila na dodržování povinností pořizovat auditní záznamy jednotlivých přístupů k pořízeným záznamům. Kontrolou nebylo shledáno porušení povinností stanovených zákonem o ochraně osobních údajů.

Se shodným výsledkem dopadla kontrola kamerového systému provedená na Celním ředitelství příslušného krajského města.

Na základě obdržení podnětů byly uskutečněny kontroly ve čtyřech školách, kde byly jak ve vnitřních, tak venkovních prostorách umístěny kamerové systémy. Bylo zjištěno, že v jednom případě dochází ve škole k neoprávněnému využívání kamerového systému, neboť šlo o monitorování žáků, učitelů a návštěvníků v rozsahu, který nebyl nezbytný pro naplnění stanoveného účelu, jímž byla ochrana majetku školy. U další kontrolované školy bylo zjištěno, že škola jako provozovatel kamerového systému nesplnila povinnost informovat monitorované osoby v rozsahu, který zákon o ochraně osobních údajů ukládá, a současně škola nesplnila povinnost podat u Úřadu oznámení o zahájení zpracování osobních údajů prostřednictvím kamerového systému.

Přesto se projevuje účinná spolupráce s příslušnými institucemi v oblasti školských zařízení a kontrolní činnost České školní inspekce a metodické ovlivňování Ministerstva školství, mládeže a tělovýchovy přispívá ke změně přístupů jednotlivých škol k využívání kamerových systémů. V podstatě žádné případy excesů typu provozování kamerových systémů ve třídách, kabinetech či ředitelnách nebyly zaznamenány.

V roce 2010 byly kontrolovány dva sportovní areály s bazény. Společným důvodem umístění kamer v těchto zařízeních jsou časté drobné krádeže v šatnách a v prostorách skříněk. Úřad při kontrole však konstatoval, že není přípustné monitorovat a zaznamenávat převlékání návštěvníků, neboť v takovém případě je narušen princip proporcionality. V nápravných opatřeních bylo proto uloženo ukončit takové monitorování a provozovateli doporučeno, aby zajistil pro převlékání samostatný prostor, oddělený od místnosti, kde jsou umístěny skřínky pro návštěvníky.

Velice komplikovaná byla kontrola provedená inspektorkou Úřadu na základě podnětu zástupkyně veřejného ochránce práv ve dvou psychiatrických léčebnách. Obě léčebny jsou současně využívány i jako detenční zařízení, ve kterých jsou umístěny osoby na základě rozhodnutí soudu o nařízené ochranné léčbě. Jedná se o pacienty po výkonu trestu odnětí svobody, kterým je ve většině případů nařízena sexuologická ochranná léčba. Pacienti jsou přijímáni běžnými zdravotnickými pracovníky přímo od policie nebo od vězeňské služby, navíc často v neklidném stavu. Vzhledem k předchozímu šetření kanceláře veřejného ochránce práv bylo v rámci kontrol Úřadu zjištěno, že v obou léčebnách byl provoz kamerových systémů změněn tak, že nyní není pořizován záznam z kamerového systému a nedochází tak ke zpracování osobních údajů pacientů ve smyslu § 4 písm. e) zákona o ochraně osobních údajů. Inspektorka Úřadu však rovněž konstatovala, že ač je tato léčebna využívána jak pro

zdravotnické pacienty s běžnou léčbou, tak i pro pacienty umístěné na základě rozhodnutí soudu, není otázka bezpečnosti, včetně zákonné úpravy používání kamerových systémů, řešena ani rezortem zdravotnictví, ani rezortem spravedlnosti. Zástupci obou léčeben téměř ve shodě uváděli, že v zařízení dochází k napadání zaměstnanců, spolupacientů a k poškozování majetku. Kromě své zdravotnické náplně tak léčebny suplují dosud neexistující detenční ústavy, ovšem bez oprávnění, kterými disponují vězeňská zařízení.

Několik kontrol bylo provedeno na základě podnětů občanů u obecních nebo městských úřadů, provozujících městské kamerové systémy. V jednom případě stěžovatel napadl umístění jedné z kamer v obci, která měla být namířena na jeho dům a mířit do jeho oken. Stěžovatel se na Úřad obrátil až poté, co písemně požádal o vysvětlení starostu obce, který mu odpověděl neurčitě. Na základě této skutečnosti provedla inspektorka Úřadu v obci kontrolu. Kontrolou však nebylo zjištěno porušení zákona o ochraně osobních údajů.

Typickým případem byla zjištění, která vyplynula při šetření provozu kamerového systému v jednom severomoravském městě. V daném případě rozhodlo vedení města o umístění jedné kamery na střechu radnice. Důvodem pro umístění kamery bylo zpřístupnit prostřednictvím on-line záběrů život čápů, kteří si na komíně radnice vybudovali hnízdo. Radnice informaci o tomto záměru, včetně on-line záběru, umístila na svých webových stránkách. Problém nastal v okamžiku, kdy jedna z občanek města zjistila, že v záběru kamery je zachycen i její dům, včetně zahrady, a proto se obrátila na Úřad s žádostí o pomoc. V tomto případě stačilo k nápravě pootočit kameru tak, aby v záběru zůstalo skutečně jen čapí hnízdo.

Další stížnost obdržel Úřad od fyzické osoby, jejíž soused si stěžoval, že jej provozovatel kamery sleduje. Na místě bylo zjištěno, že kamery sledují výhradně soukromý majetek provozovatele kamer.

Spojovacím článkem podnětů, na jejichž základě došlo k těmto kontrolám, je ve své podstatě neschopnost řešit drobné sousedské problémy přiměřeným způsobem a nepochopení podstaty ochrany soukromí. Na druhé straně se však Úřad zabýval v rámci své dozorové činnosti i zneužíváním kamerové technologie. V rámci kontroly byla například řešena stížnost na umístění kamer na toaletách v restauraci. V tomto případě provozovatel jako správce osobních údajů porušil zásadu přiměřeného zásahu do soukromí, ale především nezabezpečil ani přístup k pořizovaným záznamům. Provozovateli byla v následném správním řízení uložena pokuta za porušení povinností stanovených zákonem o ochraně osobních údajů.

Je třeba zmínit výrazný nárůst žádostí o konzultaci ze strany Policie České republiky, obecní policie, obcí, krajských úřadů, magistrátů měst i dalších institucí, jejichž obsahem byly možnosti provozování tzv. městských kamerových systémů. Opět ve spolupráci, tentokrát s Ministerstvem vnitra, bylo Úřadem dosaženo stavu, kdy tyto kamerové systémy využívané především k prevenci pouliční kriminality provozují orgány příslušné k zabezpečování veřejného pořádku, nikoliv přímo města a obce.

V roce 2010 se také zvýšil počet oznámení a případů postoupených Policií ČR, městskou, resp. obecní policií a jednotlivými správními orgány ve věcech spadajících do kompetence Úřadu. Jeden z takto postoupených podnětů byl řešen v rámci správního řízení. Bylo zjištěno a dokázáno, že provozovatel ubytovny instaloval v jednom z pokojů kameru a pořizované záznamy si uchovával ve svém soukromém počítači, přičemž kamera byla zamaskována. V počítači provozovatele bylo zdokumentováno 577 uložených videonahrávek, zachycujících návštěvníky pokoje v intimních osobních situacích, a to za období téměř tří let. Tento provozovatel nejenže neměl od monitorovaných osob souhlas s pořizováním nahrávek, ale nesplnil ani zákonnou informační povinnost o skutečnosti, že v ubytovně je instalován kamerový systém. V tomto případě Úřad v rámci správního řízení konstatoval, že provozovatel kamerového systému porušil povinnost správce osobních údajů zpracovávat osobní údaje pouze v souladu se stanoveným účelem, a zejména porušil povinnost, že zpracování osobních údajů nesmí být v rozporu s právem subjektu údajů, tedy monitorované osoby, na ochranu jeho soukromého a osobního života. Musí se vždy jednat o rovnováhu mezi dvěma právy, kdy v daném případě prokazatelně převažuje právo na ochranu soukromí subjektu údajů nad právem na deklarovanou ochranu majetku. Za tuto činnost byla provozovateli uložena pokuta ve výši 100 000 Kč.

O dlouhodobém jednotném, a tudíž předvídatelném postupu Úřadu svědčí i skutečnost, že v rámci druhostupňových řízení, a to jak námitkových, tak i rozkladových, byly všechny podané opravné prostředky předsedou Úřadu zamítnuty.

NEBANKOVNÍ SUBJEKTY

V poslední době prudce narůstá zájem klientů o služby poskytované jinými společnostmi, než jakými jsou banky a obdobné peněžní instituce, přičemž hovoříme o činnosti tzv. nebankovních subjektů. Jedná se o obchodní společnosti, které jsou podle ustanovení § 56 odst. 1 zákona č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů (dále jen „obchodní zákoník“), právnickými osobami, založenými podle příslušných ustanovení obchodního zákoníku, poskytující úvěry svým klientům na základě uzavřených smluv o úvěru podle ustanovení § 497 a násl., a nikoliv o bankovní subjekty, jež jsou podle ustanovení § 1 odst. 1) zákona č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, právnickými osobami, a to akciovými společnostmi, založenými také podle obchodního zákoníku, které podle ustanovení § 1 odst. 1 písm. b) zákona o bankách, poskytují také úvěry, ale které k výkonu této činnosti, na rozdíl od ostatních obchodních společností, mají bankovní licenci.

Tyto obchodní společnosti, které k poskytování produktů nemají bankovní licenci, nazýváme v této kapitole nebankovními subjekty. Produkty poskytované nebankovními subjekty mají oproti obvyklým produktům bankovních institucí pro klienty zdánlivě mnoho výhod a vyznačují se velmi nízkými požadavky na zákazníka. Půjčky a úvěry jsou snadno získatelné a kontrola klientovy bonity a spolehlivosti splácet je minimální. Výhodou je rychlé vyřízení půjčky, peníze zákazník získá hned na ruku, nebo v krátké době. Smluvní vztah je sjednáván často neformálně přes internet nebo mobilní telefon. Po odeslání formuláře, či pouhé SMS, je klient kontaktován operátorem s obchodními podmínkami a pokyny k odsouhlasení půjčky či obdobného finančního produktu. Leckdy jsou půjčka nebo úvěr poskytnuty nebankovním subjektem klientovi, který by u bankovní společnosti na finanční produkt nedosáhl prostě proto, že není schopen splácet. Často je poskytována peněžní půjčka a úvěr na koupi věci denní potřeby, například mobilního telefonu. Finanční produkty jsou poskytovány na zdánlivě neformální bázi, kdy ke kladnému vyřízení není leckdy zapotřebí ani doklad o výši příjmů nebo například výpis z registru dlužníků. Tato zdánlivá bezproblémovost získání produktu však vede až k lehkomyšlnému uzavření smlouvy, kdy klientovi teprve při čerpání produktu vyvstávají před očima podmínky plnění. Ruku v ruce s tím, jak klient zjišťuje realitu, vzrůstá jeho potřeba si stěžovat.

Mezi nebankovní subjekty řadíme i ty společnosti, které nabízejí klientům finanční poradenství. Tyto nebankovní subjekty mohou kromě finančního poradenství nabízet prostřednictvím svých obchodních zástupců i finanční produkty vybraných bankovních subjektů, s nimiž mají uzavřeny příslušné smlouvy.

Obchodní zástupci, resp. spolupracovníci nebankovního subjektu, vyhledávají potenciální klienty a poskytují jim jednak poradenské služby a konzultace z oblasti finančního poradenství a také sjednávají smlouvy na finanční produkty pouze portfolia těch bankovních subjektů, s nimiž má nebankovní subjekt uzavřenu smlouvu, neboť mají osvědčení, certifikát vydaný Českou národní bankou, dříve Komisí pro cenné papíry, pro tuto činnost. Každou uzavřenou smlouvu klienta s bankovním subjektem předává obchodní zástupce jak klientovi, tak i bankovnímu subjektu z portfolia nebankovního subjektu a třetí stejnopis smlouvy si ponechává. Obchodní zástupci, resp. spolupracovníci, jsou v právním vztahu ke klientovi, kterého získali a jemuž poskytují zmíněné poradenské služby a konzultace nebo s nímž uzavírají předmětnou smlouvu či smlouvy, ve smyslu ustanovení § 4 písm. j) zákona o ochraně osobních údajů správci, neboť v těchto případech oni určují účel a prostředky zpracování osobních údajů, provádějí zpracování a odpovídají za něj. V důsledku uvedeného se na obchodní zástupce, resp. spolupracovníky, v tomto případě vztahuje ustanovení § 16 odst. 1 zákona o ochraně osobních údajů, které stanoví, že ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování podle zákona o ochraně osobních údajů, s výjimkou zpracování uvedených v § 18 zákona o ochraně osobních údajů, je povinen tuto skutečnost písemně oznámit Úřadu před zpracováním osobních údajů.

Obchodní zástupci, resp. spolupracovníci, si získávají své nové spolupracovníky, kteří by také měli poskytovat předmětné poradenské služby a konzultace a uzavírat smlouvy s klienty, jež získají, s obchodními partnery svého nebankovního subjektu.

Zřejmě vzhledem ke zde uvedenému Úřad v poslední době konstatuje enormní nárůst stížností na nezákonné zpracovávání osobních údajů těmito společnostmi. Je třeba si uvědomit, že objem obchodu s úvěrovými a obdobnými produkty prudce stoupá a nebankovní subjekty se tak stávají jedním z významných soukromých správců osobních údajů. K personifikaci klienta nebankovní společnosti vyžadují velké množství osobních údajů, které klient poskytuje leckdy ještě před uzavřením smluvního vztahu. Jednou z oblastí, ke které zaměřil Úřad svoji kontrolní pozornost, byla proto logicky také činnost nebankovních subjektů a tyto kontroly byly zařazeny do plánu kontrolní činnosti Úřadu.

V roce 2010 inspektoři Úřadu dokončili několik kontrol, jejichž předmětem bylo plnění povinností podle zákona o ochraně osobních údajů obchodními společnostmi jakožto správci ve smyslu ustanovení § 4 písm. j) tohoto zákona při zpracování osobních údajů za účelem, k němuž mají být osobní údaje zpracovány, jímž je zpracování osobních údajů fyzických osob, s nimiž příslušná obchodní společnost, resp. kontrolovaný, je ve smluvním vztahu. Při uzavírání úvěrových smluv a při jejich plnění dochází ze strany těchto obchodních společností ke zpracování osobních údajů fyzických osob, s nimiž příslušná obchodní společnost, resp. kontrolovaný, uzavřela úvěrové smlouvy. Stížnosti na nebankovní společnosti se zpravidla týkaly toho, že v souvislosti s uzavřenou smlouvou dochází ke zneužívání poskytnutých osobních údajů. Kontroly nebankovních subjektů byly provedeny komplexně z pohledu celého zákona o ochraně osobních údajů, tedy nad rámec skutečností uvedených v podnětech stěžovatelů, a zabývaly se veškerým zpracováváním osobních údajů kontrolovanými. Nejčtenějším zjištěným porušením bylo zpracování osobních údajů bez souhlasu klienta a nadbytečné shromažďování osobních údajů.

Jako modelový příklad pochybení lze uvést kontrolní zjištění u podnikatele fyzické osoby, který je prodejcem spotřebního zboží a pro zákazníky zprostředkovává zaplacení prodávaného zboží sjednáním úvěru u finanční společnosti, přičemž prodejce je zároveň obchodním zástupcem na základě smlouvy o obchodním zastoupení s nebankovním subjektem. Nastala zde, z pohledu zákona o ochraně osobních údajů, zajímavá situace, kdy prodejce zboží získává osobní údaje svých zákazníků, což však nečiní pro účel prodeje zboží, ale pro účel sjednání úvěru. Prakticky došlo k tomu, že údaje zákazníka získané pro uzavření úvěru použil i k jinému účelu. Tento kontrolovaný si neuvědomil, že jedná v rozporu se zákonem, když osobní údaje zákazníka použil k jinému než stanovenému účelu a zároveň tak učinil bez souhlasu subjektu údajů pro takové zpracování.

Jako další příklad lze uvést stížnost na to, že během platnosti smlouvy a pravidelného splácení se klientovi několikrát stalo, že na číslo jeho účtu připisovala jistá společnost platby od cizího (jiného) klienta, což bylo dokonce uváděno i na výpisech, které mu při každém pohybu na jeho účtu společnost na jeho náklady posílala, takže platil i výpisy, jež se týkaly cizích úhrad na jeho účet. Na všechny případy cizích plateb na jeho účet vždy okamžitě společnost telefonicky upozornil, ta ale, přestože si telefony nahrávala, nikdy nesjedнала nápravu. V tomto případě bylo kontrolou zjištěno, že se kontrolovaná společnost dopustila spáchání správního deliktu, když zpracovávala nepřesné osobní údaje v případě plateb k účtu, které neodpovídaly povinnosti správce zpracovávat pouze přesné osobní údaje, které získal v souladu se zákonem; že věc neproověřil a neprovedl potřebnou nápravu, takto zpracovával nepřesné osobní údaje.

Porušení bylo zjištěno ve vztahu ke klientům kontrolovaného, když kontrolovaný získal vinou selhání telefonní operátorky nepřesné údaje o svém klientovi, údaje dále zpracovával a přes telefonické upozornění subjektu údajů věc neproověřil a neprovedl potřebnou nápravu. Takto bylo porušeno ustanovení § 5 odst. 1 písm. c) zákona o ochraně osobních údajů. Zpracováním nepřesného osobního údaje z důvodu selhání telefonní operátorky, přestože na to subjekt údajů opakovaně upozorňoval a kontrolovaný nesjednal nápravu, nebankovní subjekt zpracovával nepřesné osobní údaje, které neodpovídaly povinnosti správce zpracovávat pouze přesné osobní údaje, a tak porušil i ustanovení § 21 odst. 2 zákona o ochraně osobních údajů. Další stížnost byla podána na jinou společnost (nebankovní

subjekt), která měla nahrávat veškeré telefonní hovory, aniž by o tom informovala svoje potenciální nebo i stávající klienty, kteří běžně sdělují svoje interní, mnohdy i velmi osobní informace nebo iniciály, neboť se firma zabývá půjčováním peněz formou zpětných nebo obyčejných leasingů; navíc do firmy zpravidla telefonují lidé, kteří jsou ve finanční tísní, telefonní hovory jsou ukládány v archivu a mají k nim přístup prakticky všichni zaměstnanci. U této společnosti bylo zjištěno porušení povinnosti ve vztahu ke zpracovávaným osobním údajům zaměstnanců společnosti.

Jako další příklad lze uvést i stížnost na společnost, která měla zneužít osobní údaje klienta získané za účelem uzavření smlouvy o úvěru prodejcem spotřebního zboží tak, že je použil ve svém vyjádření v otištěném novinovém článku jako reakci ve sporu o reklamaci zboží. I zde inspektor Úřadu zjistil porušení zákona o ochraně osobních údajů.

Právně zajímavá situace u nebankovních subjektů byla zjištěna při určování správce a zpracovatele osobních údajů. Nebankovní subjekty totiž poskytují služby (zpravidla půjčky a úvěry) jednak přímo, a takto stojí v pozici správce osobních údajů podle ustanovení § 4 písm. j) zákona o ochraně osobních údajů, ale také velmi často služby poskytují prostřednictvím jiných osob. Tito obchodní zástupci pak podle vztahu mohou být samostatnými správci osobních údajů nebo jsou zpracovateli osobních údajů ve smyslu ustanovení § 4 písm. k) zákona o ochraně osobních údajů. V takovém vztahu správce zpracovatel bylo téměř pravidlem zjištění porušení ustanovení § 6 zákona o ochraně osobních údajů a z kontrol vyplývá obecné zjištění, že řádně uzavřená zpracovatelská smlouva je více výjimkou než pravidlem. Takto pro provázanost ustanovení zákona o ochraně osobních údajů bylo velmi častým zjištěním porušení ustanovení § 13 zákona o ochraně osobních údajů, tedy zjištění, že nebyla přijata dostatečná opatření při zabezpečení osobních údajů.

Dalším zjištěným porušením bylo to, že kontrolované subjekty buď vůbec nestanovily lhůty pro uchovávání osobních údajů zejména ze zpracování osobních údajů zaměstnanců, uchazečů o zaměstnání a bývalých zaměstnanců, nebo lhůty stanovily bezúčelně dlouhé, nebo také tak, že nevytvořily tlak na odpovědné zaměstnance, aby nepotřebné dokumenty okamžitě zlikvidovali.

Kontrolování často nedbali na ochranu soukromého a osobního života subjektu údajů, ale naopak tam, kde kontrolovaný pořizoval kopie dokladů s údaji, které vypovídaly o soukromí osob, aniž byl dán účel jejich zpracování, do jeho soukromí a osobního života zasahovali. V mnoha případech kontrolované subjekty odstranily zjištěná porušení již v průběhu kontroly tak, že nebylo třeba ukládat nápravná opatření, čímž došlo k odstranění protiprávního stavu, tedy nejvýznamnějšímu cíli prováděných kontrol Úřadem. Tam, kde k tomu nedošlo, pro odstranění zjištěných nedostatků byla uložena nápravná opatření spočívající zejména v ukončení shromažďování osobních údajů – pořizování fotokopie občanského průkazu, fotokopie karty VZP, fotokopie vysvědčení o státní závěrečné zkoušce a shromažďování evidenčního čísla občanského průkazu, neprodlenému naplňování informační povinnosti v rozsahu stanoveném ustanovením § 11 odst. 1 zákona o ochraně osobních údajů, a také o dalších právech stanovených v § 21 zákona o ochraně osobních údajů; musely být zlikvidovány nadbytečné osobní údaje ze zpracování osobních údajů – to vše dle výsledků jednotlivých posouzení. Na základě výsledků kontrol vedl Úřad s kontrolovanými subjekty také správní řízení, v nichž byla vždy za porušení zákona uložena sankce.

Kontrolami bylo zjištěno, že porušení ustanovení zákona o ochraně osobních údajů se v zásadě opakují bez ohledu na předmět činnosti kontrolovaného. Lze zobecnit, že činnost nebankovních subjektů sice má svá specifika, avšak četnost ani druhy spáchaných správních deliktů se od jiných kontrolovaných výrazně neodlišují. Zjištěná porušení zákona o ochraně osobních údajů nasvědčují spíše neznanosti zákonných ustanovení a z nich plynoucích práv a povinností než vědomému a úmyslnému porušování zákona o ochraně osobních údajů, což ovšem nikterak nesnižuje odpovědnost za spáchané správní delikty. Činnost nebankovních subjektů nelze paušálně negativně posuzovat. Musí si však uvědomit, že se při zpracovávání osobních údajů nemohou chovat úplně stejně jako bankovní instituce. Především je však třeba, aby si klienti i v rizikové situaci, jakou je potřeba financí či úvěru, uvědomili, že zpracování osobních údajů a s tím související operace může znamenat riziko pro jejich soukromí, a neposkytovali osobní údaje bez rozmyslu výměnou za získání zdánlivých výhod.

V roce 2010 byla na základě podnětu provedena kontrola dodržování povinností vyplývajících ze zákona o ochraně osobních údajů Společenstvím vlastníků bytů (dále jen „Společenství“) při zpracování osobních údajů vlastníků bytů a jejich rodinných příslušníků, nájemníků a jiných osob v souvislosti s vydáváním elektronických čipů pro ovládání vstupů do bytových objektů.

Čipy k otvírání dveří distribuovali vlastníkům jednotlivých bytů členové výboru Společenství, kteří jim zároveň předložili dotazník, na jehož vyplnění bylo vydání čipů vázáno. Stěžovatelé považovali vyžadování informací o jednotlivých uživateli čipů (jejich vztah k majiteli, uvedení adresy u jiných osob atd.) za nedůvodné a vyvolalo v nich podezření, že dochází k porušení zákona o ochraně osobních údajů. Jejich pochybnost vyvolala také informace výboru, že použití čipů k otevření vchodových dveří bude výborem průběžně monitorováno, neboť každý čip je opatřen specifickým kódem, který je registrován na konkrétního vlastníka či nájemníka, a lze tak sledovat, kdo a kdy přichází.

Společenství v souvislosti s instalací elektromagnetických zámků oznámilo Úřadu účel a právní titul ke zpracování osobních údajů uživatelů bytů. Důvodem pro zavedení čipů (elektromagnetických zámků) byly škody na majetku Společenství i jednotlivých vlastníků bytových jednotek a ochrana života a zdraví nájemníků (v jednom z domů došlo k vraždě). V oznámení bylo uvedeno, že shromážděné osobní údaje budou zpracovávány na základě poskytnutého souhlasu uživatelů bytů.

Členové výboru Společenství na základě vyjádřeného souhlasu majitelů či spolumajitelů bytů přítomných na shromáždění Společenství požadovali při předání čipů základní údaje o uživateli bytu v rozsahu jméno, příjmení, vztah k majiteli a u jiných osob i adresu pobytu odlišnou od bytového objektu. V souvislosti s instalací elektromagnetických zámků Společenství vytvořilo databázi čipů ve spojení s konkrétními uživateli bytů, a při průchodu objektem tak byl evidován průchod uživatele s datem a časem příchodu a odchodu.

Kontrolující se zaměřili zejména na zpracování osobních údajů v nezbytném rozsahu, na právní titul ke zpracování a splnění informační povinnosti Společenství.

Podle § 5 odst. 1 písm. d) zákona o ochraně osobních údajů musí správce shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. U jiných osob, které nejsou příslušníky domácnosti majitele (spolumajitele) bytu, bylo zcela nadbytečné ve smyslu § 5 odst. 1 písm. d) zákona o ochraně osobních údajů zpracovávat údaje pro účely evidence elektronických čipů v rozsahu vztahu k majiteli bytu a adresy těchto osob. Společenství tak porušilo ustanovení § 5 odst. 1 písm. d) zákona o ochraně osobních údajů a kontrolou bylo Společenství uloženo nápravné opatření – zcela zlikvidovat databázi jiných osob, tj. odlišných od majitelů bytů.

Společenství jako správce osobních údajů musí plnit povinnosti stanovené zákonem o ochraně osobních údajů. Bez souhlasu tak může osobní údaje zpracovávat pouze tehdy, jsou-li naplněny podmínky pro výjimku podle § 5 odst. 2 písm. a) zákona o ochraně osobních údajů, tedy jestliže provádí zpracování podle zvláštních právních předpisů. Další výjimkou, kterou lze uplatnit, je § 5 odst. 2 písm. e) zákona o ochraně osobních údajů – souhlas subjektu údajů není vyžadován, jestliže je zpracování nezbytné pro ochranu práv a právem chráněných zájmů správce, zpracovatele, příjemce nebo jiné dotčené osoby.

Z důvodu personalizace distribuovaných čipů a monitorování průchodů nebylo možné uplatnit žádnou z výjimek stanovených zákonem o ochraně osobních údajů, a tedy zpracovávat osobní údaje bez souhlasu. Uvedené zpracování osobních údajů bylo možné provádět pouze na základě poskytnutého souhlasu všech nájemníků a jiných osob. Kontrolou bylo prověřováno, zda udělený souhlas splňuje veškeré náležitosti podle ustanovení § 5 odst. 4 a § 11 zákona o ochraně osobních údajů.

Kontrolou bylo zjištěno, že při shromažďování osobních údajů v souvislosti s přidělováním čipů uvedli někteří majitelé písemný nesouhlas se zpracováním osobních údajů. Taktéž při hlasování o monitorování průchodu objektů na shromáždění Společenství nedalo souhlas se zpracováním osobních údajů dalších sedm hlasujících. Společenství tak zpracováním osobních údajů uvedených osob, které nedaly souhlas se zpracováním osobních údajů nebo následně souhlas odvolaly proto, že nesouhlasily s monitorováním, porušilo ustanovení § 5 odst. 2 věta první zákona o ochraně osobních údajů.

Společenství bylo uloženo opatření upravit zpracování osobních údajů majitelů bytů, příslušníků jejich domácnosti, nájemníků a jiných osob pro vydávání elektronických čipů tak, aby evidence vstupů neobsahovala osobní údaje osob, které ke zpracování svých osobních údajů nedaly souhlas s poskytnutím osobních údajů k uvedenému účelu, případně ho odvolaly.

V souvislosti s kontrolním zjištěním je třeba uvést, že zabezpečovací zařízení vchodových dveří nesporně podstatně snižuje možnost vstupu do objektu neoprávněným osobám, a je tak i podstatně zvýšena bezpečnost osob a ochrana majetku v objektu samém. K uvedenému účelu pak u bytových objektů slouží elektronická zařízení zpravidla na principu čipu či číselného kódu, která umožňují bezproblémový vstup oprávněných osob, přičemž není nezbytné takový vstup evidovat tak, aby bylo určitelné, kdy oprávněná osoba do objektu vstoupila. Z hlediska účelu zabezpečovacího zařízení postačuje, že je evidován vstup oprávněné osoby, které byl vstup umožněn, a to bez její možné identifikace.

Společenství také nedostatečně naplnilo informační povinnost, jelikož informace o zpracování osobních údajů byla při shromažďování osobních údajů podána neúplně. Nebyl uveden zákonný důvod pro povinné poskytnutí osobních údajů a důsledky neuvedení osobních údajů a nebyla poskytnuta informace o dobrovolném poskytnutí osobních údajů. Společenství tím porušilo (nesplnilo) informační povinnost podle § 11 odst. 2 zákona o ochraně osobních údajů.

Proto byla kontrola uzavřena uložení opatření dodatečně zajistit důsledné splnění informační povinnosti podle § 11 odst. 2 zákona o ochraně osobních údajů. Za prokázané porušení zákona byla společnosti uložena pokuta.

APLIKACE ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ V KYNOLOGII

V Evropě, a tedy rovněž v České republice, existují dvě navzájem se neuznávající kynologické organizace. *Uvedme na vysvětlenou: Československá kynologická unie vznikla v roce 1929 (ČSKU) a zastupovala kynologii vůči zahraničí. Na generálním zasedání FCI (Fédération Cynologique Internationale) pořádaném ve dnech 21.–23. března 1934 v Monte Carlu se stalo Československo řádným členem zastoupeným právě ČSKU. V současné době je právním nástupcem Českomoravská kynologická unie. Současně existuje i Českomoravská kynologická federace, která je členem UCI – United kennel Clubs International, což je kynologická organizace, která byla založena před 50 lety v tehdejší Spolkové republice Německo.*

Kynologie je zájmová činnost, sloužící k zachování charakteristických vlastností jednotlivých plemen.

Majitelé psů, tj. jejich chovatelé, se organizují do klubů dle příslušných psích ras. Každý klub se řídí vlastními stanovami a je zřízen dle občanského zákoníku jako zájmové sdružení osob. Tyto kluby se za účelem zahraničního zastoupení sdružují do výše uvedených organizací. Každý z nich zpracovává osobní údaje svých členů; zpracováním osobních údajů je třeba chápat nejen informace o členech, ale i většinu informací o jednotlivých psech, neboť tyto psi jsou vlastněni svými majiteli, a tudíž se *de facto* jedná o osobní údaje jejich majitelů. Osobní údaje, jak stanoví zákon o ochraně osobních údajů, lze v daném případě zpracovávat pouze se souhlasem subjektu údajů, tedy jednotlivých členů. Rozsah zpracovávaných údajů se musí řídit příslušným účelem, rozsah nad nutný rámec daný účelem nelze rozšířit ani se souhlasem majitele psa (subjektu údajů vlastního psa).

Je nepochybné, že většinu pravidel zpracování osobních údajů majitelů psů lze zpracovat do stanov jednotlivých klubů a majitelé potom dávají souhlas se zpracováním svých údajů jakožto majitelé určitého psa vstupem do konkrétního klubu. Souhlas však bude vždy třeba pro různé další informace, týkající se jednotlivých členů či jejich psů, budou-li zveřejňovány na webových stránkách klubů či v různých písemných materiálech.

Pokud jsou však některé údaje dále předávány či zveřejňovány samotným majitelem, není takové zpracování třeba ošetřit zvláštním souhlasem, neboť ten je vyjádřen již konáním majitele. Rozsah takto předávaných informací ale musí být samozřejmě v souladu s účelem.

Kynologie nemůže být provozována komerčně, tzn. chov psů za účelem obchodu je nepřipustný, a nelze tedy pohlížet na chovatele jako na podnikatele, a ochrana osobních údajů je tak aplikovatelná v plném rozsahu.

NEVYŽÁDANÁ OBCHODNÍ SDĚLENÍ

Úřad se setkává s mylnou představou, že zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (dále jen „zákon č. 480/2004 Sb.“) a zákon o ochraně osobních údajů spolu nesouvisí. Opak je pravdou: Problematiky regulované oběma zákony jsou naopak úzce obsahově propojeny.

Úřad provádí dozor nad dodržováním povinností stanovených zákonem o ochraně osobních údajů při zpracování osobních údajů a je též příslušným orgánem pro výkon dozoru nad dodržováním povinností při šíření obchodních sdělení podle zákona č. 480/2004 Sb. V rámci tohoto dozoru se ukazuje, že firemní katalogy zákazníků obsahují (samozřejmě ne vždy) zejména jejich profil, tj. vedle identifikačních údajů pro účely dodávky a platby také informace o druzích objednaného zboží, o oblasti zájmu zákazníka a o tom, zda zákazník souhlasí s přijímáním obchodních nabídek prostřednictvím elektronických prostředků.

Jestliže je zasílána obchodní nabídka na základě nepravého souhlasu, jde o porušení jak zákona č. 480/2004 Sb., neboť jde o samotné zasílání nevyžádaného obchodního sdělení, tak i porušení zákona o ochraně osobních údajů, jelikož takový správce osobních údajů uvádí údaje chybně a nepřesně (tedy deklaruje, že disponuje předchozím prokazatelným souhlasem se zasíláním obchodních sdělení). Skutečnost, že obě právní normy nejsou více provázány obsahově, způsobuje při kontrolním procesu skutečné komplikace. O funkční propojení obou těchto zákonů se Úřad snaží prakticky již od samého počátku platnosti zákona č. 480/2004 Sb.

Některé firmy se brání tím, že u e-mailových adres, které získají buď z otevřených zdrojů (internet), či nákupem databáze či jiného seznamu, nevedou jméno a příjmení, a nejde tedy o zpracování osobních údajů. Už tato obranná argumentace a zpochybnění, zda je e-mailová adresa osobním údajem či nikoliv, svědčí o nepochopení a neznalosti definice osobního údaje, neboť osobním údajem může být v podstatě jakýkoliv údaj. Vždy záleží na souvislostech. Osobním údajem je dle dikce zákona o ochraně osobních údajů „*jakákoliv informace týkající se určeného nebo určitého subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“. E-mailová adresa jako součást souboru informací vztahených k nějaké osobě, která je předmětem obchodního zájmu, je nepochybně osobním údajem.

Otázka může vyvstávat jen v tom smyslu, zda e-mailová adresa sama o sobě je osobním údajem. Tady je třeba odlišit adresy, které se týkají přímo určitého subjektu jako např. `jmeno.prijmeni@firma.xxx`, anebo nepřímo určitého subjektu. V prvním případě jde o osobní údaj nepochybně, zatímco případ druhý může vyvolávat pochybnosti. Z praxe se dá dovodit, že pokud si někdo zřídí např. adresu `xxx@gmail.com`, je identifikovatelný i nepřímo jen velmi obtížně. Zákon o ochraně osobních údajů však neříká, pro koho je osoba identifikovatelná, a je tedy zřejmé, že pro určitý okruh osob je uvedená adresa osobním údajem jim známé osoby, a tedy se z principu o osobní údaj jedná vždy. Je tedy zřejmé, že výše uvedeným způsobem získané e-mailové adresy nemohou být využity pro zasílání obchodních sdělení, neboť jejich držitel nemohl dát příslušný souhlas, a to ani se zasíláním obchodních sdělení, ani se zpracováním osobních údajů. V těchto případech tedy dochází k porušení jak zákona o ochraně osobních údajů, tak zákona č. 480/2004 Sb.

S touto problematikou souvisí též právo subjektu údajů dle § 12 zákona o ochraně osobních údajů na přístup k informacím o své osobě. Pokud tedy subjekt údajů zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého

a osobního života subjektu údajů nebo v rozporu se zákonem o ochraně osobních údajů, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může dle § 21 zákona o ochraně osobních údajů požádat správce nebo zpracovatele o vysvětlení, dále může též požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zákon o ochraně osobních údajů v takových případech zná možnost blokování, provedení opravy, doplnění nebo likvidaci osobních údajů. V případě takových žádostí ale bude na subjektu údajů, aby v některých případech prokázal správci, že je skutečným držitelem sporné e-mailové adresy.

Úřad aktivně připomínkoval novelu zákona č. 480/2004 Sb., která je odrazem praxe Úřadu, jako dozorového orgánu, a vychází též ze zkušeností obdobných úřadů členských států Evropské unie. Účelem této novely je především zlepšení hospodárnosti a efektivity kontrolních a na ně navazujících sankčních řízení za zjištěné porušení zákona, propojení se zákonem o ochraně osobních údajů, pokud jde o procesní ustanovení; novela rovněž zohledňuje požadavky evropské právní normy – nového čl. 15a směrnice 2002/58/ES, zejména odstavce 3.

V roce 2010 obdržel Úřad 2 834 podnětů na šíření nevyžádaných obchodních sdělení, bylo vyřešeno 1 525 stížností. Zahájeno bylo 163 kontrol a v průběhu roku bylo 144 kontrol ukončeno. 344 stížností bylo shledáno neoprávněnými (288 nebylo obchodními sděleními, 116 pocházelo ze zahraničí), ve 120 případech se nepodařilo dohledat odesílatele. 578 subjektům bylo uloženo nápravné opatření. Se 96 subjekty bylo vedeno správní řízení a byla jim pravomocně uložena pokuta v celkové výši 378 000 Kč.

VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ

V roce 2010 poprvé za dobu existence Úřadu obdržel odbor pro styk s veřejností více než 1 000 stížností na protiprávní jednání při zpracování osobních údajů. Za posledních 5 let se tedy počet stížností v jednom kalendářním roce téměř ztrojnásobil, což s sebou přineslo nezbytnost přijetí odpovídajících, zejména personálních opatření. Možnosti Úřadu jsou však v tomto směru vyčerpány a nezbývá než činnosti v této oblasti zákonem o ochraně osobních údajů vymezené působnosti, tj. prvotní právní posuzování obsahu podání z hlediska porušování povinností při zpracování osobních údajů, zodpovídání dotazů a žádostí o právní výklad, i poskytování konzultací, zefektivnit. Pro příští rok je z uvedených důvodů přijato následující rozhodnutí:

Protože se Úřad domnívá, že 10 let od nabytí účinnosti zákona o ochraně osobních údajů je dostatečně dlouhá doba, aby si občané osvojili návyky odpovědného přístupu k ochraně svých osobních údajů i uplatňování práv, která jim legislativa dává vůči správcům a zpracovatelům osobních údajů, bude důsledněji než dosud činit opatření osvětově preventivního charakteru s cílem dalšího prohlubování právního vědomí subjektů osobních údajů. Nedůvodné stížnosti na porušování zákona o ochraně osobních údajů budou odkládány v souladu se správním řádem prostým sdělením, že k porušení zákona nedošlo, a Úřad tedy neshledal důvody k zahájení řízení z moci úřední, aniž by bylo často komplikovaným a časově náročným právním výkladem dovozováno, proč tomu tak je. Anonymní podání budou vyřizována jen ve výjimečných případech, kdy Úřad na základě dalších informací dospěje k závěru, že na jejich řešení je veřejný zájem. Kritériem rozhodovací činnosti Úřadu bude rozsah vedených databází osobních údajů a předpoklad možného opakování činnosti správci nebo zpracovateli zakládající závadný stav. V úvahu bude i nadále brána důvodná obava stěžovatele z postihu ze strany správce osobních údajů, což je dlouhodobě zřetelné zejména v oblasti pracovněprávních vztahů, a to včetně reálného rizika ztráty zaměstnání.

Vzhledem k tomu, že titíž odborní referenti provádějící prvotní právní posuzování obsahu podnětů a stížností vyřizují také dotazy a poskytují konzultace, bude tato činnost omezena jen na nezbytné minimum, tedy bude striktně dodržován rozsah daný zákonem o ochraně osobních údajů. Jinými slovy bude upuštěno od nadstandardního vysvětlování tazatelům, jak v dané věci postupovat, včetně poskytování výkladu v daných případech příslušných zvláštních zákonů; takovou nadstandardní službu sice Úřad tazatelům poskytoval, leč dospěl k závěru, že k takové činnosti není ani věcně oprávněn, a jeho konzultace v takových případech nabývala hodnoty nezávazného právního názoru. Při objemu více než 2 000 písemných dotazů ročně, přičemž i jejich trend má trvale vzestupnou tendenci, není jiný postup do budoucna již možný.

Pokud jde o osobní konzultace, byl jejich počet snížen již v roce 2010 (jediný ukazatel, u něhož došlo oproti roku 2009 k poklesu). I zde byl obecným kritériem výběru předpoklad veřejného zájmu na řešení věci. Převážně se jednalo o rozsáhlé databáze zpracovávaných osobních a citlivých údajů, jejichž zneužití by mohlo poškodit zájmy řádově statisíců subjektů údajů. Pro ilustraci uvádíme z uvedeného pohledu nejdůležitější osobní konzultace poskytnuté následujícím subjektům: Ministerstvo práce a sociálních věcí – zpracování osobních údajů v souvislosti s inspekcemi kvality poskytovaných sociálních služeb; Ministerstvo školství, mládeže a tělovýchovy – příprava celostátního projektu „Podpora individuálního vzdělávání občanů“; Obvodní soud pro Prahu 7 – anonymizace osobních údajů v soudních rozhodnutích poskytovaných žadatelům dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím; České dráhy, a. s. – kamerové systémy ve vlakových soupravách; Chrudimská nemocnice, a. s. – centrální úložiště důvěrných informací v rámci Pardubického kraje; Český telekomunikační úřad a Česká pošta, s. p. – nezbytnost úpravy poštovních podmínek; Český statistický úřad – kompetence k celostátním registrům osobních údajů; Fond ohrožených dětí, o. s. – možnosti provozování kamerových systémů; Generální ředitelství hasičského záchranného sboru – evidence dávek radiačního záření.

Jak bylo avizováno již v závěru roku 2009 na webových stránkách Úřadu, telefonicky budou poskytovány jen základní informace v obecné rovině a tazatel bude instruován směrem k písemné nebo elektronické komunikaci.

Podnětů k zahájení řízení z moci úřední bylo vyřízeno celkem 1 039, což je oproti roku 2009 nárůst o 18 %. Nejmarkantněji se zvýšil, a to přesně zdvojnásobil, počet podání předaných přímo ke správnímu řízení, aniž by bylo potřebné a účelné provádět kontrolu. Tento přístup je sice hospodárnější, nicméně ne vždy efektivní. Bylo zaznamenáno několik případů, kdy správce osobních údajů, kterému byla uložena sankce, se opakovaně dopustil prakticky stejného přestupku nebo jiného správního deliktu, a to jak z nedbalosti, tak vědomě, přičemž motivem takového jednání byla jednoznačně ekonomická výhodnost. Zejména subjektům s rozsáhlými databázemi klientů se vyplatí riskovat i zaplatit pokutu, neboť zisk od ostatních oslovených zákazníků ztrátu minimálně nahradí. Úřad proto přistoupí u opakovaného protiprávního jednání k ukládání sankcí v horní hranici rozpětí umožněného zákonem o ochraně osobních údajů.

Obdobné zpřísnění postupu Úřadu lze očekávat i při následných kontrolách.

K nejčastějším porušením zákona o ochraně osobních údajů správci nebo zpracovateli osobních údajů dlouhodobě patří:

- neposkytnutí informací na písemnou žádost subjektu údajů podle § 12 nebo § 21 zákona o ochraně osobních údajů,
- nepřijetí adekvátních opatření k zabezpečení zpracovávaných osobních údajů ve smyslu § 13 téhož zákona,
- zpracovávání osobních údajů bez souhlasu subjektu údajů a bez právního titulu umožňujícího zpracovávat osobní údaje i bez tohoto souhlasu.

Statistika stížností vyřízených v roce 2010

Celkem	1 039
Z toho:	
předáno ke kontrole	161
předáno na zahájení řízení	86
postoupeno příslušným orgánům	26
odloženo jako nedůvodné	766

Častým předmětem zájmu občanů v postavení subjektů údajů byly i v roce 2010 kamerové systémy, zveřejňování osobních údajů na internetu, zpracovávání citlivých osobních údajů ve zdravotnictví a rozsáhlé databáze studentů a žáků vedené často neoprávněně školskými zařízeními. Těmito problematikám jsou věnovány samostatné pasáže výroční zprávy o kontrolní činnosti, podrobněji ozřejmující charakter nejčastějších přestupků nebo jiných správních deliktů. Na základě průběžně prováděné analýzy obsahu obdržených podání byly uvedené problematiky zařazeny do kontrolního plánu na rok 2011, a budou tedy předmětem zvýšeného zájmu Úřadu i do budoucna.

Za nový jev v roce 2010 lze považovat vzrůstající nasazování kamerových systémů v městské hromadné dopravě, vlakové a autobusové přepravě. Dále byl zaznamenán nárůst žádostí o konzultaci ze strany orgánů místní samosprávy ve věci provozování tzv. městských kamerových systémů, využívaných především k prevenci pouliční kriminality a ochraně obecního majetku. Po zásazích Úřadu jsou provozovateli těchto systémů orgány příslušné k zabezpečování veřejného pořádku, tedy Policie ČR nebo obecní policie. Do budoucna však lze očekávat, v souvislosti s rušením obecních policií menšími městy z finančních důvodů, snahy místní samosprávy provozovat kamerové systémy ve vlastní režii. Úřad se bude této problematice věnovat samozřejmě z pohledu ochrany osobních údajů, tedy hlavně zabezpečení pořízených záběrů proti jejich zneužití a nevyužívání pro jiný než deklarovaný účel. Nevyhne se ovšem ani posuzování legálnosti a legitimnosti prováděného zpracování osobních údajů a proporcionality mezi chráněnými zájmy a zásahy do soukromí jednotlivých občanů.

POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

Po zhodnocení uplynulého roku z hlediska proběhnuvších správních řízení a oblastí, v nichž se vyskytly nejasnosti na straně účastníků řízení, Úřad shledal, že je vhodné upozornit na následující problematické okruhy a vyjádřit se v několika poznámkách k:

- povaze řízení podle § 17 zákona o ochraně osobních údajů,
- pojmu osobní údaj,
- povinnosti zpracovávat pouze přesná data,
- poskytování osobních údajů při vracení kreditu z anonymních předplacených telefonních karet,
- problémům spojeným se službou Street View.

Povaha řízení podle § 17 zákona o ochraně osobních údajů

Jednou z Úřadem často komentovaných otázek v oblasti plnění registrační povinnosti je povaha řízení podle § 17 zákona o ochraně osobních údajů a možné podoby rozhodnutí Úřadu v tomto řízení.

Obecně je předmětem takového řízení posouzení, zda v případě realizace zpracování osobních údajů, které bylo v souladu s § 16 zákona o ochraně osobních údajů Úřadu oznámeno, nedojde následně k porušení tohoto zákona. Jinak řečeno: Předmětem takového řízení je posouzení toho, zda bude správce oznámeným zpracováním, které s odkazem na § 16 zákona o ochraně osobních údajů ještě provádět nemá, resp. nesmí, porušovat podmínky stanovené uvedeným zákonem. Úřad v těchto řízeních vychází jednak z podkladů nashromážděných v registračním řízení dle § 16 zákona o ochraně osobních údajů, tj. z oznámení o zpracování osobních údajů a případně jeho doplnění na výzvu Úřadu, konkrétně jeho samostatného oddělení registračního, které registrační řízení podle § 16 zákona o ochraně osobních údajů vede (toto řízení není správním řízením v režimu správního řádu – srov. § 16 odst. 6 zákona o ochraně osobních údajů), a jednak z důkazních prostředků nashromážděných ve správním řízení podle § 17 zákona o ochraně osobních údajů, které vede odbor správních činností.

Řízení dle § 17 zákona o ochraně osobních údajů je sice správním řízením (v režimu správního řádu – platí zde tedy mimo jiné i jeho § 3), nicméně z povahy věci je zřejmé, že zde dochází k jisté modifikaci, když má být obecně posuzováno něco, co se teprve v budoucnu má uskutečnit. V rámci tohoto řízení tedy více než v jiných případech záleží rozhodnutí Úřadu na správním uvážení, zda by předmětným zpracováním tak, jak byly jeho parametry zjištěny, resp. sděleny, k porušování zákona o ochraně osobních údajů docházelo či nikoli. Řízení podle § 17 zmíněného zákona má tedy fakticky preventivní funkci, vzhledem k tomu, že jeho prostřednictvím, resp. v jeho rámci vydaným negativním individuálním správním aktem může dojít k zákazu určité činnosti z důvodu existence reálného rizika, že by k porušení zákona o ochraně osobních údajů dojít mohlo.

Oznámené zpracování musí být v řízení podle § 17 zákona o ochraně osobních údajů zásadně hodnoceno jako celek, což je pak určující skutečností pro možné závěry správního orgánu. Zákon v tomto případě předpokládá buď zaregistrování oznámeného zpracování, zastavení řízení z důvodu, že účastník řízení od svého záměru upustil, nebo vydání negativního rozhodnutí o tom, že se zpracování osobních údajů v rozsahu a s parametry, jak bylo oznámeno, nepovoluje. Z uvedeného pak vyplývá, že – byť je na straně správního orgánu důvodné mít za to, že jen jeden prvek z oznámeného zpracování není v souladu se zákonem o ochraně osobních údajů – tato jedna část vede k závěru, že zpracováním bude docházet k porušování zmíněného zákona, tudíž není možné oznámené zpracování zaregistrovat, a to ani zčásti, jelikož správní orgán v tomto typu správního řízení není oprávněn provádět v oznámeném zpracování jakékoli změny, nerozhodne-li se účastník řízení (oznamovatel – potenciální správce osobních údajů) pro takovou změnu sám. Ve správním řízení podle § 17 zákona o ochraně osobních údajů jde tedy o komplexní posouzení oznámeného zpracování a jeho souladu se zákonem o ochraně osobních údajů.

K řízení podle § 17 zákona o ochraně osobních údajů lze v relaci k uvedenému dodat ještě následující: V řízení tohoto typu, kdy je zkoumáno, zdali oznámené zpracování tak, jak je má správce/oznamovatel v úmyslu činit, bude v souladu se zákonem, když je plně v pravomoci Úřadu (který je dle § 2 zákona o ochraně osobních údajů povolán k výkonu dozoru pro oblast ochrany osobních údajů), aby na základě správního uvážení rozhodl, zda v daném případě nebude docházet k neproporcionálnímu zásahu do soukromí subjektu údajů; zejména pak v případech, kdy se má oznamované zpracování osobních údajů opírat o právními předpisy uznaný důvod (uvedený v § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, s odkazem na podmínku ve větě za středníkem tohoto ustanovení ve spojení s § 10 zmíněného zákona). V případě aplikace správního uvážení na tyto případy Úřad vždy postupuje dle testu proporcionality, jak je uveden např. v rozhodnutích Ústavního soudu České republiky sp. zn. Pl. ÚS 4/94, Pl. ÚS 15/96, Pl. ÚS 16/98, Pl. ÚS 40/08 a další.

Několik poznámek k pojmu osobní údaj

Bezesporu nejdiskutovanějším pojmem v oblasti ochrany osobních údajů je pojem nejzákladnější, tj. pojem osobní údaj. V uplynulém roce Úřad v rámci správních řízení řešil několik případů, kdy na straně správců osobních údajů vznikaly pochyby o tom, zda zrovna jimi zveřejněné údaje mají povahu údajů osobních. V této souvislosti byla nejčastěji užívána argumentace, že zveřejněná informace má povahu osobního údaje maximálně pro toho, kdo ji již beztak zná.

K naznačené argumentaci Úřad v odůvodnění svých rozhodnutí zopakoval následující a v současné době již tradiční a obecně uznávaný a rozšířený postoj, resp. názor, který vychází z pojetí osobního údaje, jak jej vymezují příslušné předpisy EU:

Osobní údaj je absolutní pojem. Není rozhodující, pro kolik příjemců je určitá informace osobním údajem. Osobním údajem je tak každá informace, která je spojitelná s konkrétní, resp. určitou nebo určitelnou fyzickou osobou. Takovou povahu má tedy i informace o tom, že osoba někde byla, vlastní nějaký majetek, anebo i o tom, že jsou její movité věci v prostorech, k nimž má užívací právo, uspořádány určitým způsobem atp. Z hlediska § 4 písm. a) zákona o ochraně osobních údajů je tedy osobním údajem každá informace, kterou lze přiřadit ke konkrétní fyzické osobě a která tak vypovídá o jejím soukromém a osobním životě, a to i tehdy, jestliže je možnost přiřazení informace k takové fyzické osobě podmíněna určitou nutnou znalostí dalších skutečností u jejího příjemce. Zásadní skutečností, která je odvislá od otázky rozsahu nutné předchozí znalosti údajů o fyzické osobě, k níž je možné zveřejněné údaje vztáhnout, je míra zásahu do soukromí.

Několik poznámek k povinnosti zpracovávat pouze přesná data

Mezi základní povinnosti správce osobních údajů patří dle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů povinnost zpracovávat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. K tomu je dále připojena povinnost správce, je-li to nezbytné, osobní údaje aktualizovat. Zjistí-li správce, že jím zpracované osobní údaje nejsou přesné, je bez zbytečného odkladu povinen provést přiměřená opatření, zejména zpracování blokovat a osobní údaje opravit nebo doplnit, osobní údaje zlikvidovat. Nepřesné osobní údaje lze zpracovávat pouze v mezích uvedených v § 3 odst. 6 zákona o ochraně osobních údajů s tím, že nepřesné osobní údaje se musí označit. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem (oprávněným) příjemcům.

Kategorie nepřesných dat však není určena pouze tím, že správce osobních údajů zpracovává osobní údaje, které neodpovídají faktickému stavu věcí, nýbrž může být určena i tak, že správce zpracovává osobní údaje nekompletní pro možnost dosažení sledovaného účelu – zejména pro případy, kdy rozsah zpracovávaných dat vymezuje právní předpis.

K naplnění jakéhokoli účelu zpracování osobních údajů je třeba vždy disponovat určitou minimální sumou osobních údajů, které vytvářejí obraz o identitě určité osoby a vypovídají o dalších (pro daný případ souvisejících a rozhodných) skutečnostech. V případě, že tato nezbytná suma dat, zejména

tehdy, kdy je určena prostřednictvím právního předpisu a dále např. na něj navazujícího interního aktu správce, není shromážděna (některé údaje scházejí), anebo sice shromážděna je, ale údaje v ní obsažené nejsou přesné, není jejím prostřednictvím relevantním způsobem možné sledovaného účelu dosáhnout. Současně prostřednictvím takového souboru neúplných, resp. nesprávných dat vzniká chybná představa o identitě subjektu údajů, která zasahuje do jeho osobnostních práv právě tím, že neodpovídá objektivní realitě. Mimo jiného i z obou těchto důvodů je ustanovením § 5 odst. 1 písm. c) zákona o ochraně osobních údajů správci uloženo zpracovávat pouze přesné osobní údaje a tyto údaje případně patřičným způsobem aktualizovat.

Zpracování osobních údajů v souvislosti s vrácením kreditu z předplacené telefonní karty

Úřad se v jednom ze svých správních rozhodnutí zabýval otázkou, zda je telekomunikační operátor oprávněn v okamžiku, kdy se sám zavázal při zrušení předplacené anonymní telefonické karty k vrácení neprovolaného kreditu, požadovat osobní údaje toho, komu má být zbývající kredit vyplacen.

V této věci Úřad konstatoval, že pro každé zpracování osobních údajů potřebuje správce právní titul, kterým může být souhlas subjektů údajů nebo splnění některé z výjimek stanovených v § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů. Ve smyslu § 5 odst. 4 zákona o ochraně osobních údajů musí být subjekt údajů informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Souhlas musí být správce schopen prokázat po celou dobu zpracování. Jelikož účastník řízení podmiňoval vrácení kreditu poskytnutím osobních údajů, je zřejmé, že v tomto případě nelze jednání směřující k poskytnutí osobních údajů považovat za souhlas, který by byl platným právním úkonem ve smyslu zákona č. 40/1964 Sb., Občanský zákoník. Účastník řízení tedy nedisponoval souhlasem stěžovatele, jehož osobní údaje požadoval. K tomu lze doplnit, že v e-mailové zprávě, prostřednictvím které poskytl stěžovatel své osobní údaje účastníkovi řízení, současně uvedl, že souhlas k jejich zpracování neuděluje. Dále lze k vyjádření účastníka řízení konstatovat, že ustanovení všeobecných obchodních podmínek nenahrazují ani nepředstavují souhlas subjektu údajů se zpracováním osobních údajů ve smyslu § 4 písm. n) zákona o ochraně osobních údajů.

Úřad se tedy zabýval otázkou, zda je za stanoveným účelem možné zpracovávat osobní údaje bez souhlasu subjektu údajů, tj. na základě některé z výjimek stanovených v § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů. V případě účastníka řízení bylo možné uvažovat o aplikaci ustanovení § 5 odst. 2 písm. b) a e) zákona o ochraně osobních údajů.

Podle § 5 odst. 2 písm. b) zákona o ochraně osobních údajů je možné provádět zpracování osobních údajů bez souhlasu subjektu údajů v případě, že je toto zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo v případě jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů. V tomto případě bylo nutné konstatovat, že jestliže došlo k aktivaci služby u stěžovatele a jejímu využívání bez toho, aby účastník řízení potřeboval jeho osobní údaje, není oprávněn od něj požadovat tyto osobní údaje při jejím ukončení a vyplacení zbývajícího kreditu. Pokud tedy nejsou osobní údaje nezbytné pro uzavření smlouvy, nebudou dle Úřadu nezbytné ani pro její ukončení.

Zpracování osobních údajů bez souhlasu subjektu údajů, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby, umožňuje ustanovení § 5 odst. 2 písm. e) zákona o ochraně osobních údajů. Pro účely identifikace osoby, které má být vyplacen zbývající kredit (což bylo hlavním důvodem, proč účastník řízení požadoval osobní údaje od stěžovatele), je nepochybně dostačující, pokud tato osoba předloží originál SIM karty spolu s průvodním dopisem obsahujícím kódy PIN a PUK a číslo bankovního účtu, na který má být zůstatek převeden. Osobní údaje jsou tedy požadovány nadbytečně a v rozporu s principem aktivované služby, která je anonymní; SIM karta je přenosná, a v důsledku toho tedy může být konečný majitel karty odlišný od toho, kdo ji aktivoval. Z toho vyplývá také oprávnění žádat vrácení kreditu držitele karty bez ohledu na jeho identifikaci. Navíc Úřad konstatoval, že zaslání kopie občanského průkazu prostřednictvím

elektronické pošty není žádným relevantním důkazem v případě podvodu a účastník řízení nemůže mít žádnou jistotu, že se bude jednat o občanský průkaz skutečného žadatele. I z tohoto důvodu nelze považovat požadování kopie občanského průkazu a osobních údajů na ní uvedených za nezbytné pro identifikaci osoby žadatele o vyplacení zbývajících kreditů.

Služba Street View

Dne 18. února 2010 oznámila podle § 16 odst. 1 zákona o ochraně osobních údajů společnost mající na území České republiky zájem provozovat službu Google Street View Úřadu prostřednictvím registračního formuláře záměr zmíněnou službu realizovat, tzn. zpracovávat osobní údaje pro účely jejího poskytování. Ve svém oznámení společnost uvedla, že by při realizaci služby Google Street View docházelo k pořizování snímků ulic a dalších míst, které mají ve smyslu právních předpisů statut veřejných prostranství. K pořizením snímků by docházelo za běžného denního provozu, kdy by na těchto fotografiích byly zachyceny jak všechny osoby a vozidla nacházející se v konkrétní době průjezdu speciálního vozidla pořizujícího fotografie na místě, tak veškeré budovy a pozemky nacházející se v blízkosti komunikace, po které by se toto vozidlo pohybovalo.

Úřadem bylo v dané věci shledáno, že by pořizováním fotografií docházelo ke shromažďování osobních údajů. Tento závěr Úřadu vycházel ze skutečnosti, že kvalita, ve které měly být fotografie pořizovány, by byla dostatečná k tomu, aby byly osoby na nich zachycené rozpoznatelné. Oznamovatel v této souvislosti uvedl, že bude docházet k rozmazání obličejů osob. K tomu Úřad konstatoval, že tato skutečnost je relevantní pouze částečně, a to jednak proto, že k rozmazání by mělo dle oznamovatele docházet až po předání dat do USA, a jednak proto, že i přes částečné rozmazání by byla zachycená osoba po zveřejnění fotografie pro určité příjemce dat určitelná.

Ohledně rozsahu zpracovávaných osobních údajů došel Úřad dále k závěru, že pořizené fotografie by kromě osobních údajů vztahujících se k zachycené osobě, tj. zejména údaje o tom, že daná osoba byla na konkrétním místě atd., obsahovaly i další osobní údaje. Konkrétně by jejich prostřednictvím došlo k zachycení domů, pozemků, automobilů, uspořádání věcí na pozemku atd. V této souvislosti Úřad připomněl, že osobním údajem ve smyslu § 4 písm. a) zákona o ochraně osobních údajů se rozumí jakákoli informace, která vypovídá o fyzické osobě, resp. o jejím soukromém a osobním životě a je alespoň pro určitou skupinu příjemců s daným subjektem údajů spojitelná.

Předmětné zpracování osobních údajů se mělo opírat o právními předpisy uznaný důvod uvedený v § 5 odst. 2 písm. e) zákona o ochraně osobních údajů.

Obecně je při zjišťování, zda lze aplikovat v rámci zmíněného ustanovení uvedenou výjimku pro zpracování osobních údajů bez souhlasu subjektu údajů, třeba s ohledem na podmínku vyjádřenou ve větě za středníkem tohoto ustanovení, která říká, že zpracování osobních údajů „*nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života*“, zhodnotit (z hlediska priority) dle testu proporcionality poměr mezi právem na soukromí subjektu údajů a zájmem, který má být zpracováním osobních údajů dosažen (chráněn). Zmíněný test užil například Ústavní soud České republiky ve svém nálezu sp. zn. Pl. ÚS. 4/94, anebo např. Evropský soudní dvůr ve věci Fedesa (C-31/88 Fedesa (1990) ECR 4023).

Po provedení testu proporcionality (zjednodušeně řečeno) došel Úřad k závěru, vedle shora uvedeného zejména s přihlédnutím k tomu, že vzhledem k deklarované výšce (2,7 m) kamery, ze které mělo k pořizování snímků docházet, tzn. s ohledem na skutečnost, že by pořizené snímky poskytovaly pohled z větší výšky, nežli umožňuje běžný pohled z ulice (navíc bylo záměrem oznamovatele snímky pořizovat i z oblastí, kam nemají povolen vjezd nákladní automobily, z nichž je případně takový pohled možný, a dále i z oblastí, kam nemají povolen vjezd dokonce ani osobní automobily), že by realizací oznámeného zpracování osobních údajů docházelo k neproporcionálnímu zásahu do práv subjektů údajů na ochranu jejich soukromého a osobního života, tzn. právo na ochranu soukromí (ochranu osobních údajů) v tomto případě převyšuje zpracováním osobních údajů sledovaný zájem.

Jinak řečeno, Úřad dospěl k závěru, že podmínky pro možnost zpracovávat osobní údaje na základě právního titulu uvedeného v § 5 odst. 2 písm. e) zákona o ochraně osobních údajů by nebyly naplněny,

tzn. oznamované zpracování osobních údajů by nemělo žádný relevantní právní podklad (oporu v zákoně).

Na základě obsahu oznámení o zpracování osobních údajů a jeho doplnění na výzvu Úřadu zde tedy vznikla důvodná obava ve smyslu § 17 odst. 1 zákona o ochraně osobních údajů, že by při zpracování osobních údajů v podobě, jak bylo oznámeno, mohlo dojít k porušení zákona. Na jejím základě pak Úřad z úřední povinnosti zahájil správní řízení podle § 17 zmíněného zákona, v němž po provedení příslušných procesních kroků s odkazem na shora uvedené a po zjištění skutkového stavu v rozsahu § 3 zákona č. 500/2004 Sb., Správní řád (s limity uvedeným shora v příspěvku „Povaha řízení podle § 17 zákona o ochraně osobních údajů“) svým rozhodnutím konstatoval, že oznámené zpracování nesplňuje podmínky stanovené zákonem o ochraně osobních údajů, zejména proto, že by při jeho realizaci došlo k porušení § 3 odst. 5 písm. b), § 5 odst. 2 a § 10 zmíněného zákona. Oznámené zpracování osobních údajů pak Úřad z uvedeného důvodu nepovolil.

Proti rozhodnutí správního orgánu I. stupně podal oznamovatel rozklad k předsedovi Úřadu. Předseda Úřadu následně svým rozhodnutím rozhodnutí správního orgánu I. stupně potvrdil.

REGISTRACE

Podobně jako v předešlých letech, i v roce 2010 pokračoval trend nárůstu počtu registračních oznámení. V roce 2010 Úřad přijal 4 037 oznámení o zpracování podle § 16 zákona o ochraně osobních údajů. Oproti minulému roku se jednalo o 23,2% nárůst. Vedle posuzování přijatých registračních oznámení vydává Úřad rozhodnutí o zrušení registrace podle § 17a odst. 2 zákona o ochraně osobních údajů. V roce 2010 bylo zrušeno celkem 119 zpracování na žádost správce, nejčastěji z důvodů zániku či sloučení společnosti, zrušení podnikatelské činnosti nebo ukončení zpracování osobních údajů. Zde došlo naopak k poklesu o 14,4 %. Informace o zrušených registracích Úřad zveřejňuje ve svém Věstníku. V souvislosti s narůstajícím počtem registračních oznámení narůstá i počet oznamovaných změn či doplnění již zaregistrovaných zpracování. Změny se nejčastěji týkají adresních údajů, doplnění rozsahu zpracovávaných osobních údajů, kategorií subjektů údajů, doplnění účelů zpracování.

V případech zpracování prostřednictvím kamerových systémů se změny týkají převážně navýšení počtu kamer a prodloužení doby uchování pořizovaných záznamů, jelikož Úřadem doporučovaná doba 3 dnů v mnoha případech pro správce není dostačující. V letošním roce šlo o 906 změn či doplnění, což je nárůst o 10,9 % oproti roku 2009.

V rámci řízení o oznámení o změně zpracování dochází někdy k revizi registrovaného zpracování, a to na doporučení Úřadu. Často se jedná o případy, kdy v souvislosti se vznikem nových právních norem či jejich novelizací se na dané zpracování již registrační povinnost nevztahuje, a to vzhledem k výjimce uvedené v § 18 odst. 1 písm. b) zákona o ochraně osobních údajů. V takovém případě je správci doporučeno zpracování zrušit.

V roce 2010 Úřad zahájil celkem 742 řízení o registraci podle § 16 odst. 4 zákona o ochraně osobních údajů. Častým výsledkem registračních řízení je, že správce přistoupí, na základě upozornění Úřadu, ke korekci předpokládaného zpracování (např. upustí od zpracování citlivých údajů, pokud je jejich zpracování neúčelné, nebo upraví zpracování kamerovým systémem tím, že změní umístění, nastavení či režim chodu kamer).

Na základě obsahu oznámení o zpracování, případně jeho doplnění na výzvu Úřadu podle § 16 odst. 4 zákona o ochraně osobních údajů, může vzniknout důvodná obava, ve smyslu § 17 odst. 1 tohoto zákona, že by při zpracování osobních údajů v podobě, jak bylo oznámeno, mohlo dojít k porušení zákona o ochraně osobních údajů. V roce 2010 bylo zahájeno celkem u 64 podaných oznámení o zpracování správní řízení podle § 17 zákona o ochraně osobních údajů. Z toho 61 oznámení se týkalo kamerových systémů a zbylá 3 zpracování prostřednictvím webové aplikace, vstupního čipového systému a zpracování osobních údajů pro účely uzavírání smluv. Celkem u 42 oznámení došlo k jejich úpravě, doplnění nebo zdůvodnění oznamovatelem, což vedlo k následné registraci, ve 4 případech oznamovatel odstoupil od registrace nebo po změnách oznámení již nepodléhalo registraci a ve 4 případech nebylo zpracování osobních údajů povoleno (ve 3 případech šlo o kamery umístěné na oděvu zaměstnance, které snímaly jeho činnost v desetisekundových intervalech a v 1 případě šlo o umístění kamer v kancelářích, u šatních skříněk apod.). U 14 oznámení dosud řízení nebylo ukončeno.

POVAHA REGISTRACE PŘI DALŠÍ ČINNOSTI ÚŘADU

Současná podoba a koncepce registračního řízení byla v rámci zákona o ochraně osobních údajů nastavena novelou, která byla provedena zákonem č. 439/2004 Sb., s účinností k 25. červenci 2004. Ani za více než pět let účinnosti však není v rámci veřejnosti ve všech případech zcela jasné, jakou povahu má registrace jako taková a jaké důsledky a účinky má zaregistrování oznámeného zpracování na další činnost Úřadu, zejména z hlediska závaznosti registrace. Stále není výjimkou, že na straně osob, na které dopadá působnost zákona, v tomto případě správců, dochází k nepochopení toho, jakou povahu má registrace jimi zaslání oznámení o zpracování osobních údajů ve smyslu § 16 odst. 1

zákona o ochraně osobních údajů. V mnohých případech se např. kontrolovaní odvolávají, že s ohledem na to, že akt registrace má povahu individuálního správního aktu, je jím Úřad ve své další činnosti (např. kontrole) vázán.

K tomuto je třeba konstatovat, že uvedený názor, vztahující se k povaze registrační povinnosti, resp. zaregistrování oznámeného zpracování osobních údajů, tj. aktu registrace, je mylný. Zaregistrování zaslání oznámení dle § 16 zákona o ochraně osobních údajů je správním aktem, jenž má ze správně teoretického hlediska povahu mlčení správního orgánu. Tento akt správního orgánu nezakládá subjektivní právo kontrolovanému zpracovávat osobní údaje – nejedná se o individuální správní akt (povolení). Je nicméně třeba připustit, že jestliže jsou v rámci registračního procesu sděleny Úřadu pravdivě všechny relevantní skutečnosti a tento po řádném posouzení věci zpracování osobních údajů zaregistruje, nemělo by s odkazem na právní jistotu správce při další činnosti Úřadu docházet k rozporům v otázce koncepční přípustnosti takového zpracování – např. ze strany kontrolujícího v rámci případné budoucí kontroly. Uvedené však neznamena, že v rámci správního řízení o správním deliktu (v širším smyslu) či kontroly nemůže být předmětem hodnocení plnění jednotlivých povinností správce osobních údajů, které mu vyplývají z právních předpisů (zejména zákona o ochraně osobních údajů).

OKRUHY ZPRACOVÁNÍ ŘEŠENÉ V RÁMCI REGISTRAČNÍHO ŘÍZENÍ

Služba Street View

V roce 2010 proběhlo registrační řízení se společností provozující na území ČR službu Google Street View. Podrobné informace přináší kapitola „Poznatky ze správního řízení“, které se v daném případě uskutečnilo.

Zpracování kamerovými systémy

Nejčastějším typem oznamovaných zpracování v roce 2010 byla zpracování prostřednictvím kamerových systémů (33,4 % z celkového množství podaných oznámení). V registru zpracování osobních údajů bylo zapsáno celkem 5 312 subjektů, které zpracovávají osobní údaje kamerovými systémy. Podrobná informace je obsažena v kapitole Poznatky inspektorů z kontrolní činnosti v části Zpracování osobních údajů prostřednictvím kamerových systémů, která přináší ucelený pohled na problematiku využívání kamerových systémů ve vztahu ke zpracování osobních údajů.

Zpracování za účelem provozování internetového obchodu

V roce 2010 výrazně narostl počet zpracování v souvislosti s provozováním internetového obchodu. V rámci registru zpracování je uvedeno celkem 1 193 subjektů, které v účelu zpracování osobních údajů uvedly internetový obchod nebo e-shop. Z toho počtu bylo v letošním roce nově zapsáno do registru celkem 621 subjektů.

V případě, že internetový obchod používá získané osobní údaje pouze k příjmu objednávek a jejich vyřízení včetně dodávky zboží zákazníkovi a dále s údaji již nepracuje, potom se na něj oznamovací povinnost vztahovat nebude, neboť jsou zpravidla zpracovávány nezbytné osobní údaje v rámci činností uložených zvláštními zákony. Opačný případ nastane, pokud dochází k tvorbě databáze registrovaných zákazníků, která je dlouhodobě využívána k další komunikaci se zákazníky po vyřízení jejich objednávky k usnadnění této další komunikace, k zaslání obchodních sdělení, k marketingovým účelům, k hodnocení bonity zákazníka apod.

Zpracování spojené s použitím věrnostních karet

Věrnostní karty se mohou skrývat pod různě definovanými účely zpracování osobních údajů: např. zákaznické karty, poskytování zákaznických výhod, zákaznický servis, zákaznický program, věrnostní program, zákaznický klub, věrnostní systém, vydávání zákaznických karet, evidence členů zákaznického klubu, zjištění zákaznických potřeb a nákupních zvyklostí, účast v zákaznickém programu, správa registrovaných zákazníků, vystavení čipové karty, tankovací karty, platební karty, čipové karty v autobusové dopravě. Dají se předpokládat i pod obecněji definovanými účely: např. klientská databáze, vedení databáze zákazníků, zlepšování zákaznických služeb, marketingové účely. Správci, kteří oznamují úmysl zpracovávat osobní údaje v souvislosti s poskytováním výhod věrnostní karty, uvádějí, že tak budou činit se souhlasem subjektu údajů (tj. v případě věrnostních karet se souhlasem klienta). Účelem zpracování je obecně možnost čerpání různých slev a výhod na nákupy prováděné držitelem karty, který uvede své jméno, příjmení, případně další kontaktní údaje, pokud má zájem dostávat sdělení o marketingových akcích. Velkou oblibu si získaly věrnostní karty u lékáren. Zde klienti uvádějí nejen adresní a identifikační údaje, ale rovněž citlivé údaje o zdravotním stavu (krevní tlak, alergie, hladina glukózy, cholesterolu apod.). Vždy se tak děje pouze se souhlasem klienta. Objevují se i tendence k evidenci realizovaných nákupů.

Zpracování v souvislosti s provozováním systému whistleblowing

Účelem zpracování je provoz a implementace systému whistleblowing. Jde o systém zavedený společnostmi, které buď přímo pocházejí, nebo jsou podílově vlastněny a ovládnuty společnostmi se sídlem v USA. Zavedení tohoto oznamovacího systému je povinností uloženou americkým zákonem SOX (tj. Sarbanes-Oxley Act). Institut oznamování představuje doplňkový mechanismus, umožňující zaměstnancům oznamovat protiprávní jednání vnitřní cestou, s využitím zvláštního informačního kanálu (většinou standardizovaný formulář na webových stránkách). Nejčastěji systém zahrnuje vyšetřování a nakládání s oznámeními týkajícími se podvodu, korupce, zneužití důvěrných interních informací, bezpečnosti IT. Předmětem oznámení bývají zpravidla pouze skutečnosti či jednání, které představují právní rizika nebo jiná vážná rizika pro určitý nadnárodní koncern, nikoliv např. stížnosti ohledně výše platu, povýšení, neshod s kolegy či drobných přestupků. Pro tento druh oznámení většinou funguje zavedený systém oznámení prostřednictvím nadřízeného, e-mailem, dopisem nebo telefonicky, která jsou podávána přímo či anonymně. V souvislosti s provozem systému whistleblowing mají oznamovatelé nejčastěji problémy s určením rolí správce a zpracovatele. K tomu problému lze stručně konstatovat, že úloha správce či zpracovatele vyplývá z jeho konkrétních činností v určitém kontextu, čili určení úlohy správce nebo zpracovatele je nutno posoudit s ohledem na konkrétní soubory údajů nebo úkonů.

Další zpracování

Ve velké míře jsou oznamována 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 výchovu a vzdělávání, vytváření databází klientů, dodavatelů, přepravců, obchodních partnerů apod.

■ PŘEDÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Podmínky, za nichž mohou být osobní údaje předány do zahraničí, upravuje zákon o ochraně osobních údajů v § 27. Povolení má povahu správního řízení podle zákona č. 500/2004 Sb. (správní řád). Povinnost požádat Úřad o povolení k předání osobních údajů do třetích zemí se týká pouze případů předání, které se uskutečňuje v režimu § 27 odst. 3 zákona o ochraně osobních údajů. Týká se tedy většiny případů, kdy osobní údaje subjektu údajů nejsou v přijímající zemi adekvátním způsobem chráněny.

V roce 2010 Úřad zaznamenal klesající počet podávaných žádostí o povolení předání osobních údajů do třetích zemí. Tento trend je způsoben zejména tím, že správci ve zvýšené míře využívají pro předání osobních údajů do třetích zemí nástroje, jež vytvořila Evropská komise speciálně pro zabezpečení adekvátní ochrany předaných osobních údajů ve třetí zemi a které tak umožňují správcům předávat osobní údaje v režimu § 27 odst. 2 zákona o ochraně osobních údajů, bez zvláštního povolení Úřadu.

„Safe Harbor“

Jedná se zejména o institut „Safe Harbor“ („bezpečný přístav“), upravený rozhodnutím Komise ze dne 26. července 2000 podle směrnice Evropského parlamentu a Rady 95/46/ES o odpovídající ochraně poskytované podle zásad „bezpečného přístavu“, které byly speciálně vytvořeny pro předání osobních údajů do Spojených států amerických. Jsou to právě Spojené státy, do kterých jsou předávány osobní údaje z ČR nejčastěji, většinou ze strany dceřiných společností. Jedná se převážně o předání zaměstnaneckých osobních údajů v rámci nadnárodní korporace pro účely odměňování zaměstnanců, včetně poskytování veškerých odměn a benefitů, koordinace při změnách odměňování, výběru a přidělování vhodných zaměstnanců, výběru vhodných kandidátů na absolvování pracovních cest a zahraničních stáží apod. Dovozece údajů ve Spojených státech musí být na seznamu „Safe Harbor“, tedy se musí veřejně přihlásit k dodržování zásad „bezpečného přístavu“. Úřad v roce 2010 zaznamenal celkem 35 takových případů předání údajů do Spojených států. Na základě častých dotazů i počtu subjektů, které jsou na seznamu „Safe Harbor“, můžeme ovšem předpokládat počet mnohonásobně větší. I když se předání může uskutečnit bez předešlého povolení Úřadu, Úřad správcům (vývozcům údajů) doporučuje před samotným předáním ověřit, zda je certifikace příslušné organizace stále platná, zda a jakým způsobem jsou fyzické osoby informovány o vnitřních postupech pro vyřizování stížností, případně zda je „privacy policy“ příslušné společnosti ve Spojených státech veřejně přístupná, např. prostřednictvím webových stránek. V případě zjištěných nedostatků při uplatňování principů „bezpečného přístavu“ je namístě o tom informovat Úřad.

Standardní smluvní doložky

Standardní smluvní doložky obsahují povinnosti týkající se správce osobních údajů, který hodlá předat osobní údaje do třetích zemí, a dále povinnosti pro ty správce či zpracovatele osobních údajů, kteří jsou příjemci osobních údajů. Podobně jako v případě „Safe Harbor“ není nutné žádat Úřad o povolení k předání, pokud správce zajistí přiměřenou úroveň ochrany údajů prostřednictvím smlouvy, jejíž nedílnou součástí budou standardní smluvní doložky. Úřad v letošním roce zaznamenal 50 případů předání údajů podle příslušného rozhodnutí Komise o standardních smluvních doložkách. Podobně jako v případě „bezpečného přístavu“ je možné předpokládat, že počet předání osobních údajů na základě standardních smluvních doložek bude mnohonásobně větší.

Zásadní změnu v oblasti aplikace smluvních doložek přineslo rozhodnutí Komise 2010/87/EU ze dne 5. února 2010 o standardních smluvních doložkách pro předání osobních údajů zpracovatelům usazeným ve třetích zemích. Hlavním důvodem vydání nového rozhodnutí byl, zjednodušeně řečeno, nástup „celosvětového externího zajišťování služeb“, neboť stále více společností předává své údaje nejen

zpracovateli, ale i „díličím zpracovatelům“ a někdy i následným „dalším díličím zpracovatelům“. V souladu s citovaným rozhodnutím může tedy zpracovatel údajů ve třetí zemi (tj. u dovozce údajů) pověřit částí zpracování další subjekt, který se tím dostane do pozice díličího zpracovatele. Podmínkou pro takový postup však je předchozí písemný souhlas správce údajů (vývozce) a existence písemné smlouvy mezi zpracovatelem a díličím zpracovatelem, v níž jsou díličímu zpracovateli uloženy stejné povinnosti ohledně ochrany osobních údajů, jakými je vázán dovozce. Plnou odpovědnost vůči správci údajů (vývozci) má však vždy zpracovatel (dovozce), tj. odpovídá i za porušení pravidel na straně díličího zpracovatele.

Předání podle § 27 odst. 3 zákona o ochraně osobních údajů

Podle výjimky uvedené v § 27 odst. 3 písm. b) zákona o ochraně osobních údajů může Úřad povolit předání do třetí země, pokud správce poskytne dostatečná ochranná opatření pro ochranu soukromí a základních práv a svobod osob. Ochranná opatření mohou vyplývat zejména ze závazných podnikových pravidel (Binding Corporate Rules, dále jen „BCR“). BCR představují určitý kodex ochrany osobních údajů, uplatňovaný v rámci nadnárodní společnosti. S ohledem na skutečnost, že nadnárodní společnosti nemají zpravidla své hlavní sídlo na území ČR, nebyl Úřad doposud požádán, aby se stal tzv. vedoucí autoritou (lead authority), která v rámci EU koordinuje celý schvalovací proces. Rovněž Úřad nebyl doposud požádán o vydání povolení k předání údajů do třetích zemí, i když na území ČR působí mnoho nadnárodních koncernů prostřednictvím svých dceřiných společností, které již mají ze strany vedoucího dozorového orgánu EU schválené BCR, a lze tedy předpokládat, že je používají pro mezinárodní předání. V této souvislosti je často zaměňován schvalovací proces na evropské úrovni s požadavky národních orgánů dozoru takové předání autorizovat. Prvním krokem k vytvoření a fungování BCR je jejich schválení prostřednictvím zvoleného vedoucího dozorového úřadu v rámci EU (většinou se řídí dle sídla mateřské společnosti). Toto schválení však ještě neumožňuje jejich automatické používání pro předání osobních údajů z ČR do třetích zemí. Povinnost požádat Úřad o předání údajů do třetích zemí by se vztahovala na dceřinou společnost se sídlem v ČR.

Pokud se týká samotných žádostí o povolení k předání osobních údajů do třetích zemí, správci se nejčastěji dovolávají plnění ustanovení § 27 odst. 3 písm. a) zákona o ochraně osobních údajů, tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů. Povolení se týkala zpravidla předání zaměstnaneckých údajů (základní kontaktní údaje, případně údaje o postavení zaměstnance v rámci struktury mezinárodní skupiny, výjimečně i dalších údajů, např. výše mzdy a přidělených odměn) v rámci nadnárodní korporace pro účely: zajištění účasti zaměstnanců na vzdělávacích programech, zřízení vnitřní sociální sítě, zúčtování cestovních náhrad, zařazení zaměstnanců do programu udílení zaměstnaneckých akcií, řízení odměňování a bonusů v rámci skupiny.

V případech předání na základě souhlasu se fakticky jedná o odchylku od zásady přiměřené úrovně ochrany v přijímající zemi, vyjádřené ve směrnici 95/46/ES, a tedy i v zákoně o ochraně osobních údajů. Tato výjimka umožňuje předání údajů do třetích zemí, které nezajišťují odpovídající úroveň ochrany. Pro jednotlivce to znamená, že jeho osobní údaje v přijímající zemi nebudou požívat ochrany, která je mu v ČR zaručena zákonem. Proto Úřad v takových případech zvláště dbal na to, aby byly v souladu s § 5 odst. 1 písm. d) zákona o ochraně osobních údajů předány pouze osobní údaje nezbytné k naplnění stanoveného účelu a aby souhlas subjektu údajů s předáním jeho osobních údajů do třetí země splňoval náležitosti § 4 písm. n), § 5 odst. 4 a § 11 zákona o ochraně osobních údajů, tedy aby tento souhlas byl svobodným, vědomým a informovaným projevem vůle subjektu údajů, který je správce schopen prokázat po celou dobu zpracování. Vedle souhlasu bylo nejčastěji vydáno povolení k předání na základě splnění požadavku ustanovení § 27 odst. 3 písm. e) a f), podle kterých předání může proběhnout, pokud je to nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, resp. pokud je nezbytné pro plnění smlouvy uzavřené v zájmu subjektu údajů mezi správcem a třetí stranou. Týkalo se to zejména cestovních kanceláří, které předávají osobní údaje svých klientů hotelům a dalším obchodním partnerům, kteří zajišťují pro dané cestovní kanceláře organizaci pobytu jejich klientů ve třetí zemi.

PNR data

V roce 2010 Evropský parlament odložil hlasování o souhlasu s definitivním uzavřením prozatímně fungujících bilaterálních dohod o zpracování a předávání údajů jmenné evidence cestujících (Passenger Name Record, dále jen „PNR data“), které vyjednala Evropská unie se Spojenými státy americkými a s Austrálií. Na základě těchto prozatímních dohod jsou letečtí dopravci nuceni předávat PNR data, tzn. osobní údaje o všech cestujících, kteří se dopravují letecky z Evropské unie do uvedených států, uchovávané v leteckých rezervačních systémech. Evropský parlament vybídl Evropskou komisi, aby iniciovala jednání o změně či upřesnění těchto dohod v tom smyslu, aby bylo dosaženo souladu těchto dohod s evropskou úpravou ochrany osobních údajů. Evropský parlament rovněž vybídl Evropskou komisi, aby přistupovala jednotně ve všech případech, kdy jsou nebo budou vyjednávány další bilaterální dohody Evropské unie se státy vyžadujícími předání PNR dat.

Evropská komise proto ohlásila záměr ještě před zahájením bilaterálních jednání o výše uvedených dohodách definovat jednotný standard předání PNR dat, a to ve Sdělení Evropské komise o globálním přístupu k přenosům údajů jmenné evidence cestujících (PNR) do třetích zemí ze dne 21. září 2010. Na tento materiál reagovali evropští ochránci osobních údajů jednak ve stanovisku Evropského inspektora ochrany osobních údajů, jednak ve stanovisku 7/2010 (WP 178) pracovní skupiny pro ochranu dat WP29. Obě stanoviska vítají, že Evropská komise zahrнула výslovně některé principy ochrany osobních údajů do navrženého záměru. Zároveň však stanovené principy v mnoha bodech doplňují a zdůrazňují nutnost tyto principy konkretizovat, aby je bylo možné skutečně prosadit v realizovatelné podobě do budoucích smluv (push systém, kdy vyžádané údaje předává správce rezervačního systému, má nahradit dosavadní pull systém s volným přístupem druhé, přijímající, strany do rezervačního systému; stanovit možnost předání údajů pouze v jednotlivých případech, které má nahradit hromadné transfery údajů; přísná regulace dalšího předání již předaných údajů do dalších třetích zemí; pravidelné společné vyhodnocování realizovaných předání atd.).

S odvoláním na základní princip ochrany údajů, totiž zásadu, podle níž mohou být shromažďovány a zpracovávány pouze údaje nezbytné k naplnění stanoveného účelu, zároveň obě výše jmenovaná stanoviska upozorňují na palčivou skutečnost, že dosud neexistuje žádná analýza, která by prokázala, že hromadné předávání údajů o cestujících z rezervačních systémů nějakým způsobem napomáhá v boji proti terorismu a závažné mezinárodní trestné činnosti.

LEGISLATIVNÍ ČINNOST

Rok 2010 byl aktivním obdobím přípravy několika právních regulací, které se bytostně týkají problematiky ochrany soukromí.

Jednou z nejdůležitějších, na nichž se Úřad podílel, byla práce skupiny expertů směřující k vytvoření **právní úpravy zpracování vzorků lidské DNA**. Odborná debata k problematice DNA zahrnuje široké spektrum otázek týkajících se nakládání s DNA v soukromé sféře, využití ve zdravotnictví i potřeby pro orgány činné v trestním řízení. Výsledky práce skupiny ukázaly především potřebnost standardizace úrovně nakládání se vzorky DNA tak, aby přitom byla garantována jistá kvalita i požadavky na bezpečnost. Mezinárodní srovnání právních úprav ve vztahu k DNA ukázalo, že Česká republika je jeden z mála evropských států bez kvalitní právní úpravy týkající se policejních DNA databází a zpracování v rámci policie může být ve značném rozsahu modifikováno pouhým rozkazem policejního prezidenta. Lze očekávat, že výsledky práce výše uvedené odborné skupiny budou do budoucna podkladem pro přípravu jednoho či více právních předpisů týkajících se zacházení s lidskou DNA.

V případech společensky často diskutovaných **kamerových systémů** Úřad připomínkoval návrh právní úpravy k jejich regulaci. K finalizaci návrhu v roce 2010 nedošlo, z pohledu Úřadu se tak stalo mj. kvůli širokému záměru tvůrců této „kamerové“ novely zákona o ochraně osobních údajů, kteří zamýšleli navrhnout regulaci ne pouze kamerových, ale širší skupiny sledovacích systémů, ať jsou provozovány veřejně či soukromě. Úřad považoval za vhodnější přistoupit toliko k právní regulaci mnohdy problematických a diskutovaných případů kamer používaných na veřejných prostranstvích či na jiných místech veřejně přístupných. V případech některých dalších, specifických sledovacích systémů, resp. sledování umožňujících technologií, Úřad vyjádřil názor, že považuje za vhodné stanovit detailněji ve zvláštních předpisech konkrétní pravidla a postupy zahrnující zpracování osobních údajů.

V oblasti justice Úřad přivítal, že Ministerstvo spravedlnosti konečně přehodnotilo účelnost **zpracování osobních údajů v rámci databáze a internetového portálu obchodního rejstříku**. Zástupci Úřadu v uplynulých letech opakovaně uplatnili připomínky k obchodnímu rejstříku a předložili Ministerstvu argumentaci k nedostatkům při zveřejňování údajů v obchodním rejstříku. Vyvolali tak expertní jednání, jehož výsledkem bude omezení dostupnosti nejčastěji zneužívaných údajů z obchodního rejstříku na internetu. Nejedná se jen o nezveřejňování tolik „populárních“ rodných čísel, v rejstříku by neměly být vedeny ani podpisové vzory. Dosažený stav však Úřad nepovažuje za dostatečný, neboť je třeba, aby rejstříky a evidence v oblasti justice byly řešeny komplexně s přihlédnutím k možnostem i hrozbám elektronického zpracování dat na internetu a také vzhledem k novým službám eGovernmentu. Jde o mnohé dílčí otázky týkající se např. datových rozhraní pro přístup k rozsáhlému množství údajů v obchodním rejstříku či otázky formy výpisů z rejstříku pro různé účely jejich použití. Nová úprava obchodního rejstříku, vyjmutá ze zákona o obchodních společnostech, bude tedy muset lépe navazovat na právní předpisy nejen z oblasti informačních systémů veřejné správy a eGovernmentu, ale také ochrany soukromí.

V souvislosti s novelou **zákona o rejstříku trestů** Úřad upozornil na značné množství výpisů z tohoto rejstříku velmi citlivých údajů, které jsou běžně vyžadovány v soukromém i ve veřejném sektoru. Jak vyplývá ze zkušenosti v oblasti elektronizace administrativy, se zavedením elektronických přístupů do centrálních databází lze očekávat, že počet výpisů poroste. Tato situace bude vyvolána nejen snazším, automatizovaným způsobem elektronického přístupu, ale může být podpořena také souvisejícími legislativními problémy, zejména nedostatečným vymezením pojmu „spolehlivost“ či „bezúhonnost“ v právních předpisech, a tedy i případů, v nichž lze opisy či výpisy vyžadovat. To vede jak k nadužívání výpisů, tak k jisté stigmatizaci osob (s výpisy se předávají a uchovávají také údaje o trestných činech, které s konkrétní bezúhonností nesouvisejí) – a takový stav lze vnímat jako výraz apriorní nedůvěry státu ke svým občanům. Úřad proto doporučil zabývat se kromě předcházení falšování výpisů také alternativními možnostmi zabezpečení všech forem výpisů či zvýšenými riziky zneužití při elektronických vyžádáních výpisů orgány veřejné moci. Úřad bude tuto problematiku nadále sledovat, neboť z ní vyplývající poznatky bude možno využít ve vztahu k vládou plánovanému registru podobných citlivých údajů – registru přestupků.

Také v roce 2010 vnímal Úřad přetrvávající zájem vytvořit právní úpravu týkající se **sledování spotřeby léků a nakládání s recepty skrze centralizovanou databázi**. Úřad podpořil jednoznačně vymezený způsob evidence a dohledu nad zacházením se zneužívanými léky (včetně všech osob, které s takovými léky přicházejí do styku). Jeho návrh však ministerstvem zdravotnictví nebyl využit. Jednoznačně však odmítl rozšířit uvažovaná opatření na všechny pacienty s léky, u nichž nedochází ke zneužívání. Úřad považuje za zásadní, aby před návrhem centrální databáze citlivých údajů, tedy i navrhované evidence lékových záznamů pacientů, proběhla podrobná společenská i odborná diskuse a byly vyhodnoceny všechny dopady a rizika, což se v předmětné problematice dosud nestalo.

Z hlediska kompetence Úřadu a jeho působení zejména v oblasti elektronických komunikací a služeb informační společnosti je zásadní v roce 2010 zahájená **implementace směrnice 2009/136/ES**.¹ Směrnice nařizuje do 25. května 2011 přijetí předpisů nezbytných pro dosažení souladu s problematikou, kterou upravuje. Směrnice mj. zavádí **nové postupy v případech narušení bezpečnosti osobních údajů (tzv. data breaches)**, související opatření zejména ve prospěch uživatelů dotčených konkrétním narušením bezpečnosti. V připomínkovém řízení, které bylo zahájeno na sklonku roku 2010, Úřad uplatnil řadu připomínek k zákonu o elektronických komunikacích (nad nímž vykonává v oblasti ochrany osobních údajů také dozor). Jedná se o konkretizaci pravidel ochrany osobních údajů (např. ustanovení týkající se přístupu k osobním údajům uživatelů) či zpřesnění působnosti v dozoru nad zpracováním osobních údajů. Vzhledem k tomu, že projednání správních deliktů spočívajících v porušení pravidel zpracování osobních údajů v elektronických komunikacích logicky navazuje na postupy Úřadu podle zákona o ochraně osobních údajů, navrhl Úřad přehodnotit některá sankční ustanovení zákona o elektronických komunikacích, která jsou duplicitní s ustanoveními zákona o ochraně osobních údajů, případně postih speciálních deliktů promítnout do zákona o ochraně osobních údajů.

Úřad také vykonává dozor nad ustanovením zákona o některých službách informační společnosti, které upravují podmínky pro zasílání obchodních sdělení; proto přivítal požadavek výše uvedené implementované směrnice na **zajištění dostupnosti informací nezbytných pro šetření zasílání nevyžádaných obchodních sdělení**. Pro vynucení práva v oblasti internetu je podstatné, aby bylo možné ověřit identitu osob, které provozují elektronické prostředky, jejichž prostřednictvím jsou šířeny

¹Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele.

obtěžující a nevyžádané zprávy. Z hlediska akceschopnosti Úřadu jako dozorové instituce je tedy žádoucí, aby zákon jasným způsobem nařídil součinnost takových osob v úředních řízeních, formy poskytování součinnosti Úřadu a aby byl současně patrný rozsah informací, které lze v rámci řízení vedených Úřadem požadovat. Úřad dále na základě svých dosavadních kontrolních zkušeností v rámci připomínkování novely navrhl, aby v problematice obchodních sdělení byl kladen důraz na skutečně závažné případy, a byla tudíž trestně postihována pouze hromadná a opakovaná zaslání nevyžádaných obchodních sdělení.

Rok 2010 byl v oblasti legislativy pravděpodobně poznamenán vyčkáváním i přípravou řady změn v souvislosti s probíhajícími volbami. Fakticky tento stav znamenal mírné či větší prodlení v řešení několika zásadních právních úprav, významně se dotýkajících ochrany soukromí a zpracování osobních údajů. V případě nového občanského zákoníku Úřad v minulosti doporučil, aby modernějším a praktičtějším způsobem – zejména s přihlédnutím k možnostem moderních technologií – bylo regulováno **pořizování obrazových a zvukových záznamů o lidech**. Namísto toho, aby autoři zákoníku jasně navodili právní podmínky, z nichž lze dovodit potřebnost či alespoň meze pořizování záznamů, omezili se na konstatování, že dotčené osoby vstupující do sledovaných prostor se sledováním souhlasí. Takový přístup k ochraně soukromí občanů považuje Úřad za zkratovitý a shledává, že je v rozporu se základními zásadami ochrany osobních údajů. Proto bude v nadcházejícím připomínkovém řízení požadovat vyjasnění příslušných ustanovení.

Úřad také marně očekával obnovení zásadní debaty nad zákony o zdravotnických službách, kde s přihlédnutím k zahraničním standardům v minulosti požadoval zohlednění vůle, resp. souhlasu pacientů v případě, že stát v některém z mnoha **zdravotnických registrů** hodlá vést jejich citlivé údaje.

Obdobně nedošlo na nový **zákon o kontrole**, od něhož si Úřad slibuje zefektivnění postupů v oblasti jím vykonávaného dozoru.

Ve volebním roce nastalo prodlení i s vylepšením volebních zákonů, k jejichž návrhu novelizace Úřad před časem přispěl doporučením, aby ve všech volebních zákonech byly jednotně upraveny vybrané postupy zpracování osobních údajů **volebních kandidátů**.

Dorešen nebyl ani nový způsob identifikace občana očekávaný v rámci **služeb eGovernmentu**, a to nejen z hlediska ochrany soukromí a s tím spojená diskuse nad podobou nového občanského průkazu, klíčového nástroje pro komunikaci mezi občanem a státem. Úřad vnímal probíhající debatu nad požadavky, aby stát „elektronickou identitu“ umožnil využívat i v soukromém sektoru, upozornil však, že právě elektronické aplikace a přenosy dat umožňují poskytnout možnost občanovi, aby byl vždy plně informován a v soukromých záležitostech v zásadě rozhodoval o tom, jaké informace a k jakému účelu mají být u elektronického průkazu (či jeho prostřednictvím) uchovávány a dále zpracovávány.

V závěru roku 2010 byl Úřad osloven se žádostí o vyjádření k návrhu **Strategie vlády v boji proti korupci** na období let 2010 až 2012. Úřadu předložený materiál obsahoval návrh řady legislativních opatření bezprostředně se dotýkajících problematiky ochrany osobních údajů, vztahující se k mnoha stávajícím agendám (např. změně podmínek použití odposlechů telekomunikačního provozu a nasazení agenta podle trestního řádu, rozvoji sdílení a ochrany dat v rámci Policie ČR, analýze whistleblowingu a ochrany oznamovatelů korupčního jednání) i agendám zcela novým. Úřad upozornil, že konkrétní opatření musí respektovat principy ochrany osobních údajů, tedy prakticky musí být formulována tak, aby umožnila zpracování a zpřístupnění osobních údajů pouze pro přesně stanovené účely, k dispozici jasně vymezeným oprávněným orgánům, za přesně určených postupů a v míře jen zcela nezbytné pro potírání korupčního jednání.

K zavedení **registru přestupků** Úřad upozornil, že není zřejmá nezbytnost úplné centralizace přestupků z různých oblastí lidského života, a dále připomenul, že režim registru citlivých údajů musí obsahovat dostatečné výslovné záruky (právní normy) pro zpracování osobních údajů, obdobně přísnému modelu rejstříku trestů. K zavedení institutu „**testů spolehlivosti**“ pro další osoby působící v orgánech veřejné moci Úřad namítl, že tento nový institut se týká úředníků, kteří nejsou ve

služebním poměru a jejich pracovněprávní poměr se řídí běžnou právní úpravou. Provokace se v případě této velké skupiny osob jeví jako nadměrný zásah do jejich soukromí. V případě elektronického registru chráněných informací od finančních institucí (**centrální registr účtů**) Úřad zpochybnil navrhovanou centralizaci údajů, neboť stávající právní úprava poskytuje řadu kompetencí a současně i mechanismy proti zneužívání dat. Záměr registru se prakticky dotýká všech občanů ČR, což v porovnání s předloženou statistikou odhalování korupce v předchozích letech znamená plošné sledování, což je silně diskutabilní. Úřad upozornil, aby všem výše uvedeným tématům byla věnována pozornost již ve fázi přípravných prací, a požádal, aby s ním byly konzultovány již ve fázi přípravy věcných záměrů legislativních změn.

STYKY SE ZAHRANIČÍM A MEZINÁRODNÍ SPOLUPRÁCE

V roce 2010 měl Úřad čest pořádat ve dnech 29. a 30. dubna prestižní akci – **Konferenci evropských komisařů ochrany dat a soukromí**. Konference se zúčastnilo přes sto delegátů z většiny zemí Evropy, mezi přednášejícími byli vedle zástupců evropských úřadů pro ochranu osobních údajů zástupci Evropské komise, Rady Evropy a vědeckí pracovníci, také ze zámoří. Motto konference „Hodnotit minulost, myslet na budoucnost“ našlo odezvu v celém programu konference a odráželo např. nejen význam nových, zejména technologických trendů ochrany osobních údajů, ale vystihovalo i období počátku roku 2010 jako dobu zamyšlení před přípravami revize základního evropského předpisu v oblasti ochrany osobních údajů – směrnice 95/46/ES.

Konference byla rozdělena do těchto základních tematických panelů: „**Internet věcí a všudypřítomné monitorování v prostoru a čase**“ byl zaměřen na technologický fenomén zasahující prakticky každého jednotlivce v moderní společnosti a ukázal, jak technologie ovlivňují dosavadní chápání pojmu soukromí. Téma dalšího panelu „**Děti v pavučině sítí**“ úzce navazovalo na předchozí, přičemž se zaměřilo na mládež, která možnosti a nástrahy světa moderních technologií vnímá často odlišně než starší generace. Panel „**Ochrana osobních údajů na rozcestí**“ byl věnován úvahám a námětům na modernizaci evropského práva ochrany osobních údajů. Téma čtvrtého panelu je zřejmé z jeho názvu: „**Veřejný sektor: respektovaný partner, nebo privilegovaný zpracovatel dat?**“ – zabýval se specifiky ochrany osobních údajů v oblasti, v níž je oprávnění ke zpracování dat občanů tradičně pojímáno jako samozřejmá kompetence státu a jeho úřadů – stále se však ukazuje, že ne vždy s dostatečným poskytnutím záruk pro přiměřené zpracování a bezpečnost osobních údajů. Závěrečný specializovaný panel konference byl věnován problematice **etnického profilování**.

Za shrnutí práce konference je možno považovat přímo na konferenci prodiskutované a následně přijaté **rezoluce konference** vyjadřující se k otázkám dalšího vývoje v oblasti (právní) ochrany osobních údajů a soukromí, k přípravě společných kroků zaměřených na informovanost a vzdělávání mladých lidí na evropské a mezinárodní úrovni, k nezbytnosti a podmínkám používání tělesných skenerů pro účely bezpečnosti na letištích a k problémům připravovaného mechanismu (dohody) o standardech ochrany osobních údajů mezi USA a EU v oblasti policie a justiční spolupráce.

Evropská konference ukázala živý potenciál zásad ochrany dat v globalizované společnosti, při využití nových technologií a zpracování dat na internetu. S přihlédnutím k těmto trendům byl rok 2010 v zahraničních agendách Úřadu naplněn revizí pravidel ochrany osobních údajů a diskusí nad přípravou zcela nových.

Předně se revizí ústředního a tradičního evropského předpisu, směrnice 95/46/ES, zabývala **Pracovní skupina pro ochranu dat podle čl. 29** (dále jen „WP29“), jejímž je Úřad stálým členem, a to na plenárních zasedáních i v činnostech podskupin WP29, jichž se zástupci Úřadu pravidelně

účastnili. Výsledkem činnosti skupiny WP29 bylo v roce 2010 mj. několik stanovisek ke klíčovým pojmům a principům ochrany osobních údajů, jako je např. zásada odpovědnosti, role správce a zpracovatele osobních údajů či k otázkám aplikovatelného (rozhodného) práva ochrany osobních údajů.

Aktivní členství v této skupině, umocněné v roce 2010 **zvolením předsedy Úřadu RNDr. Igora Němce za místopředsedu WP29**, umožňuje Úřadu prezentovat poznatky a vlastní zkušenosti na nadnárodní úrovni a tak přispívat k tvorbě celoevropských přístupů v regulaci ochrany osobních údajů. Praktický přínos národních příspěvků jednotlivých dozorových úřadů se odvíjí zejména od dostatečnosti jejich dozorových kompetencí. Úřad v rámci nadnárodní spolupráce proto očekává jistou adekvátnost kompetencí partnerských úřadů a bude to prosazovat i v nadcházející novelizaci práva ochrany osobních údajů na území EU jako zásadní otázku pro **efektivní přeshraniční spolupráci** v oblasti ochrany osobních údajů.

V rámci WP29 Úřad také připomínkoval návrh struktury a definiční části historicky prvního **ISO standardu ochrany osobních údajů**.

Mimo WP29 byl Úřad v roce 2010 již tradičně účasten prací dalších **evropských skupin, zejména společných dozorových orgánů**. Zástupkyně Úřadu PhDr. Miroslava Matoušová se zúčastnila inspekce společných kontrolních orgánů v Europolu i v Eurojustu a dále byla expertem na pravidelném hodnocení úrovně ochrany osobních údajů při naplňování požadavků tzv. schengenské *acquis* (tedy Schengenské úmluvy a souvisejících právních dokumentů) ve Španělsku a Portugalsku.

Neméně aktivně byla novelizace přístupů k ochraně osobních údajů rozpracovávána poradní skupinou **Rady Evropy** k Úmluvě 108, o automatizovaném předávání osobních dat (dále jen „T-PD“), voleného zástupci 47 členských států. V červnu 2010 byla PhDr. Hana Štěpánková zvolena její první místopředsedkyní. Skupina završila práci na doporučení o profilování osobních údajů, které bylo přijato Radou ministrů členských států a může být aplikováno členskými státy. T-PD započala v roce 2010 také práce na novele Úmluvy 108, která v lednu 2011 bude připomínána u příležitosti 30. výročí své existence jakožto první závazný dokument, který v Evropě zakotvil ochranu osobních údajů jako součást základních lidských práv na ochranu soukromí. (V závěru roku 2010 byla Rada Evropy naléhavě vybídnu ta k modernizaci Úmluvy 108 také parlamentním shromážděním.)

V minulých letech získal Úřad zkušenost i odborné renomé v tzv. twinningových projektech podporovaných EU. Také s přihlédnutím k této skutečnosti byl v roce 2010 Úřad, příp. přímo jeho zaměstnanci, osloven s žádostí o **účasť v mezinárodních týmech** zaměřených na vyhodnocení standardů ochrany osobních údajů a pozice příslušných úřadů ochrany osobních údajů v zemích zavádějících či vylepšujících ochranu osobních údajů. Zaměstnanec Úřadu JUDr. Jiří Maštalka se stal hlavním expertem projektu v Albánii zaměřeného na revizi právního rámce ochrany osobních údajů a optimalizace postupů albánského úřadu pověřeného dozorem nad ochranou dat. Do obdobného projektu v Makedonii plánovaného na období 2011 Úřad nominoval 4 krátkodobé experty. Uvedené projekty jsou hrazeny z prostředků EU, a neomezí tedy rozpočet Úřadu.

Na žádost bulharské komise pro ochranu osobních údajů Úřad uspořádal v Praze na podzim roku 2010 **dvoudenní seminář**, který seznámil bulharské kolegy s praktickými **poznatky kontrolních postupů** Úřadu, zejména s přihlédnutím k schengenským agendám.

V roce 2010 se uskutečnila pracovní setkání odborníků polského, českého a maďarského úřadu, pracujících na **mezinárodním projektu v rámci programu Leonardo da Vinci** financovaného Evropskou unií. Záměrem řešitelů je zvýšení povědomí o ochraně osobních údajů mezi odbornou i laickou veřejností v podnikání a pracovních vztazích. Výstupem projektu bude příručka, která nabídne zaměstnavatelům i zaměstnancům srozumitelné a užitečné informace o podmínkách zpracování a ochrany dat a přinese instrukce, jak postupovat ve vybraných situacích při podnikání.

Za již dlouhodobě prověřenou tradici upevněnou mimo jiné spoluprací s ministerskými resorty v době českého předsednictví EU je proces vyjadřování se k materiálům či k průběhu prací nad materiály připravovanými na různých ministerstvech v rámci expertních skupin při plnění úkolů vyplývajících z členství EU. Úřad zde má možnost upozorňovat na **aspekty zpracování osobních údajů v mezinárodních a eurounijních závazcích** ještě předtím, než jsou uzavírány dohody

a aplikovány či implementovány schválené předpisy. V roce 2010 to byly materiály z téměř dvou desítek okruhů týkajících se především trestních procedur a boje proti kriminalitě.

Zvláště intenzivní práci si v roce 2010 vyžádaly na evropské úrovni již několik let diskutované otázky **dohod mezi USA a EU o ochraně osobních údajů při policejní a justiční spolupráci**. Zde Úřad opakovaně více či méně úspěšně uplatňoval připomínky k návrhu národní pozice ČR k celé problematice, lze však očekávat, že zásadnější vliv bude mít expertní výzva, kterou národní úřady ochrany dat v závěru roku adresovaly Evropské komisi z pozice výše zmiňované skupiny WP29 a jež obsahuje souhrn problémů patrných v aktuálním návrhu obecné dohody mezi USA a EU (tzv. umbrella agreement).

V problematice předávání dat cestujících v letecké přepravě do třetích zemí (tzv. agenda PNR) se v roce 2010 stalo mezníkem Sdělení Evropské komise o globálním přístupu k přenosům údajů jmenné evidence cestujících (PNR) do třetích zemí. Dokument byl vydán za stavu kritiky bilaterální smluvní agendy PNR – za nedostatečnost smluv i způsob jejich sjednávání a za faktický dopad vzniklé nejasné právní situace na jednotlivé národní dopravce. Sdělení EK shrnuje možné budoucí přístupy (neudržitelnost stávajícího systému bilaterálních smluv, volání po globálním přístupu) a vyjmenovává nedořešené otázky, týkající se zejména účelnosti budovaného systému PNR a z toho vyplývající potřebné míry ochrany osobních údajů. Zde jsou zohledněny připomínky ochránců osobních údajů, k nimž v uplynulých letech aktivně přispíval i Úřad.

Účastníci Konference evropských komisařů ochrany dat a soukromí

Foto: Pavel Hořejší



ÚŘAD, SDĚLOVACÍ PROSTŘEDKY A KOMUNIKAČNÍ NÁSTROJE

Roku 2010 Úřad soustředil komunikaci s médii na aktivní denní servis a aktuální informování prostřednictvím webových stránek. Kromě dvou tiskových konferencí si značnou časovou pracovní kapacitu vyžádala příprava dubnové Konference evropských komisařů ochrany dat, jejímž pořadatelem byl český Úřad.

Na zimní tiskové konferenci pořádané tradičně u příležitosti Dne ochrany osobních údajů byl vyhlášen čtvrtý ročník soutěže pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“, jehož cílem v daném roce bylo obrátit pozornost dětí a mladých lidí na rizika spojená s komunikací prostřednictvím internetu a při využívání sociálních sítí.

Právě na tuto problematiku spojenou s vyhlášenou soutěží navázal také diskusní panel „Děti v pavučině sítí“, který byl součástí jmenované celoevropské jarní konference.

Podzimní tisková konference bilancovala práci Úřadu a byla zaměřena především na ta šetření Úřadu, jimž byla věnována soustředěná pozornost médií. Především šlo o rozhodnutí Úřadu ve věci Google Street View a šetření spojené s databází vedenou Státním ústavem pro kontrolu léčiv.

Zájem novinářů o tiskové konference pořádané Úřadem se stabilně pohybuje na úrovni 20–25 přítomných novinářů. Jako podstatné se ovšem jeví, že je zastoupena celá škála mediální scény – agenturní, elektronická i tištěná média.

Rozsah zveřejněných zpráv týkajících se ochrany osobních údajů, které vycházejí v návaznosti na tiskovou konferenci, byl roku 2010 co do množství obdobný jako v roce předcházejícím (30–60 výstupů v následujících 3 dnech po tiskové konferenci).

V přílohách k tiskovým zprávám Úřad poskytuje soustavně informace o kontrolách ukončených správním řízením. Za přínosné pro šíření znalosti problematiky ochrany osobních údajů v mediálním světě a jeho prostřednictvím mezi širokou veřejností považuje Úřad zveřejňování důvodů uložených pokut, v němž spatřuje možnost, jak velmi organicky prohlubovat také právní povědomí o způsobu aplikace zákona o ochraně osobních údajů.

Kontakty s médii

S jistotou lze říci, že zákon o ochraně osobních údajů je dnes již samozřejmou součástí agendy médií; dotazy novinářů jsou detailnější a fundovanější, než tomu bylo v počátcích existence Úřadu. Sami novináři svými dotazy také upozorňují na „kauzy“, které jsou většinou z hlediska porušení zákona o ochraně osobních údajů skutečně relevantní. (Tato konstatovaná praxe odpovídá i zkušenostem se stížnostmi, které na Úřad přicházejí.) Dá se tedy do jisté míry zobecnit, že v zájmu veřejnosti se začíná uplatňovat synergie mezi prací nezávislé dozоровé autority a institutem médií jakožto služby veřejnosti.

Rozhodně ubylo obecně formulovaných otázek o „ochraně osobních údajů“, naopak přibýlo specializovaných témat. Mezi nejšíř a nejsoustavněji sledované případy v médiích v roce 2010 patřila opakovaná otázka zveřejňování osobních údajů v zápisech z jednání zastupitelstev obcí, problematika využívání kamer v bytových domech, sledování zaměstnanců na pracovištích – jmenovitě sledování elektronické korespondence a v závěru roku geolokalizace. Velkou pozornost vyvolávala kontrola Úřadu provedená ve Státním ústavu pro kontrolu léčiv, postoj Úřadu k CERD – registru dlužníků, a v předvolebním období zveřejnění dlužníků kandidujících stran v Chomutově.

Problém služby Google Inc. Street View se několikrát vrátil do zorného pole médií – především v návaznosti na informace, které přicházely ze zahraničí, kde uvedená služba Googlu rovněž rozpoutala soustavné sledování práce ochránců osobních údajů. Bohužel je třeba také konstatovat, že některé elektronické informační kanály (lupa.cz) – obdobně jako jednotliví občané – zaslepeně hájily tuto službu Googlu, aniž vůbec braly na zřetel právní aspekty, z nichž vycházela rozhodnutí Úřadu, tím méně jevíly ochotu snažit se jim porozumět. Zarážející trivialita výroků, které Úřad zaznamenal, připomíná někdy až anarchicky primitivní příklon k nejjednodušším a pozičně silovým řešením.

Úřad musel také bohužel opakovaně uvádět na pravou míru zavádějící vyjádření ČOI, že zákon o ochraně osobních údajů brání zveřejnění čerpacích stanic, kde dochází k nekorektní obsluze řidičů.

Webové stránky Úřadu

Mediální výstupy Úřad obvykle publikuje na svých webových stránkách (po dohodě, a jedině na jejím základě, s konkrétním médiem). Je tak posílena i možnost, aby veřejnost sledovala názorovou kontinuitu Úřadu a novináři měli okamžitou odpověď na kladené dotazy – není zajisté žádným tajemstvím, že jistá témata, jakmile jsou otevřena, spustí větší, někdy i lavinovitý mediální zájem. Nejen v takových případech informuje Úřad o svých názorech a stanoviscích prostřednictvím tiskových zpráv a tiskových prohlášení, které jsou na webových stránkách zveřejňovány v samostatné rubrice „Tiskové zprávy a konference“.

Kromě toho rubrika „Novinky“ v záhlaví webových stránek slouží jako orientační vodítko ke konkrétním krokům Úřadu a dění, s nímž se aktuálně vyrovnává.

V posledním měsíci roku 2010 otevřel Úřad na svých webových stránkách diskusní fórum k tématu využívání zákaznických (věrnostních) karet. Zodpovězením řady položených dotazů upozornil mj. na rizika spojená s poskytováním osobních údajů, kterým je získání zákaznické karty podmíněno. Úřad sáhl k využití diskusního fóra, aby zjistil, nakolik si veřejnost uvědomuje, že potřeba ochrany soukromí je spojena také s využíváním klientských či věrnostních karet. Zdá se, že reakce, které jsou trvale přístupné na webu v rubrice Diskusní fórum / Ukončená diskusní fóra / Zákaznické karty, vycházejí nejvíce z obhajoby této marketingové strategie; bohužel je zřejmé, že možné důsledky pro sledování soukromého života buď občany vůbec nezajímají, nebo je nezajímají proto, že nejsou o využívání svých osobních údajů dostatečně informováni, nebo je pro ně zajímavější sebemenší finanční prospěch než ochrana vlastního soukromí, případně reakce v diskusi přicházela od profesionálních marketérů více než od občanů. V každém případě se potvrzuje opodstatnění pro to, aby Úřad uplatnil svou dozorovou povinnost v této oblasti.

Šíření znalostí o ochraně osobních údajů

V kontextu příprav tzv. Jarní konference – Konference evropských komisařů ochrany dat a soukromí – byla jako podklad jednání panelové diskuse „Děti v pavučině sítí“ připravena „bílá kniha“ dobré praxe (trvale dostupná na www.uouu.cz, rubrika Publikace), která shrnula poznatky a postupy jednotlivých evropských partnerských úřadů v přístupu k šíření znalostí o smyslu ochrany osobních údajů mezi mladou generací – zejména ve vztahu k šíření poznatků o riziku plynoucím pro soukromí kvůli neobvyčejné ochotě mladých lidí zveřejňovat o sobě téměř cokoli na tzv. sociálních sítích. Velmi vlašný až odmítavý postoj brát ohled na to, co o sobě zveřejňují, projevíli mladí účastníci na konferenci Kyberšikana a ochrana osobních údajů aneb Kam až to může zajít na internetu, pořádané Výborem pro vzdělávání, vědu, kulturu, lidská práva a petice Senátu ČR, které se zúčastnil také předseda Úřadu.

Pozvání mladí lidé víceméně skutečně dali najevo, že jsou zajedno se zakladatelem Facebooku, dnes už známým jako osobnost roku 2010, a jeho negací soukromí. Úřad má ovšem na základě příspěvků do soutěže, kterou pořádá pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“, poznatky o té části mladé generace, vnímající soukromí jako hodnotu života a považující ochranu osobních údajů, které se stále prokazatelněji stávají vyhledávanými klíči k němu, za potřebný a oprávněný požadavek i v technicky a technologicky bohatém světě. Dávat možnost vyjadřovat svůj postoj i této části mladé populace Úřad považuje za opodstatněné podporovat. Proto považuje za důležité pokračovat ve spolupráci se školstvím a má připraven další projekt.

Nepochybně přínosné jsou i přednášky pracovníků Úřadu (právníci Úřadu odpřednášeli v loňském roce 215 hodin) a setkání předsedy, inspektorů a vedení Úřadu se Stálou komisí senátu pro ochranu soukromí i s dalšími institucemi.

Knihovna a publikace Úřadu

Knihovna nadále slouží jako odborné zázemí pro pracovníky Úřadu, ale je otevřena na individuální vyžádání také odborné veřejnosti. Využívají ji studenti pro své seminární a diplomové práce dotýkající se ochrany osobních údajů. V roce 2010 poskytla svůj fond 6 studentům a rozrostla se o 3 jejich práce. Fond knihovny narostl v průběhu roku o 60 dalších svazků.

Vydávaný Věstník Úřadu publikoval ve svých 3 částkách zásadní dokumenty o ochraně osobních údajů zahraniční provenience i zásadní stanoviska Úřadu. Publikované dokumenty jsou dostupné rovněž v elektronické podobě a lze je dohledat na základě zveřejněných obsahů jednotlivých částek Věstníku.

Informační bulletin vydávaný od roku 2010 s výhradně tematickým zaměřením byl věnován problematice ochrany soukromí dětí komunikujících po internetu. Rozpracované je číslo soustřeďující se na otázky DNA – ve vztahu k ochraně soukromí a otázkám žádoucí legislativní úpravy při využívání DNA.

SPOLUPRÁCE S INSTITUCEMI

SPOLUPRÁCE S AMERICKOU OBCHODNÍ KOMOROU

Úřad se společně s ÚOHS a ČTÚ zapojil již třetím rokem do Projektu rozvoje kvality regulační činnosti, který je realizován AmCham s cílem vyhodnotit „kritéria“, na základě kterých vyjmenovaní regulátoři vykonávají svou působnost a tím ovlivňují vývoj v oblasti regulace. V rámci tohoto projektu byla v únoru realizována společná akce zástupců jednotlivých úřadů, kdy formou prezentací a následné diskuse nejprve vždy předseda Úřadu a následně další zástupci vysvětlovali účastníkům semináře, jakým způsobem se nastavených kritérií (konzistentnost a kvalita rozhodování, informace o jednáních v rozporu se zákonem o ochraně osobních údajů) Úřad zhostil. Projekt bude pokračovat i v následujících letech.

SPOLUPRÁCE S ČESKÝM TELEKOMUNIKAČNÍM ÚŘADEM

V návaznosti na případ, který Úřad řešil společně s Kanceláří veřejného ochránce práv a jenž se týkal podmínek pro používání rodného čísla adresáta poštovní zásilky na zásilce samotné, vyvolal Úřad jednání se zástupci ČTÚ, jehož předmětem byla možnost změny současných poštovních podmínek.

Současná právní úprava poštovních podmínek, která vychází z podmínek zákona o poštovních službách, totiž možnost použití rodného čísla adresáta poštovní zásilky nijak neomezuje, ačkoliv existuje speciální právní úprava pro použití rodného čísla vymezená zákonem o evidenci obyvatel, která obsahuje poměrně přesný právní rámec. Tato skutečnost ve svém důsledku znamená, že odesílatel může libovolně zvážit, zda v případě adresáta poštovní zásilky použije jeho rodné číslo nebo datum narození, aniž by zohlednil míru možného narušení soukromí neuváženým zpřístupněním tohoto poměrně významného osobního údaje.

Výsledkem jednání zástupců obou úřadů byla dohoda, že s účinností od 1. ledna 2011 bude ze strany ČTÚ změna poštovních podmínek realizována ve prospěch ochrany osobních údajů.

SPOLUPRÁCE S ČESKOU POŠTOU

Zástupci České pošty se v návaznosti na záměr realizovat projekt nové služby „Avízo“, jehož obsahem by byla možnost, aby adresáti poštovních zásilek byli informováni na telefonním čísle nebo elektronické adrese o tom, že jim Česká pošta hodlá doručovat novou poštovní zásilku, obrátili na Úřad

s požadavkem zajištění souladu těchto podmínek se zákonem o ochraně osobních údajů. I když se má nepochybně jednat o službu určenou široké veřejnosti, nelze se odklonit od podmínek i požadavků, které před každého správce klade platná právní úprava. Úřad se tedy nejprve zabýval otázkou sběru těchto údajů. Návrh Úřadu, aby Česká pošta sama jako odpovědný subjekt oslovila své klienty s návrhem této nové služby a vyžádala si přímo jejich kontaktní údaje, nebyl ze strany zástupců České pošty podpořen, ale byl pouze diskutován jako možnost realizace projektu. Naopak byl ze strany České pošty navržen postup, aby to byl sám odesílatel, kdo předá České poště kontaktní údaje adresáta, které předtím získal právě pro tento účel. I když lze v zásadě počítat i s touto variantou postupu, vyjádřili se zástupci Úřadu v tom směru, že zatímco běžné osobní kontakty obsahující telefonní nebo jiné elektronické údaje slouží osobám pro naplnění jejich osobních potřeb a zákon o ochraně osobních údajů se na takové zpracování v kontextu § 3 odst. 3 tohoto zákona nebude aplikovat, v případě následného zpracování stejných kategorií informací ze strany České pošty by se již jednalo o zpracovávání osobních údajů v režimu zákona o ochraně osobních údajů. Jednání dosud nebyla ukončena.

SPOLUPRÁCE SE SVAZEM MĚST A OBCÍ

Úřad díky svým kontrolním poznatkům z uplynulého období, kdy se obce a jejich orgány často velmi obtížně vypořádávají se svými povinnostmi správce osobních údajů, vyvolal v letošním roce jednání se zástupci SMO, jehož cílem bylo dosáhnout větší míry informovanosti pro zastupitele a úředníky obcí, kteří v návaznosti na výsledky komunálních voleb v roce 2010 vykonávají svou činnost, jejíž součástí je i zpracovávání osobních údajů. Výsledkem této spolupráce byl podíl Úřadu na publikaci s názvem „Příručka pro člena zastupitelstva obce po volbách v roce 2010“, kdy se právě problematika ochrany osobních údajů stala nedílnou součástí této publikace. Současně byli předseda Úřadu a další zástupci pozváni na XIII. Celostátní finanční konferenci SMO, v jejímž rámci byl organizován seminář k tématu ochrany osobních údajů při výkonu působnosti obcí.

Výstava dětských prací ze soutěže pořádané Úřadem se stala vítaným doplňkem konference. V jejím průběhu byla instalována spolu s prezentací uplatnění programu dalšího vzdělávání pedagogických pracovníků na území ČR a kampaní distribuce letáků se základní informací pro místní samosprávné orgány pod názvem „Vizitka vyspělých demokracií – ochrana osobních údajů“.

Aktivity Úřadu budou v oblasti samosprávy pokračovat i směrem k dalším sdružením působícím nejen v rámci obcí, ale i v rámci krajů.

INFORMAČNÍ SYSTÉM ORG

Zákon č. 111/2009 Sb., o základních registrech a jeho změna zákonem č. 100/2010 Sb., přinesly Úřadu nový úkol: Do 30. 6. 2012 vytvořit Informační systém ORG jako součást systému Základních registrů, který bude zajišťovat procesy spojené s identifikací fyzických osob.

Financování investiční části požadovaného systému bylo zajištěno usnesením vlády č. 1019/2009 a projekt je spolufinancován z projektu Evropské unie ve výši 85 % uznatelných nákladů na základě vydání právního aktu o poskytnutí dotace ze dne 30. 11. 2010.

Základním smyslem Informačního systému ORG (který je v některých materiálech nazýván převodníkem identifikátorů) je zajistit v celém systému Základních registrů ochranu osobních údajů, a to cestou náhrady dosavadního používání rodného čísla jako univerzálního identifikátoru fyzické osoby systémem bezvýznamových identifikátorů. Tyto identifikátory se budou pro jednotlivé agendy nebo skupiny agend lišit, a neumožní tak při znalosti jednoho identifikátoru vyhledávat údaje o fyzické osobě v agendě jiné. Jediným místem, kde budou všechny tyto identifikátory uloženy, je právě Informační systém ORG. V tomto systému však nebudou uložena žádná jména fyzických osob, takže ani znalost všech identifikátorů neumožní Úřadu zjistit jejich přiřazení jednotlivým fyzickým osobám. Touto cestou by měla realizace projektu Základních registrů výrazně přispět k ochraně osobních údajů občanů.

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

Veřejná zakázka na návrh a dodávku Informačního systému ORG byla zahájena 27. 11. 2009 předběžným oznámením na stránkách Informačního systému veřejných zakázek. Vlastní zadávací řízení na tuto veřejnou zakázku bylo na stránkách ISVZ otevřeno 2. 3. 2010 pod evidenčním číslem 60042442 a názvem Dodávka informačního systému ORG.

Na základě uveřejnění této zakázky bylo Úřadu podáno uchazeči celkem 6 nabídek. Všechny doručené nabídky byly otevřeny 20. 4. 2010 a všechny byly přijaty.

První jednání hodnotící komise proběhlo 27. 4. 2010. V průběhu hodnocení byl jeden z uchazečů vyloučen pro nesplnění požadavků zadavatele. Jednání hodnotící komise pokračovalo až do 25. 6. 2010, kdy byla člena komise podepsána Zpráva o posouzení a hodnocení nabídek a předána předsedovi

Úřadu. Předseda Úřadu se ztotožnil s doporučením hodnotící komise a dne 2. 7. 2010 podepsal Rozhodnutí o výběru nejvhodnější nabídky.

Proti tomuto Rozhodnutí podali uchazeči, kteří se umístili na 2., 4. a 5. místě, námitky k předsedovi Úřadu. Po posouzení námitek všech uchazečů bylo 30. 7. 2010 rozhodnuto o jejich zamítnutí.

Dne 11. 8. 2010 se na základě tohoto zamítnutí uchazeč, který se umístil na 4. místě, odvolal k Úřadu pro ochranu hospodářské soutěže (dále jen „ÚOHS“), který zahájil 30. 8. 2010 správní řízení ve věci přezkoumání úkonů zadavatele při zadávání výše uvedené zakázky. Dne 5. 10. 2010 zmíněný uchazeč svoje podání doplnil a Úřad se k tomuto doplnění vyjádřil dne 14. 10. 2010.

Dne 10. 12. 2010 zamítl ÚOHS jak doplňující podání uchazeče, tak i jeho původní odvolání. Proti tomuto rozhodnutí může uchazeč podat rozklad k předsedovi ÚOHS do 15 dnů ode dne doručení.¹

Start realizace projektu IS ORG je touto situací zatím proti původnímu harmonogramu zpožděn o minimálně půl roku. Tento stav není problémem pouze systému ORG. Dva další z celkem šesti projektů systému Základních registrů jsou v podobné situaci, takže koordinace výstavby systému Základních registrů je velice obtížná. Protože všechny tyto související projekty jsou spolufinancovány z prostředků EU, je časové zpoždění nebezpečné i z pohledu nečerpání plánovaných finančních prostředků.

Přijetím zákona č. 100/2010 Sb., kterým se mění zákon č. 111/2009 Sb., o základních registrech, se prodloužilo období pilotní provozu systému a zákon předpokládá ostrý start systému k 1. 7. 2012. Další odkládání startu realizace celého systému Základních registrů by tento termín mohlo ohrozit, pokud se tak již nestalo.

¹ Dne 10. 1. 2011 zaslal ÚOHS rozhodnutí o zastavení správního řízení v této věci, neboť uchazeč všechny svoje návrhy vzal zpět. Vítězem soutěže na dodávku IS ORG se stalo TESCO SW, a. s.

PERSONÁLNÍ OBSAZENÍ ÚŘADU

Úřad měl pro rok 2010 státním rozpočtem stanoveno 102 funkčních míst. Na základě Usnesení vlády č. 715/2009 byl počet funkčních míst oproti roku 2009 snížen o 5 a následně navýšen o 12 z důvodu přidělených kompetencí vyplývajících pro Úřad ze zákona č. 111/2009 Sb., o základních registrech. K 1. 1. 2010 byl fyzický počet zaměstnanců v Úřadu 93, z toho 90 zaměstnanců bylo v evidenčním stavu a 3 zaměstnanci v mimoevidenčním stavu. K 31. 12. 2010 měl Úřad 101 zaměstnanců, z toho 5 zaměstnanců v mimoevidenčním stavu. V průběhu roku nastoupilo do Úřadu 15 nových zaměstnanců a 7 zaměstnanců pracovní poměr ukončilo. Průměrný evidenční počet zaměstnanců za rok 2010 činil 94,42. Většina zaměstnanců Úřadu má vysokoškolské vzdělání, vysokoškolské vzdělání je předpokladem pro výkon většiny činností v Úřadu. Úřad svým zaměstnancům proto zajišťuje a umožňuje kromě prohlubování kvalifikace i její zvyšování a také jazykovou výuku. Jazykové znalosti pak zaměstnanci uplatňují v rámci mezinárodní spolupráce v oblasti ochrany osobních údajů.

Členění zaměstnanců Úřadu podle věku a pohlaví – stav k 31. 12. 2010

Věk	muži	ženy	celkem	%
do 20 let	0	0	0	0,0 %
21–30 let	7	9	16	16,7 %
31–40 let	6	7	13	13,5 %
41–50 let	6	10	16	16,7 %
51–60 let	17	17	34	35,4 %
61 let a více	11	6	17	17,7 %
Celkem	47	49	96	100,0 %
%	49,0 %	51,0 %	100,0 %	

Členění zaměstnanců Úřadu podle vzdělání a pohlaví – stav k 31. 12. 2010

Vzdělání	muži	ženy	celkem	%
Střední odborné + VL	1	1	2	2,1 %
Střední odborné	0	1	1	1,0 %
Střední odborné	0	1	1	1,1 %
Úplné střední všeobecné	3	5	8	8,3 %
Úplné střední odborné + VL	1	1	2	2,1 %
Úplné střední odborné	4	17	21	22,0 %
Vyšší odborné vzdělání	0	1	1	1,0 %
Vysokoškolské	37	22	59	61,5 %
VŠ + vyšší kvalifikace	1	1	2	2,1 %
Celkem	47	49	96	100,0 %

Celkový údaj o vzniku a skončení pracovních poměrů zaměstnanců v roce 2010

	Počet
nástupy	15
odchody	7

HOSPODAŘENÍ ÚŘADU

Rozpočet Úřadu byl schválen zákonem č. 487/2009 Sb., o státním rozpočtu České republiky na rok 2010.

ČERPÁNÍ STÁTNÍHO ROZPOČTU KAPITOLY 343 – ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

Souhrnné ukazatele	v tisících Kč
Příjmy celkem	6 665,78
Výdaje celkem	96 732,95
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	6 665,78
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	41,05
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	6 624,73
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	96 732,95
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	48 883,00
Povinné pojistné placené zaměstnavatelem*)	16 620,00
Převod fondu kulturních a sociálních potřeb	935,00
Platy zaměstnanců v pracovním poměru	38 099,00
Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	8 613,00
Výdaje spolufinancované z rozpočtu Evropské unie bez SZP celkem	249,76
v tom: ze státního rozpočtu	31,31
podíl rozpočtu Evropské unie	218,45
Výdaje vedené v informačním systému program. financování celkem	4 890,50

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

Příjmy

Příjmy pro rok 2010 byly schváleným rozpočtem stanoveny ve výši 76 186 tisíc Kč, a to v souvislosti s projekty spolufinancovanými z rozpočtu EU – IOP „Informační systém ORG v systému základních registrů“, projektem IOP č. 184 „Elektronizace procesu podávání oznámení o zpracovávání osobních údajů“ a projektem Partnerství Leonardo da Vinci „Zvyšování povědomí o ochraně dat mezi podnikateli působícími v EU“, který je 100% financován z rozpočtu EU.

Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částkou 6 665,78 tisíc Kč.

Jednalo se zejména o refundace zahraničních cest zaměstnanců Úřadu Evroplem a Evropskou komisí, o sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti, o sankce uložené podle zákona o ochraně osobních údajů a jiných zákonů, o náhrady nákladů řízení, o úroky z finančních prostředků uložených na bankovních účtech, o refundace výdajů týkajících se komunitárního programu Leonardo da Vinci, o příjmy vztahující se k roku 2009 (odvod zůstatku depozitního účtu po vyplacení platů a přidělu do FKSP za prosinec 2009).

Úroky z finančních prostředků uložených na účtech u ČNB činily 1,96 tisíc Kč.

Přijaté sankční platby byly ve výši 5 331,33 tisíc Kč, neinvestiční dotace z EU ve výši 41,05 tisíc Kč a přijaté nekap. příspěvky a náhrady týkající se minulých let ve výši 1 291,44 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

1. OSTATNÍ BĚŽNÉ VÝDAJE

Čerpání běžných výdajů ve výši 26 548,17 tisíc Kč odpovídá běžným provozním výdajům, které vyplývají z hlavní činnosti Úřadu; jde zejména o položky spojené s nákupem drobného hmotného majetku, materiálu, služeb, cestovného, vzdělávání, údržby a o výdaje související s neinvestičními nákupy.

Výdaje za vodu, plyn a elektrickou energii činily v roce 2010 – 1 216,12 tisíc Kč.

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

2. PLATY ZAMĚSTNANCŮ A OSTATNÍ PLATBY ZA PROVEDENOU PRÁCI

Čerpání rozpočtu na platy zaměstnanců a ostatní výdaje za provedenou práci odpovídají kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. 12. 2010 byl 101 zaměstnanců.

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

V souladu se schválenou dokumentací programu 143V01 „Rozvoj a obnova materiálně-technické základny Úřadu pro ochranu osobních údajů – od r. 2007“ bylo celkem vyčerpáno 4 890,50 tisíc Kč.

V podprogramu 143V01100 „Pořízení, obnova a provozování ICT ÚOÚ“ bylo v roce 2010 v souladu s UV č. 552/2010 vázáno 200 tisíc Kč a čerpáno celkem 4 890,50 tisíc Kč na investiční systémově určené výdaje SR na následující akce:

v tisících Kč

akci 143V011000008 „Prodloužení smlouvy Enterprise na používání produktů Microsoft“	1 764,47
akci 143V011000010 „IS ÚOOÚ – Informační modul“	630,26
akci 143V011000025 „Upgrade ek. systému PC účetnictví JASU“	262,44
akci 143V011000026 „Prodloužení platnosti licencí AVG“	108,11
akci 143V011000029 „IS ÚOOÚ Registr“	142,93
akci 143V011000030 „Upgrade externích poštovních antivirových a antispamových služeb“	341,41
akci 143V011000031 „Dodávka centrálního dat. úložiště a zařízení pro zálohování a archivaci dat“	1 321,77
akci 143V011000032 „Rozšíření spisové služby GINIS a funkčnost časových razítek“	110,40
akci 143V0110018 „Elektronizace procesu podávání oznámení zprac. os. údajů“ – projekt IOP č. 184 – spolufinancovaný z rozpočtu EU	0,00
akci 143V0110019 „Informační systém ORG v systému základních registrů“ – projekt IOP spolufinancovaný z rozpočtu EU 208,71	208,71

Finanční prostředky na tento projekt byly čerpány z nároků z nespotřebovaných výdajů roku 2009.

V podprogramu 143V01200 „Reprodukce majetku ÚOOÚ“ byla v souladu s UV č. 552/2010 vázána částka 1 000 tis. Kč a tímto nebylo uskutečněno žádné čerpání plánovaných investičních systémově určených výdajů.

PŘEHLED ČERPÁNÍ STÁTNÍHO ROZPOČTU V ROCE 2010

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2010 v tis. Kč	Rozpočet po změnách 2010 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2010 v tis. Kč	Skut./uprav. rozpočet v %
	PŘÍJMY CELKEM	76 186	76 186	6 665,78	8,75
501	Platy	47 724	47 724	46 712,00	97,88
5011	Platy zaměstnanců	39 111	39 111	38 099,00	97,41
5014	Platy zaměstnanců odvozované od platů úst. činitelů	8 613	8 613	8 613,00	100,00
502	Ostatní platby za provedenou práci	2 289	2 960	2 171,00	73,34
5021	Ostatní osobní výdaje	1 319	2 960	2 171,00	73,34

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2010 v tis. Kč	Upravený rozpočet 2010 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2010 v tis. Kč	Skut./uprav. rozpočet v %
5024	Odstupné	288	0	0,00	0
5026	Odchodné	682	0	0,00	0
503	Povin. pojist. placené zaměstnavatelem	17 005	17 234	16 620,00	96,44
5031	Povin. pojist. na sociální zabezpečení	12 504	12 672	12 221,00	96,44
5032	Povin. pojist. na veřejné zdrav. pojištění	4 501	4 562	4 399,00	96,43
513	Nákup materiálu	2 721	2 779	1 693,88	60,95
514	Úroky a ostatní fin. výdaje	15	16	6,34	39,63
515	Nákup vody, paliv a energie	2 077	1 872	1 490,84	79,64
516	Nákup služeb	18 868	30 090	16 250,01	54,00
5167	Školení a vzdělávání	1 415	1 019	972,07	95,39
517	Ostatní nákupy	5 950	6 172	3 737,61	60,56
5171	Opravy a udržování	1 505	1 664	805,65	48,42
5173	Cestovné	2 871	2 803	1 705,63	60,85
519	Výdaje souvis. s neinv. nákupy	2 490	2 796	2 282,69	81,64
5342	Převody FKSP	955	955	935,00	97,91
536	Ostatní neinv. transf. jin. veřej. rozp.	14	22	16,97	77,14
542	Náhrady plac. obyvatelstvu	250	250	134,83	53,93
5424	Náhrady v době nemoci	250	250	134,83	53,93

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2010 v tis. Kč	Upravený rozpočet 2010 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2010 v tis. Kč	Skut./uprav. rozpočet v %
590	Ostatní neinv. výdaje jinde nezařazené	0	16	0,00	0
	Běžné výdaje celkem	100 358	112 886	92 051,17	81,54
611	Pořízení dlouh. nehmot. majetku	65 935	57 555	3 018,60	5,24
612	Pořízení dlouh. hmot. majetku	26 923	22 775	1 663,18	7,30
	Kapitálové výdaje celkem	92 858	80 330	4 681,78	5,83
	VÝDAJE CELKEM	193 216	193 216	96 732,95	50,06

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 12. 2010.

PŘEHLED VÝDAJŮ NA PROJEKTY SPOLUFINANCOVANÉ Z ROZPOČTU EU V ROCE 2010

Název projektu	Schválený rozpočet (v tis. Kč)	Rozpočet po změnách 2010 (v tis. Kč)	Skutečnost dle účetních výkazů k 31. 12. 2010	Skutečnost/rozpočet po změnách v %
„Informační systém ORG v systému základních registrů“ - projekt IOP	83 250	83 250	208,71	0,25
„Elektronizace procesu podávání oznámení a zpracovávání osobních údajů“ - č. 184 - projekt IOP	5 601	4 760	0,00	0,00
„Zvyšování povědomí o ochraně dat mezi podnikateli působícími v EU“ - projekt partnerství „Leonardo da Vinci“	192,00	192,00	41,05	21,38
Celkem za projekty spolufinancované z EU	89 601,00	88 676,00	249,76	0,28

POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ

Úřad v roce 2010 obdržel dvacet žádostí o poskytnutí informace podle zákona o svobodném přístupu k informacím. V roce 2010 Úřad těchto žádostí obdržel deset, v roce 2008 šest. Dá se tedy říci, že počet žádostí o informace vztahující se v dané souvislosti k působnosti Úřadu má setrvale stoupající tendenci.

V roce 2010 byla ve dvou případech žádost o informace odmítnuta, ve dvou případech Úřad vydal rozhodnutí o částečném odmítnutí žádosti. V žádném z těchto případů nebylo rozhodnutí Úřadu ze strany žadatelů napadeno opravným prostředkem – rozkladem k předsedovi Úřadu. Postup Úřadu při vyřizování žádosti o informace nebyl napaden ani jednou stížností podle § 16a zákona o svobodném přístupu k informacím.

Žadatelé nejčastěji požadovali zaslání konkrétních správních aktů či jiných úředních písemností Úřadu, dále informace o řízení, které bylo zahájeno na základě jejich podnětu, a rovněž další dokumenty Úřadu, např. jeho vnitřní předpisy, kontrolní plán na rok 2010 atd. Úřad byl rovněž požádán o zpřístupnění informace o tom, kolik zakázek malého rozsahu a v jaké výši zadal v období let 2007, 2008 a 2009, stejně jako o informace, komu, za jaké služby a jakou částku v roce 2009 a 2010 vyplatil v rámci poskytování poradenských, právních a konzultačních služeb.

V souladu s § 5 odst. 3 zákona o svobodném přístupu k informacím byly všechny poskytnuté informace zveřejněny rovněž na internetových stránkách Úřadu.



VÝROČNÍ ZPRÁVA 2010

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2010

Úřad pro ochranu osobních údajů

Pplk. Sochora 27, 170 00 Praha 7

E-mail: posta@uouu.cz

Internetová adresa: www.uouu.cz

Na základě povinnosti, kterou mu ukládá zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, § 29, písm. d), a § 36, zveřejnil Úřad pro ochranu osobních údajů tuto výroční zprávu v únoru 2011 na svých webových stránkách.

Editor: PhDr. Hana Štěpánková, telefon 234 665 286

Redakční zpracování: PhDr. David Pavlát

Grafické řešení: Eva Lufferová

Jazyková korektura: Tiskové odd. ÚOOÚ a Mgr. Eva Strnadová

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

Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011

ISBN 978-80-210-5428-8