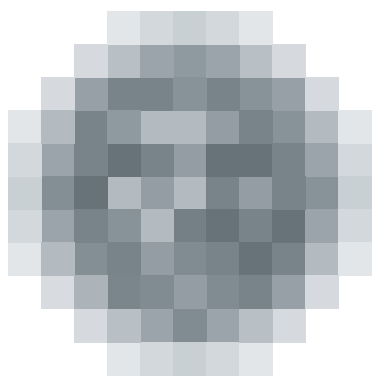




# Výroční zpráva 2011



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



# Ohlédnutí předsedy Úřadu za rokem 2011



V roce 2011 pokračovalo pro Úřad pro ochranu osobních údajů přelomové období: K novým inspektorům, Peadr. Janě Rybínové a Ing. Josefu Vaculovi, kteří se na deset let ujali svých funkcí v srpnu roku 2010, se od 1. června 2011 přidali tři další noví inspektoři: MVDr. František Bartoš, PhDr. Petr Krejčí a Mgr. Daniel Rován, a pro druhé funkční období byla zvolena inspektorkou Mgr. et Mgr. Božena Čajková. Je zřejmé, že obsazení inspektorských funkcí zcela novými osobnostmi znamená pro Úřad větší přelom než nové desetiletí činnosti, do něhož vstoupil.

Přestože noví inspektoři přejali některé složité úkoly, kterými se zabývali jejich předchůdci – například bylo třeba sledovat a dokončit proces realizace vytváření pražské opencard vydávané, aniž by docházelo ke zpracovávání osobních údajů (v tomto zájmu Úřad oslovoval i nezanedbatelný počet Pražanů) – ve velmi krátké době se ujali také dalších závažných úkolů: To, že se podařilo nalézt metodologii přístupu pro ochranu osobních údajů osob, jejichž údaje jsou zpracovávány bez jejich souhlasu, považují za skutečný úspěch, byť odstranění takových údajů lze žádat pouze od poskytovatelů služeb webhostingu v dosahu evropského práva.

Dne 1. ledna 2011 nabyl účinnosti zákon č. 468/2011 Sb., který, mimo jiné, mění též zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů. Jedná se o změny, které se týkají oblasti zasílání obchodních sdělení, a tudíž i kompetencí svěřených Úřadu, který se na tuto povinnost v závěru roku adekvátně připravil.

Výrazně se v loňském roce odráží intenzivní zájem Úřadu šířit znalosti o ochraně osobních údajů. Svědčí o tom řada seminářů a konferencí, jichž se účastnili odborníci z Úřadu na domácí i zahraniční půdě, o čemž vypovídají příslušné kapitoly této výroční zprávy. Opomenout nemohu ani spolupráci českého Úřadu s našimi partnery z Polska a Maďarska. Společným úsilím se nám podařilo vytvořit speciální publikaci, která pomáhá podnikatelům orientovat se v problematice právní ochrany osobních údajů v uvedených státech i celkově v Evropské unii. Oprávněně proto byla přijata se zájmem jak v Evropské komisi, tak v Radě Evropy.

Jistě není zanedbatelné, že v prosinci loňského roku Úřad vydal už 60. částku svého Věstníku, který přináší zásadní právní dokumenty týkající se ochrany osobních údajů celoevropského dosahu a právní stanoviska Úřadu k problémům, s jejichž řešením se meritorně vyrovnává v rámci českého právního řádu.

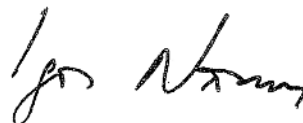
Dvěma čísly svého Informačního bulletinu Úřad předložil široké veřejnosti různé úhly pohledu svědčící o dvou problémech, které by z pohledu Úřadu zasluhovaly speciální legislativní úpravu: jde o využívání genetických údajů a zpracování DNA dat a o obdobně závažné využívání kamer a kamerových systémů, které postrádá ucelené legislativní zakotvení. Samozřejmě s potěšením musím konstatovat, že zejména o využívání kamerových systémů jevíla velký zájem veřejnost i média.

V kontextu složité ekonomické situace se zatím Úřad dokázal vyrovnávat rovněž s finančními a personálními požadavky, které na něj kladou nové kompetence. Dosud zcela dokázal splnit veškerá zadání, jež na něj klade elektronizace veřejné správy, a pokročit také termínově odpovídajícím způsobem v budování systému ORG, svěřeného do jeho správy v rámci e-Governmentu.

Přál bych si, aby se stejné pozornosti a péče dostávalo ochraně osobních údajů také v legislativním procesu. Činíme v tomto ohledu veškeré kroky, které jsou nám právním řádem umožněny, a věřím, že se ochraně soukromí zejména v nadcházející éře a boomu „cloudu“ dostane náležitá pozornost a péče.

Na sklonku roku začal Úřad vytvářet podmínky pro to, aby byl schopen dostát své povinnosti při řešení případů porušení ochrany osobních údajů (tzv. data breaches), které poskytovatelům služeb v elektronických komunikacích výslovně stanoví jako nový nástroj ochrany osobních údajů a soukromí evropské právní předpisy, implementované ve změně tří zákonů – o elektronických komunikacích, o ochraně osobních údajů a o službách informační společnosti, účinných od 1. ledna 2012.

Přestože je obtížné odhadovat rozsah povinností, které právě tento úkol přinese, hledím do příštího roku s optimismem. Především proto, že po sedmi letech působení ve funkci předsedy Úřadu a interakce s jeho zaměstnanci i zkušenosti ze spolupráce s podstatně inovovaným kolegiem inspektorů vím, že zatím všechny složité i časově náročné úkoly se nám podařilo se ctí vyřešit. Jsem si jist, že mě to opravňuje přinejmenším k nebojácnému pohledu do roku 2012.



Igor Němec

# Obsah

ÚŘAD V ČÍSLECH 2011	7
KONTROLNÍ ČINNOST ÚŘADU	10
■ KONTROLNÍ PLÁN PRO ROK 2011	10
I. Obecná témata pro zaměření kontrolní činnosti inspektorů Úřadu	10
1. Informační systémy veřejné správy	10
2. Informační systémy v oblasti soukromoprávní	12
3. Zpracovávání a zpřístupňování osobních údajů v oblasti prevence kriminality a boje proti terorismu	13
II. Kontroly zahájené v roce 2011 na základě podnětu předsedy	13
■ POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI	16
Kontrola doručování soudních písemností prostřednictvím datových schránek	16
Osobní údaje v rezortu zdravotnictví	18
Osobní údaje v rezortu pojišťovnictví (zdravotní pojištění)	18
Zjišťování příjmů a majetkových poměrů u žadatelů o jednorázové příspěvky na opatření zvláštních pomůcek pro zdravotně postižené občany	21
Kontrola obchodního rejstříku	22
Využívání rodného čísla ve veřejné správě	23
Osobní údaje zaměstnanců	24
Osobní údaje v kontextu všeobecných obchodních podmínek	24
Vymahačské společnosti, zejména působící přes internet	27
Zpracování osobních údajů prostřednictvím kamerových systémů	28
Zpřístupňování videozáznamu z jednání zastupitelstva	32
Nedostatečné zabezpečení osobních údajů (§ 13 zákona o ochraně osobních údajů)	36
Tzv. „Náhubkový zákon“	39
■ VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ	43

■ POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ	46
Zpracování osobních údajů při plnění zákona o svobodném přístupu k informacím	46
Povinnost zpracovávat přesné osobní údaje	48
■ POZNATKY ZE SOUDNÍCH PŘEZKUMŮ	50
Úřadu pravomoc vést návrhové řízení o uložení povinnosti k odstranění závadného stavu a přiznání náhrady za způsobenou újmu nepřísluší	50
Zákon o ochraně osobních údajů se na advokáty vztahuje	53
■ REGISTRACE	55
■ PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ	57
 LEGISLATIVNÍ ČINNOST	 59
 STYKY SE ZAHRANIČÍM A MEZINÁRODNÍ SPOLUPRÁCE	 63
 ÚŘAD, SDĚLOVACÍ PROSTŘEDKY A KOMUNIKAČNÍ NÁSTROJE	 67
Kontakty s médii	67
Šíření znalostí o ochraně osobních údajů	68
Knihovna a publikace Úřadu	69
Webové stránky Úřadu	69
 INFORMAČNÍ SYSTÉM ORG	 70
 PROJEKT „OPTIMALIZACE PROCESŮ ÚOOÚ“	 73
 PERSONÁLNÍ OBSAZENÍ ÚŘADU	 74
 HOSPODAŘENÍ ÚŘADU	 76
 POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA Č. 106/1999 SB., O SVOBODNÉM PŘÍSTUPU K INFORMACÍM, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ	 81

# Úřad v číslech 2011

<b>Dotazy a konzultace</b>	dotazy ČR	2294
	zahraničí	110
	konzultace	
	státní správě	104
	samosprávě	160
	právníkům osobám	301
	fyzickým osobám	
	podnikajícím fyzickým osobám	216 1544
<b>Podání a stížnosti</b>	přijaté podněty dle zákona o ochraně osobních údajů	1119
	stížnosti předané ke kontrole	197
<b>Nevyžádaná obchodní sdělení</b> (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	4613
	vyřešených podnětů	2283
	zahájených kontrol	157
	ukončených kontrol	137
	správních rozhodnutí o pokutě	63
<b>Kontroly</b> (vyjma kontrol týkajících se zákona č. 480/2004 Sb.)	zahájeno	179
	ukončeno	144
	předáno jiným státním úřadům	1
	napadeno námitkami	25
	námitkám vyhověno	9
	nevyhověno	9
	převážně vyhověno	1
	převážně nevyhověno	4

<b>Správní trestání</b>	správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb.	110
	přestupková řízení podle zákona č. 101/2000 Sb.	16
	správní a přestupkové řízení podle zákona č. 101/2000 Sb. – § 44 a, 45 a	5
	přestupková řízení o porušení zákona č. 159/2006 Sb., o střetu zájmů	1
	rozklady napadená rozhodnutí o porušení zákona (Pozn.: ** z toho k § 17)	49 (2**)
	zamítnutých rozkladů	25
	zrušeno a vráceno k novému projednání	8
	zrušených rozhodnutí a zastaveno řízení	10
	změna rozhodnutí	5
	<b>Soudní přezkum</b> (Pozn.: * celkem od r. 2001)	podaných žalob k soudu
	zamítnutých žalob soudem	4
	zrušených rozhodnutí soudem	5
	postoupení k vydání rozhodnutí (dle § 21 zák. č. 101/2000 Sb.)	0
	ukončených/neukončených soudních řízení	1/9 (50/41*)
<b>Registrace</b>	přijátá oznámení (podle § 16 zákona č. 101/2000 Sb.)	4421
	zaregistrovaná zpracování	3856
	dosud v řízení	953
	zrušené registrace	49
	oznámení o změně zpracování	866
	řízení podle § 17	82
	zastaveno (nedochází k porušení zákona)	68
	zastaveno z procesních důvodů (např. oznámení vzato zpět)	8
nepovoleno	6	
<b>Povolení k předávání osobních údajů do zahraničí</b>	přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	9
	rozhodnutí o povolení předávání	3
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	6
<b>Stížnosti podle § 175 správního řádu</b>	přijatých stížností	28
	vyřízených jako důvodné	5



	vyřízených jako částečně důvodné	9
	vyřízených jako bezdůvodné	17
<b>Žádosti podle zákona č. 106/1999 Sb.</b>	přijatých žádostí	23
	vyřízených žádostí	21
	odmítnutých žádostí	2
<b>Publikované materiály</b>	Věstník Úřadu (počet částek)	3
	Bulletin Úřadu (počet čísel)	2
<b>Tiskové konference</b>	pravidelné	3
	mimořádné	0
<b>Připomínkované legislativní návrhy</b>	zákony	75
	prováděcí předpisy	91
	návrhy nařízení vlády	21
	návrhy vyhlášek	70
	ostatní	51
	zahraniční materiály	29

# Kontrolní činnost Úřadu

## ■ KONTROLNÍ PLÁN PRO ROK 2011

V oblasti ochrany osobních údajů se v roce 2011 Úřad pro ochranu osobních údajů (dále jen „Úřad“) v rámci svých kontrolních aktivit zabýval takovými tématy, která přinášela celospolečenskou odezvu a přispěla mimo jiné k prohloubení povědomí veřejnosti o potřebě chránit své osobní informace před jejich nezákonným zpracováním.

Úřad, vědom si současně potřeb hledání možností mezinárodní spolupráce v oblasti kontroly, přijal jako jeden z kontrolních záměrů možnost koordinace a provedení kontroly vůči subjektům, které vyvíjejí své aktivity související se zpracováním osobních údajů nejen na území České republiky, ale i na území některého jiného členského státu EU.

Vzhledem ke skutečnosti, že někteří inspektoři skončili své funkční období k 31. 5. 2011 a nově jmenovaní inspektoři se svého mandátu ujali od 1. 6. 2011, bylo třeba v průběhu první poloviny roku 2011 kontrolní plán přepracovat a jeho upravené záměry byly projednány a schváleny předsedou Úřadu společně s inspektory na druhé pololetí roku 2011.

### I. OBECNÁ TÉMATA PRO ZAMĚŘENÍ KONTROLNÍ ČINNOSTI INSPEKTORŮ ÚŘADU

#### 1. INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

**1.1** V roce 2011 bylo provedeno celosvětové sčítání obyvatelstva a s tím souvisejících informací. Úřad se zapojil do přípravy podmínek pro takto rozsáhlé zpracování dat a provedení sčítání sledoval včetně navazujícího zpracování statistických informací v souladu se zákonem č. 296/2009 Sb. a prováděcími předpisy k němu.

K naplnění tohoto záměru zahájila inspektorka kontrolu Českého statistického úřadu, která se zaměřila zejména na vyřizování stížností účastníků sčítání spojených nejen s prováděním sčítání, ale hlavně s uchováváním anonymizovaných formulářů v Národním archivu a výsledků sčítání lidu ve Statistickém úřadu. Kontrola byla zahájena ke dni 2. června 2011 a není dosud ukončena.

**1.2** V návaznosti na dynamicky se rozvíjející prostředí elektronických komunikací v oblasti ISVS (Informační Systémy Veřejné Správy) se Úřad zaměřil na úroveň zabezpečení elektronických úkonů orgánů veřejné moci prostřednictvím datových schránek provozovaných v rámci informačního systému datových schránek v souladu se zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi, ve znění pozdějších předpisů.

K naplnění tohoto záměru zahájil inspektor kontrolu Ministerstva vnitra jako správce a České pošty jako provozovatele tohoto systému. Následně se ukázalo jako potřebné rozšířit kontrolu i na další subjekt, a to Ministerstvo spravedlnosti.

Výsledky kontroly jsou publikovány v kapitole Kontrola doručování soudních písemností prostřednictvím datových schránek.

**1.3** V souladu se závazky České republiky v oblasti III. pilíře EU včetně Schengenské úmluvy a s ohledem na blížící se hodnocení jejich dodržování se očekává provedení pravidelné kontroly některého z povinných subjektů.

K naplnění tohoto záměru bylo provedeno několik dozorových aktivit zaměřených na provádění vízové a další konzulární činnosti několika zastupitelských úřadů (dále jen „ZU“). Všechny tyto inspekce, které se soustředily na kontrolu zabezpečení osobních údajů žadatelů o víza a na jejich práva na informace, vyústí ve společné závěry, které budou projednány s Ministerstvem zahraničních věcí.

Kontrola ZU v Mexiku byla provedena 3. listopadu 2011, kontrola ZU v Makedonii byla provedena o týden později; kontrola ZU v Moldávii byla provedena ve dnech 6. až 8. prosince 2011.

Dalším kontrolním záměrem v této oblasti byla kontrola Informačního systému EURODAC. Vzhledem k tomu, že se kontrolní aktivity v oblasti schengenského prostoru ukázaly jako aktuálnější záměry (v únoru 2012 proběhne evaluační mise v České republice a Úřad bude společně s dalšími partnery prezentovat své výsledky), byla tato kontrola přesunuta do dalšího roku. Kontrola se týká několika subjektů, a to Ministerstva vnitra, Ministerstva spravedlnosti a Ministerstva zahraničních věcí.

Naopak byla zahájena kontrola Schengenského informačního systému (SIS), včetně kontroly logování přístupů do něho. Důraz je při této kontrole kladen na prověřování čl. 96 Schengenské prováděcí úmluvy o vkládání osobních údajů cizinců do SIS v případě závažného narušení veřejného pořádku a bezpečnosti státu.

**1.4** S ohledem na rostoucí požadavky a nároky provozovatelů integrovaných zabezpečovacích a dopravních systémů, které využívají technologické možnosti pro naplnění svých povinností, je zájmem Úřadu prověřovat dodržování povinností těchto subjektů ve vztahu k ochraně osobních údajů.

K naplnění tohoto záměru provedla inspektorka kontrolu systému multifunkčních karet v dopravě a městě provozovaného Statutárním městem Plzeň. Kontrola byla provedena v únoru až březnu roku 2011 a nezjistila žádná pochybení.

**1.5** Dalším kontrolním záměrem vycházejícím z kontrolního plánu byla kontrola dodržování povinností správce při zpracování osobních údajů klientů a jejich rodinných příslušníků u vytipovaného subjektu v souvislosti s poskytováním služeb v oblasti sociální péče. K naplnění tohoto úkolu zahájil inspektor kontrolu vytipovaného subjektu v listopadu 2011.

## 2. INFORMAČNÍ SYSTÉMY V OBLASTI SOUKROMOPRÁVNÍ

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

### 2.1 PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI S VYDÁVÁNÍM VĚRNOSTNÍCH ZÁKAZNICKÝCH KARET VE VŠECH TYPECH SLUŽEB SE ZAMĚŘENÍM NA DODRŽOVÁNÍ POVINNOSTÍ ODPOVĚDNÝCH OSOB PŘI SBĚRU TĚCHTO INFORMACÍ PŘÍMO OD JEDNOTLIVÝCH SUBJEKTŮ

K naplnění tohoto záměru provedla inspektorka v období od února do srpna roku 2011 kontrolu subjektu dm drogerie markt, s. r. o., zaměřenou na zpracování osobních údajů v souvislosti s vydáváním a používáním zákaznických karet. I když kontrola nezjistila závažnější pochybení při zpracovávání osobních údajů zákazníků tohoto subjektu, dosáhla inspektorka cestou doporučení změny dosavadní praxe při sběru a uchovávání kopií dokumentů deklarujících nároky zákazníků na poskytované výhody a slevy zboží. Této oblasti se věnoval i inspektor, který v období února až května provedl kontrolu společnosti BAUMAX ČR, s. r. o., zaměřenou na zpracování osobních údajů zákazníků prostřednictvím zákaznické karty. Touto kontrolou nebylo shledáno porušení zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“).

Zpracováním osobních údajů v souvislosti s používáním zákaznických karet se zabývala i kontrola, která byla u společnosti Česká lékárna, a. s. zahájena v únoru roku 2011. Tato kontrola dosud probíhá a její ukončení se očekává v lednu 2012.

### 2.2 PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ CESTUJÍCÍCH OSOB PŘI PROVOZU KAMEROVÝCH SYSTÉMŮ V PROSTŘEDCÍCH HROMADNÉ PŘEPRAVY

K naplnění tohoto záměru provedla v září a říjnu roku 2011 inspektorka kontrolu Dopravního podniku Ostrava. Kontrola byla ukončena bez zjištění porušení povinností kontrolovaného subjektu, neboť v době provedení kontroly žádné zpracovávání sledovaných informací neprobíhalo.

### 2.3 PODMÍNKY ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PACIENTŮ PŘI PROVOZU INFORMAČNÍCH SYSTÉMŮ SUBJEKTŮ POSKYTUJÍCÍCH SLUŽBY ZDRAVOTNÍ PÉČE V OBLASTI ZDRAVOTNICTVÍ

Pro naplnění tohoto záměru kontrolního plánu zahájila v říjnu roku 2011 inspektorka kontrolu Nemocnice Na Homolce, příspěvkové organizace. Kontrola byla ukončena v lednu 2012 a konstatovala, že kontrolovaný subjekt neporušil povinnosti správce osobních údajů, zpracovávaných prostřednictvím evidenčních náramků.

### 2.4 PODMÍNKY PRO ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZÁKAZNÍKŮ V OBLASTI NABÍDKY ZBOŽÍ A SLUŽEB, A TO NEJEN V RÁMCI ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ, ALE SOUČASNĚ I DALŠÍ OBLASTI PŮSOBNOSTI ÚŘADU TÝKAJÍCÍ SE NĚKTERÝCH SLUŽEB INFORMAČNÍ SPOLEČNOSTI VE SMYSLU ZÁKONA Č. 480/2004 SB., O NĚKTERÝCH SLUŽBÁCH INFORMAČNÍ SPOLEČNOSTI, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ

K naplnění záměru prověřit zpracování osobních údajů zákazníků a dalších osob v souvislosti se službami marketingu zahájil inspektor kontrolu společnosti Alza cz. Tato kontrola byla prováděna v součinnosti se slovenským úřadem pro ochranu osobních údajů, což se ukázalo jako náročný úkol vzhledem k rozsáhlé síti služeb tohoto kontrolovaného subjektu. Kontrola dosud ukončena nebyla, očekává se ukončení v lednu 2012.

## 2.5 PODMÍNKY PRO ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ V SOUVISLOSTI S VÝKONEM ČINNOSTI SOUKROMÉ BEZPEČNOSTNÍ AGENTURY NEBO SOUKROMÉ DETEKTIVNÍ AGENTURY

Pro naplnění záměru prověřit dodržování povinností správce a zpracovatele v souvislosti s monitorováním návštěvníků sportovních utkání a při zajišťování výkonu činnosti soukromé bezpečnostní agentury zahájil inspektor kontrolu Fotbalového klubu Teplice. Kontrola byla ukončena bez zjištění porušení povinností správce při zpracovávání osobních údajů. Kontrolující konstatoval, že odpovědný subjekt zpracovává osobní údaje návštěvníků stadionu prostřednictvím kamerového systému provozovaného městskou policií. Jestli jde o možné zpracování osobních údajů návštěvníků v souvislosti s nákupem vstupenek na stadion, takové zpracování nebylo zjištěno.

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

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

### 3.1 KONTROLU DODRŽOVÁNÍ PRAVIDEL PRO ZPŘÍSTUPŇOVÁNÍ PROVOZNÍCH ÚDAJŮ TELEFONIE A E-KOMUNIKACÍ V SOULADU S TRANSPOZICÍ SMĚRNICE Č. 2006/24/ES

Tento záměr byl v souvislosti s přípravou nové právní úpravy těchto podmínek odložen na rok 2012.

### 3.2 KONTROLU DODRŽOVÁNÍ PODMÍNEK PRO ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ ZA SITUACE, KDY MEZI SPRÁVCEM A ZPRACOVATELEM JE UZAVŘENA SMLOUVA O ZPRACOVÁNÍ INFORMACÍ PODLE § 6 ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ

Pro naplnění tohoto záměru zahájili inspektoři kontrolu integrovaného městského kamerového systému v Praze (kontrolovaný subjekt Magistrát hl. m. Prahy). Tento záměr současně sleduje naplnění záměru dle bodu 2.2. Tato kontrola dosud probíhá a bude ukončena v březnu 2012.

## II. KONTROLY ZAHÁJENÉ V ROCE 2011 NA ZÁKLADĚ PODNĚTU PŘEDSEDY

Předseda Úřadu i v roce 2011 využíval institutu pokynu konkrétnímu inspektorovi Úřadu k provedení kontroly, a to především v případech aktuálních a společensky významných kauz, které bylo třeba řešit bez větší prodlevy.

V roce 2011 se konkrétně jednalo o následující pokyny předsedy:

1. Pokyn ke kontrole Ministerstva spravedlnosti, na jehož základě zahájil inspektor dne 25. ledna 2011 kontrolu. Dle informací zveřejněných sdělovacími prostředky a Ministerstvem spravedlnosti bylo patrné, že toto ministerstvo v rámci zveřejnění dokumentů „Seznam soudců – bývalých členů KSČ“ na webových stránkách [www.justice.cz](http://www.justice.cz) zveřejnilo nepravdivé osobní údaje o členství některých soudců a státních zástupců v Komunistické straně Československa. Tímto jednáním mohlo dojít k porušení především § 5 odst. 1 písm. c), § 5 odst. 2 a příj. i další ustanovení zákona o ochraně osobních údajů. Kontrola byla uzavřena uložením pokuty ve výši 100 tis. Kč a kontrolovaný ji uhradil.

2. Pokyn ke kontrole subjektu Telefónica O<sub>2</sub> Czech Republic, a. s., kterou v květnu roku 2011 provedla inspektorka. Pokyn byl učiněn v návaznosti na veřejně publikované informace týkající se informací o sledování manažera elektrárenské společnosti ČEZ, z nichž vyplývalo, že vzniklo podezření týkající se porušení zákona o ochraně osobních údajů. Nebylo zjištěno porušení povinností uložených společnosti Telefónica O<sub>2</sub> Czech Republic, a. s.
3. Pokyn ke kontrole Velvyslanectví České republiky v Mexiku, kterou v říjnu 2011 provedla inspektorka. Požadavek provést tuto kontrolu z důvodu schengenského hodnocení je obsažen v obecné části kontrolního plánu Úřadu pro rok 2011, splnění tohoto úkolu bylo důležitým krokem k úspěšnému absolvování schengenského hodnocení a splnění závazků, které v souvislosti s tímto hodnocením Úřadu vznikají a budou předloženy v průběhu evropské kontrolní mise Schengenského systému v únoru 2012.
4. Pokyn ke kontrole Středočeského kraje. V návaznosti na informace dostupné z veřejných zdrojů dospěl Úřad k závěru, že je nezbytné zahájit kontrolu zpracování osobních údajů osob, které žádají Středočeský kraj o poskytnutí účelového daru na úhradu regulačních poplatků ve zdravotnických zařízeních. Zveřejňování osobních údajů prostřednictvím webových stránek Středočeského kraje zakládalo podezření, že by tímto jednáním mohlo docházet k porušení povinností stanovených zákonem o ochraně osobních údajů, zejména pak § 5 odst. 1 písm. f) tohoto zákona, uvedeným subjektem. Kontrola dosud nebyla ukončena.
5. Pokyn ke kontrole Městského dopravního podniku Opava, a. s. Pokyn byl učiněn v souvislosti s předchozími podněty Oborového svazu pracovníků dopravy, silničního hospodářství a autoopravárenství Čech a Moravy, které směřovaly proti uvádění jmen a příjmení řidičů autobusů městské dopravy na jízdenkách a v návaznosti na podnět zástupkyně veřejného ochránce práv, která se dopisem ze dne 19. září 2011 obrátila na Úřad v téže věci. Předmětem kontroly bylo dodržování povinností správce osobních údajů vyplývajících ze zákona o ochraně osobních údajů, zejména § 5 odst. 1 a 2 a § 10 tohoto zákona. Společnost Městský dopravní podnik Opava, a. s., tím, že zpracovává osobní údaje svých zaměstnanců – řidičů vozidel MHD – v rozsahu jméno, příjmení a osobní číslo formou tisku na jízdním dokladu o zaplacení jízdného bez souhlasu subjektu údajů, porušila povinnost správce osobních údajů uloženou § 5 odst. 1 písm. d) a § 5 odst. 2 zákona o ochraně osobních údajů. Současně bylo kontrolované společnosti uloženo opatření k nápravě nezpracovávat osobní údaje zaměstnanců – řidičů vozidel MHD – prostřednictvím tisku jejich jména, příjmení a osobního čísla na jízdním dokladu (jízdence) vydávaném ve vozidle MHD.
6. Pokyn ke kontrole oprávnění Městského soudu v Praze pro zpracovávání osobních údajů, které stěžovatel hodnotil jako možné porušení povinností správce podle zákona o ochraně osobních údajů. Kontrola probíhá, předpokládáné zpracování kontrolního protokolu je do poloviny února 2012.
7. Pokyn ke kontrole způsobu předávání údajů osob zpracovávaných společnostmi Vodafone Czech Republic a. s. do registru dlužníků vedeného společností SOLUS. Pokyn byl adresován inspektorce s tím, že kontrola se měla zaměřit jak na společnost Vodafone, tak na společnost SOLUS. Kontrola po analýze souvisejících skutečností nebyla zahájena a pokyn byl předán odboru správních činností k zahájení správního řízení ve věci samé. Detailní informace je zveřejněna v této VZ v kapitole Poznatky ze správních řízení.

8. Pokyn ke kontrole Městského úřadu Kuřim. Podnět se týkal zjišťování příjmů a majetkových poměrů u žadatelů o jednorázové příspěvky na opatření zvláštních pomůcek podle ustanovení § 33 vyhlášky č. 182/1991 Sb. Podnět byl adresován inspektorce pro prověření dodržování povinností všech odpovědných subjektů podle zákona o ochraně osobních údajů v souvislosti s uplatňováním podmínek pro přiznání dávek sociální péče. Kontrola byla ukončena 4. 8. 2011, konstatováno porušení zákona o ochraně osobních údajů a postoupeno odboru správních činností ke správnímu řízení.
9. Pokyn ke kontrole Okresního soudu v Teplicích, týkající se provozu datových schránek, respektive odpovědnosti za nesprávné doručení soudní písemnosti do datové schránky subjektu, který nebyl účastníkem řízení. Úřad byl veřejným ochráncem práv požádán o uplatnění svých dozorových pravomocí. Podnět byl činěn pro prověření dodržování povinností odpovědných subjektů podle zákona o ochraně osobních údajů v souvislosti se zasíláním zpráv prostřednictvím informačního systému datových schránek, resp. zejména v souvislosti s jednoznačnou identifikací příjemců těchto zpráv. O výsledku kontroly pojednává kapitola Kontrola doručování soudních písemností prostřednictvím datových schránek.

# POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

## KONTROLA DORUČOVÁNÍ SOUDNÍCH PÍSEMNOSTÍ PROSTŘEDNICTVÍM DATOVÝCH SCHRÁNEK

V roce 2010 a 2011 se začaly množit stížnosti na doručování soudních písemností určených advokátům do schránek podnikajících fyzických osob. Vzhledem k tomu, že v jednom případě byly písemnosti určené advokátovi zaslány jeho jmenovci opakovaně, a to přesto, že chybné doručení dotyčná osoba soudu oznámila, obrátila se dotyčná osoba na veřejného ochránce práv, který v únoru a opakovaně v květnu 2011 požádal předsedu Úřadu o prošetření případu. Z příloženého stanoviska Ministerstva spravedlnosti vyplynulo, že na základě šetření (které na základě žádosti ministerstva provedla firma CCS Group, a. s., dodavatel informačního systému soudů) došlo k chybnému doručení u řady soudů. Kromě toho eviduje Ministerstvo spravedlnosti i individuální stížnosti tří advokátů na chybné doručování do datové schránky v roce 2010.

Na základě těchto informací byla 5. srpna 2011 zahájena v souladu s plánem kontrolní činnosti Úřadu pro rok 2011 kontrola Ministerstva vnitra. Předmětem kontroly bylo v návaznosti na dynamicky se rozvíjející prostředí elektronických komunikací v oblasti informačních systémů veřejné správy zjistit úroveň zabezpečení elektronických úkonů orgánů veřejné moci prostřednictvím datových schránek provozovaných v rámci informačního systému ISDS v souladu se zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů. Kontrola se zaměřila zejména na systémové podmínky vytvořené pro plnění povinností správců při zpracování osobních údajů v rámci ISDS, se zvláštním ohledem na plnění povinností osob při zabezpečení osobních údajů stanovených § 13 zákona o ochraně osobních údajů.

Občanský soudní řád (dále „o. s. ř.“) uvádí následující způsoby doručování a určuje adresy pro doručování u jednotlivých způsobů:

### **Doručování soudem při jednání či při jiném soudním úkonu**

Na prvním místě § 45 o. s. ř. uvádí doručování soudem při jednání nebo jiném soudním úkonu. V důvodové zprávě se k tomu uvádí, že soud může pro účely doručování využít i jiného řízení, kterého se osoba, jíž je třeba doručit, účastní, a doručit jí při této příležitosti. Soud se tedy nemusí omezovat pouze na doručení při řízení, kterého se doručovaná písemnost týká.

### **Doručování prostřednictvím veřejné datové sítě (§ 45 odst. 2, § 46 o. s. ř.)**

Nedošlo-li k doručení při jednání nebo jiném soudním úkonu, doručuje soud prostřednictvím veřejné datové sítě do datové schránky (§ 46 odst. 1 o. s. ř.). Adresou pro doručování v tomto případě je adresa datové schránky vedená v evidenci podle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, který upravuje i postup takového doručování.

Pokud není doručení provedeno dle odstavce 1), pokoušejí se soudy doručit písemnost advokátům prostřednictvím veřejné datové sítě.

Advokáti však nemají, na základě přechodných ustanovení § 31 zákona 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, povinnost zřídit si datové schránky. Dle ustanovení odst. 3) uvedeného paragrafu Ministerstvo vnitra zřídí advokátu a daňovému poradci datovou schránku podnikající fyzické osoby prvním dnem prvního



kalendářního měsíce třetího roku po dni nabytí účinnosti zákona (tj. 1. července 2012). Tím není dotčeno právo advokáta a daňového poradce na zřízení datové schránky podnikající fyzické osoby na vlastní žádost. Advokáti nemají svůj vlastní příznak, jsou zařazeni mezi podnikající fyzické osoby – **PFO**.

Mezi povinné identifikační údaje takové žádosti patří: jméno, popřípadě jména, a příjmení, popřípadě obchodní firma, rodné příjmení, den, měsíc a rok narození, místo a okres narození; pokud se podnikající fyzická osoba narodila v cizině, místo narození a stát, na jehož území se narodila, státní občanství, není-li podnikající fyzická osoba státním občanem České republiky, identifikační číslo osoby, bylo-li přiděleno, a místo podnikání, popřípadě sídlo podnikání. **Povinným údajem však není předmět podnikání.**

Vyhledávání advokáta ve skupině PFO pro odeslání zprávy do datové schránky je z devadesáti procent neúspěšné. Advokáti většinou nepatří mezi příznivce datových schránek. Pokud pracovník soudu, který odeslání zprávy provádí, nalezne jmenovce advokáta, ovšem nezkontroluje další identifikační údaje, zejména adresu, a zprávu odešle, dostává se zpráva do nepovolovaných rukou. Jedná se o selhání lidského faktoru.

Systémovým řešením popisovaného problému by bylo vytvoření samostatného příznaku pro advokáty, tj. vytvoření oddělené databáze.

Vzhledem k tomu, že hlavním cílem kontroly je zjednáání nápravy a vytvoření systémových podmínek k eliminaci lidských chyb, proběhla již ve dnech 23. září 2011, 12. října 2011 a 15. prosince 2011 tři místní šetření s odpovědnými pracovníky Ministerstva vnitra, které datové schránky zřizuje a spravuje. Při posledním šetření byli k součinnosti přizváni i pracovníci Ministerstva spravedlnosti, zejména proto, že všechny stížnosti se týkají soudů.

Dle sdělení zástupců obou ministerstev se k datu, kdy budou advokátům zřízeny datové schránky ze zákona, tj. 1. července 2012, počítá s vytvořením separátního příznaku pro advokáty.

To je sdělení potěšující. Vzniká ovšem nepříjemný pocit, že vážne komunikace mezi Ministerstvem vnitra a advokáty zastoupenými Českou advokátní komorou. Ještě v říjnovém Bulletinu advokacie je uvedeno: „Advokáti budou dle způsobu výkonu advokacie patřit do kategorie podnikající fyzické osoby či právnické osoby.“ To je právě, jak vyplývá z předchozího popisu, ten největší problém, který zapříčiňuje častou chybu doručování při záměně jmen.

Příznak by však měl být používán ještě před datem 1. 7. 2012 v případě, že si advokát zřizuje schránku na vlastní žádost. Žádost může být následně ověřena Českou advokátní komorou, která potvrdí, že existuje advokát toho jména.

V praxi však nelze prokazovat svou advokátní kompetentnost vlastnictvím datové schránky, ale vždy jen a pouze příslušnými doklady. Soud si ověří identitu právního zástupce klasickým způsobem a teprve při zasílání příslušných dokumentů bude zjišťovat ID datové schránky.

Pokud tedy budou datové schránky opatřeny typem „31“ – advokát bez ověření advokátní komorou, nemůže to způsobit zneužití. Ostatně bude to stejná situace, jako když dnes advokát nahlásí soudu ID své schránky sám.

Vzhledem k tomu, že je v současném systému velmi obtížné dohledat vlastnictví datové schránky advokátem, na základě kontroly byla doporučena urychlená implementace typu „PFO\_ADVOK“ do systému datových schránek a převedení stávajících schránek na tento typ.

## OSOBNÍ ÚDAJE V REZORTU ZDRAVOTNICTVÍ

V roce 2011 byly v oblasti ochrany osobních údajů ve zdravotnictví provedeny incidenční kontroly, v nichž se jednalo o údajnou ztrátu zdravotnické dokumentace, podobně jako v roce 2010 o změnu registrace pacientů k jiné zdravotní pojišťovně, a to bez jejich vědomí, či podezření z neoprávněného vniknutí do e-mailové schránky lékaře.

Incidenční kontrola se zaměřením na zpracování osobních údajů v souvislosti s vedením zdravotnické dokumentace pacientů byla vedena na základě stížnosti pacienta, který uvedl, že požádal svou praktickou lékařku o pořízení kopie své zdravotnické dokumentace; lékařka však uvedla, že předmětnou zdravotnickou dokumentaci nemá k dispozici. Při kontrole pak lékařka sdělila, že při předávání zdravotnické dokumentace postupuje zdravotní sestra tak, že si nechá na výměnný list předání podepsat, tento list však lékařka v době kontroly nepředložila. Zároveň sdělila, že není možné, vzhledem k zavedeným bezpečnostním opatřením, aby zdravotnickou dokumentaci stěžovatele ztratila. Následně skutečně zdravotnickou dokumentaci stěžovatele našla v souvislosti s výměnou staré kartotéky za novou. Zdravotnická dokumentace se nacházela pod ostatní zdravotnickou dokumentací pacientů. V daném případě tedy nedošlo k porušení § 13 odst. 1 zákona o ochraně osobních údajů, nedošlo k trvalé ztrátě zdravotnické dokumentace ani ke zneužití osobních a citlivých údajů stěžovatele, které se nacházejí v jeho zdravotnické dokumentaci.

Kontrolní orgán je v daném případě toho názoru, že evidence zapůjčených karet a předávání kopií obsahu zdravotnických karet byla prováděna nedostatečně. Na základě této skutečnosti kontrolní orgán lékařce doporučil, aby byla evidence o pořízených kopiích ze zdravotnické dokumentace, případně při zapůjčení či předání celé zdravotnické dokumentace, vedena jak v kartě pacienta, tak duplicitně mimo zdravotnickou dokumentaci. Tímto postupem se předejde případným a zbytečným konfliktům. Kontrolní orgán dále lékařce doporučil věnovat maximální pozornost při ukládání zdravotnické dokumentace pacientů v ordinaci. K nevědomému založení zdravotnické dokumentace pacienta či k její ztrátě by v žádném případě nemělo docházet.

## OSOBNÍ ÚDAJE V REZORTU POJIŠŤOVNICTVÍ (ZDRAVOTNÍ POJIŠTĚNÍ)

Změna registrace pacientů k jiné zdravotní pojišťovně, a to bez jejich vědomí, byla předmětem několika kontrol, podobně jako v roce 2010. V rámci kontroly jedné ze zdravotních pojišťoven bylo zjištěno, že zdravotní pojišťovna pro získávání nových pojištěnců uzavírala mandátní či zprostředkovatelské smlouvy s externími subjekty. Ze smluv vyplývalo, že zprostředkovatelé budou přihlášky předávat fyzicky přímo zástupcům zdravotní pojišťovny, zprostředkovatelé však měli také přístup do pomocného softwaru, do kterého zadávali pod svým přihlašovacím jménem a přístupovým heslem údaje o pojištěncích, které byly uvedeny v přihláškách. Zdravotní pojišťovna v době kontroly vedla aktuální evidenci o podvodných jednáních v souvislosti s falešnými přihláškami zdravotního pojištění a měla zaregistrováno celkem 100 případů podvodných jednání, které vyšetřovala Policie ČR. Zdravotní pojišťovna sama však podávala trestní oznámení pouze v jednom případě, o ostatních případech podvodného jednání se zdravotní pojišťovna dozvěděla od orgánů činných v trestním řízení. Dle vyjádření Policie ČR spočívala podvodná činnost jednoho z konkrétních zprostředkovatelů v tom,

že si patrně vymyslel nebo si z volně dostupných zdrojů opsal jméno a příjmení osoby, dále patrně vymyslel nebo z volně přístupných zdrojů opsal adresu, která neměla žádný vztah ke jménu a příjmení osoby, z obchodního rejstříku opsal náhodně rodná čísla existujících osob a náhodně, na základě zkušeností, si vymyslel číslo občanského průkazu. Následně takto upravené přihlášky byly odevzdány pojišťovně, s níž měl uzavřenou zprostředkovatelskou smlouvu.

Další případ podvodů s přihláškami zdravotního pojištění evidovala Policie ČR v souvislosti s dalším zprostředkovatelem. Ten pravděpodobně získal osobní údaje domnělých „pojištěnců“ ze smluv, které tito uzavírali např. s telekomunikačními společnostmi, u kterých byl tento zprostředkovatel také přítomen, nebo ze smluv, s nimiž přišel do styku ve svém zaměstnání. Takto zfalšoval přihlášky zdravotního pojištění celkem ve 47 případech.

Stěžovatelka v případě této zdravotní pojišťovny žádala o prošetření ve věci neoprávněné evidence její přihlášky. Kontrolou bylo zjištěno, že v jejím případě došlo ke zneužití osobních údajů ze strany dalšího zprostředkovatele. Zprostředkovatel využil informace o stěžovatelce v rozsahu jméno, příjmení a rodné číslo, padělal její podpis, uvedl nesprávné bydliště a takto upravenou přihlášku zdravotního pojištění předal k evidenci zdravotní pojišťovně. Zdravotní pojišťovna přihlášku převzala a dále osobní údaje zpracovávala v dobré víře, že tak činí se souhlasem osoby uvedené v přihlášce, neboť ho dokládal podpis na přihlášce zdravotního pojištění. Jelikož zdravotní pojišťovna v daném případě zprostředkovateli zcela důvěřovala a spoléhala na to, že zprostředkovatel bude postupovat v souladu s uzavřenou mandátní smlouvou a platnými právními předpisy, přihlášku převzala, aniž dále zkoumala její pravost. V tomto případě sama stěžovatelka podala ke zdravotní pojišťovně žádost o zrušení přihlášky, v níž uvedla, že nikdy žádnou přihlášku o převodu zdravotního pojištění k této zdravotní pojišťovně nepodepsala a ani adresa jejího bydliště uvedená na přihlášce neodpovídá skutečnosti. Zdravotní pojišťovna zpětně zjistila, který ze zprostředkovatelů neoprávněně za stěžovatelku vyplnil a předložil žádost o zrušení přihlášky. Zdravotní pojišťovna tedy stížnost vyhodnotila jako oprávněnou a vyjednala zpětnou přeregistraci stěžovatelky u původní zdravotní pojišťovny. Kontrola byla ukončena se závěrem, že sama zdravotní pojišťovna zákon o ochraně osobních údajů neporušila. V kontrolním protokolu však kontrolující konstatovala, že problematiku trestné činnosti související se zajišťováním nových pojištěnců by měla zdravotní pojišťovna řešit zejména preventivními opatřeními, a to zvolením účinných kontrolních mechanismů. Pojišťovna by měla před vložením nového pojištěnce do databáze prověřit, zda osobní údaje pojištěnce, včetně jeho podpisu na přihlášce, odpovídají skutečnosti. Účinné kontrolní mechanismy je zapotřebí vytvořit zejména s ohledem na objem trestné činnosti páchané vyhotovením falešných přihlášek pojištěnců. Tomu, že kontrolní mechanismy zdravotní pojišťovny a zprostředkovatelů selhaly, odpovídá i počet evidovaných trestných činů, které byly spáchány v souvislosti s neoprávněně vyplněnými přihláškami zdravotního pojištění. Kontrolující si jsou vědomi, že pojišťovna nemůže trestnou činnost podvodů v souvislosti s falešnými přihláškami zdravotního pojištění odhalit v celém rozsahu, musí však vyvinout maximální možné úsilí, aby tomuto druhu trestné činnosti preventivně a účinně zabránila.

Další kontrola byla zahájena na základě stížnosti, kterou Úřad obdržel prostřednictvím Kanceláře veřejného ochránce práv. V tomto případě stěžovatelka rovněž podala trestní oznámení na Policii ČR. V dané stížnosti stěžovatelka uvedla, že se dostavila ke své ošetřující lékařce, od které se dozvěděla, že je „formálně“ pojištěncem jiné zdravotní pojišťovny. Svě lékařce sdělila, že neprovedla změnu zdravotní pojišťovny. Stěžovatelka požádala v pobočce „své nové“ zdravotní pojišťovny o vysvětlení. Pracovnice pojišťovny jí ukázala „její“ registrační formulář, na základě něhož se stala pojištěncem. Její rodné příjmení ale bylo uvedeno špatně,

rovněž podpis na registračním formuláři nebyl její. Stěžovatelka prohlásila, že shora uvedený dokument nesepsala a není tak vyjádřením její svobodné vůle změnit zdravotní pojišťovnu. Stěžovatelka sama podala trestní oznámení na neznámého pachatele Policii ČR. Na základě této stížnosti byla provedena kontrola zdravotní pojišťovny, ke které byla bez svého vědomí stěžovatelka přeregistrována. I tato zdravotní pojišťovna využívá registrace klientů prostřednictvím akviziční činnosti externí společnosti na základě smluvního ujednání. Zdravotní pojišťovna však sdělila, že samotný proces registrace pojištěnce na základě předloženého registračního formuláře zahajuje výhradně sama s tím, že registrace probíhá za podmínek uvedených v zákoně č. 48/1997 Sb., o veřejném zdravotním pojištění v platném znění. V případě nesrovnalostí údajů na předloženém registračním formuláři je klient vždy kontaktován pracovníky zdravotní pojišťovny zpravidla telefonicky (pokud uvádí tel. číslo), případně písemně, a je vyzván k návštěvě zdravotní pojišťovny k dořešení záležitosti. K případu stěžovatelky však zdravotní pojišťovna nesdělila, zda takový postup zvolila. Registrace však nebyla provedena, o čemž byla stěžovatelka zdravotní pojišťovnou informována dopisem. S pracovníci, která fyzicky provedla její přeregistraci, zdravotní pojišťovna ukončila spolupráci.

K uvedené problematice je nutno uvést, že právo pacienta na změnu zdravotní pojišťovny upravoval v době uvedených kontrol zákon č. 48/1997 Sb., o veřejném zdravotním pojištění, ve znění pozdějších předpisů. Dle ustanovení § 11 odst. 1 písm. a) má pojištěnec právo na výběr zdravotní pojišťovny. Zdravotní pojišťovnu lze změnit jednou za 12 měsíců, a to vždy jen k 1. dni kalendářního čtvrtletí.

Dne 1. prosince 2011 vstoupila v platnost novela zákona č. 48/1997 Sb., o veřejném zdravotním pojištění a s ní bylo novelizováno ustanovení § 11 odst. 1 písm. a): Pojištěnec má právo na výběr zdravotní pojišťovny, nestanoví-li tento zákon jinak. Zdravotní pojišťovnu lze však změnit jednou za 12 měsíců, a to vždy jen k 1. lednu následujícího kalendářního roku; přihlášku je pojištěnec nebo jeho zákonný zástupce povinen podat vybrané zdravotní pojišťovně nejpozději 6 měsíců před požadovaným dnem změny.

V dalším případě Policie ČR postoupila Úřadu podnět, který se týkal podezření na možný únik informací v souvislosti s neoprávněným vniknutím do e-mailové schránky evidované na portálu Centrum.cz. Podezření na možný únik informací oznámil Policii ČR lékař, provozovatel soukromé praxe, který uvedl, že e-mailovou schránku používá také ke komunikaci se svými pacientkami, které se s ním touto cestou radí o svém zdravotním stavu. Přístupové heslo do jeho e-mailové schránky bylo dle jeho sdělení jednoduché a neobsahovalo žádné zástupné znaky ani číslice. Dle vyjádření Policie ČR je možné, že by odborník mohl zaheslování do předmětné e-mailové schránky překonat. V závěru sdělení Policie ČR uvedla, že lékař mohl nedostatečným zabezpečením přístupu ke svojí e-mailové schránce zpřístupnit citlivé údaje týkající se zdravotního stavu svých pacientek, čímž by mohl porušit zákon o ochraně osobních údajů.

Na základě uvedeného podnětu bylo v předmětné věci provedeno šetření inspektorkou Úřadu. Policie ČR byla požádána o postoupení spisového materiálu ve věci šetření podnětu lékaře. Ze spisového materiálu vyplynulo, že skutečnosti, které zjistila Policie ČR, nevedou k žádným konkrétním závěrům, podle nichž by bylo možné jednoznačně určit, kdo a jakým způsobem mohl údaje, resp. dílčí korespondenci z e-mailové schránky lékaře získat, přestože lékař sdělil Policii ČR, kdo dle jeho názoru mohl zabezpečení e-mailové schránky překonat. Šetřením Úřadu nebylo prokázáno, že by došlo k závažnému zneužití osobních údajů, které měly být uloženy v e-mailové schránce lékaře. V dopise následně Policie ČR Úřadu sdělila, že stále šetří, zda vůbec ke vniknutí do e-mailové schránky lékaře došlo. Inspektorka na základě šetření učinila závěr, že v souvislosti s podezřením lékaře na zneužití osobních údajů, které

byly uloženy v jeho e-mailové schránce, nedošlo k porušení zákona o ochraně osobních údajů, proto inspektorka navrhla podnět odložit.

## ZJIŠŤOVÁNÍ PŘÍJMŮ A MAJETKOVÝCH POMĚRŮ U ŽADATELŮ O JEDNORÁZOVÉ PŘÍSPĚVKY NA OPATŘENÍ ZVLÁŠTNÍCH POMŮCEK PRO ZDRAVOTNĚ POSTIŽENÉ OBČANY

Veřejný ochránce práv se obrátil na předsedu Úřadu se žádostí o součinnost při šetření podnětu stěžovatele, který se týkal zjišťování příjmů a majetkových poměrů u žadatelů o jednorázové příspěvky na opatření zvláštních pomůcek pro zdravotně postižené občany podle ustanovení vyhlášky č. 182/1991 Sb., kterou se provádí zákon o sociálním zabezpečení a zákon České národní rady o působnosti orgánů České republiky v sociálním zabezpečení. Uvedl, že provedl šetření postupu městského úřadu za účelem prověření praxe při zjišťování sociálních a majetkových poměrů žadatelů o jednorázové příspěvky na opatření zvláštních pomůcek. Šetřením zjistil, že jmenovaný úřad zjišťuje uvedené skutečnosti, přestože se nejedná o skutečnosti rozhodné pro nárok na dávku a stanovení její výše. Nejedná se o ojedinělý exces, ale plošně nastavenou správní praxi, která vychází z metodického vedení krajských úřadů a Ministerstva práce a sociálních věcí (dále jen „MPSV“). MPSV zastává názor, že zjišťování sociálních a majetkových poměrů žadatele o dávku lze opřít o ustanovení § 73 odst. 1 zákona o sociálním zabezpečení. Uvedená správní praxe by mohla naplňovat skutkovou podstatu správního deliktu podle zákona o ochraně osobních údajů. Výše příjmu žadatele a majetkové poměry totiž nejsou obsaženy v kritériích pro přiznání nároku a stanovení příspěvku na kompenzační pomůcky podle uvedené vyhlášky. Veřejný ochránce práv požádal o poskytnutí stanoviska k nastíněnému problému, jakož i o provedení kontroly dodržování povinností podle zákona o ochraně osobních údajů městským úřadem.

Předseda Úřadu podal podnět k provedení kontroly, zejména ohledně prověření, zda existuje právní podklad pro zjišťování údajů o majetkových poměrech žadatelů o předmětnou dávku, a v případě, že ano, zda praxe města, zejména co do rozsahu shromážděných dat, odpovídá zásadám minimalizace.

Inspektorkou byla u městského úřadu zahájena kontrola zpracování osobních údajů žadatelů při posuzování a přiznávání jednorázového příspěvku na opatření zvláštních pomůcek podle vyhlášky MPSV. Odbor sociálních věcí městského úřadu se vyjádřil ke shromažďování osobních údajů žadatelů v tom smyslu, že při zjišťování celkových sociálních a majetkových poměrů u fakultativní dávky pro zdravotně postižené občany – příspěvek na opatření zvláštní pomůcky – postupoval podle zákona o sociálním zabezpečení, dále podle vyhlášky, kterou se provádí zákon o sociálním zabezpečení, a také v souladu s metodikou Krajského úřadu a MPSV.

Kontrolou správních spisů bylo zjištěno, že obsahují žádost o poskytnutí jednorázového příspěvku na opatření zvláštní pomůcky a doklady k sociálním a majetkovým poměrům, tj. prohlášení o příjmech žadatele, prohlášení o majetku, kopie výměry důchodů, potvrzení o příjmu. V případě existence společně posuzované osoby jsou součástí spisu stejné doklady o majetkových poměrech u těchto osob jako u žadatele s uvedením jména a příjmení, data narození a adresy bydliště. Formulář *Žádosti o poskytnutí jednorázového příspěvku na opatření zvláštní pomůcky pro zdravotně postiženého občana* obsahoval kromě údajů o žadateli i údaje o manželovi (manželce, druhovi, družce, včetně rodného čísla a jména, příjmení, zaměstnání

a jména, příjmení a data narození nezaopatřených dětí, žijících s žadatelem ve společné domácnosti). Součástí žádosti byl i text souhlasu žadatele s tím, aby městský úřad na základě zákona o ochraně osobních údajů shromažďoval, zpracovával a uchovával jeho osobní údaje, popř. jeho nezletilých dětí, za účelem poskytování dávek nebo služeb sociální péče, a to v nezbytném rozsahu a po nezbytnou dobu.

Spisy dále obsahovaly *Prohlášení žadatele o příspěvek na opatření zvláštních pomůcek pro zdravotně postiženého občana a Vyjádření účastníka řízení, že souhlasí se zjišťováním, shromažďováním a uchováváním osobních údajů pro řízení ve věci dávky sociální péče.*

Kontrolou bylo zjištěno, že městský úřad při posuzování a přiznávání jednorázového příspěvku na opatření zvláštních pomůcek podle vyhlášky zjišťuje příjmové a majetkové poměry žadatele a společně posuzované osoby jako podklad pro správní rozhodnutí (u společně posuzovaných osob jsou shromažďovány její další osobní údaje v rozsahu jméno, příjmení, datum narození, rodné číslo, zaměstnání).

Městský úřad jako správce je povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Nezbytný rozsah je pak stanoven citovanou právní úpravou, která pro řízení o poskytnutí jednorázového příspěvku na opatření zvláštních pomůcek neupravuje povinnost zjišťovat, shromažďovat a uchovávat osobní údaje o příjmech a majetkových poměrech žadatele o příspěvek, případně i dalších osob (manžel/ka, druh/družka). Nad rámec nezbytného rozsahu bylo i shromažďování dalších osobních údajů jiných osob, jejichž osobní údaje byly městským úřadem shromažďovány pro řízení o přiznání příspěvku (rodné číslo, zaměstnání). Pokud výše uvedené osobní údaje nejsou pro řízení nezbytné, pak je nelze zpracovávat ani se souhlasem žadatele podle zákona o ochraně osobních údajů, neboť souhlasem nelze zhojit výkon státní správy, který se řídí zvláštními právními předpisy.

I když celá sociální péče představuje doplňkový nástroj, kterým stát pomáhá občanům, jejichž životní potřeby nejsou dostatečně zabezpečeny příjmy z pracovní činnosti, dávkami důchodového pojištění nebo nemocenského pojištění, případně jinými příjmy, a občanům, kteří takovou pomoc potřebují vzhledem ke svému zdravotnímu stavu či věku, popřípadě se nacházejí v obtížné životní situaci či nepříznivých životních poměrech a nemohou je překonat bez pomoci společnosti, **nelze dle stávající právní úpravy shromažďovat osobní údaje žadatelů o dávku sociální péče ve větším rozsahu, než připouštějí uvedené zvláštní právní předpisy.**

Praxe městského úřadu při zpracování osobních údajů žadatelů o dávku a současně zpracování osobních údajů společně posuzovaných osob byla v rozporu se zákonem o ochraně osobních údajů.

## KONTROLA OBCHODNÍHO REJSTŘÍKU

(elektronické podoby obchodního rejstříku dostupné přes webový portál [www.justice.cz](http://www.justice.cz).)

Webový portál obchodního rejstříku je významným veřejným informačním systémem, jehož závažnost je potvrzena důležitostí pro e-Government. Prostřednictvím tohoto portálu dochází ke zpracovávání osobních údajů na internetu, kde je vyšší riziko zneužití osobních údajů. Kontrolující při této kontrole vycházeli kromě zákona o ochraně osobních údajů zejména z čl. 2 odst. 3 Ústavy ČR, podle kterého *státní moc slouží všem občanům a lze ji uplatňovat jen v případech, mezích a způsoby, které stanoví zákon.*

Kontrola předně upozornila na to, že každé zpracování osobních údajů musí mít svého správce, který je za toto zpracování zodpovědný, a této odpovědnosti se nelze zříci. Správcem je v tomto případě Ministerstvo spravedlnosti. Ministerstvo tudíž zodpovídá za to, že rozsah zveřejňovaných údajů a doba, po kterou jsou zveřejňovány, odpovídá účelu zpracování. Webový portál [www.justice.cz](http://www.justice.cz) má sloužit jako informace o obchodních společnostech a řídí se Směrnicí Evropského parlamentu a Rady 2009/101/ES ze dne 16. září 2009, o koordinaci ochranných opatření, která jsou na ochranu zájmů společníků a třetích osob vyžadována v členských státech od společností ve smyslu čl. 48 druhého pododstavce Smlouvy, za účelem dosažení rovnocennosti těchto opatření. U všech ostatních dokumentů, které obsahují osobní údaje, je třeba zvažovat, zda jsou nezbytné vůči výše danému účelu z hlediska zákona o ochraně osobních údajů. Podobně doba jejich uchování na webovém portálu musí být nezbytná vůči účelu, tj. informovanosti třetích osob.

Dále kontrola poukázala na problematiku zveřejňování rodného čísla na webovém portálu. K radosti kontrolujících je v této souvislosti třeba uvést, že se podařilo do připravované novely zákona č. 513/1991 Sb., obchodní zákoník, doplnit ustanovení k § 28 odst. 1, a to tak, že se doplňuje věta „*Rodné číslo se zapisuje do obchodního rejstříku, neuvádí se však ve výpisu z obchodního rejstříku ani se nezveřejňuje v Obchodním věstníku*“.

Dále kontrola připomenula problematiku „personálního indexu“. Neboť účelem obchodního rejstříku je poskytnutí informací o obchodních společnostech k ochraně zájmů společníků a třetích osob v souvislosti s obchodováním, resp. podnikáním. Vyhledávání podle jména a příjmení fyzické osoby, a to nejen v obchodním rejstříku, ale zároveň i např. v nadačním rejstříku a rejstříku bytových družstev, je zpracování osobních údajů k jinému účelu. Personální index v současné době již není na webovém portálu obchodního rejstříku dostupný.

Zkvalitnění právní úpravy ve výše uvedených ustanoveních bylo kontrolou shledáno jako zásadní vzhledem k ustanovení § 5 odst. 3 zákona o ochraně osobních údajů, které ukládá, že „*provádí-li správce zpracování osobních údajů na základě zvláštního zákona, je povinen dbát práva na ochranu soukromého a osobního života subjektu údajů*“.

Zpracování osobních údajů z obchodního rejstříku formou webového portálu si tudíž zaslouží jasná pravidla včetně odpovědnosti Ministerstva spravedlnosti, která jsou v souladu s principy ochrany osobních údajů. Současný stav právní úpravy, kdy dochází ke zpracování osobních údajů pouze na základě obecných ustanovení § 27 a 28 obchodního zákoníku a ustanovení § 5 odst. 5 zákona o svobodném přístupu k informacím, nezohledňuje principy ochrany osobních údajů.

## VYUŽÍVÁNÍ RODNÉHO ČÍSLA VE VEŘEJNÉ SPRÁVĚ

Samospráva a státní správa je podle ustanovení § 13c zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů, oprávněna používat rodná čísla v případech, kdy je k tomu zákonem o obcích a jinými zvláštními zákony výslovně oprávněna. Rodná čísla smí ovšem používat pouze k danému, zákonem určenému účelu a k žádnému jinému. V ostatních případech, např. při udělování darů a stipendií, při konání společenských akcí, zveřejňování kandidátů apod., není ani veřejná správa, stejně jako jakákoli jiná organizace, oprávněna rodná čísla pro vyhledávání v databázi používat.

## OSOBNÍ ÚDAJE ZAMĚSTNANCŮ

V rámci kontrolní praxe Úřadu se opětovně setkáváme s tím, že zaměstnavatelé požadují po uchazečích o zaměstnání osobní údaje, pro jejichž shromáždění a další zpracování nelze, nebo lze jen velmi obtížně, najít odpovídající právní podklad. Stává se to v rámci jednání o uzavření pracovního poměru, tedy ještě předtím, než je o uzavření pracovního poměru rozhodnuto. Vyžadování takových osobních údajů pak zaměstnavatelé ospravedlňují charakterem budoucí vykonávané práce.

Pro příklad může posloužit případ poměrně velké potravinářské společnosti. Ta při výběrovém řízení na pozici řezník nebo prodavačka požaduje poskytnutí takových osobních údajů, jako jsou např. informace o pracovní neschopnosti v posledním roce, rodinný stav nebo počet dětí, zda je adept kuřák či nikoli, a to aniž by uchazeči o zaměstnání byla poskytnuta informace o zpracování osobních údajů v souvislosti s výběrem a přijímáním nových zaměstnanců podle ustanovení § 11 odst. 1 a odst. 2 zákona o ochraně osobních údajů. Hlavně pak je ale takovéto **vyžadování osobních údajů v tvrdém konfliktu se zákoníkem práce**.

Lze totiž poukázat na § 4 odst. 2 zákona č. 435/2004 Sb., o zaměstnanosti, podle kterého „při uplatňování práva na zaměstnání je zakázána přímá i nepřímá diskriminace z důvodu pohlaví, sexuální orientace, rasového nebo etnického původu, národnosti, státního občanství, sociálního původu, rodu, jazyka, zdravotního stavu, věku, náboženství či víry, majetku, manželského a rodinného stavu nebo povinností k rodině, politického nebo jiného smýšlení, členství a činnosti v politických stranách nebo politických hnutích, v odborových organizacích nebo organizacích zaměstnavatelů...“ atd. Podle § 12 odst. 1 zákona č. 435/2004 Sb., o zaměstnanosti: „Účastníkům právních vztahů vznikajících podle tohoto zákona je zakázáno činit nabídky zaměstnání, které mají diskriminační charakter, dále vyžadovat informace, které odporují dobrým mravům, a také osobní údaje, které neslouží k plnění povinností zaměstnavatele stanovených zvláštním právním předpisem. Na žádost uchazeče o zaměstnání je zaměstnavatel povinen prokázat potřebnost požadovaného osobního údaje. Hlediska pro výběr zaměstnanců musí zaručovat rovné příležitosti všem fyzickým osobám ucházejícím se o zaměstnání. Ustanovení § 4 odst. 3 zákona o zaměstnanosti platí i zde.“ Konečně je pak třeba poukázat na § 30 odst. 2 zákoníku práce, podle kterého **zaměstnavatel smí vyžadovat v souvislosti s jednáním před vznikem pracovního poměru od fyzické osoby, která se u něj uchází o práci, nebo od jiných osob jen údaje, které bezprostředně souvisejí s uzavřením pracovní smlouvy**.

Při provedené kontrole tak informace o poslední pracovní neschopnosti uchazeče (zájemce o zaměstnání) ani výše uvedené další požadované údaje nebyly vyhodnoceny jako nezbytné pro naplnění stanoveného účelu. Bylo tedy zjištěno porušení povinnosti ukládané § 5 odst. 2 zákona o ochraně osobních údajů.

Navíc s přihlédnutím k dikci § 5 odst. 4 tohoto zákona bylo jasné, že kontrolovaná společnost souhlas se zpracováním předmětných údajů neprokázala.

## OSOBNÍ ÚDAJE V KONTEXTU VŠEOBECNÝCH OBCHODNÍCH PODMÍNEK

V souvislosti s řadou smluvních vztahů, zejména tzv. spotřebitelskými smlouvami mezi *dodavatelem a spotřebitelem*, dochází ke zpracování osobních údajů spotřebitele.



Dodavatel (podnikatel) poskytuje určité služby nebo zboží, k čemuž využívá osobních údajů spotřebitele, a ocitá se tedy v postavení správce osobních údajů; spotřebitel, pokud je fyzickou osobou, je v postavení subjektu údajů.

Problému vznikajícímu z hlediska zákona o ochraně osobních údajů na základě výše uvedeného vztahu se Úřad delší dobu a opakovaně věnuje, a tak v srpnu 2011 vydal Stanovisko č. 2/2011, které vyjadřuje jeho právní názor na zpracovávání osobních údajů podmíněné souhlasem zakotveným ve smlouvě nebo ve Všeobecných obchodních podmínkách (dále „VOP“).

V praxi se lze velmi často setkat s tím, že součástí smluvních ujednání jsou tzv. VOP, kterými si dodavatel upravuje formulářovým způsobem podmínky jím uzavíraných smluvních vztahů.

V případě smluvního vztahu mezi podnikatelem (správcem osobních údajů) a klientem (subjektem údajů) nepochybně dochází a musí docházet ke zpracování osobních údajů, a to k řadě účelů. Tím nejběžnějším a základním účelem zpracování je uzavření a plnění smlouvy a s tím související identifikace smluvních stran. Je logické, že podnikatel potřebuje v řadě případů identifikovat svého klienta tak, aby mohli uzavřít platnou smlouvu, a potřebuje znát jeho identifikační údaje, aby mohl řádně plnit, tj. doručit zboží, poskytnout službu apod. Ke zpracování osobních údajů za účelem uzavření smlouvy není tudíž potřeba souhlasu subjektu údajů, a také zákon o ochraně osobních údajů proto tyto případy předpokládá a nevyžaduje tak nadbytečné poskytování souhlasu pro účel vlastního uzavření smlouvy.

Lze přitom uvést, že se Úřad trvale setkává s případy, kdy VOP obsahují ustanovení o souhlasu se zpracováním osobních údajů za účelem uzavření a plnění smlouvy, a dokonce existencí tohoto souhlasu podmiňují trvání smluvního vztahu. Taková ustanovení jsou pro klienta zavádějící. Jeho případné odvolání souhlasu nemění nic na skutečnosti, že podnikatel pro plnění uzavřené smlouvy může dále zpracovávat osobní údaje klienta bez jeho souhlasu.

Obvykle se setkáváme s tím, že klient v rámci VOP stvrzuje, že poskytl své osobní údaje dobrovolně a že byl o tomto řádně poučen. Dále tímto podpisem uděluje souhlas se zpracováním svých osobních údajů a někdy tento souhlas platí pro předávání osobních údajů v rámci koncernu nebo svému obchodnímu zástupci, či dokonce do zahraničí.

Ve VOP se lze dále setkat s dalšími účely zpracování osobních údajů, ke kterým je již souhlas subjektu údajů nezbytný. Těmito účely jsou zejména přímý marketing, předání údajů do dlužnických registrů, nahrávání telefonních hovorů na zákaznické lince apod. V takových případech VOP obsahují formulaci o tom, že klient souhlasí se zpracováním osobních údajů za shora uvedeným účelem.

K problematice souhlasu se Úřad vyjádřil již ve stanovisku č. 2/2008 (Souhlas se zpracováním osobních údajů). Použití obecných závěrů tohoto stanoviska na problematiku VOP vede především k otázce posouzení dobrovolnosti úkonu klienta ve chvíli, kdy je mu předkládána formulářová smlouva, resp. VOP, obsahující text souhlasu se zpracováním osobních údajů.

Souhlas klienta je ze zákona svobodný a vědomý projev vůle. Svobodný znamená, že rozhodnutí subjektu údajů nemá vliv na ostatní smluvní podmínky. Vědomý znamená, že si je vědom, k čemu vlastně dal souhlas a jaké to může mít důsledky.

První podmínka jednoznačně znamená možnost výběru, tj. že neposkytnutí tohoto souhlasu nesmí být podmínkou, která by znemožňovala uzavření smluvního vztahu. Uvědomělost souhlasu je právě v rámci VOP velkým otazníkem. Klient obvykle chce smlouvu uzavřít (potřebuje půjčit peníze, chce nový telefon apod.) a v této situaci má tendenci podepsat stručnou a přehlednou smlouvu, ale už nevěnuje dostatek času studování VOP, a to zejména vzhledem k jejich rozsahu a formátu.

Z pohledu zákona poskytovatel služby sice formálně splnil zákonné povinnosti, ale ve skutečnosti lze o charakteru plnohodnotného vědomého souhlasu pochybovat.

Ze zkušeností Úřadu vyplývá, že stěžovatel se vlastně až po kontrolním přezkoumání podnětu dovídá, co vlastně podepsal a jaké to má pro něho důsledky.

Proti tomuto nešvaru může Úřad působit jednak tlakem na poskytovatele služeb, aby souhlas zakomponovali do řádné smlouvy, nebo alespoň v rámci VOP zvýraznili příslušnou pasáž, případně osvětou subjektů údajů vedoucí k jejich vyšší gramotnosti v této oblasti.

Projev vůle, znamenající to, že klient nemá v úmyslu poskytnout souhlas se zpracováním osobních údajů, může být zaznamenán několika způsoby. V případě, kdy je uzavírána smlouva písemně, může klient buď konkrétní ustanovení o souhlasu ve VOP přeškrtnout, nebo k tomuto ustanovení (nebo na jiné vhodné místo ve smlouvě) dopsat poznámku, ze které by byla jeho vůle zřejmá (např. „nesouhlasím se zpracováním osobních údajů za účelem marketingu“). Je přitom povinností správce tento projev vůle respektovat a, jak bylo shora uvedeno, nepodmiňovat uzavření smluvního vztahu (tj. vynucovat si) udělením souhlasu. V případě, kdy klient uzavře smlouvu s takto upravenými VOP, znamená to, že souhlas se zpracováním osobních údajů správci neudělil.

Velmi důležité pro klienta je vědět, že v případě, kdy je souhlas z jeho strany při uzavření smlouvy udělen, nic mu nebrání ani po uzavření smlouvy, pokud dospěje k závěru, že si již nepřeje, aby byly jeho osobní údaje zpracovávány, svůj souhlas odvolat. Již proto je vynucování si souhlasu na straně správců při uzavírání smluv zbytečné.

Reálně jsou ale standardizované postupy velkých firem vůči drobným klientům nátlakové a často využívají toho, že si klienti vlastně neuvědomují možné následky vzešlé z daného paušálního souhlasu.

Dalším projevem nátlaku na klienta v rámci VOP je již zmíněný souhlas s poskytováním jeho osobních údajů dalším subjektům v rámci jakési „sounáležitosti“ uvedených firem, které ovšem klienta vůbec nemusejí zajímat. Skutečným účelem tohoto souhlasu jsou samozřejmě marketingové akce a obchodní sdělení.

Dále v rámci VOP dávají subjekty údajů souhlasy s tím, že jejich osobní údaje včetně rodného čísla sdružení SOLUS zpřístupní svým členům, a opět klient podepisuje, že tento souhlas dává dobrovolně.

Zcela běžně je v části VOP věnované souhlasu i odstavec o monitorování jeho komunikace, přičemž monitorováním se rozumí zejména záznam hovorové či datové korespondence.

Existují i VOP, ve kterých klient dává souhlas s tím, že jeho smluvní partner bude zpracovávat jeho osobní údaje i po vypořádání práv a povinností ze smlouvy pro účely nabízení obchodu a služeb, tedy po i ukončení smluvního vztahu.

Pro klienty je velmi důležité vědět, že mohou souhlas odmítnout. V praktické rovině je proto čistě na vůli klienta, zda s částí VOP, která obsahuje souhlas se zpracováním osobních údajů, vysloví svůj souhlas tím, že smlouvu v předložené podobě uzavře, nebo nikoli. Již z principu jsou VOP pro subjekty údajů nevhodné. Z přímého dialogu smluvních partnerů posouvají vzájemný kontakt do informační povinnosti. Pro klienta to znamená, že poskytovatel služby jej informuje prostřednictvím svých webových stránek, čehož si běžný zákazník nemusí vůbec všimnout. Tato forma ulehčuje velkým firmám s mnoha drobnými klienty komunikovat „hromadně“, nikoliv individuálně, a snímá to z nich značnou část odpovědnosti.

V případě používání VOP pro oblast zpracování osobních údajů je třeba rozlišovat situace, kdy je souhlas se zpracováním osobních údajů nezbytný (marketing, dlužnické registry atd.) a kdy souhlas není potřeba (uzavření a plnění smlouvy, vymáhání pohledávek ze smlouvy). Těmto

případům je třeba uzpůsobit formulaci souhlasu a případné plnění informační povinnosti. V případě poskytování souhlasu je třeba umožnit subjektu údajů projevit svoji vůli a tento projev respektovat tak, aby se jednalo o svobodně a dobrovolně udělený souhlas se zpracováním osobních údajů. Jako nejvhodnější způsob lze doporučit samostatně formulované části VOP doplněné o „zaškrtačací“ pole, jehož vyplněním by subjekt údajů souhlas udělil. Pokud je souhlas přímo v textu VOP, musí správce respektovat vyškrtnutí takové části VOP ze strany subjektu údajů. Pro předávání osobních údajů třetím subjektům musí být nejprve subjekt údajů informován o účelu zpracování třetím subjektem a o identifikaci tohoto subjektu.

Závěrem je nutné konstatovat, že princip uzavírání smluv včetně VOP je pro drobné klienty nevhodný. Subjekt údajů v dané chvíli nemá možnost veškeré smluvní podmínky řádně prostudovat nebo dokonce konzultovat s odborníkem. Je vystaven nepřímému časovému nátlaku, což v kombinaci s množstvím předloženého textu neumožňuje seznámit se uvědoměle s celým obsahem smlouvy. Tento postup některých velkých firem sice není v rozporu se zákonem, není ale vůči drobnému klientu zcela korektní.

V zájmu objektivity je ale třeba uznat, že tato praxe není vlastní všem poskytovatelům služeb. Lze nalézt i firmy, které zcela jednoznačně a srozumitelně informují v rámci VOP své zákazníky o zpracování jejich osobních údajů z důvodů zákonné povinnosti a pouze k tomuto účelu.

## VYMAHAČSKÉ SPOLEČNOSTI, ZEJMÉNA PŮSOBÍCÍ PŘES INTERNET

V současné době se objevily – většinou pouze na internetu (tzn. virtuálně existující) – společnosti, které nabízejí vymožení dluhu. Na základě dotazníku, který vyplní věřitel a uvede v něm svého dlužníka, je uzavírána mandátní smlouva či předána plná moc k vymožení dluhu, na podkladě které, s příslušnou přidanou odměnou pro sebe, se společností pokusí dluh vymoci – často pouze pošlou dopis.

Z hlediska ochrany osobních údajů je ale třeba se ptát, na základě jakého právního titulu zpracovávají osobní údaje dlužníků.

Relevantní ustanovení zákona č. 40/1964 Sb., občanský zákoník, ve znění pozdějších předpisů, umožňuje postoupení pohledávky někomu jinému bez vědomí dlužníka. Podmínkou ovšem je, že postupitel musí dlužníkovi postoupení pohledávky oznámit nebo postupník postoupení pohledávky dlužníkovi prokázat, neboť dle § 526 odst. 1 platí, že *postoupení pohledávky je povinen postupitel bez zbytečného odkladu oznámit dlužníkovi. Dokud postoupení pohledávky není oznámeno dlužníkovi nebo dokud postupník (nový věřitel) postoupení pohledávky dlužníkovi neprokáže, zproští se dlužník závazku plněním postupiteli.*

Další možností je uzavřít mandátní smlouvu mezi věřitelem a Společností o vymožení dluhu. Při uzavření této smlouvy ovšem, jako při každé jiné smlouvě, musí být obě strany jednoznačně identifikovány a smlouva musí být buď oběma stranami osobně, nebo elektronicky podepsána. Za platnou smlouvu nelze považovat zakliknutí v počítačovém programu, kdy není věřitel žádným způsobem identifikován, a tudíž společnost nemá žádnou možnost si ověřit, že se jedná o skutečnou osobu věřitele a o skutečný dluh.

Je třeba upozornit, že tyto vymahačské společnosti užívají k vyvolání tlaku na dlužníka možnosti uvést dlužníka v tzv. veřejném registru dlužníků, přístupném každému prostřednictvím internetu. K tomuto postupu neexistuje žádný právní podklad, neboť souhlas dlužníka evidentně chybí. V těchto případech bývá často zasahováno do osobnostních práv osob,

neboť společnost prostřednictvím registru dlužníků často neoprávněně označí za dlužníka osobu, která nikomu nic nedluží. Přičemž se o faktu svého zveřejnění jako dlužníka nemusí ani dozvědět.

## ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PROSTŘEDNICTVÍM KAMEROVÝCH SYSTÉMŮ

### Podání ve věci kamerových systémů

Počet podání směřujících proti provozovatelům kamerových systémů obdržených v roce 2011 byl srovnatelný s rokem 2010. Z celkového počtu 375 podání se téměř 90 % týkalo sledování zaměstnanců na pracovišti, provozu kamerových systémů v bytových a soukromých domech. Lze tedy shrnout, byť absolutní zobecnění by bylo zavádějící, že většina občanů je víceméně smířena s kamerami např. na letišti, v metru, bance, ale je značně citlivá k zásahům do svého soukromí zejména na pracovišti a v bydlišti.

Při řešení případů využívání kamer se záznamem na pracovišti existuje dlouhodobá spolupráce Úřadu s oblastními inspektoráty práce, neboť primárně dochází k porušování ustanovení § 316 zákoníku práce, které až na výjimky spočívající ve zvláštní povaze činnosti zaměstnavatele zakazuje sledování zaměstnanců na pracovišti a ve společných prostorách. Takovéto jednání již nepodléhá dozorové působnosti Úřadu.

Podle § 3 odst. 3 se zákon o ochraně osobních údajů nevztahuje na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu. Typickým příkladem je využití kamerových systémů k ochraně vlastního majetku, nejčastěji soukromých domů. Ochrana soukromého majetku je nezadatelné ústavní právo každého občana. Úřad však nemůže nahrazovat působnost orgánů činných v trestním řízení, občanskoprávních soudů ani věcně příslušných správních orgánů mj. proto, že není vybaven kompetencemi ke vstupu do soukromého obydlí a ke kontrole z něho pořízených kamerových záznamů.

### Vzhledem k uvedenému Úřad deklaruje, že nadále nebude řešit sousedské spory typu:

*Policie ČR postoupila městskému úřadu oznámení o spáchání přestupku, kterého se měla dopustit fyzická osoba tím, že dlouhodobě natáčela videokamerou a mobilním telefonem svého souseda na jeho pozemku, a městský úřad oznámení dále postoupil Úřadu. Potenciální pachatel přestupku zaslal Úřadu mnohostránkovou stížnost na oznamovatele, který využívá kamerový systém k monitorování jeho pozemku, a veřejné cesty, o jejíž vlastnictví vedou obě strany několikaletý spor a pořízené záznamy využívají jako důkazní prostředky.*

Z řešení řádově stovek podání směřujících proti provozovatelům kamerových systémů obdržených v roce 2011 vyplývá, že nejčastějšími typy porušení povinností uložených zákonem o ochraně osobních údajů byly následující:

- zneužívání shromážděných záběrů k jiným než deklarovaným účelům,
- zpřístupňování či zveřejňování kamerových záběrů neoprávněným osobám,
- nepřijetí adekvátních technicko-organizačních opatření minimalizujících rizika neoprávněného přístupu ke kamerovým záznamům,
- překračování principů proporcionality mezi chráněným zájmem (účelem) a zasahováním do soukromí fyzických osob,
- neplnění informační a oznamovací povinnosti.

## Kazuistika

Na základě stížnosti Stálé komise Senátu pro ochranu soukromí, z které vyplývalo podezření na porušování zákona o ochraně osobních údajů, a to v souvislosti se zneužíváním kamerových záznamů k propouštění některých zaměstnanců z pracovního poměru, a dále neplnění informační a oznamovací povinnosti správce kamerového systému, byla provedena kontrola v jednom obchodním centru (dále jen „OC“).

Šetřením byly zjištěny tyto skutečnosti: Účelem pořizování kamerového záznamu (zpracovávání osobních údajů) je bezpečnost osob a ochrana majetku. Záznamy z kamerového systému se uchovávají po dobu 14 dnů. Areál OC je rozlehlý, OC se nachází ve čtyřpatrové budově. V OC je umístěno 111 kamer. Informace o pořizování kamerového záznamu je umístěna na vchodech do objektu (někde je i obrazovka, na které běží on-line záběry z kamery).

Kontrolující se seznámili s chodem tzv. velína, kde jsou sledovány jednotlivé kamery. Bylo zjištěno, že ke kamerovému záznamu je možný přístup pouze po zadání hesla. Přístup k záznamu má pouze „velínář“, vedoucí útvaru G4S v OC a ředitel centra OC. Každá z těchto osob má upraveno oprávnění vzhledem k rozsahu pravomocí své pracovní pozice.

V případě mimořádné události se pořizuje výpis ze záznamu z kamerového systému, a to na základě požadavku na vytvoření/zhlédnutí obrazového záznamu z uzavřeného kamerového systému. Zde se uvádějí údaje o osobě, která o záznam požádala, dále jaké věci (případně jakého trestného činu) se záznam týká, služební číslo policisty, důvod požadavku, doba a místo, ze kterého je obrazový záznam požadován. O pořízení kamerového výpisu se dále sepisuje protokol o převzetí výpisu z obrazového záznamu z uzavřeného kamerového systému.

V tomto protokolu se uvádějí následující údaje: jméno a příjmení žadatele (pokud jde o policistu, jeho služební číslo), kdy byl požadavek na záznam doručen, kdo požadavek schválil, kdo výpis provedl, na jaké médium byl uložen, počet kamerových záznamů, z kterého dne je záznam pořizován a jeho délka a dále kdo záznam převzal. Jednotlivé vstupy v souvislosti s nahlížením a pořizováním kamerového výpisu jsou logovány, avšak záznam o tomto je uchováván jen po dobu 14 dnů, seznam přístupů se pak maže společně se záznamem.

Právním titulem pro zpracovávání osobních údajů je souhlas subjektu údajů anebo právní důvod přímo citovaný v zákoně. V posuzovaném případě se jedná o zpracovávání osobních údajů bez souhlasu, proto musí dané zpracovávání osobních údajů vyhovět podmínkám ustanovení § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, tzn. *Správce může zpracovávat, pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života.*

Z výše uvedeného vyplývá, že právě hlediska:

- a) zda daný prostředek zasahuje do základních práv a svobod,
- b) zda v konkrétním případě jiný právem chráněný zájem převáží nad právem na ochranu soukromí,
- c) zda právě záznam z kamerového systému je jediný a nejvhodnější prostředek pro ochranu takového zájmu,
- d) zda záznam z kamerového systému je schopen naplnit deklarovaný účel, jsou při kontrole Úřadem rozhodující pro posouzení legality použití kamerového systému.

Účelem, pro který v daném případě dochází ke zpracování osobních údajů, je ochrana osob a majetku. Jak bylo předesláno, OC je rozsáhlý komplex, který se rozprostírá ve čtyřpodlažní budově. Společnost je odpovědná za zajištění bezpečnosti osob a ochranu majetku v tomto

komplexu. Dle slov zástupců kontrolovaného docházelo k občasnému poškození majetku a ohrožení osob (nehody v garážích, krádeže, poškozování vstupních dveří). Rozsah zpracovávaných osobních údajů musí být dle ustanovení § 5 odst. 1 písm. d) zákona o ochraně osobních údajů minimální vzhledem k danému účelu. Tudíž je nutné ověřit, zda je opravdu každá kamera nezbytná a zda uchovávané záběry z ní nezasahují v míře neúměrné sledovanému účelu do soukromí osob. Určité pochybnosti nastávají v případě otočné kamery, která sleduje také restaurační prostory a lze při využití zoomu velmi dobře sledovat jednotlivé návštěvníky, nicméně i zde je možno přihlížet k tomu, že se tu občas zdržují osoby bez domova a dochází k obtěžování hostů a ke krádežím. Vzhledem ke zmíněnému je tedy účel zpracovávání osobních údajů legitimní a v souladu s ustanovením § 5 odst. 2 písm. e) zákona o ochraně osobních údajů.

Správce musí plnit všechny povinnosti uvedené v ustanovení § 5 odst. 1 zákona o ochraně osobních údajů, včetně stanovení **doby** nezbytné pro **uchovávání záznamů** z kamer (písm. e). Ta je obecně Úřadem **doporučena** maximálně **jako týdenní**.

Záznamy nesmějí být použity k žádnému jinému účelu, než ke kterému byly pořízeny: ochraně majetku Společnosti a bezpečnosti zákazníků. S tím úzce souvisí bezpečnost uchovávaných záběrů z kamer.

Oprávnění vstupovat do záznamů z kamer je možné pouze v případě porušení právem chráněného zájmu, např. dojde ke krádeži, rozbití dveří, ohrožení zákazníků. Stejně tak je možno záznamy z kamer předávat v těchto případech Policii ČR, avšak na základě písemné žádosti včetně odůvodnění této žádosti, jímž je vyšetřování konkrétního protiprávního jednání. Dokonce ani správce objektu nemá právo nahlížet do záznamů bez důvodu, spočívajícím v nahlášeném protiprávním jednání.

Při automatizovaném zpracovávání vyplývá správci nebo zpracovateli navíc povinnost *pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány* – tzv. logování (§ 13 odst. 4 písm. c) zákona o ochraně osobních údajů. S ohledem na ochranu osobních údajů není dokumentace, kdy jsou logy po 14 dnech mazány, odpovídající, neboť společnost v případě porušení zákona o ochraně osobních údajů v souvislosti s neoprávněným nakládáním se záznamy z kamerového systému nebude schopna po 14 dnech identifikovat, resp. ověřit, kdy, kdo a z jakého důvodu se záznamem pracoval, což je proti smyslu uvedeného ustanovení, a tudíž nejsou dostatečně splněna opatření k ochraně osobních údajů. Dobu logování vstupů ke kamerovým záznamům je tedy nezbytné prodloužit, a to minimálně na dobu 3 měsíců.

Základní informační povinnost v souladu s ustanovením § 11 zákona o ochraně osobních údajů byla splněna, neboť vstupující zákazníci jsou informováni o kamerovém systému se záznamem prostřednictvím informačních tabulí. Informační tabulky je však třeba doplnit o odkaz, kde se mohou lidé dozvědět všechny informace, které má správce povinnost sdělit např. prostřednictvím odkazu na [www stránky](#).

Zneužívání kamerového záznamu za účelem rozvázání pracovního poměru se zaměstnanci nebylo zjištěno.

Každoročně narůstá počet stížností na **provozování kamerových systémů v bytových domech**. Ve většině případů se jedná o stížnosti na rozsah kamerového systému, tj. počet kamer, rozsah monitorovaných prostor, dobu uchovávání záznamů, zajištění řádného plnění informační povinnosti (kromě informace o sledování prostor kamerovým systémem se záznamem má být subjektům údajů – procházejícím osobám – poskytnuta minimálně informace o správci kamerového systému, který je schopen podat požadované detailní informace),

a přetrvávají problémy se souhlasem subjektů údajů s pořizováním záznamů z těchto systémů. Provozování kamerových systémů v bytových domech stále zůstává pro mnoho subjektů údajů citlivým problémem. Bezesporně jde o zásah do soukromí, a přestože Úřad již v roce 2008 vydal stanovisko s doporučenými postupy při instalaci kamerových systémů v bytových domech, stále se setkává ve své kontrolní činnosti s nepochopením základních aspektů ochrany osobních údajů. Úřad průběžně reflektuje svůj postoj k provozování kamerových systémů v bytových domech vyjádřený ve stanovisku č. 1/2008. S ohledem na praktické zkušenosti se bude Úřad eventuálně snažit stanovisko revidovat tak, aby bylo ještě návodnější pro správce a obecně srozumitelné pro každého čtenáře.

Jako typické lze uvést kontroly provedené na základě stížnosti ve dvou činžovních domech, jejichž vlastníkem bylo společenství vlastníků. V obou domech byl instalován kamerový systém se záznamem, který se skládal ze čtyř kamer a digitálního videorekordéru. Dvě kamery byly instalovány do suterénních prostor (po jedné v každém domě) a dvě kamery do prostor schodiště do 1. podlaží (v době kontroly byly vypnuté). Účelem, dle sdělení kontrolovaných, bylo zamezit nepořádku na chodbě domu, u poštovních schránek, snaha o zamezení používání osobních výtahů popeláři, v důsledku kterého docházelo k poškozování výtahu – záznamy chtěli kontrolovaní použít pro následné jednání s popeláři, dále k ochraně majetku obecně, včetně získání informací o osobách, které nemají oprávnění vstupu do sledovaných prostor. Digitální videorekordér typu AVC785 se záznamem na pevný disk byl instalován v kanceláři společenství, k ovládání videorekordéru sloužil notebook, instalovaný v kanceláři společenství vlastníků. Kamerový systém byl v nepřetržitém provozu 24 hodin denně. Doba uchovávání pořízených záznamů byla cca 10 dnů, tato doba nebyla určena nastavením parametrů kamerového systému, ale kapacitou pevného disku videorekordéru, kdy se po jeho zaplnění automaticky mazaly nejstarší uložené záznamy. Doba uchování tak mohla kolísat dle četnosti pořizování nových záznamů. Společenství neprokázalo, že disponuje souhlasem všech obyvatel domů se zpracováním jejich osobních údajů prostřednictvím kamerového systému se záznamem.

Inspektorka Úřadu v kontrolním protokolu konstatovala, že kamerový systém se záznamem, tak jak byl v domech instalován a nastaven, sleduje a zaznamenává neustále činnost osob ve sklepních prostorách domů, dále pak je zamýšleno shromažďovat a zpracovávat záznamy o aktivitách každého, kdo do domů vstupuje nebo z nich odchází (kamery na podestách do 1. podlaží). Vzhledem k tomu, že se jedná o dva rozdílné prostory, zvažila kontrolující inspektorka míru zásahu do soukromého a osobního života sledovaných osob v daných prostorách a jeho proporcionalitu vzhledem ke stanovenému účelu pro každý prostor zvlášť. Zároveň konstatovala, že vlastní shromažďování osobních údajů kamerovým systémem se záznamem uvedeným způsobem přitom zcela postrádá preventivní funkci ve smyslu přímého zabránění či odvrácení nežádoucích aktivit, jeho funkce je omezena pouze na odstrašení potenciálního pachatele. Osobní údaje, resp. záznamy z kamerového systému, shromážděné v prostorách domu, v rozsahu zjištěném v průběhu kontroly, tak mohou sloužit pouze jako podpůrný prostředek pro následné objasnění či vyšetření incidentů, nemohou však samy o sobě zajistit žádoucí ochranu ve smyslu účelů, které byly určeny společenstvím vlastníků, tedy zabránit nežádoucímu jednání. Vlastností kamerového systému, vyplývajících z jeho podstaty, je to, že nepřetržitě shromažďuje záznamy o všech aktivitách veškerých osob, které jsou právě v dosahu jednotlivých kamer, nezávisle na tom, zda se jedná o aktivity v souladu či rozporu s určeným účelem. Znamená to, že pouze nepatrný zlomek shromážděných a uchovávaných kamerových záznamů obsahuje údaje, které mohou být využity k naplnění určeného

účelu, zbytek je shromážděn a uchováván nadbytečně, a to za cenu více než nepřiměřeného zásahu do soukromí dotčených osob. V případě pořizování záznamu ve sklepních prostorách konstatovala inspektorka, že zásah do soukromého a osobního života není značný, protože do uvedených prostor vstupují dotčené osoby pouze nepravidelně a zřídka, přičemž jejich aktivity se zpravidla omezuje pouze na vyhození odpadu do popelnic. Tyto prostory nejsou průchozí, tj. neslouží pro vstup do dalších částí domů, kam by dotčené osoby musely nezbytně vstupovat. Z hlediska stanoveného účelu, tedy kontrola vstupu a pobytu neoprávněných osob a jejich nežádoucích aktivit, posoudila inspektorka jako mírně rizikové, neboť společenství již dříve realizovalo účinné opatření pro zabránění vstupu neoprávněných osob do domů (uzamykatelné mříže u vstupu).

Na základě tohoto zvážení lze na předmětné zpracování aplikovat výjimku dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů. Současně je však nezbytné posuzovat aplikaci této výjimky jako hraniční případ, neboť i při běžné činnosti, jako je vynášení odpadu, může dojít k situaci, jejíž zveřejnění by mohlo dotčenou osobu značně poškodit. V případě zamýšleného pořizování záznamů z kamer, instalovaných na podestách schodišť do prvního podlaží domů, uvedla, že je nezbytné nejprve konstatovat, že oblast ochrany soukromí každého jednotlivce není vázána pouze na vnitřní prostory jeho bytu, ale i na prostory, kterými daný jedinec musí nezbytně procházet, aby mohl vstoupit do vlastního obydlí nebo ho opustit. Dotčené osoby (subjekty údajů) přitom nemají možnost volby, jak vstoupit do svého bytu nebo ho opustit, aniž by o tom byl pořízen záznam. Je nutno zdůraznit, že sledování by bylo až na výjimky soustavné a dlouhodobé, nikoliv nahodilé či jednorázové, a proto by bylo možné ze shromážděných záznamů snadno získat informace zneužitelné k poškození některého ze sledovaných subjektů údajů, k čemuž značně přispívá i to, že záznamy jsou automaticky opatřovány údajem o datu a čase. Pořizování záznamů prostřednictvím kamerového systému za uvedených podmínek a uvedeným způsobem je nutno posuzovat jako zasahující vysokou měrou do osobního a soukromého života obyvatel domu, tedy jako velmi invazivní.

Z hlediska dosažení stanoveného účelu, tedy ochrany majetku společenství, majetku obyvatel domů a jejich zdraví a bezpečnosti, je nutno konstatovat, že při daném nastavení kamer by byl sledován pouze omezený prostor a vybavení domů. Jak již bylo uvedeno výše, funkce by se omezila pouze na odstrašení případného pachatele a následné zdokumentování nežádoucího jednání pro účely vyšetřování, v žádném případě by však toto jednání nebylo možno přímo odvrátit. Dle kontrolující inspektorky by bylo zpracování osobních údajů společenstvím prostřednictvím kamerového systému se záznamem v popsáném rozsahu a popsáním způsobem prostřednictvím kamer na podestách natolik významným a hrubým zásahem do soukromého a osobního života subjektů údajů, přičemž tento zásah by byl neúměrný dosaženému účinku, že na něj nelze aplikovat ustanovení výjimky uvedené v § 5 odst. 2 písm. e) zákona o ochraně osobních údajů. Zpracováním osobních údajů bez souhlasu subjektů údajů prostřednictvím záznamů z kamer na podestách by společenství porušilo povinnost uloženou v § 5 odst. 2 zákona o ochraně osobních údajů.

## ZPŘÍSTUPŇOVÁNÍ VIDEOZÁZNAMU Z JEDNÁNÍ ZASTUPITELSTVA

*Pořizování a následné zpřístupňování videozáznamu z jednání zastupitelstva obce se v roce 2011 stalo ostře sledovaným jak občanskou, tak i novinářskou veřejností.*



Úřad se opírá ve své kontrolní činnosti o platnou legislativu, kterou zákonodárce přijal k dané problematice. Jedná se zejména o Ústavou zaručená práva. Podle článku 10 Základní listiny práv a svobod má každý občan právo na to, aby mu byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno. Rovněž má každý právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života. A také má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě. Tato ústavní práva dále upřesňují platné zákony, zejména zákon o ochraně osobních údajů, zákon č. 128/2000 Sb., o obcích, zákon č. 40/1964 Sb., občanský zákoník aj. Na druhé straně stojí rovněž Ústavou zaručené právo občanů na informace, podle článku 17 Listiny. A v tomto vymezeném prostoru Úřad zjišťuje, je-li soulad mezi skutkovým stavem a platnou právní úpravou.

Současná uspěchaná doba a neustále se zdokonalující technické možnosti zaznamenávat, uchovávat a následně zpřístupňovat na internetu události vedou mnohá zastupitelstva k rozhodnutí vyhovět silné poptávce a pořizovat videozáznam z jednání nejvyššího orgánu obce, obecního zastupitelstva a následně tento videozáznam zpřístupňovat na svých webových stránkách. Co víc by mělo být veřejné než jednání zastupitelstva? Na tuto otázku lze odpovědět kladně, ale je nutno dodat, že pouze při dodržování platných zákonů.

**Obec musí jasně stanovit účel pořizování audio nebo videozáznamu z jednání zastupitelstva.** Rozhodne-li se zastupitelstvo pořizovat záznam tak, že je celý pořad zastupitelstva snímán v autentické podobě bez jakýchkoliv úprav, pak se jedná o vytváření dokumentu, na který se vztahují ustanovení zákona č. 499/2004 Sb., o archivnictví a spisové službě. Takto vzniklý dokument může sloužit pouze jako podklad pro pořizování zápisu z jednání zastupitelstva. Po vyhotovení zápisu musí být tento záznam zlikvidován dle povinností stanovených uvedeným zákonem.

Rozhodne-li se obec pro přímý přenos z jednání zastupitelstva bez pořizování záznamu, pak se nejedná o shromažďování osobních údajů a na tento on-line přenos se nevztahují ustanovení zákona o ochraně osobních údajů. (stanovisko Úřadu 1/2006)

Podle § 93 odst. 3 zákona č. 128/2000 Sb., o obcích, jsou zasedání zastupitelstva obce veřejná a může se jich zúčastnit kdokoli. To znamená, že se ho mohou účastnit všichni občané, kteří projeví zájem a dostaví se osobně na jednání tohoto nejvyššího orgánu obce. O průběhu zastupitelstva se pořizuje zápis, který je podle § 95 odst. 2 zákona o obcích k nahlédnutí na obecním úřadě. V zápise se vždy uvádí počet přítomných členů zastupitelstva obce, schválený pořad jednání zastupitelstva obce, průběh a výsledek hlasování a přijatá usnesení. Zápis je úřední dokument, který musí obsahovat i přesné osobní údaje o občanech, kteří se obrátili na obec například s žádostí o koupi nemovitosti z majetku obce nebo s žádostí o úpravu výše nájemného či odpuštění případného dluhu na nájemném v obecním bytě. Nahlížet do zápisů z jednání zastupitelstva a do usnesení zastupitelstva a pořizovat si z nich výpisy může dle ustanovení § 16 odst. 2 písm. e) zákona o obcích občan obce, který dosáhl věku 18 let. Stejně právo má i fyzická osoba, která dosáhla věku 18 let a vlastní na území obce nemovitost. Rovněž tak i fyzická osoba, která dosáhla věku 18 let, je cizím státním občanem a je v obci hlášena k trvalému pobytu, stanoví-li tak mezinárodní smlouva, kterou je Česká republika vázána. To je zákonem stanovený okruh občanů, kteří se mohou seznamovat i s osobními údaji spoluobčanů v souvislosti se zastupitelstvem projednávanými materiály. Nikdo jiný nemá právo seznamovat se s osobními údaji uvedenými v zápise. (stanovisko Úřadu 2/2004)

Je-li účelem natáčení videozáznamu pořízení televizního zpravodajství, které by občanům přiblížilo dění na zastupitelstvu bez uvádění osobních údajů, pak by se nejednalo o dokument, ale pouze o zpravodajství, na které se vztahuje ustanovení zákona 40/1964 Sb., občanský zákoník. V části ochrana osobnosti § 11 zákona stanoví, že fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy. Následný § 12 toto obecné ustanovení upřesňuje: (1) *Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.* (2) *Svolení není třeba, použijí-li se písemnosti osobní povahy, podobizny, obrazové snímky nebo obrazové a zvukové záznamy k účelům úředním na základě zákona.* (3) **Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby poříditi nebo použít přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. Ani takové použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.**

K problematice možnosti obcí zpřístupňovat průběh jednání zasedání zastupitelstva je nutno vzít v úvahu i zákon o ochraně osobních údajů, zejména ust. § 4 písm. a), podle kterého je „osobním údajem jakákoliv informace týkající se určeného nebo určitelného 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“. Videozáznam z jednání zastupitelstva většinou obsahuje informace o osobách a jejich záležitostech, které jsou na zasedání zastupitelstva řešeny. Informace o těchto osobách jsou většinou zveřejněny v rozsahu jméno, příjmení, datum narození a přesná adresa bydliště. Dle těchto údajů jsou osoby bezpochyby identifikovatelné, jedná se tedy o osobní údaje dle ustanovení § 4 písm. a) zákona o ochraně osobních údajů.

Dle ustanovení § 4 písm. l) zákona o ochraně osobních údajů „je zveřejněným osobním údajem osobní údaj zpřístupněný zejména hromadnými sdělovacími prostředky, jiným veřejným sdělením nebo jako součást veřejného seznamu“. Zveřejněním záznamu ze zasedání zastupitelstva prostřednictvím webových stránek obce dochází opakovaně ke zpřístupnění osobních údajů subjektů údajů.

Podle ustanovení § 5 odst. 2 zákona o ochraně osobních údajů „správce (v tomto případě obec) může zpracovávat osobní údaje pouze se souhlasem subjektu údajů“. Bez tohoto souhlasu je může zpracovávat pouze v případech, které jsou uvedeny v ustanovení § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů. Z tohoto ustanovení vyplývá, že ke zveřejnění osobních údajů je zapotřebí svobodný a informovaný souhlas všech dotčených osob, což je prakticky nemožné.

Dle ustanovení § 11 odst. 1 zákona o ochraně osobních údajů, „je správce při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21“. Z těchto ustanovení vyplývá, že obec není schopna po celou dobu zpracování prokázat, že dotčené subjekty údajů byly informovány o tom, že jejich osobní údaje mohou být zpracovány při pořizování videozáznamu z průběhu jednání zastupitelstva, a tím dochází k porušování ustanovení § 11 odst. 1 zákona o ochraně osobních údajů.

Na základě výše uvedených právních ustanovení lze konstatovat, že chybí právní základ jednoznačně podporující legitimitu zpracování informací z jednání obecních zastupitelstev s využitím moderních audiovizuálních zařízení a internetu.

Společenská poptávka si žádá novelizaci příslušných právních předpisů, upravujících jednání orgánů obcí v tom smyslu, aby bylo možné pořizovat z nich záznamy a tato činnost, prováděná v zájmu dobré informovanosti občanů, byla v souladu se zákonem.

V současnosti lze obcím, které občanům zprostředkovávají nebo hodlají zprostředkovávat dění na zastupitelstvu, doporučit, aby se držely následujících zásad.

V případě, že se obec rozhodne provádět **přímé přenosy** z jednání zastupitelstva, by mělo být splněno několik podmínek:

- Rozhodnutí zastupitelstva provádět on-line přenos by mělo být schváleno usnesením zastupitelstva (byl stanoven účel zpracování osobních údajů).
- Způsob a prostředky provádění on-line přenosu (umístění kamer, záběry kamer atp.) z jednání by měly být stanoveny v jednacím řádu zastupitelstva.
- Každý, kdo na takové jednání přichází, by měl být předem informován o této skutečnosti i o způsobu dosažitelnosti tohoto přenosu (internet bez omezení, s omezením přístupu, uzavřený televizní okruh nebo kabelová televize).

**Na přímý přenos ze zasedání zastupitelstva se ustanovení zákona o ochraně osobních údajů neaplikuje**, protože nedochází záznamem ke shromažďování osobních údajů.

V případě, že se obec rozhodne pořizovat audio nebo videozáznam ze zasedání zastupitelstva obce jen pro účely vyhotovení písemného zápisu ze zasedání, je povinnost po pořízení zápisu nebo po uplynutí doby určené pro skartaci záznam zlikvidovat.

S ohledem na oprávněný zájem občanů o dění v obecních zastupitelstvech a s odkazem na § 97 zákona o obcích, který říká, že obec informuje občany o činnosti orgánů obce na zasedání zastupitelstva obce a dále jiným způsobem v místě obvyklým, lze při absenci příslušné právní úpravy, která by jednoznačně řešila provádění audio nebo videozáznamu z jednání zastupitelstva pro účely následného informování veřejnosti, a s ohledem na skutečnost, že platná právní úprava zákona o obcích byla koncipována v roce 1991, tedy v době neznalosti možností a vlastností internetu, a s ohledem na změnu společenského vývoje od doby vydání tohoto zákona, lze tento § 97 použít přiměřeně při respektování ochrany osobnosti podle § 12 zákona 40/1964 Sb. občanského zákoníku. Proto je nezbytně nutné anonymizovat osobní údaje subjektů údajů, zveřejňovaných a zpřístupňovaných v audio a videozáznamech ve formě zpravodajství ze zasedání zastupitelstva obcí na webových stránkách obce tak, aby nedocházelo k jejich zpřístupňování neoprávněným osobám ve smyslu ustanovení § 16 odst. 2 zákona o obcích. Odbor pro styk s veřejností Úřadu obdržel v roce 2011 deset žádostí orgánů veřejné správy, včetně Magistrátu hlavního města Prahy, k zaujetí stanoviska ve věci pořizování a zveřejňování obrazových a zvukových záznamů z jednání zastupitelstev.

Odbor správních činností Úřadu pokutoval v roce 2011 jediné zveřejnění údajů v souvislosti se zpřístupňováním záznamů z jednání obcí. Toto řízení není dosud pravomocně ukončeno.

Z kontrolní činnosti Úřadu jednoznačně vyplývá **nezbytnost přijetí opatření legislativního charakteru**, která by řešila, případně precizovala, mj. i problematiku přímých přenosů a pořizování obrazových a zvukových záznamů z jednání zastupitelstev volených orgánů, tedy novelu zákona o obcích, krajích, hl. m. Praze.

## NEDOSTATEČNÉ ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ (§ 13 ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ)

### Nejčastější nedostatky zjišťované v roce 2011 a v letech předcházejících při dozorové činnosti Úřadu v oblasti naplnění § 13 zákona o ochraně osobních údajů.

Ustanovení § 13 zákona o ochraně osobních údajů o zabezpečení osobních údajů je v podstatě velice přísné, neboť říká, že je *nutno učinit taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům*. Z čehož obrácením implikace vyplývá, že pokud k takovému přístupu došlo, nebyla opatření dostatečná.

Vývoj výkladu tohoto paragrafu také doznal značného posunu. Na počátku aplikace zákona o ochraně osobních údajů pojem neoprávněný, resp. oprávněný přístup zahrnoval široký okruh osob a oprávněným byl každý člen či pracovník oprávněné osoby: Například pokud byla správce osobních údajů žáků škola, považovalo se za normální, že kdokoliv z učitelů měl k těmto osobním údajům přístup.

Novela zákona o ochraně osobních údajů v r. 2007 upřesnila, kdo se míní tím skutečně oprávněným: Správce osobních údajů je povinen *„zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovanou zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby“*.

Také charakter úniků osobních údajů, kterými se Úřad zabýval, se v čase proměňoval. V prvních letech po vzniku zákona o ochraně osobních údajů, tj. po roce 2000, se často stávalo, že byly nalezeny dokumenty obsahující osobní údaje – a někdy i citlivé (zdravotnické) – v popelnících, ve vlaku, v příkopě, ve starých opuštěných domech, bývalých hotelech, opuštěných provozovnách nebo nepoužívaných částech nemocnic. Úřad se setkal i s případem nedokonalé spálených dokumentů, popř. omylem vyhozených krabic plných dokumentů obsahujících osobní údaje do sběru.

Často se také stávalo, že nepozornost způsobila opravdovou ztrátu dokumentů.

- Došlo k:
- odcizení flashdisků z neuzamčené ordinace,
  - ke krádežím notebooku z pracoviště, které nebylo dostatečně zajištěno,
  - odcizení služebního notebooku z domova,
  - ke krádeži dokumentů z neuzamčeného vozidla,
  - odcizení lékařských dokumentací z automobilu,
  - odcizení disket se zdravotnickou dokumentací z neuzamčeného automobilu na parkovišti nákupního střediska, když majitel vracel nákupní vozík apod.

Lidé si ale postupně zvykali na ochranu soukromí, na bezpečnostní zóny u lékaře nebo v bance, na přístupová práva a hesla, na směrnice pro zacházení s osobními údaji, na přísnost při předávání informací o osobách. Nicméně pokračovaly stížnosti:

- na neuzamčené kartotéky umístěné v čekárnách,
- na posílání osobních údajů nezabezpečeným e-mailem,
- na zaslání zdravotnické dokumentace obyčejnou poštou (což nezaručuje doručení oprávněnému subjektu a jedná se o citlivé údaje),
- ponechání zdravotnické dokumentace na schodech domu,
- předání zdravotnické dokumentace příbuznému bez souhlasu pacienta,
- dokumenty s osobními údaji pohozené po stolech,
- dokumenty s osobními údaji používané jako papír pro poznámky.

V roce 2011 jsme zaznamenali, že obchodní zástupce bankovního domu oznámil policii odcizení notebooku a plastového řadiče s papírovými listy obsahujícími osobní údaje cca 100 klientů banky za poslední rok v rozsahu jméno, příjmení, bydliště, rodné číslo, číslo občanského průkazu a podpis. Ke krádeži došlo z uzamčeného osobního vozidla na parkovišti v Liberci.

Závažné byly také případy, kdy správci osobních údajů tyto předali třetí osobě, aniž by si uvědomili, že tak činit nemohou. Šlo například o:

- záběry z bezpečnostních kamer předané policii bez řádného vyžádání,
- předání zdravotní zprávy policii při konfliktu s pacientem taktéž bez řádného vyžádání,
- varování před údajnou zlodějkou rozesílané spřáteleným firmám,
- předání výplatních listů bývalého zaměstnance spřátelené firmě,
- předání citlivých údajů žáka členům správní rady školy, které správní radě samozřejmě nejsou určeny.

Jindy správci zveřejnili osobní údaje na internetu, aniž by si uvědomili, že tak činit nemohou:

- výsledky zkoušek,
- studentské karty,
- záběry z bezpečnostních kamer,
- seznamy zlodějů v samoobsluhách,
- seznamy neplatičů v ubytovnách apod.

V mnoha případech šlo o selhání jednotlivce, kdy lze správce osobních údajů vyvinít, resp. bylo možné aplikovat ustanovení, že *„právní osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila ( § 46 odst. 1 zákona o ochraně osobních údajů )*. Kupříkladu se prokázalo, že konkrétní zaměstnanec/kyně vyrazil/a osobní údaje rozvádějícímu se manželovi, prozradil/a údaje o dluhu apod., přestože v příslušných směrnicích o bezpečnosti osobních údajů byl jasný příkaz mlčenlivosti. Takový případ lze posuzovat podle ustanovení § 44 zákona o ochraně osobních údajů jako přestupek konkrétní fyzické osoby.

K porušení povinnosti při zabezpečení osobních údajů také dochází pouhou neopatrností: Například odesílání e-mailové zprávy velké skupině osob, kdy se adresy nedají do kolonky „Skruté“. Podobně nelze posílat osobní údaje nezabezpečeným (nešifrovaným) e-mailem, neboť možnost omylu v adrese je značná a ani jinak není garantováno, že k údajům nemá přístup neoprávněná osoba – na rozdíl od běžné pošty, kde je listovní tajemství garantováno a v zásadě naplněno.

Vyskytly se případy, kdy byly zveřejněny na internetu informace o obci a osobní údaje ve zveřejněných dokumentech byly sice „začerněny“, ale tak špatně, že bylo snadné toto začernění odstranit. Podobně došlo v tiskárně, která tiskla dokumenty obsahující mj. osobní údaje, k tomu, že nebyly skartovány chybné výtisky. Úřad byl také nucen potrestat finanční úřad, kdy při jednání s problematickým klientem došlo ke „zmizení“ jednoho z dokumentů, o kterých se jednalo.

Speciálním případem možného porušení ustanovení § 13 zákona o ochraně osobních údajů jsou nesprávně technicky zabezpečené webové stránky pro klienty: Klient má právo se podívat na své osobní údaje. Špatným nastavením webové stránky se ovšem stávalo, že po náhodné změně adresy získal informace i o dalších klientech.

V roce 2011 byla pokutována jistá společnost za to, že na svých internetových stránkách ponechávala dostupné vystavené faktury včetně osobních údajů zákazníků v rozsahu jméno, příjmení, adresa, případně dodací adresa, telefon, e-mailová adresa, předmět objednávky a cena. Rovněž se stalo, že exekutorka nezabezpečila, aby na jejích webových stránkách nebyly přístupné osobní údaje oprávněného v rozsahu jméno, příjmení, titul, adresa bydliště, a osobní údaje povinného v rozsahu jméno, příjmení, rodné příjmení, adresa bydliště a rodné číslo a dále výše dlužné částky, uvedené v *Předvolání k rozvrhovému jednání*; uvedený dokument bylo možné vyhledat např. prostřednictvím internetového vyhledávače Google.

Úřad také zaměřil svou kontrolní činnost na státní správu, konkrétně na veřejný registr zveřejněný na adrese [www.justice.cz](http://www.justice.cz) a na registr Státního fondu životního prostředí. Úřad požadoval, aby bylo na takový registr vždy pohlíženo jako na zpracování osobních údajů, neboť k němu takto dochází, a tudíž aby vždy existoval jasně určený správce, který plní povinnosti ze zákona o ochraně osobních údajů. Všeobecně je třeba vždy zvažovat, zda a které osobní údaje lze zveřejňovat na internetu: pokud se jedná o zákonnou povinnost, mělo by v zákoně být jasně řečeno, co přesně má být zveřejněno: např. v případě dotací pouze ti, kteří dotaci obdrželi. Pokud např. má podle zákona č. 123/1998 Sb., o právu na informace o životním prostředí *žadatel* (jednotlivá právnická nebo fyzická osoba, jež o informaci požádá) právo obdržet konkrétní informaci o životním prostředí včetně informací o jeho poškozování a o osobách, které byly pravomocně odsouzeny za přestupek vůči životnímu prostředí, nelze to vykládat tak, že je možno **zveřejňovat informace** o všech fyzických osobách, které porušily různé ekologické zákony a dopustily se přestupku.

Odstavec 2 ustanovení § 13 zákona o ochraně osobních údajů navíc požaduje, aby byl *„správce nebo zpracovatel povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy“*. Tudíž kontrola často, nejen až když k úniku osobních údajů dojde, zjistí, že žádná směrnice o ochraně osobních údajů a jejich bezpečnosti v kontrolované instituci neexistuje, že je používán jeden počítač více zaměstnanci, přístupové heslo je všem známé, popř. přilepené na počítači, počítač zůstává stále otevřený a všem přístupný apod.

Odstavec 3 ustanovení § 13 zákona o ochraně osobních údajů požaduje posuzovat rizika a odstavec 4 navíc *„zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby; fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby, a hlavně aby byly nastaveny funkce pro pořízení elektronických záznamů, které umožní určit a ověřit kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány“*.

V současné době proti rozhodnutí předsedy Úřadu o povinnosti logovat veškeré přístupy do společného registru finančních úřadů je podána žaloba Ministerstva financí.

Podobně z osobní konzultace poskytnuté pracovníkům IT jedné pojišťovny vyplynulo, že mají problém přesvědčit svůj vrcholový management, aby plně respektoval povinnosti ukládané § 13 zákona o ochraně osobních údajů a investoval nezbytné finanční prostředky do softwaru umožňujícího požadované logování přístupů do používaných systémů zpracovávajících osobní a citlivé osobní údaje.

Speciálními případy jsou uchovávané záznamy z kamer, které jsou pořizovány k ochraně majetku a odhalování trestné činnosti. Úřad požaduje, aby byly nastaveny tak, že do záznamů lze nahlížet teprve poté, kdy dojde k incidentu. Jako krajní přípouští Úřad výjimku pro bezpečnostního ředitele, který kontroluje podezřelé osoby např. v uměleckých galeriích.

V každém případě je však nutné logování s přesnými údaji o důvodu nahlížení. Není možné používat záznamy bezpečnostních kamer k jinému účelu (například při kontrole průběhu cyklistického závodu). Tyto záznamy nelze v žádném případě předávat médiím (televizi) nebo policii, aniž ta zahájila vyšetřování.

Pseudoanonymní údaje jsou údaje, které vznikají z osobních údajů anonymizací: např. je vynecháno příjmení a rodné číslo, ale jsou ponechány jiné údaje, které dovolí určitou osobu identifikovat. Je třeba vždy mít na mysli, že anonymizace je proces, který nedává ani nepřímo možnost konkrétní osobu identifikovat.

## TVZ. „NÁHUBKOVÝ ZÁKON“

*/dodržování § 8a – § 8c zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád) /*

V roce 2011 byly provedeny dvě kontroly dodržování ustanovení § 8a zákona č. 141/1961 Sb., trestní řád, resp. dodržování povinností správce osobních údajů stanovených zákonem o ochraně osobních údajů v souvislosti s poskytováním informací veřejnosti a sdělovacím prostředkům o průběhu šetření fyzické osoby; v obou případech se jednalo o postup Policie ČR.

V případě prvním bylo ve sdělovacích prostředcích zveřejněno jméno stěžovatele v souvislosti s šetřením Policie ČR a zveřejněny byly i informace o jeho obvinění. Osoba stěžovatele byla v daném městě veřejně známa, zároveň byla zveřejněna jeho fotografie, pořízená v okamžiku, kdy byla tato osoba předváděna k podání vysvětlení na Policii ČR.

V § 8a odst. 1 zákona č. 141/1961 Sb. (trestní řád) je uvedeno, že *„při poskytování informací o své činnosti veřejnosti orgány činné v trestním řízení dbají na to, aby neohrozily objasnění skutečností důležitých pro trestní řízení, nezveřejnily o osobách zúčastněných na trestním řízení údaje, které přímo nesouvisí s trestnou činností, a aby neporušily zásadu, že dokud pravomocným odsuzujícím rozsudkem není vina vyslovena, nelze na toho, proti němuž se vede trestní řízení, hledět, jako by byl vinen (§ 2 odst. 2). V přípravném řízení nesmějí zveřejnit informace umožňující zjištění totožnosti osoby, proti které se vede trestní řízení, poškozeného, zúčastněné osoby a svědka“.*

V průběhu kontroly nebylo prokázáno, že by Policie ČR poskytla před zahájením domovní prohlídky nebo v průběhu přípravného řízení telefonicky ani jinak informace, jež by vedly k identifikaci stěžovatele. Policie ČR na tiskové konferenci, která se konala následující den po domovní prohlídce, jméno a příjmení osoby, proti níž se vede řízení, konkludentně potvrdila. Je zapotřebí konstatovat, že jméno a příjmení bylo již v souvislosti s podezřením ze spáchání přečinu veřejnosti známo, jelikož bylo zveřejněno před tiskovou konferencí na webových stránkách deníku, který v daném městě vychází. Kontrolující na místě zjistili, že jméno a příjmení stěžovatele znali před tiskovou konferencí i další novináři.

Osoba stěžovatele tak byla v souvislosti s podezřením ze spáchání přečinu ztotožněna veřejností ještě před zahájením tiskové konference. Policie ČR tedy na tiskové konferenci informovala novináře o okolnostech, které již byly veřejnosti známé.

Kontrolovaná součást Policie ČR neporušila v souvislosti s poskytováním informací o fyzické osobě sdělovacím prostředkům na tiskové konferenci ustanovení zákona o ochraně osobních údajů.

V druhém případě se jednalo o podobnou kontrolu: prověřováno bylo dodržování ustanovení § 8b odst. 2 zákona č. 141/1961 Sb. (trestní řád). Stěžovatelka uvedla ve své stížnosti, že v souvislosti s šetřením podezření ze spáchání trestného činu týrání svěřené osoby došlo

k uvedenému porušení zákona tím, že reportérům televize byly poskytnuty jedním ze svědků či dalšími osobami informace, které mohly vést ke zjištění totožnosti stěžovatelčiny nezletilé dcery. Televize odvysílala reportáž, ve které svědkyně uváděla některé informace, které se týkaly trestního stíhání, a i když v reportáži nebylo zmíněno jméno poškozené nezletilé, z údajů, které zazněly, bylo dle stěžovatelky zřejmé, že pro ty, kdo ji i její dceru znají, byla jejich totožnost zřejmá. Stěžovatelka byla toho názoru, že údaje reportérům poskytla vědomě a úmyslně svědkyně. Stěžovatelka také uvedla, že po odvysílání reportáže se její dcera obává chodit do školy. Odvysílání reportáže způsobilo její dceři také zhoršení zdraví, což v příloze podnětu doložila lékařskou zprávou. Ze shromážděného důkazového materiálu vyplynulo, že Policie ČR poskytla sdělovacímu prostředku pouze informace, které nebyly v rozporu s ustanovením § 8a zákona č. 141/1961 Sb. (trestní řád). Policie ČR ve zveřejněné reportáži pouze uvedla, že vyšetřovatelka sdělila obvinění pro podezření ze spáchání trestného činu týrání svěřené osoby. Informace o věku obviněné není dostatečným identifikátorem, podle kterého by se dal určit konkrétní subjekt údajů. Kontrolou nebylo prokázáno, že by Policie ČR reportérům sdělila dílčí informace, které by vedly ke zjištění totožnosti stěžovatelky pro účely reportáže.

Inspektorka konstatovala, že Policie ČR neporušila § 8a zákona č. 141/1961 Sb. (trestní řád), ani ustanovení zákona o ochraně osobních údajů. Žádné konkrétní informace, na základě kterých by se dala identifikovat nezletilá dcera stěžovatelky nebo stěžovatelka sama, nebyly v televizní reportáži uvedeny. Zda údaje, které vedly televizi k identifikaci nezletilé, poskytla svědkyně, nebylo kontrolujícími provedeným šetřením prokázáno.

Zdroje svých informací, které následně využije za účelem realizace reportáže, televize nikomu nesděljuje. Pokud se informace o konkrétním subjektu údajů shromáždí v reportáži z více zdrojů, je pak v souvislosti s jejím odvysíláním možné, že se subjekt údajů stane identifikovatelným pouze pro určitý ohraničený okruh osob. Těmto osobám jsou většinou odvysílané skutečnosti již částečně známy. Televize ve zveřejněné reportáži žádné konkrétní identifikační údaje o dceři stěžovatelky ani o stěžovatelce samotné neuvedla. Kontrolujícím se provedeným šetřením a dokazováním nepodařilo zjistit žádné skutečnosti, které by vedly ke zjištění konkrétního subjektu, který televizi poskytl informace, na základě nichž mohli reportéři identifikovat stěžovatelku nebo její nezletilou dceru, za účelem natočení reportáže.

Správní řízení

*/dodržování § 8a – § 8c zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád) /*

Úřad ve správním řízení řešil zveřejnění informací, které vedly ke zjištění totožnosti poškozené v trestním řízení vedeném s obviněným Policí ČR, mimo jiné pro přečin vydírání podle § 175 odst. 1 zákona č. 40/2009 Sb., trestní zákoník, neboť obviněný zveřejnil kopie usnesení okresního státního zastupitelství a příkaz okresního soudu k provedení domovní prohlídky, které obsahovaly jméno, příjmení a v jednom případě datum narození poškozené a jméno, příjmení a datum narození jejího přítele, a dále také počáteční číslice jejich čísel mobilního telefonu. Tím obviněný porušil povinnost stanovenou v § 8b odst. 2 zákona č. 141/1961 Sb. (trestní řád) – tedy zákaz zveřejnit informace umožňující zjištění totožnosti poškozeného, vůči němuž byl spáchán některý z trestných činů proti svobodě a lidské důstojnosti. Úřad jakožto správní orgán dospěl po prošetření k závěru, že byly naplněny všechny znaky uvedené v § 8b zákona č. 141/1961 Sb. (trestní řád), který je jedním z ustanovení, na které odkazuje blanketní skutková podstata správního deliktu vyjádřená v § 45a odst. 1 zákona o ochraně osobních



údajů. V daném případě šlo o poškozenou, vůči níž byl spáchán trestný čin proti svobodě a lidské důstojnosti a byly zveřejněny informace umožňující zjištění její totožnosti. Vzhledem k tomu, že k uvedenému jednání došlo v internetovém periodickém tisku, byla naplněna i podmínka § 45a odst. 3 zákona o ochraně osobních údajů, tedy správní delikt byl spáchán tiskem. Při stanovení výše sankce bylo jako k polehčujícím okolnostem přihlédnuto zejména ke skutečnosti, že zveřejnění se týkalo pouze jedné osoby (poškozené). Úřad také přihlédl ke skutečnosti, že předmětné články měly nízkou návštěvnost, a že tedy jednáním účastníka řízení nedošlo k významnému rozšíření zákonem chráněné informace; sama poškozená se v dané věci neobrátila na účastníka řízení ani na správní orgán ve věci porušení zákona.

Úřad dále přihlédl k povaze jednání, které je posuzováno jako trestný čin a kterým měla být stěžovatelka poškozena. Jako k přitěžující okolnosti přihlédl k okolnostem jednání, jak vyplývají z předmětných podání a dokumentů v trestním řízení, které byly zveřejněny, neboť samotný popis tohoto jednání směřujícího vůči poškozené lze vnímat jako zásah do jejího soukromí. Po zhodnocení všech těchto okolností Úřad rozhodl o uložení sankce při samé spodní hranici zákonné sazby.

Dalším z rozhodnutí v souvislosti s tzv. „náhubkovým zákonem“ bylo správní rozhodnutí ve věci zveřejnění informace o tom, že nezletilá osoba je poškozenou v trestním řízení vedeném Policií ČR pro zločin pohlavního zneužití podle § 187 odst. 1, 2 zákona č. 40/2009, trestní zákoník. Informace byla zveřejněna účastníkem řízení – vydavatelem známého časopisu prostřednictvím článku v roce 2010, přičemž v článku bylo mj. uvedeno jméno a příjmení poškozené nezletilé. Dle rozhodnutí Úřadu vydavatel časopisu spáchal správní delikt podle § 45a odst. 1, 3 zákona o ochraně osobních údajů, neboť porušil zákaz zveřejnění osobních údajů stanovený jiným právním předpisem (trestním řádem) a tohoto se dopustil tiskem.

Společnosti jako účastníku řízení byla za naplnění skutkové podstaty správního deliktu podle § 45a odst. 1, 3 zákona o ochraně osobních údajů (kterého se dopustila v důsledku porušení povinnosti stanovené v § 8b odst. 2 trestního řádu, když v článku, který byl otištěn v jí vydávaném časopise, byla zveřejněna informace o nezletilé, jež byla poškozenou v trestním řízení vedeném Policií ČR s obviněnou pro podezření ze spáchání zločinu pohlavního zneužití) uložena v souladu s § 45a odst. 3 zákona o ochraně osobních údajů pokuta ve výši 50 000 Kč a v souladu s ustanovením §79 odst. 5 správního řádu povinnost nahradit náklady řízení v paušální výši 1 000 Kč.

Rozhodnutím předsedy Úřadu jako odvolacího orgánu došlo k zamítnutí výše uvedeného rozkladu.

Účastník řízení – uvedená vydavatelská společnost – namítal absenci pravomocného rozsudku o vině v předmětném řízení. Předseda v rozhodnutí o rozkladu shrnul, že zákaz zveřejňování informací o nezletilé není vázán na rozsudek o vině. Postačí, že se o určitém skutku vede trestní řízení. Předseda Úřadu zdůraznil, že pokud by byl zastáván opačný výklad, došlo by k popření samotného smyslu § 8b odst. 2 trestního řádu, protože by do právní moci rozsudku nebylo soukromí nezletilé nijak chráněno a ochrana zaručená tímto ustanovením by zcela postrádala smysl. Odvolací orgán, předseda Úřadu, mimo jiné uvedl, že ustanovení § 8b trestního řádu ve znění zákona 52/2009 Sb. je třeba rozumět tak, že se povinnost ohledně nesdělování informací vztahuje na celou dobu od zahájení trestního řízení až do jeho skončení, a to bez ohledu na jeho způsob. Ve svých závěrech dosažením užití jak standardního, tak nadstandardního interpretačního instrumentária odvolací orgán vycházel mj. i z důvodové zprávy k zákonu č. 52/2009 Sb. (Poslanecká sněmovna Parlamentu České republiky 2006–10,

sněmovní tisk č. 443), v níž se mimo jiné uvádí, že „je nezbytné oběť (poškozeného) chránit vzhledem k jejímu věku nebo povaze případu, kdy jsou uváděny detailní informace týkající se osoby oběti, její rodiny a soukromí, neboť v případě, že dojde k zveřejnění těchto informací, se oběť musí vyrovnávat nejen s následky trestného činu, ale i s nepříznivými dopady zvýšeného zájmu veřejnosti o její kauzu, přičemž může dojít k jejímu dalšímu poškozování“. Dle odvolacího orgánu, předsedy Úřadu, je také zásadní neopomíjet skutečnost, že jakékoli šíření informací o identifikované nebo identifikovatelné osobě je zásahem do její osobnosti, ke kterému musí mít případný šířitel jasné zákonné zmocnění, jelikož jím zakládá povinnost dotyčné osoby tento zásah strpět. Odvolací orgán konstatoval, že zveřejnění informací o tom, že nezletilá je v postavení poškozené v rámci trestního řízení vedeného pro podezření ze zločinu pohlavního zneužití, bylo v rozporu s § 8b odst. 2 trestního řádu, když nebylo prokázáno naplnění žádné z výjimek podle § 8b odst. 5 trestního řádu, na základě kterého lze povinnost uloženou § 8b odst. 2 uvedeného zákona překonat. Vyšší uložené pokuty odvolací orgán považoval za adekvátní s přihlédnutím k míře způsobeného následku, který je odvozen od závažnosti jednání vyplývajícího ze způsobu spáchání předmětného deliktu: Informace byla šířena prostřednictvím časopisu a v budoucnu tak bude kdykoli dohledatelná, poškozená byla nízkého věku a v ohled byl brán i charakter trestného činu, který na ní měl být spáchán, a bylo i zohledněno, že účastník řízení musí být z povahy věci v oblasti žurnalistiky a mediálního práva profesionálem, jelikož vydává řadu periodik; dále byl brán ohled na účel trestu v rámci správního trestání, který je rámcově totožný s účelem trestu v rámci trestání trestního. Proto odvolací orgán Úřadu rozhodl, že rozklad účastníka řízení se zamítá.

## ■ VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ

Poprvé během šestileté existence Odboru pro styk s veřejností se zastavil každoroční dynamický nárůst počtu podnětů a stížností na protiprávní jednání při zpracování osobních údajů. Úřad obdržel celkem 1 119 takovýchto podání a oproti roku 2010 tak došlo pouze k mírnému zvýšení jejich počtu o 8 %. Tato skutečnost měla pozitivní vliv na stabilizaci veškeré činnosti pracovníků odboru, tj. na prvotní právní posuzování obsahu podání z hlediska porušování povinností při zpracování osobních údajů, zodpovídání dotazů a žádostí o právní výklad i poskytování osobních konzultací správcům a zpracovatelům osobních údajů, jakož i fyzickým osobám majícím postavení subjektů údajů.

### Statistika stížností vyřízených v roce 2011

Celkem.....	1 119
z toho:	
předáno ke kontrole .....	197
předáno na zahájení řízení.....	70
postoupeno příslušným orgánům...	30
odloženo jako nedůvodné.....	822

Pokud jde o oblasti, do nichž obdržené stížnosti směřovaly, zaujímá dlouhodobě první místo provozování kamerových systémů (230 podání). Vlivem systematického přístupu a nekompromisního postoje Úřadu byl zaznamenán pozitivní posun v přístupu provozovatelů kamerových systémů k plnění zákonných povinností. Problematičtějšími místy sledovanými kamerami zůstávají prakticky pouze bydliště a pracoviště subjektů údajů. Úsilí Úřadu bude do budoucna soustředěno na bytové domy; sledování na pracovišti, primárně porušující zákoník práce, bude nadále řešeno ve spolupráci s inspektoráty práce. K ústavnímu právu každého občana chránit si vlastní majetek je nutné konstatovat, že na zpracování osobních údajů, které provádí fyzická osoba výlučně pro osobní potřebu, se zákon o ochraně osobních údajů nevztahuje. Úřad nemůže nahradit působnost věcně příslušných správních orgánů nebo orgánů činných v trestním řízení mj. proto, že není vybaven kompetencemi ke vstupu do soukromého obydlí a ke kontrole z něho pořízených kamerových záznamů. Kritériem možného uplatnění dozorové působnosti Úřadu tak může být jen překročení mezí osobní potřeby, např. zveřejnění pořízených kamerových záznamů.

Největší nárůst počtu podání byl v roce 2011 zaznamenán v oblasti moderních informačních apod. technologií, obecně označitelných jako prostředí internetu (220 podání). Internetový fenomén – sociální sítě – využívá stále více uživatelů ke sdílení informací, zážitků, fotografií a videí s ostatními uživateli. Jde o sítě typu [www.lide.cz](http://www.lide.cz) nebo [www.facebook.com](http://www.facebook.com), existuje jich však celá řada. Je nutné si uvědomit, že údaje publikované na těchto sítích a na internetu obecně se stávají dostupnými v lepším případě definovanému okruhu osob, častěji však není jejich okruh ničím omezen. Subjekt údajů ztrácí kontrolu nad těmito zveřejněnými informacemi, jež lze v digitalizované podobě jednoduše dál šířit a nakládat s nimi. Proto by si měl každý uživatel předem uvědomit možné následky jejich publikování, neboť zde dvojnásob platí, že ochráncem svých osobních údajů je především sám subjekt údajů.

Aktuálním problémem je publikování osobních údajů fyzické osoby na internetu jiným uživatelem, např. bývalým partnerem. Úřad zaznamenal výrazný vzestup i stížností tohoto typu. Vždy je v první řadě nutné zkoumat postavení osoby, která s osobními údaji nakládá bez souhlasu toho, kterého se týkají. Zpravidla se zde bude jednat o občanskoprávní spor a dotčená osoba má samozřejmě právo požadovat, aby tyto údaje byly odstraněny, případně kontaktovat s tímto cílem administrátora stránek.

S moderními technologiemi souvisí i další fenomén roku 2011, s nímž se Úřad setkal zejména v rámci konzultační činnosti, a to tzv. využití cloudu. Jedná se o poměrně složitý a strukturovaný problém, který je předmětem zájmu ochránců dat v celé Evropě. Základním principem je využití hardwaru poskytovatele za úplat. Jinými slovy, jde o nájem výpočetního výkonu nebo úložného prostoru poskytovatele, např. v době nejvyšší vytíženosti internetových stránek. Pokud je v cloudu nakládáno s osobními údaji, je nutné posoudit, zda dochází k jejich zpracování ve smyslu zákona o ochraně osobních údajů poskytovatelem či nikoli. Půjde-li o prosté uložení dat (osobních údajů) na úložné místo poskytovatele (jde o nejčastější využití cloudu), aniž by byl poskytovatel pověřen dalšími operacemi s osobními údaji, nebude se jednat o zpracování osobních údajů. Při využití zahraničního poskytovatele cloudu bude stěžejní i posouzení, zda dochází k předání osobních údajů ve smyslu § 27 zákona o ochraně osobních údajů. U prostého využití úložného prostoru nebude zpravidla k předání do zahraničí docházet. Nicméně je nutné upozornit, že správce osobních údajů je povinen dodržovat § 13 uvedeného zákona, který upravuje povinnosti při zabezpečení osobních údajů. Správce tak musí klást důraz na výběr věrohodného poskytovatele úložného místa či výpočetního výkonu a smluvně zajistit organizačně-technické parametry využití cloudu, včetně odpovídajících záruk zabezpečení údajů v cloudu uložených. V případě úniku údajů obsahujících osobní údaje leží odpovědnost za vzniklý stav na správci. Nelze tedy doporučit využívání cloudu v tzv. třetích zemích, jejichž právní systém neposkytuje záruky standardní ochrany osobních údajů.

Stabilně frekventované jsou i stížnosti směřující proti finančním institucím a poskytovatelům elektronických služeb (210), jejichž závažnost je dána mj. velkým objemem zpracovávaných osobních údajů řádově statisíců subjektů údajů. Nejčastějším porušením bylo pořizování kopií občanských průkazů bez právního titulu, respektive na základě souhlasu klienta zpracovaného do všeobecných obchodních podmínek. Podrobněji k této problematice viz kapitola Osobní údaje v kontextu všeobecných obchodních podmínek v této VZ.

Poslední homogenní oblast představovaly přijaté stížnosti (115) na postup obecních úřadů, přičemž nejfrekventovanějším obsahem bylo neoprávněné zveřejňování tazatelů podle zákona o svobodném přístupu k informacím a zveřejňování záznamů z jednání zastupitelstev. V souvislosti s medializací posledně jmenovaného problému bylo vyvoláno jednání s primátorem hl. m. Prahy s cílem systémového řešení respektujícího principy ochrany osobních údajů, k čemuž by měla přispět i spolupráce s věcně příslušným Ministerstvem vnitra ČR.

Úřad důsledně dodržoval přístup k anonymním podáním, deklarovaný ve výroční zprávě za rok 2010. Ze 42 podnětů podaných anonymně bylo pouze 6 předmětem dozorových kompetencí Úřadu, kdy se jednalo o závažné nedostatky při provozování kamerových systémů se záznamovým zařízením v bytových domech a při zpracování osobních údajů získaných v rámci sčítání lidu. Vzhledem k závažnosti obsahu bylo 9 podnětů podepsaných „zaměstnanci“, upozorňujících na sledování zaměstnavatelem na pracovišti, postoupeno věcně příslušným orgánům inspektorátu práce. Odloženo bylo zbývajících 27 podnětů s tím, že podávající osoba bude podrobněji informována o postupu Úřadu až tehdy, sdělí-li své adresní údaje v souladu se správním řádem, tedy jméno, příjmení, datum narození a adresu pro doručení listinné pošty.

Z poskytnutých osobních konzultací pro ilustraci uvádíme následující subjekty a řešené otázky:

Ministerstvo spravedlnosti	- možnosti vedení databáze žáků škol romského etnika;
Ministerstvo zahraničních věcí	- možnosti vedení databáze občanů ČR dlouhodobě pracujících v zahraničí;
Nejvyšší kontrolní úřad	- tvorba interní směrnice upravující ochranu zpracovávaných osobních a citlivých údajů;
Všeobecná zdravotní pojišťovna	- povinnosti správce osobních údajů podle § 13 zákona o ochraně osobních údajů, zejména tzv. logování přístupu do systémů automatizovaného zpracování osobních údajů;
Magistrát města Zlína	- postup v souvislosti s rozhodnutím Nejvyššího správního soudu k poskytování osobních údajů žadatelům podle zákona o svobodném přístupu k informacím;
TSP Data, a. s.	- možnost využití speciálního software umožňujícího čtení SMS zpráv odesílaných ze služebních mobilních telefonů.

K nejčastějším a současně nejzávažnějším porušením zákona správci nebo zpracovateli osobních údajů, na které bude soustředěna i nadále pozornost Úřadu, dlouhodobě patří: nepřijetí adekvátních opatření k zabezpečení zpracovávaných osobních údajů a jejich zpracování bez souhlasu subjektu údajů a bez právního titulu umožňujícího zpracovávat osobní údaje i bez tohoto souhlasu.

## POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

Úřad se ve správních řízeních, která vede, zabývá nejrůznější problematikou vztahující se k porušování zákona o ochraně osobních údajů, ale i zvláštních zákonů, zejména pak zákona o některých službách informační společnosti a zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel).

Ze správních řízení Úřad získává v každém roce poznatky, jejichž zveřejněním prostřednictvím výroční zprávy přispívá k odstranění některých problémů v následujících letech.

V minulém roce se jednalo zejména o problematiku zveřejňování (resp. obecně zpřístupňování) osobních údajů žadatelů o informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, a povinnost zpracovávat přesné osobní údaje vyjádřenou v § 5 odst. 1 písm. c) zákona o ochraně osobních údajů.

### ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PŘI PLNĚNÍ ZÁKONA O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

Úřad se stále častěji setkává s případy, kdy při plnění povinnosti stanovené § 5 odst. 3 zákona o svobodném přístupu k informacím, tj. povinnosti zveřejnit do 15 dnů od poskytnutí informací na žádost tyto informace způsobem umožňujícím dálkový přístup, dochází ke zveřejňování osobních údajů původních žadatelů o informace, a to v různém rozsahu. Některé povinné subjekty dokonce na svých webových stránkách informace zveřejňované na základě tohoto ustanovení podle osobních údajů žadatelů (u fyzických osob většinou v rozsahu příjmení, titul, příp. i jméno) třídí.

Přestože Úřad není kompetentní k obecnému výkladu zákona o svobodném přístupu k informacím, musel v rámci výkonu své dozorové činnosti posuzovat vztah tohoto právního předpisu a zákona o ochraně osobních údajů, přičemž došel k následujícím závěrům:

Povinné subjekty ve smyslu zákona o svobodném přístupu k informacím jsou nepochybně správci osobních údajů osob, které je požádaly o poskytnutí informací, ve smyslu § 4 písm. j) zákona o ochraně osobních údajů, přičemž nezbytné osobní údaje dotčených subjektů údajů zpracovávají ve smyslu § 4 písm. e) tohoto zákona za účelem vyřízení příslušné žádosti, neboť je shromažďují, třídí, používají, uchovávají, tedy s nimi provádějí operace tímto zákonem předpokládané. Jako správci osobních údajů jsou proto povinni dodržovat veškeré povinnosti zákonem o ochraně osobních údajů stanovené.

Osobním údajem je přitom podle § 4 písm. a) zákona o ochraně osobních údajů jakákoliv informace týkající se určeného nebo určitého subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže jej lze 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.

Subjekt údajů je dle názoru Úřadu identifikovatelný i tehdy, dojde-li ke zveřejnění informací v rozsahu jméno a příjmení, případně titul, a další údaje identifikující tuto osobu spojením s informacemi vyplývajícími z kontextu zveřejněného obsahu odpovědi na žádost, neboť je zjevné, že i v těchto případech je žadatel o informace na základě zveřejněných údajů určitelný. Za zvláštní skupinu identifikovatelných subjektů údajů je pak nutno považovat případy, kdy dochází ke zveřejnění příjmení, případně jména a titulu nebo titulů, jsou-li tyto údaje ve

svém spojení dostatečně specifické, přičemž tato specifičnost vyplývá z neobvyklosti příjmení, množství titulů atd.

Dále je nutné uvést, že podle ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů je správce povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje v mezích § 3 odst. 6 tohoto zákona, nebo pokud k tomu dal subjekt údajů předem souhlas. Účel zpracování osobních údajů žadatelů o informaci, k němuž byly tyto údaje shromážděny, tj. přijetí, zaevidování žádosti o informaci a její vyřízení, je přitom následným zveřejněním osobních údajů prostřednictvím webových stránek zjevně překročen.

Žádné ustanovení zákona o svobodném přístupu k informacím (ani žádný jiný právní předpis) neukládá, resp. neumožňuje povinným subjektům zveřejnit osobní údaje žadatelů o informace. Povinný subjekt má sice podle § 5 odst. 3 uvedeného zákona povinnost zveřejnit do 15 dnů od poskytnutí informací na žádost tyto informace způsobem umožňujícím dálkový přístup, nicméně účelem tohoto ustanovení jednoznačně není identifikovat jednotlivé žadatele, nýbrž umožnit ve veřejném zájmu široké veřejnosti seznámit se s informací, kterou žadatelé poskytli. To, že zveřejnění těchto osobních údajů není možné, lze přitom vyvodit též z ustanovení § 8a zákona o svobodném přístupu k informacím, podle kterého osobní údaje povinný subjekt poskytne jen v souladu s právními předpisy upravujícími jejich ochranu, tj. v souladu se zákonem o ochraně osobních údajů, který, jak výše uvedeno, podobný postup neumožňuje.

K výše uvedenému právnímu názoru Úřad odkazuje též na odbornou literaturu; srov. Furek, A. – Rothanzl, L.: Zákon o svobodném přístupu k informacím. Komentář. Praha: Linde, 2010. Str. 166. Bod 6.: *„... na druhou stranu je samozřejmě možné zveřejnit i celou zaslanou odpověď (např. naskenování dopisu), v tomto případě je ovšem nutné anonymizovat osobní údaje žadatele (vlastně se zde přiměřeně uplatní postup podle § 5 odst. 7, tzn. zveřejnění informace s výjimkami předvídanými zákonem o svobodném přístupu k informacím).“* Dále zde pod bodem 7 též: *„Požadavek na uvedení 'kontextu' poskytovaných informací lze ovšem splnit i tím, že povinný subjekt zveřejní celý text doručené žádosti (např. jejím naskenování). I v takovém případě je ovšem nutné ze žádosti odstranit veškeré chráněné údaje, nejčastěji identifikační údaje žadatele (opět se uplatní postup dle § 5 odst. 7).“*

Uvedené závěry obdobně platí též pro zveřejňování osobních údajů žadatelů ve výroční zprávě vydávané na základě § 5 odst. 1 písm. g) zákona o svobodném přístupu k informacím.

Na základě doručených stížností Úřad dále řešil případ, ve kterém vedoucí stavebního odboru poskytl osobní údaje žadatelů o informace podle zákona o svobodném přístupu k informacím starostovi jiné obce, který je následně zveřejnil v místním zpravodaji. Vedoucí stavebního úřadu zaslal při vyřizování žádosti odpovědi na vědomí starostovi v mylném domnění, že se jedná o účastníka řízení, a to společně s kopií žádostí.

Vzhledem ke skutečnosti, že osobním údajem je podle § 4 písm. a) zákona o ochraně osobních údajů jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, je za osobní údaje nutno považovat též obsah dopisu, který osoba napsala, jestliže je z něj jeho autor alespoň určitelný.

Podle ustanovení § 13 zákona o ochraně osobních údajů je správce povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům. Příslušná obec jako správce osobních údajů prostřednictvím svého zaměstnance (vedoucího stavebního úřadu) postupovala v rozporu s tímto ustanovením, neboť osobní údaje žadatelů o informace v rozsahu jméno, příjmení, bydliště a text žádosti poskytla třetí osobě, konkrétně starostovi obce, který nebyl k přístupu k těmto osobním údajům oprávněn.

## POVINNOST ZPRACOVÁVAT PŘESNÉ OSOBNÍ ÚDAJE

Podle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů je každý správce povinen zpracovávat pouze přesné osobní údaje, které získal v souladu se zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracovávané osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům.

V projednávaném případě účastník řízení shromáždil osobní údaje pana A. B. na základě telefonické objednávky svých služeb, a to v rozsahu jméno, příjmení, adresa, rodné číslo a číslo občanského průkazu. Následně při poskytování svých služeb ověřil správnost jména, příjmení, adresy a čísla občanského průkazu, a to při doručování prostřednictvím České pošty. Správnost rodného čísla žádným způsobem neověřoval. Rodné číslo, které pan A. B. uvedl při objednávce služeb, přitom nebylo jeho rodným číslem, ale bylo přiděleno panu X. Y. Poté co vznikl u zákazníka pana A. B. dluh z nezaplacené faktury, zanesl účastník řízení jeho osobní údaje včetně neověřeného rodného čísla (fakticky rodného čísla pana X. Y.) do registru dlužníků SOLUS. Následně se pan X. Y. obrátil na účastníka řízení, že je jeho rodné číslo evidováno ve spojení s dluhem u účastníka řízení v registru dlužníků. Toto jeho první upozornění účastník řízení nijak nevyřídil (pochybením vlastních zaměstnanců). Teprve na základě opakované žádosti o nápravu a poté, co byl pan X. Y. nucen podat trestní oznámení na zneužití svého rodného čísla, účastník řízení opravil údaj o rodném čísle u pana A. B. a informaci o dluhu spojenou s rodným číslem pana X. Y. v registru dlužníků SOLUS vymazal.

Ze zjištění Úřadu vyplývá, že účastník řízení v případě smluv uzavřených prostředky na dálku (call centrum) neověřuje správnost rodného čísla, které mu sdělí klient, a to dokonce ani v těch případech, kdy se v jeho zákaznické evidenci shodné rodné číslo vyskytuje u dvou osob s různým jménem, příjmením a adresou.

Podle § 4 písm. a) zákona o ochraně osobních údajů jsou jméno, příjmení, adresa a rodné číslo nepochybně osobními údaji, neboť se týkají identifikované osoby. Účastník řízení tyto osobní údaje shromažďuje za účelem uzavření a plnění smlouvy v závislosti na svém předmětu podnikání (poskytování telekomunikačních služeb), a je tedy správcem osobních údajů ve smyslu § 4 písm. j) uvedeného zákona.

Obecně lze dle správního orgánu konstatovat, že je akceptovatelné, pokud správce neověří veškeré osobní údaje svého zákazníka při uzavírání smluvního vztahu. Pokud ovšem vznikne ze smluvního vztahu na straně zákazníka prodlení s plněním (dluh) a správce osobních údajů v postavení věřitele musí přistoupit k vymáhání své pohledávky, je třeba, aby pohledávku vymáhal po skutečném dlužníkovi, a nikoliv po osobě, jejíž osobní údaje mu někdo v souvislosti s uzavřením smlouvy poskytl, ale jako správce si přesnost (správnost) těchto údajů nijak neověřil. V případě smluv uzavíraných prostředky na dálku je přitom riziko uvedení nesprávných osobních údajů ze strany zákazníka nepochybně vyšší právě s ohledem na zvolený komunikační prostředek, a s vědomím tohoto rizika proto musí správce k osobním údajům a jejich přesnosti přistupovat.

Dle správního orgánu je nepochybné, že účastník řízení je oprávněn shromažďovat a dále zpracovávat rodná čísla svých zákazníků [§ 63 odst. 3 písm. b) bod 3. zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)].



V dané věci účastník řízení ověřil prostřednictvím České pošty správnost údaje o jménu, příjmení, adrese a číslu občanského průkazu svého zákazníka pana A. B. U rodného čísla, které je svou povahou jedinečným identifikátorem fyzické osoby (občana České republiky), a tedy samo o sobě slouží ke ztotožnění osoby, ovšem účastník řízení jeho správnost žádným způsobem neověřil. Přesto s tímto údajem pracoval jako s přesným osobním údajem a v okamžiku, kdy mu vznikla vůči panu A. B. pohledávka z nezaplacené faktury, předal (zpracovával) do registru dlužníků SOLUS mimo jiné jako identifikační údaj dlužníka rodné číslo, které ovšem nebylo jeho.

Tento postup je přitom dle správního orgánu porušením povinnosti dle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů. V daném případě je třeba přihlížet právě ke shora uvedenému charakteru rodného čísla – jedinečného, státem garantovaného identifikátoru fyzické osoby. Zpracování nepřesného rodného čísla může mít za následek značný zásah do soukromí a práv nositele tohoto rodného čísla. V případě účastníka řízení je proto dle názoru správního orgánu porušením jeho povinností zpracovávat přesné osobní údaje, pokud předává neověřená rodná čísla do registru dlužníků. V tomto konkrétním případě dochází s ohledem na účel dlužnických registrů k vážnému zásahu do práv skutečných nositelů rodného čísla, kteří nemusejí být k účastníkovi řízení v žádném smluvním vztahu, resp. kteří nemají vůči účastníkovi řízení žádný dluh. Tento zásah je poté násoben skutečností, že to je právě nositel rodného čísla, který musí následně (mnohdy komplikovaně a po delší dobu) prokazovat, že předmětný záznam je v registru dlužníků uveden neoprávněně.

Správní orgán je tedy toho názoru, že v případě neověřených rodných čísel by účastník řízení v souladu s § 5 odst. 1 písm. c) zákona o ochraně osobních údajů neměl přinejmenším tento údaj zpracovávat způsobem, který by mohl znamenat zásah do práv nositele rodného čísla. Účastník řízení by proto do registru dlužníků měl v těchto případech předávat pouze identifikační údaje bez rodného čísla a rodné číslo pouze tam, kde ověřil, že se jedná o přesný osobní údaj (např. při osobní návštěvě klienta v prodejně účastníka řízení).

Porušení povinnosti podle § 5 odst. 1 písm. c) zákona o ochraně osobních údajů poté správní orgán spatřuje i v postupu účastníka řízení při řešení stížnosti pana X. Y. Skutečnost, že zaměstnanci účastníka řízení neodeslali jeho stížnost na zneužití jeho rodného čísla na příslušné oddělení, je nepochybně třeba přičítat k tíži účastníkovi řízení. Jako nesprávný ovšem správní orgán považuje i požadavek účastníka řízení na podání trestního oznámení ze strany pana X. Y., se kterým účastník řízení spojuje nápravu a řešení vzniklého stavu. Je nepochybné, že ke zjištění, že u pana A. B. je účastníkem řízení evidováno nesprávné rodné číslo, postačí ověření totožnosti pana X. Y. z jím předložených dokladů. Tedy, pokud účastník řízení z občanského průkazu ověří, jaké je rodné číslo pana X. Y., a následně ve svém systému zjistí, že stejné rodné číslo má evidováno u úplně jiné osoby, jedná se o dostatečné zjištění pro to, aby u něj vznikla pochybnost o přesnosti tohoto osobního údaje. Tato pochybnost poté musí vést vždy k blokování tohoto osobního údaje a ke sdělení této skutečnosti všem příjemcům nepřesného osobního údaje (v daném případě registru dlužníků SOLUS).

Takto ovšem účastník řízení nepostupoval, když požadoval po panu X. Y. podání trestního oznámení, a teprve na jeho základě provedl opravu nepřesného rodného čísla, resp. jeho vymazání. To ve svém důsledku vedlo k prodloužení doby, po kterou účastník řízení zpracovával nepřesný osobní údaj a zasahoval tím do práv pana X. Y.

## POZNATKY ZE SOUDNÍCH PŘEZKUMŮ

Úřad je účastníkem řady soudních sporů. Pokud jde o poznatky z rozhodovací praxe soudů za rok 2011, lze poukázat na dvě významné oblasti, na dvě významné otázky. První je dlouhodobě řešená problematika pravomocí Úřadu, které mu vyplývají z ustanovení § 21 zákona o ochraně osobních údajů. Druhou je pak otázka, zda se zákon o ochraně osobních údajů vztahuje i na advokáty při výkonu advokacie.

### 1. ÚŘADU PRAVOMOC VÉST NÁVRHOVÉ ŘÍZENÍ O ULOŽENÍ POVINNOSTI K ODSTRANĚNÍ ZÁVADNÉHO STAVU A PŘIZNÁNÍ NÁHRADY ZA ZPŮSOBENOU ÚJMU NEPŘÍSLUŠÍ

V řadě případů bylo po Úřadu požadováno, aby na návrh zahájil a vedl řízení, jehož předmětem by bylo v konečném důsledku uložení povinnosti k odstranění závadného stavu či přiznání náhrady imateriální újmy. Navrhovatelé se v tomto směru opírali o ustanovení § 21 zákona o ochraně osobních údajů. Původně sice Úřadu pravomoc vést taková řízení příslušela, byla mu však s nabytím účinnosti zákona č. 439/2004 Sb., kterým se mění zákon o ochraně osobních údajů, odňata.

Původní díkce § 21 a násl. zákona o ochraně osobních údajů subjektu údajů zakládala právo, pokud zjistí, že došlo k porušení povinností správcem nebo zpracovatelem osobních údajů, obrátit se na Úřad s žádostí o zajištění opatření k nápravě, tj. k učinění mocenského zásahu (rozhodnutí) do právní sféry subjektu práva příkazem něco konat, nekonat nebo strpět. Ustanovení § 21 odst. 2 dále zakotvovalo, že „došlo-li k porušení povinností správcem nebo zpracovatelem, má subjekt údajů právo požadovat, (a) aby se správce či zpracovatel zdržel takového jednání, odstranil takto vzniklý stav či poskytl na svoje náklady omluvu nebo jiné zadosti-učinění, (b) aby správce či zpracovatel provedl opravu nebo doplnění osobních údajů tak, aby byly pravdivé a přesné, (c) aby osobní údaje byly zablokovány nebo zlikvidovány, (d) zaplacení peněžité náhrady, jestliže tím bylo porušeno jeho právo na lidskou důstojnost, osobní čest, dobrou pověst či právo na ochranu jména“.

Ustanovení § 23 zákona o ochraně osobních údajů ohledně nápravy nemajetkové újmy pak stanovilo následující. „Jestliže osoba, která vykonává pro správce či zpracovatele činnosti na základě smlouvy, poruší uložené povinnosti, má subjekt údajů právo požadovat, (a) aby se zdržela takového jednání, odstranila takto vzniklý stav či poskytla na svoje náklady omluvu nebo jiné zadostiučinění, (b) aby zlikvidovala osobní údaje, které neoprávněně zpracovává, (c) aby zaplatila peněžitou náhradu újmy, která vznikla porušením jeho práva na lidskou důstojnost, osobní čest, dobrou pověst či práva na ochranu jména. Neposkytne-li tato osoba na svoje náklady omluvu nebo jiné zadostiučinění nebo nezaplatí peněžitou náhradu, je povinen za ni tuto povinnost splnit správce nebo zpracovatel. Poruší-li uložené povinnosti osoba, která je ke správci nebo zpracovateli v pracovním poměru, řídí se její odpovědnost zákoníkem práce.“

Zákonem č. 439/2004 Sb., kterým se mění zákon o ochraně osobních údajů, však bylo ustanovení § 21 zákona o ochraně osobních údajů změněno do současné podoby a spolu s tím byla zrušena i ustanovení § 22, § 23 a 24 zákona o ochraně osobních údajů. Důvodová zpráva k zákonu č. 439/2004 Sb. (Parlament ČR, Poslanecká sněmovna, volební období 2002–2006, tisk č. 508/0) obsahovala jasné vyjádření vůle zákonodárce v tom směru, že Úřadu byla, mimo

případy ukládání opatření k nápravě na základě § 40 zákona o ochraně osobních údajů, odejmuta pravomoc ukládat opatření k odstranění závadného stavu, stejně tak jako pravomoc rozhodovat o nemajetkové újmě způsobené neoprávněným zpracováním osobních údajů. Tyto pravomoci, tj. opatření k odstranění závadného stavu, jakož i k přiřknutí zaplacení peněžité náhrady, mají náležet napříště výlučně soudu. Úřadu tak od 1. ledna 2005 přísluší při zjištění porušení zákona o ochraně osobních údajů pravomoc postupovat toliko podle části I. hlavy VII. tohoto zákona, tj. při zjištění, že došlo ke spáchání správního deliktu (v širším smyslu), uložit pachateli pokutu, resp. při zjištění porušení zákona v kontrole v jejím rámci (v kontrolním protokolu) uložit opatření k nápravě na základě § 40 odst. 1 zákona o ochraně osobních údajů a následně postupovat podle jeho části I. hlavy VII.

K otázce pravomocí Úřadu vyplývajících z § 21 zákona o ochraně osobních údajů po 1. lednu 2005 se dlouhodobě zejména Nejvyšší správní soud stavěl poněkud rozpačitě, když nereflekoval obsah shora citované důvodové zprávy. Nicméně ve věci zn. 1 As 93/2009 došlo ke znatelnému posunu, když první senát Nejvyššího správního soudu usnesením zn. 1 As 93/2009-212 ze dne 27. ledna 2011 předložil rozšířenému senátu otázku, zda by nemělo dojít ke změně rozhodovací praxe Nejvyššího správního soudu, k jejímu narovnání s vůlí zákonodárce vyjádřenou v důvodové zprávě.

Z odůvodnění zmíněného usnesení není bez významu zmínit následující argumentaci prvního senátu Nejvyššího správního soudu: *„...je třeba považovat za klíčový výklad § 21 odst. 3 a 4 zákona č. 101/2000 Sb., ve znění zákona č. 439/2004 Sb. V případě, že by tato ustanovení upravovala tzv. návrhové řízení (tj. řízení zahajované na žádost), představovalo by rozhodnutí Úřadu, stejně jako jeho předsedy, zásah do právní sféry stěžovatele, a jednalo by se o rozhodnutí ve smyslu § 65 odst. 1 s.ř.s. Pokud by ovšem podání dle § 21 odst. 3 a 4 tohoto zákona adresované Úřadu bylo pouze podnětem pro zahájení řízení ex officio, nepředstavovalo by sdělení Úřadu o tom, že neshledal důvody pro zahájení řízení z moci úřední, zásah do právní sféry stěžovatele. Takový úkon by nebyl rozhodnutím ve smyslu § 65 odst. 1 s.ř.s. (...). První senát nesusouhlasí s názorem zaujatým druhým senátem (pozn. uvedeným v rozhodnutích zn. 2 Ans 8/2008-52, Ans 9/2008-55 a 2 Ans 10/2008-54), neboť je přesvědčen, že podání subjektu údajů adresované Úřadu na základě § 21 odst. 3 zákona č. 101/2000 Sb. je pouhým podnětem pro výkon dozоровé pravomoci Úřadu stanovené v § 29 tohoto zákona, jejíž uplatnění může vyústit v uložení nápravných opatření (...). Dle prvního senátu není podání dle § 21 odst. 3 uvedeného zákona žádostí, která by měla za následek zahájení správního řízení (...) slovo 'žádost' a 'požadovat' se používají v § 21 odst. 1 až 3 pouze pro vztah mezi subjektem údajů a zpracovatelem (správcem) údajů, nikoli pro vztah mezi subjektem údajů a Úřadem (...). Právní názor vyjádřený v rozsudku NSS č. 8 Ans 4/2006 – 68 je postaven na znění § 21 odst. 1 zákona č. 101/2000 Sb. před změnou provedenou zákonem č. 439/2004 Sb., dle něhož měl subjekt údajů právo obrátit se na žalovaného s žádostí o zajištění opatření k nápravě. Dle prvního senátu však zákon o ochraně osobních údajů, ve znění zákona č. 439/2004 Sb., již toto subjektivní veřejné právo jedinice (subjektu údajů) nezakotvuje, což ostatně vyplývá i z důvodové zprávy k zákonu č. 439/2004 Sb. Jedinec disponuje pouze právem obrátit se se svým podnětem na žalovaného. Právní úprava tedy nadále nepočítá se zahájením správního řízení podáním žádosti jednotlivce, plně se prosadil princip oficiality, kdy všechna správní řízení vedená žalovaným mohou být zahájena jen z moci úřední (zpravidla na základě podnětu či stížnosti jednotlivce).*

První senát se neztotožňuje s přístupem druhého senátu, který rozlišuje povahu podání subjektu údajů (tj. zda se jedná o žádost, či podnět) v závislosti na tom, jestli se subjekt údajů předtím, než se obrátil na žalovaného, domáhal nápravy přímo u zpracovatele či správce osobních

údajů. Toto rozlišování je dle prvního senátu umělé a není založeno na žádném rozumném podkladu. Jestliže § 21 odst. 3 zákona č. 101/2000 Sb. dává subjektu údajů, který se neúspěšně domáhal zjednáání nápravy přímo u zpracovatele či správce osobních údajů, oprávnění obrátit se na žalovaného, a ustanovení § 21 odst. 4 dodává, že podmínkou pro přístup k žalovanému není marné využití postupu dle § 21 odst. 1, je nelogické dovozovat, že zatímco v prvním případě má podání subjektu údajů učiněné vůči žalovanému povahu žádosti, zatímco v druhém případě se jedná pouze o podnět. Dle názoru prvního senátu upravuje § 21 odst. 3 a 4 jeden a týž procesní nástroj – právo dát podnět žalovanému k prošetření postupu zpracovatele a správce při nakládání s osobními údaji. Nejedná se o dva různé postupy, odst. 4 pouze doplňuje, že podmínkou postupu dle odst. 3 není vyčerpání možnosti domáhat se nápravy přímo u zpracovatele či správce osobních údajů dle odst. 1 (...).

Na tomto místě lze učinit dílčí závěr, dle něhož § 29 ani § 21 odst. 3 či 4 nezakládají žalovanému pravomoc vést správní řízení o žádostech subjektů údajů, jimiž by se domáhali uložení nápravných opatření ze strany žalovaného zpracovatelům či správcům osobních údajů. Opačný závěr by se mohl dle prvního senátu dostat do rozporu s čl. 2 odst. 2 Listiny základních práv a svobod, dle něhož lze státní moc uplatňovat jen v případech a v mezích stanovených zákonem, a to způsobem, který zákon stanoví (shodně čl. 2 odst. 3 Ústavy). Pokud tedy subjekt údajů neuspěje u žalovaného se svým podnětem, může se ochrany svých práv domoci žalobou na ochranu osobnosti dle § 13 obč. zák., kterýžto prostředek je plně v dispozici subjektu údajů. Projednání nároku subjektu údajů na náhradu imateriální újmy a náhradu škody pak zákon o ochraně osobních údajů svěřuje do pravomoci soudů v občanském soudním řízení (§ 21 odst. 5 a § 25), což ostatně potvrdil i zvláštní senát zřízený dle zákona č. 131/2002 Sb. v usnesení ze dne 24. 2. 2010, čj. Konf 56/2009 – 7(...).

První senát navrhuje, aby rozšířený senát zaujal právní názor, že podání subjektu údajů dle § 21 odst. 3 a 4 zákona č. 101/2000 Sb., ve znění zákona č. 439/2004 Sb., jímž žádá Úřad pro ochranu osobních údajů o uložení opatření k nápravě zpracovateli či správci osobních údajů, nemá za následek zahájení správního řízení. Jedná se toliko o podnět k zahájení řízení (či jiného postupu) z moci úřední. Sdělení žalovaného adresované stěžovateli, že jeho podání nemá za následek zahájení správního řízení a že správní orgán nehodlá zahájit řízení z moci úřední, není rozhodnutím ve smyslu § 65 s. ř. s.“

Nejvyšší správní soud se tak svým rozhodnutím přiklonil k názoru, který zaujal zvláštní senát zřízený podle zákona č. 131/2000 Sb. např. ve věci zn. Konf 56/2009, v níž uvedl: „Úřad je nyní oprávněn dle § 29 zákona o ochraně osobních údajů mimo jiné provádět dozor nad dodržováním povinností stanovených zákonem o ochraně osobních údajů, přijímat podněty a stížnosti na porušení povinností stanovených zákonem, projednávat přestupky a jiné správní delikty a udělovat pokuty. Není však oprávněn rozhodovat o výši náhrady škody za porušení povinností zpracovatele osobních údajů, nemůže rozhodovat o náhradě za nemajetkovou újmu. Tyto pravomoci přísluší soudům.“

Právě uvedený názor byl pak konkretizován zvláštním senátem zřízeným podle zákona č. 131/2002 Sb., o rozhodování některých kompetenčních sporů, ve věci zn. Konf 11/2011: „Citované ustanovení (§ 21 zákona o ochraně osobních údajů) reguluje podmínky práva na přístup k osobním údajům tehdy, pokud subjekt údajů zjistí nebo se domnívá, že správce 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 (srov. stanovisko Úřadu pro ochranu osobních údajů č. 2/2007 – Zdravotnická dokumentace a ochrana osobních údajů z pohledu nové právní úpravy, dostupné na [www.uoou.cz](http://www.uoou.cz)). Předmětné ustanovení však v žádném

případě (a to ani ve znění před novelizací provedenou zákonem č. 439/2004 Sb.) nezakládá pravomoc Úřadu rozhodovat ve sporech mezi subjektem údajů a správcem o poskytnutí kopií zpracovávané dokumentace, případně určit, zda informace mají být subjektu údajů na jeho žádost zpřístupněny. Z ustanovení § 29 zákona vyplývá, že pravomoci Úřadu na úseku ochrany osobních údajů jsou spíše kontrolní a dozorové. Ustanovení § 21 zákona tak míří spíše na situace, kdy subjekt údajů brojí proti způsobu či rozsahu nakládání s jeho osobními údaji správcem a obrací se na Úřad s podnětem či stížností na porušení zákona [§ 29 odst. 1 písm. c) zákona]; o takovou situaci se ale v posuzovaném případě nejedná (...).

Odkaz okresního soudu na usnesení zvláštního senátu č. j. Konf 11/2003 – 12 a č. j. Konf 15/2003 – 24 je v posuzované věci nepřipadný. Ve zmiňovaných usneseních se zvláštní senát vyjadřoval k otázce, který orgán je příslušný rozhodnout o návrhu subjektu údajů na zdržení se jednání porušujícího povinnosti správce při zpracování osobních údajů. V předmětné věci mezi žalobkyní a žalovanou je spor veden o vydání kopie dokumentace. Předmět sporu je tedy odlišný než ve shora citovaných usneseních, proto nelze ze závěrů tam vyslovených v řešené věci vycházet. Nadto lze poznamenat, že v předmětných usneseních zvláštní senát aplikoval znění zákona o ochraně osobních údajů účinné ještě před novelou provedenou zákonem č. 439/2004 Sb., z něhož v posuzovaném případě nelze vycházet, neboť zvláštní senát rozhoduje o kompetenčním sporu podle skutkového a právního stavu ke dni svého rozhodnutí (srov. usnesení zvláštního senátu ze dne 24. 11. 2004, č. j. Konf 3/2003 – 18, publikované pod č. 485/2005 Sb. NSS, [www.nssoud.cz](http://www.nssoud.cz)).

Z podané žaloby zřetelně vyplývá, že žalobkyně se nedomáhá postupu podle § 21 zákona o ochraně osobních údajů (nestěžuje si na postup správce osobních údajů); nejde jí o výkon pravomoci kontrolní či dozorové nad správcem údajů, jímž je žalovaná. Žalobkyně požaduje po žalované vydání kopií v žalobě blíže specifikovaných dokumentů, o čemž přísluší rozhodovat soudu.“

## 2. ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ SE NA ADVOKÁTY VZTAHUJE

Další z dlouhodobě diskutovaných otázek v oblasti ochrany osobních údajů je, resp. bylo, zda se zákon o ochraně osobních údajů vztahuje na advokáty při výkonu advokacie, či nikoli. Jednoznačnou odpověď na ni dal Nejvyšší správní soud mj. ve věci zn. 1 As 13/2011.

Nejvyšší správní soud konkrétně uvedl: „Stěžovatel tvrdí, že se na činnost advokáta vůbec nevztahuje zákon o ochraně osobních údajů, jelikož účel shromažďování a zpracování osobních údajů určuje výhradně klient a advokát je vázán mlčenlivostí.

K tomu soud konstatuje, že z textu zákona o ochraně osobních údajů takovou výlukou přímo dovodit nelze. Působnost tohoto zákona je totiž koncipována velmi široce a vztahuje se – kromě orgánů veřejné moci – i na fyzické a právnické osoby, které zpracovávají osobní údaje (§ 3 odst. 1), pokud se samozřejmě nejedná o zpracování výlučně pro osobní potřebu fyzické osoby, případně nejde jen o nahodilé shromažďování osobních údajů. Zákon tedy osobu advokáta ze své působnosti nevylučuje, jelikož se jedná o fyzickou osobu a při výkonu svojí profese osobní údaje nezpracovává výlučně pro svoji osobní potřebu. V řadě, a možná dokonce ve většině případů činnost advokátů představuje ‘nahodilé’, nikoliv systematické, shromažďování osobních údajů, a tady se na ně skutečně citovaný zákon nevztahuje. Stejně tak ale existují případy, kdy advokáti zpracovávají osobní údaje systematicky, protože pokud by tak nečinili, nehájili by dostatečně zájmy svého klienta. Zdejší soud má za to, že zpracovávání databáze dlužníků Dopravního podniku

představuje typický příklad zpracovávání osobních údajů, spadající do působnosti uvedeného zákona (...).

Současně je ovšem třeba uvést, že z § 18 odst. 1 písm. b) cit. zákona plyne, že se na správce osobních údajů nevztahuje oznamovací povinnost v případě zpracování uloženého zvláštním zákonem nebo jestliže je takových osobních údajů třeba k uplatnění práv a povinností vyplývajících ze zvláštního zákona. Zdejší soud zastává ve shodě se žalovaným názor, že tato výjimka z oznamovací povinnosti se vztahuje i na advokáty při výkonu jejich profese. Z povahy věci je totiž zřejmé, že advokát nezpracovává osobní údaje samoúčelně, nýbrž právě z důvodu uplatnění práv a povinností za svého klienta a zmíněná oznamovací povinnost se ho proto netýká.

Nejvyšší správní soud tak činí dílčí závěr, že ze zákonné úpravy nelze dovodit výluky působnosti zákona o ochraně osobních údajů na profesi advokátů, nýbrž toliko výjimku ze zmíněné oznamovací povinnosti. Je totiž třeba mít na zřeteli, že advokátní profese není tak specifická či ojedinelá, jak se snaží dovodit stěžovatel. Lze dokonce říci, že povinnost mlčenlivosti, resp. přinejmenším diskrétnosti, je typická i pro všechny ostatní profese, v nichž se pracuje s osobními údaji. Týká se činností vykonávaných ve zdravotnictví, v ozbrojených složkách, daňovém poradenství, psychologů, školství i činnosti kněžské. Stěžovatel se proto mylí, pokud má za to, že koncepce zákona o ochraně osobních údajů je vytvářena tak, že jeho působnost může implicitně, pouze poukazem na povahu určité činnosti, zcela vyloučit jiný zákon. Jeho působnost je totiž definována obecně s tím, že pouze v určitých případech se nepoužijí některá ustanovení tohoto zákona, nikoliv zákon celý (viz § 3 odst. 6 zákona o ochraně osobních údajů).

Stěžovatel v této souvislosti poukazuje i na stanovisko představenstva ČAK ze dne 10. října 2000, z něhož plyne, že 'zákon č. 101/2000 Sb. se na výkon advokacie, tj. poskytování právních služeb advokáty, nevztahuje. K tomuto závěru dospělo v podstatě ze shodných důvodů, které jsou uváděny v článku JUDr. S., uveřejněném v č. 10/2000 Bulletinu advokacie.' K tomu je třeba zdůraznit, že toto stanovisko není pro řešení právních otázek v současnosti projednávaných Nejvyšším správním soudem relevantní, jelikož se jedná pouze o vyjádření názoru orgánu ČAK ohledně možnosti aplikace určitých právních předpisů na činnost advokátů, nikoli o obecně závazný právní předpis, ze kterého by advokátům vyplývala práva či povinnosti (...).

Soud má za to, že stěžovatel ve své argumentaci příliš klade důraz na ochranu práv a oprávněných zájmů svého klienta a zcela opomíjí, že pokyny klienta není vázán, pokud jsou protiprávní. Zakládá totiž svoji argumentaci na tvrzení, že je vázán profesní mlčenlivostí a naznačuje, že není vyloučeno, že předmětné tiskové prohlášení vydal na základě pokynu klienta, a proto za ně nemůže být sankcionován. Zde soudu nezbyvá než připomenout, že takto vedená argumentace by mohla vést k absurdním důsledkům, kdy by např. advokát po spáchání trestného činu odmítal za něj nést odpovědnost poukazem na profesní mlčenlivost. Soud má za to, že zákonná úprava je v tomto směru jednoznačná: ani prosazování zájmů klienta a sledování jeho pokynů nesmí vést k vědomému porušování právního řádu. Pokud by tomu tak nebylo, nic by advokátovi nemohlo zabránit např. v umlčení svědka, vypovídajícího proti jeho klientovi v trestním řízení.“

## REGISTRACE

Podobně jako v minulých letech tak i v roce 2011 pokračoval trend nárůstu počtu registračních oznámení. V roce 2011 Úřad přijal 4421 oznámení o zpracování podle § 16 zákona o ochraně osobních údajů. Vedle posuzování přijatých registračních oznámení vydává Úřad rozhodnutí o zrušení registrace podle § 17a odst. 2 zákona o ochraně osobních údajů. V roce 2011 bylo zrušeno celkem 49 zpracování na žádost správce, nejčastěji z důvodů zániku či sloučení společnosti, zrušení podnikatelské činnosti nebo ukončení zpracování osobních údajů. Informace o zrušených registracích Úřad zveřejňuje ve Věstníku.

V souvislosti s narůstajícím počtem registračních oznámení narůstá i počet oznamovaných změn či doplnění již zaregistrovaných zpracování. Změny se nejčastěji týkají adresných údajů, doplnění rozsahu zpracovávaných osobních údajů, kategorií subjektu údajů, doplnění účelů zpracování. 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 případě, že oznámení neobsahuje všechny náležitosti, je správci zaslána výzva k doplnění informací.

V roce 2011 Úřad zahájil celkem 953 řízení o registraci podle § 16 odst. 4 zákona. Z velké části se řízení týkala zpracování prostřednictvím kamerových systémů, zpracování citlivých údajů, zpracování osobních údajů bez právního titulu. V rámci registračních řízení správce velmi často přistoupí 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 kamer). V případě, že se tak nestane a vznikne důvodná obava, že by při zpracování osobních údajů v podobě, jak bylo oznámeno, mohlo dojít k porušení zákona o ochraně osobních údajů, je zahájeno předběžné řízení podle § 17 zákona o ochraně osobních údajů. V roce 2011 bylo zahájeno správní řízení podle § 17 zákona u 91 podaných oznámení o zpracování. Z toho u 67 oznámení došlo k jejich úpravě, doplnění nebo zdůvodnění oznamovatelem, což vedlo k následné registraci, v 5 případech oznamovatel odstoupil od registrace a v 5 případech nebylo zpracování osobních údajů povoleno. U 14 oznámení dosud řízení nebylo ukončeno.

Registrační povinnost se vztahuje pouze na správce osobních údajů, nikoliv na zpracovatele či jiné subjekty, které se na zpracování podílejí. Je tedy nutné, aby si subjekt oznamující zpracování vždy předem ujasnil, zda se skutečně nachází v pozici správce osobních údajů. Je třeba přiznat, že rozlišení role správce a zpracovatele údajů se stává v praxi stále složitější a veřejnost si v tomto směru často neví rady. Tento stav může být zapříčiněn rostoucí složitostí prostředí, v němž jsou tyto pojmy používány, a rostoucí tendencí k organizační diferenciaci v soukromém i veřejném sektoru.

V rámci vyřizování registračních oznámení se v roce 2011 vyskytlo několik případů zpracování – monitorování služebních vozidel satelitním sledovacím zařízením (GPS). Data jsou zpracovávána za účelem automatického generování knihy jízd, k lokalizaci polohy vozidla za účelem optimalizace organizace práce, k využití pro statistické účely. Otázka, která je často správci kladena, souvisí s oznamovací povinností podle § 16 zákona o ochraně osobních údajů, resp. s možností aplikovat výjimku z oznamovací povinnosti podle § 18 odst. 1 písm. b) tohoto zákona. Při rozhodování je vždy nutné vycházet z účelu zpracování. Pokud by účelem zpracování

byla ochrana autoparku, ekonomika provozu a zpracování podkladů pro knihu jízd, pak lze konstatovat, že takové zpracování osobních údajů oznamovací povinnosti nepodléhá, neboť slouží k výkonu práv a povinností zaměstnavatele vyplývajících ze zvláštního zákona.

V souvislosti s rychlým technologickým vývojem zaznamenal Úřad i nové způsoby shromažďování osobních údajů, které jsou stále propracovanější a lze je hůře odhalit. Jedná se např. o rostoucí využívání geolokačních zařízení umožňujících snadněji zjistit polohu určité osoby jednoduše díky jejímu mobilnímu zařízení.

Úřad zaznamenal v roce 2011 zvýšenou tendenci monitorovat prostřednictvím speciálního počítačového systému, jakým způsobem zaměstnanci využívají výpočetní techniku na svém pracovišti. Takové zpracování spočívá ve sběru informací o pohybu zaměstnanců na internetu (jaké konkrétní webové stránky navštěvuje a po jakou dobu, způsob využívání různých softwarových programů apod.). Jako účel takového zpracování je nejčastěji uváděna právně neopodstatnitelná kontrola efektivity využívání pracovní doby, zjišťování znalosti a orientace zaměstnance na internetu a monitorování jednotlivých úkonů prováděných na firemním počítači.

Nadále jsou Úřadu oznamována zpracování, která registrační povinnosti nepodléhají. Zejména se to týká zpracování zaměstnaneckých údajů pro účely vedení personální a mzdové agendy v rozsahu stanoveném zvláštními právními předpisy. Výjimka z registrační povinnosti se, kromě zpracování pro vedení personální a mzdové agendy, týká rovněž vedení docházky zaměstnanců.

Ve zvýšené míře byl v roce 2011 Úřadu oznamován úmysl samosprávných orgánů obce zpracovávat osobní údaje prostřednictvím pořizování zvukových či obrazových záznamů z jednání zastupitelstva obcí a jejich následné umístění na webové stránky (blíže viz kapitola Zpřístupňování videozáznamu z jednání zastupitelstva v této VZ).

Nejčastějším typem oznamovaných zpracování byla podobně jako v minulých letech zpracování prostřednictvím kamerových systémů (36 % z celkového množství podaných oznámení). V registru zpracování osobních údajů bylo zapsáno do dnešní doby celkem 1586 subjektů, které zpracovávají osobní údaje kamerovými systémy. (Podrobnější informace o problematice ochrany osobních údajů za využití kamerových systémů viz kapitola Zpracování osobních údajů prostřednictvím kamerových systémů v této VZ.)

Velké procento oznamovaných zpracování osobních údajů trvale souvisí s využíváním věrnostních karet. Účelem zpracování je obecně možnost čerpání různých slev a výhod na nákupy prováděné držitelem karty, který uvede své jméno, příjmení, případně další kontaktní údaje, pokud má zájem dostávat sdělení o marketingových akcích.

Další rozsáhlý okruh oznamovaných zpracování souvisel s provozováním internetového obchodu. V tomto případě se však nejedná o rizikové zpracování z pohledu zásahu do práv a svobod subjektu údajů. Okruh zpracovávaných údajů se omezuje výlučně na jméno, adresu, telefonní číslo, e-mail, čili údaje nezbytné k vyřízení objednávky včetně dodávky zboží zákazníkovi, případně pro využití k další komunikaci se zákazníky po vyřízení jejich objednávky, např. k zasílání obchodních sdělení, k marketingovým účelům apod.

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



## ■ PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Na základě směrnice 95/46/ES jsou členské státy povinny zajistit, aby k předávání osobních údajů do třetích zemí docházelo, pouze pokud dotyčná třetí země zajišťuje odpovídající úroveň ochrany a pokud před předáním údajů budou dodrženy právní předpisy členských států provádějící ostatní ustanovení této směrnice. Zásada odpovídající úrovně ochrany vyjádřená v článku 25 odst. 2 směrnice 95/46/ES je ve vztahu k předávání zcela zásadní. Stále ovšem není výjimkou, že na straně správců předávajících osobní údaje do třetích zemí dochází k nepochopení významu pojmu „přiměřená úroveň ochrany osobních údajů“. Odpovídající úroveň ochrany mohou zajišťovat buď obecné právní předpisy, nebo odvětvová pravidla platná v zemi, ve které je příjemce usazen, nebo tuto ochranu může garantovat sám správce prostřednictvím vhodných ochranných opatření – např. použitím standardních smluvních doložek nebo přijetím závazných podnikových pravidel.

Přehled o pravidlech předávání osobních údajů do zahraničí je trvale dostupný na webové adrese Úřadu ([www.uoou.cz/Předávání osobních údajů do zahraničí/](http://www.uoou.cz/Předávání_osobních_údajů_do_zahraníčí/)).

Podobně jako v minulých letech se nejvíce předání osobních údajů uskutečnilo do USA. Z hlediska ochrany osobních údajů jsou USA považovány za třetí zemi nezajišťující přiměřenou úroveň ochrany. USA přistupují k otázkám ochrany soukromí odlišně než EU – uplatňují odvětvový přístup, který je založen na kombinaci právních předpisů, nařízení a samoregulace. Pro bezpečné předání byl smlouvou mezi USA a EU zaveden tzv. program „Safe Harbour“. Předmětem smlouvy je závazek EU umožnit volné předávání osobních údajů ze zemí EU do USA, pokud se jedná o společnosti, které jsou zařazeny na tzv. „Safe Harbour List“.

Již v minulosti bylo provádění zásad „bezpečného přístavu“ podrobena ostré kritice ze strany Evropské komise, i když v tomto směru došlo v poslední době k určitému zlepšení. Úřad správcům (vývozcům údajů) doporučuje před samotným předáním ověřit, zda je certifikace příslušné společnosti stále platná, zda a jakým způsobem jsou fyzické osoby informovány o vnitřních postupech pro vyřizování stížností, případně zda jsou „privacy policy“ příslušné společnosti veřejně přístupné např. prostřednictvím webových stránek. V případech zjištěných nedostatků při uplatňování principů „bezpečného přístavu“ je namísto o tom informovat Úřad.

Nejčastějším titulem, na jehož základě bylo povolení vydáno, bylo podobně jako v minulých letech ustanovení § 27 odst. 3 písm. a) zákona o ochraně osobních údajů, tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů. Při aplikaci této výjimky je nutné, aby správce osobních údajů předložil Úřadu znění souhlasu, ze kterého musí být jasně zřejmé, do jakých zemí dává subjekt údajů souhlas s předáváním a kdo bude jejich příjemcem. Ze znění souhlasu musí být rovněž patrné, že subjekt údajů je srozuměn s tím, že země, do kterých budou jeho osobní údaje předány, neposkytují přiměřenou úroveň ochrany osobních údajů. Dále z něj musí být zřejmé, v jakém rozsahu budou osobní údaje předány, pro jaký konkrétní účel a na jakou dobu jej subjekt údajů dává.

V rámci početných konzultací se častěji objevil problém předání výsledků zpracování osobních údajů pro účely klinických studií hodnotících účinnost a bezpečnost nově vyvíjených léků. Klinické studie jsou prováděny mj. na souhlasících pacientech v České republice, přičemž výsledky těchto studií jsou předávány zadavatelům, farmaceutickým korporacím, zpravidla do USA.

Za předpokladu, že do USA či do jiné třetí země budou předány výsledky klinických studií ve formě kódovaných dat bez kódovacího klíče umožňujícího přiřazení daných dat konkrétní osobě, a bude prakticky vyloučeno, aby zde byla data přiřazena ke konkrétní osobě, se lze přiklonit k názoru, že takto zakódovaná data bez kódovacího klíče ztrácejí u svého příjemce ve třetí zemi charakter osobních údajů. Jinými slovy lze taková data považovat ve třetí zemi za anonymizované údaje. Tento názor vychází ze Stanoviska Pracovní skupiny pro ochranu osobních údajů zřízené podle čl. 29 Směrnice 95/46/ES č. 4/2007 k pojmu osobní údaje (WP 136).

# Legislativní činnost

Rok 2011 přinesl jak dílčí úpravy působnosti, tak významnou novou kompetenci Úřadu, neboť byl vydán zákon, kterým se současně mění tři zákony týkající se oblasti elektronických komunikací, ochrany osobních údajů a služeb informační společnosti. Novela zavedla do procesů ochrany osobních údajů následující zásadní změny a k tomu upravuje související kompetence Úřadu:

V zákonu o elektronických komunikacích byl v souladu s právem EU definován nový nástroj ochrany osobních údajů a soukromí. Poskytovatelům služeb v elektronických komunikacích výslovně stanovil povinnost řešit případy porušení ochrany osobních údajů (tzv. data breaches). Není-li odpovídajícím způsobem a včas řešeno porušení ochrany osobních údajů, mohou být účastníkům služeb způsobeny značné ekonomické ztráty nebo škoda, může dojít například ke krádeži nebo podvodu (zneužití identity), významnému společenskému ponížení nebo poškození pověsti. Jakmile operátor zaznamená, že k porušení ochrany osobních údajů došlo, měl by přijmout adekvátní opatření a incident oznámit Úřadu. Ve zvlášť závažných případech musejí být přímo vyzooměni ohrožení účastníci, aby mohli učinit vlastní nezbytná opatření.

Aby porušení ochrany osobních údajů bylo řešeno efektivně a vůči dotčeným osobám korektně, může do budoucna Úřad stanovovat formát a podmínky oznámení porušení ochrany. Vzhledem k tomu, že se jedná o nové regulační opatření se zásadním dopadem na chování operátorů, které by mělo podpořit důvěru a bezpečnost účastníků a uživatelů služeb elektronických komunikací, bude Úřad své další kroky činit v návaznosti na jednání se sdruženími podnikatelů v oblasti elektronických komunikací a s příslušnými úřady, Českým telekomunikačním úřadem a Ministerstvem průmyslu a obchodu.

Zákon o některých službách informační společnosti umožní Úřadu od roku 2012 vykonávat dozor nad šířením obchodních sdělení podle zákona o ochraně osobních údajů a v souladu s ním uplatňovat procesní postupy uzpůsobené pro kontrolu zpracování osobních údajů v oblasti elektronických komunikací a automatizovaného zpracovávání dat. Dosud byl Úřad nucen postupovat podle zastaralého zákona o státní kontrole.

Dále se systém dozoru nad obchodními sděleními a mechanismus ukládání pokut za šíření nevyžádaných obchodních sdělení nastavuje takovým způsobem, aby byl možný účinný postih šířitelů hromadných a opakovaných sdělení. Naproti tomu ojedinělé případy zaslání nevyžádaných obchodních sdělení bude Úřad do budoucna řešit nikoliv přímo represivními, ale nápravnými a doporučujícími prostředky, případné odpovědnostní a odškodňovací nároky pak v takových případech přísluší rozhodovat soudům. K uvedeným opatřením se jednoznačněji upravuje definice obchodního sdělení, což by v souhrnu mělo pomoci omezit množství nevyžádaných reklamních e-mailů šířených na internetu tuzemskými subjekty.

V zákoně o ochraně osobních údajů se citovanou novelou narovnalá nejasná úprava zpracování podnětů a stížností, která přisuzovala Úřadu kompetenci k projednávání široké řady soukromoprávních sporů a žádostí o odškodnění v oblasti ochrany soukromí, namísto zákonného soudu. Úprava nemění nic na tradiční a klíčové příslušnosti Úřadu k prověření stížností občanů v případech podezření z neoprávněného zpracování či neshod se správcem ohledně požadované nápravy zpracování údajů.

K doplnění zákona o elektronických komunikacích se dále nově definuje blokování osobních údajů, které lze využít jako nápravné a bezpečnostní opatření v případech porušení ochrany osobních údajů.

Rok 2011 byl ve znamení mimořádné legislativní aktivity vlády. Úřad se vyjadřoval k řadě právních předpisů. „Legislativní smršť“ doprovázející zejména zdravotní a sociální reformu však nebyla vždy provedena standardním způsobem. Nejenže řada materiálů týkající se zpracování dat občanů a jejich uchovávání v registrech postrádala v připomínkovém řízení alespoň elementární vyhodnocení rizik ochrany a zabezpečení osobních údajů, ale mnoho připomínek s Úřadem nebylo také ani projednáno. S přihlédnutím k této zkušenosti předložil předseda Úřadu návrh, aby v procesu přípravy zákonů byla v budoucnu řádně zohledňována nezbytná pravidla ochrany osobních údajů. Posouzení dopadů legislativních opatření do soukromí jednotlivce (Privacy Impact Assessment – PIA) přispívá nejen k posílení iniciativy a svobody občanů, ale také zásadním způsobem garantuje efektivní výkon veřejné správy, neboť mezi základní náležitosti procesů PIA patří řádné vyhodnocení prospěšnosti dosavadních přístupů a posouzení potřebnosti nových metod zpracování dat zaváděných státem, což ve svém souhrnu vede k efektivnějšímu nakládání s veřejnými prostředky. Tato iniciativa Úřadu byla následně podpořena rozhodnutím místopředsedkyně vlády Karolíny Peake o tom, že parametry vyhodnocení dopadů do soukromí a souladu s pravidly ochrany osobních údajů by měly být v nejbližší době zakomponovány do legislativních pravidel vlády. Tím se identifikace možných problémů, nejasností i novinek zpracování osobních údajů stane povinnou součástí věcných záměrů a odůvodnění návrhů zákonů předkládaných ministerstvy do připomínkového řízení. Současně bude dán patřičný prostor konzultačním kapacitám Úřadu, který bohužel dnes často nahrazuje práci věcně příslušných ministerstev a musí posuzovat téměř hotové návrhy zákonů až v závěru legislativního procesu, aniž byl včas a předem se záměry a pracemi vládních úřadů seznámen a aniž získal jakékoliv vyjádření gestorů správnosti navrhovaného zpracování dat či registru.

V případě zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), který nabyl platnosti 8. prosince 2011, upravující mj. národní zdravotnický informační systém, byl předseda Úřadu ministrem zdravotnictví osloven a přizván k budoucí spolupráci až po připomínkovém řízení a schválení návrhu zákona.

U návrhu používání sociální karty nebyly podněty Úřadu prvně zohledněny vůbec, následně zpracovány částečně. Přetrvávala však nejasnost ohledně dalších účelů využití sociální karty,

zejména pokud bude kartou multifunkční, sloužící např. i osobám se zdravotním postižením, což dosud znemožňovalo vyjasnit detaily souvisejících zpracování osobních údajů.

V případě „protikorupční“ novely zákona o rozpočtových pravidlech shledával Úřad, že zákonem zaváděná „transparentnost za každou cenu“ je v rozporu s právem EU a příslušnou judikaturou. Proto se předseda Úřadu poté, co k upozorněním Úřadu nebylo přihlédnuto, obrátil na Poslaneckou sněmovnu dopisem zpravodaji sněmovního tisku této novely.

Šťastnější byla spolupráce Úřadu s ministerstvem spravedlnosti na rekonstrukci soukromého práva. Úřad přesvědčil zpracovatele osnovy zákoníku o nesprávnosti ustanovení, které by vytvářelo z mlčení občanů vstupujících do označeného kamerovaného prostoru „automatický“ souhlas se zpracováním osobních údajů při pořizování kamerového záznamu, namísto existující, běžné a spravedlivé právní konstrukce, že provoz kamerového systému musí být účelný a odůvodnitelný jasně existujícími zájmy na ochraně zákonem chráněných hodnot. Z návrhu občanského zákoníku byl navrhovaný text vypuštěn.

Při spolupráci s ministerstvem vnitra a v rámci práce nad vyhodnocením dopadů zákona č. 106/1999 Sb., o svobodném přístupu k informacím, Úřad opakovaně upozornil na problematičnost zveřejňování dokumentů na internetu. K tomuto zveřejňování dochází bez pravidel zabraňujících nedovoleným formám automatizovaného zpracování údajů, např. trasování, profilování či sběru pro jiné účely využití (tj. často zneužití) osobních údajů. Toto zveřejňování však má, namísto výčtu osobních údajů jednotlivců (jichž se týká), obsahovat pouze odkaz na úřední agendu, kde lze plné osobní údaje získat. Pokud je skutečně účelné identitu jednotlivce zpřístupňovat nejen v místě úřadu, komunikací se zájemci o informace apod., ale také masově, tj. přímo zveřejnit, je třeba zvolit takovou metodu (unikátních) odkazů z dokumentu, aby po ukončení doby, po kterou je nezbytné (účelné) příslušnou agendu řešit a dokument na internetu vyvěšovat, nebyly dále zbytečně dostupné a šířené osobní údaje. Soukromí člověka nemusí být dotčeno jen poté, co byla úřední věc vyřízena, např. paušální dostupností osobních údajů z úředních listin v internetových archivech a vyhledávacích či jiných indexačních systémech vedených často pro výdělečné účely, ale především tím, že se údaje časem stávají zastaralými a nepřesnými či prostě neúplnými, což v době informační společnosti jednotlivce výrazně poškozuje.

V související agendě Úřad předložil ministerstvu vnitra návrh právní úpravy pořizování obrazového a zvukového záznamu z jednání zastupitelstva obce, vč. podmínek zveřejňování na internetu. Návrhem Úřadu by bylo lépe umožněno používat moderní komunikační technologii, v souladu se zákonnými požadavky na zpracování osobních údajů, pro lepší informování občanů o dění v obci. K tomu, aby bylo zpracování a zveřejňování osobních údajů přiměřené a férové, považuje Úřad za nezbytné, aby pravidla jednání zastupitelstva obce obsahovala podrobnější podmínky a způsoby zpracování při pořizování i zveřejňování nahrávek obsahujících osobní údaje. Jde o parametry zpracování, které zákon o ochraně osobních údajů ukládá správci osobních údajů vždy nějakým způsobem definovat – v případě zveřejňovaných záznamů je na místě zejména stanovit dobu uchovávání nahrávek, po kterou jsou osobní údaje zpracovávány (a krátce dostupné na internetu). Nelze však vyloučit ani bližší specifikaci webových služeb, tedy konkrétní nastavení dostupnosti na internetu. Návrh Úřadu byl veden záměrem, aby podle poměrů v konkrétní obci bylo zajištěno, že zpracování osobních údajů bude prováděno účelně, což je základním imperativem ochrany osobních údajů.

Pozornost Úřad věnoval zákonu o soukromé bezpečnostní činnosti a soukromé bezpečnostní službě a o změně souvisejících zákonů. Úřad uvítal přístup zpracovatele návrhu, Ministerstva vnitra, v tom, že zpracování osobních údajů soukromými bezpečnostními službami se nebude

lišit od zpracování osobních údajů jinými soukromými subjekty, tedy že soukromé bezpečnostní služby nebudou mít v soukromí jiných nějaká zvláštní privilegia. Předložení zákona vládě bylo odloženo na jaro 2012.

Obrovskou výzvou a legislativním tématem roku 2011, do konce roku však neuzavřeným, bylo z pohledu ochrany osobních údajů uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí (data retention). Ústavní soud svým nálezením z 22. března 2011 sp. zn. Pl. ÚS 24/10 ve věci shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu zrušil ustanovení zákona č. 127/2005 Sb. a celou vyhlášku č. 485/2005, která zrušená ustanovení prováděla. V návaznosti na to byly do meziresortního připomínkového řízení předloženy návrhy dílčích novel několika zákonů. I když nová úprava byla s ohledem na citlivost a mnohými prosazovanou potřebnost agendy data retention očekávána obratem, do konce roku příprava nepřekročila práh vypořádání připomínek. Práce na nové právní úpravě byly nepochybně pod vlivem situace na mezinárodní scéně a poznamenány obecným hledáním účinných nástrojů ochrany osobních údajů. Nahradit derogovanou právní úpravu je nelehké zejména proto, že jejímu přijetí nepředcházelo řádné hledání specifických nástrojů a postupů ochrany osobních údajů při nediskriminačním plošném shromažďování osobních údajů. Za této situace, s přihlédnutím k dostupné judikatuře a při respektování reality – společensky uznávaného požadavku na dostupnost osobních údajů vytvářených v přímé souvislosti s elektronickou komunikací – Úřad důrazně prosazoval zabudování účinných a „automaticky působících“ záruk a omezení rizik při shromažďování a uchovávání údajů. Požadoval mimo jiné povinné využívání i jiných než jen obecně deklarovaných opatření k zabezpečení údajů a co nepřesnější vymezení podmínek pro používání údajů. Toho lze dosáhnout jen řádně revidovanou a zpřesněnou úpravou kompetencí a jednotlivých postupů oprávněných orgánů (nejen činných v trestním řízení, ale s ohledem na další unijní předpisy i České národní banky).

Formalitou, významnou pro kompetenci Úřadu, bylo vydání nového vládního nařízení č. 277/2011 Sb., o stanovení vzoru průkazu kontrolujícího Úřadu pro ochranu osobních údajů, kterým se do praxe Úřadu zavádějí na průkazech ochranné prvky vyvinuté ve spolupráci se státní tiskárnou cenin. Vláda nařízení schválila 31. srpna 2011, platnosti nabylo 26. září 2011 a účinnosti 1. října 2011.

# Styky se zahraničím a mezinárodní spolupráce

Rok 2011 byl na mezinárodním poli ochrany osobních údajů naplněn pracemi nad novými standardy ochrany osobních údajů. Vedle návrhů změn předpisu, který má zásadní dopad do právního řádu České republiky a je vzorem zákona o ochraně osobních údajů, směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, Úřad monitoroval a dílčími připomínkami přispíval také k pracím na novelizaci Úmluvy Rady Evropy, o ochraně osob se zřetelem na automatizované zpracování osobních dat (Úmluva 108) a Zásad OECD upravujících ochranu soukromí a přeshraniční toky osobních údajů.

V případě směrnice 95/46/ES zástupci Úřadu intenzivně vstupovali do diskusí a úvah k připravované změně právního rámce pro ochranu osobních údajů. Uplatňovali přitom připomínky založené na zkušenosti z desetileté praxe v širokém spektru výkonu dozoru nad ochranou osobních údajů v ČR. Vyjadřovali se ke stávajícím i nově navrhovaným způsobům dozoru nad zpracováním osobních údajů, např. k procesu oznamování, registrace a předběžné kontroly zpracovatelských operací, i ke klíčovým pojmům ochrany, jako je definice pojmu citlivý údaj a riziková zpracování osobních údajů. Při svých připomínkách Úřad dbal na to,

aby byly zvláště ošetřeny aktuální trendy ochrany dat, týkající se zejména přeshraničního sdílení dat a související aplikace a vynucení práva, a k tomu bylo jasně deklarováno postavení národních dozorových orgánů a mechanismu jejich spolupráce. Absenci jednotných pravidel pro přeshraniční dozor nad zpracováním osobních údajů a účinné vynucení práva na internetu pociťuje Úřad jako velkou slabinu dozoru nad ochranou dat zpracovávaných v rámci webových aplikací a na společenských sítích, a to zejména pokud správci webových služeb byli usídleni mimo území EU.

Konec úvodní etapy prací nad revizí směrnice 95/46/ES byl těsně v závěru roku 2011 signalizován návrhem na vydání zcela nového předpisu, který by nahradil tuto směrnici a to paralelně ve formě nařízení nebo nové směrnice, neoficiálně publikovaným textem, zpracovaným a předloženým k interní diskusi a dopracování v útvarech evropské Komise. K dřívějšímu nástihu revize direktivy – ke Sdělení Komise ze 4. listopadu 2010, sp. zn. KOM (2010) 609 (CELEX: 52010DC0609) – komplexní přístup k ochraně osobních údajů v Evropské unii, vypracoval Úřad ve spolupráci s dalšími dotčenými ministerstvy rámcovou pozici České republiky, kterou dne 20. dubna 2011 vzal senátní výbor pro záležitosti Evropské unie jako senátní tisk č. K 009/08 na vědomí.

Revize trendů ochrany dat a směrnice 95/46/ES se v roce 2011 pochopitelně dotýkala a byla ovlivněna mezinárodní spolupráce v rámci expertních skupin, zejména Pracovní skupiny pro ochranu dat podle čl. 29 směrnice 95/46/ES (dále jen „WP29“) a jejích pracovních podskupin, a dalších mezinárodních týmů a projektů. Připomínky a návrhy, které byly za účasti Úřadu projednávány, vesměs vycházejí z nedávno vydaných stanovisek ke klíčovým pojmům ochrany osobních údajů (stanovisko č. 1/2010 k pojmu správce a zpracovatel, stanovisko č. 8/2010 k pojmu použitelného práva a stanovisko č. 15/2011 k pojmu souhlas) a doplňují je, týkají se však i po letech revitalizovaných zásad zpracování dat, jako je např. princip „accountability“ (stanovisko č. 3/2010).

Z řady praktických témat probíraných v jednotlivých podskupinách WP29 stojí za zmínku práce na procedurálním a odborně-technickém zabezpečení nové povinnosti poskytovatelů veřejně dostupných služeb elektronických komunikací notifikovat příslušným orgánům a dotčeným jednotlivcům případy porušení ochrany osobních údajů (data breaches), kterou zavedla směrnice 2009/136/ES. Jde o novou kompetenci, se kterou se většina dozorových orgánů v Evropě bude muset teprve vypořádat. O důležitosti nového opatření vypovídá i oprávnění Komise po konzultaci s Evropskou agenturou pro bezpečnost sítí a informací (ENISA), pracovní skupinou WP29 a s evropským inspektorem ochrany údajů (EDPS) přijmout technická prováděcí opatření týkající se okolností, formátu a postupů, jež se vztahují na požadavky informování a oznamování porušení ochrany osobních údajů. Komise současně v recitálu uvedené směrnice netají záměr neomezit povinnost notifikace pouze na odvětví elektronických komunikací, ale do budoucna jako prioritu zavést požadavek na výslovné povinné oznamování vztahující se na všechna odvětví.

Mezinárodní projekt financovaný Evropskou unií z programu Leonardo da Vinci Partnerství vstoupil v roce 2011 do závěrečné fáze. Dvouletá spolupráce polského, maďarského a českého úřadu vyvrcholila vydáním populárně naučné publikace s titulem „Ochrana osobních údajů. Vybrané otázky. Příručka pro podnikatele“. Tuto událost doprovázela řada propagačních akcí ve Varšavě, Praze a Budapešti, převážně formou seminářů pro odbornou veřejnost. Knížka našla odezvu na půdě Rady Evropy a byla představena ve skupině WP29 coby poradnímu orgánu Evropské komise.



V roce 2011 pokračovalo také členství Úřadu v mezinárodním konsorciu technické pomoci dozorovému úřadu pro ochranu dat v Makedonii. Projekt, financovaný Evropskou komisí, zaměřený na harmonizaci národních předpisů v oblasti ochrany dat s legislativou EU, posilování provozní kapacity, zvyšování informovanosti o ochraně dat mezi laickou a odbornou veřejností, na modernizaci informačního a komunikačního vybavení makedonského úřadu, by měl být ukončen do poloviny roku 2012. V roce 2011 se na realizaci projektu podíleli dva naši experti, oba formou krátkodobých pracovních misí v Makedonii. První z expertů, právník, se zaměřil na finanční sektor (banky, pojišťovny), kde ochrana dat je zvlášť naléhavou otázkou, a dále na oblast zaměstnávání, ve které dochází ke zpracování řady citlivých informací o jednotlivcích. Druhý expert předával makedonským kolegům zkušenosti z oblasti mezinárodních toků dat a pomáhal optimalizovat systém registrace zpracovatelských operací.

Nadále pokračovala účast pracovníka Úřadu jako hlavního experta na legislativní a procedurální otázky v pomoci dozorovému úřadu pro ochranu dat v Albánii. Projekt je financovaný Evropskou unií z programu IPA2009. Odstartoval v listopadu 2010 a poběží do jara 2012. V rámci svých aktivit expert Úřadu analyzoval albánský zákon o ochraně osobních údajů z hlediska požadavků harmonizace s právem EU, navrhl potřebné úpravy a účastnil se všech jednání o prosazení těchto adaptací na Ministerstvu spravedlnosti v Tiraně. Stejným způsobem se věnoval také sekundárním právním předpisům, které mají klíčový dopad do ochrany dat a soukromí. Zpracoval text vyhlášek upravujících zpracování osobních údajů v hotelovém sektoru a v souvislosti s evidencí vstupu do hlídaných budov. V rámci optimalizace činností dozorového úřadu expert spoluvytvářel návrhy interních dokumentů: směrnici o dozorových činnostech, zásady pro předávání dat do zahraničí a ve spolupráci s příslušným pracovištěm Úřadu také podrobný manuál pro registraci zpracovatelských operací. Uvedené činnosti byly průběžně doplněny konzultační a přednáškovou činností.

Ke společným pravidelným hodnocením úrovně ochrany osobních údajů při naplňování požadavků Schengenské úmluvy a souvisejících předpisů byl Úřad přizván ve třech případech hodnocení Lichtenštejnska, Islandu a souhrnného vyhodnocení severských států Evropy (Dánsko, Švédsko, Finsko a Norsko).

Zástupkyně Úřadu byla přizvána rovněž k účasti na konferenci frankofonní skupiny pro ochranu osobních údajů v Dakaru, první na africkém kontinentě, se zadáním informovat o strategii a koncepci komunikace s veřejností a o šíření znalostí ochrany osobních údajů mezi mladou generací. V rámci prezentace regionálních projektů a mezinárodních právních nástrojů jakožto místopředsedkyně konzultační skupiny k Úmluvě 108 (T-PD Rady Evropy) referovala o modernizaci Úmluvy 108.

Rok 2011 lze v případě mezinárodní spolupráce a přeshraniční ochrany dat označit za podnětný i v oblasti nových technologií – byl dokončen nový technologický standard ISO 29100 – A Privacy Framework. V oblasti nových technologií, předbíhajících často svými možnostmi platné právní předpisy, Úřad efektivně využívá zahraniční zkušenosti a vyměňuje poznatky se zahraničními dozorovými úřady. Kromě výše uvedené agendy data breaches se v roce 2011 jednalo zejména o technologie cloud computing a smart metering.

V případě technologie „smart metering“, resp. „smart grid“, mohl Úřad ve svém přístupu prvně zohlednit poznatky o inovativní strategii „privacy by design“, získané při spolupráci v rámci Mezinárodní pracovní skupiny k ochraně dat v telekomunikacích (IWGDPT). Účelem „privacy by design“ je zohlednit ochranu soukromí již v návrhu systémů zpracování osobních údajů, přičemž je prokazatelné, že takový přístup se vyplatí. V případě správce či zpracovatele osobních údajů, provozovatele aplikací vede aplikace přístupu „privacy by design“ ke

zjednodušení a zrychlení implementačních, komunikačních i informačních procesů, rovněž komunikace s orgány dohledu i řešení případných stížností zákazníků je jasnější a v případě dodržení všech zásad „privacy by design“ si velmi pravděpodobně není ze strany subjektu údajů na co stěžovat.

Úřad za účelem získání poznatků a výměny informací se zahraničními partnery kontaktoval v roce 2011 vybrané výrobce a dodavatele elektrické energie. Tzv. chytré měření je součástí chytrých sítí („smart metering“ a „smart grid“), vyvoláno zejména potřebou šetřit energií a dalšími faktory. Orgány Evropské unie ve směrnici 2009/72/EC předpokládají, že v roce 2020 bude 80 % odběratelů vybaveno chytrými měřidly. Jelikož projekt vychází z velmi detailního měření spotřeby energií každou domácností, dochází k velmi významnému sledování rodinného a osobního života obyvatel. K novému typu elektroměru budou připojeni i další měřiče (voda, plyn, teplo) a měřené hodnoty budou předávány ke zpracování do datového centra. Odběratel, ale i další subjekty v řetězci navázané (distributor atd.), v budoucnu získají informace o tom, kdy je zapnut kávovar, kdy je spuštěna automatická pračka, kdy byla použita toaleta apod. Snímané údaje pomohou distributorovi lépe zmapovat odběrovou charakteristiku a zákazníkovi, za cenu předávání osobních údajů, umožní učinit si obraz o své spotřebě. Pro odběratele uvedené informace mohou přinést úspory například tím, že si spotřebu rozloží tak, aby mohl snížit nasmlouvaný příkon, nahradit neúsporné spotřebiče jinými atp. Predikce odběru, případně možnost sepnutí či odepnutí skupiny spotřebičů snad umožní dodavateli lépe využívat nestandardní zdroje, jako jsou větrné či fotovoltaické elektrárny nebo přejít na vícetarifní systém.

Pro ochranu osobních údajů znamená každá nová technologie další zdroj informací o chování jednotlivce a rodiny, velmi detailní informace o chování ve svém domově čili informace, které byly zatím nedostupné. Dosud uvažované a testované varianty chytrých měřičů jsou za dodržení zásad „privacy by design“ mírným zásahem do soukromí a z hlediska ochrany osobních údajů přijatelné a bezpečné. To rozhodně ale neznamená, že by se v takto zabezpečených systémech jednalo o anonymní údaje nepodléhající doзору Úřadu. Pro další vývoj bude potřeba zajistit bezpečnost a důvěrnost získaných dat a je jen na energetických společnostech, pro kterou cestu v rámci poskytování služeb nejen v České republice, ale i napříč Evropou se rozhodnou, zda přijmou potřebná opatření již v návrhu anebo zda budou své aplikace složitě upravovat po jejich spuštění. K tomu nabízí Úřad jak vlastní stanoviska a odborná vyjádření, tak zprostředkování zahraničních zkušeností v oblasti ochrany osobních údajů a zabezpečení soukromí zákazníků.

# Úřad, sdělovací prostředky a komunikační nástroje

V roce 2011 Úřad tradičně pořádal bilanční tiskové konference, které přivádějí na Úřad standardně novináře z tištěných médií – deníků i odborně zaměřeného tisku – agenturní novináře, zástupce hlavních rozhlasových i televizních stanic. Výstupy z tiskových konferencí se pravidelně objevovaly již v poledním zpravodajství v den konání konference. V následujících třech dnech po konferenci se ochraně osobních údajů věnuje 30–60 příspěvků, které většinou pokrývají již dříve mediálně sledované případy související s ochranou osobních údajů.

V přílohách k tiskovým zprávám poskytuje Úřad soustavně informace o kontrolách ukončených správním řízením. Důležitá je zde nejen otevřenost, s níž hovoří o výsledcích své práce, ale především zpráva o důvodech uložených pokut, čímž zároveň prohlubuje právní povědomí ve vztahu k zákonu o ochraně osobních údajů i způsobu jeho aplikace.

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

Každodenní servis poskytovaný médiím se týká bezprostředního poskytování odpovědí na dotazy novinářů, eventuálně příjem jejich podání spojený s případy, kdy se novináři setkávají s problematikou ochrany osobních údajů, na jejichž základě Úřad dále plní své kontrolní i konzultační povinnosti.

## KONTAKTY S MÉDIÍ

Z uvedeného každodenního servisu poskytovaného médiím lze soudit, že problematika ochrany osobních údajů je značně frekventovaným mediálním tématem. Je třeba ovšem také říci, že zájem novinářů o informace je v některých případech vede k zaujímání stanovisek, jimiž upřednostňují přístup k informacím bez přílišného ohledu na potřebu dodržovat vyvážené

uplatňování veškerých právních norem a zákonných ustanovení. V roce 2011 se to projevilo zejména v souvislosti se zveřejňováním platů úředníků státní správy a samosprávy (plynoucím z laicky jednostranného zobecnění výroku Nejvyššího správního soudu ve věci zveřejnění platu zaměstnance zlínského magistrátu) a v postoji ke zveřejňování videozáznamů z jednání zastupitelstev na internetu (detailní informace o problému viz kapitola Zpřístupňování videozáznamu z jednání zastupitelstva v této VZ).

Obdobně lze také soudit ze zaměření přímých vystoupení v médiích, které jsou požadovány po předsedovi Úřadu, po odborných pracovnících či tiskové mluvčí.

Veškeré mediální výstupy Úřad obvykle publikuje na svých webových stránkách (samozřejmě po dohodě s konkrétním médiem). Je tak posílána i možnost, aby veřejnost sledovala názorovou kontinuitu Úřadu a novináři měli okamžitou odpověď na kladené dotazy.

Rubrika „Novinky“ na hlavní straně webových stránek slouží jako orientační vodítko po dění v Úřadu a jeho aktuální agendě.

## ŠÍŘENÍ ZNALOSTÍ O OCHRANĚ OSOBNÍCH ÚDAJŮ

Příležitost Dne ochrany osobních údajů vždy v lednu dává možnost nejen informovat o běžné agendě Úřadu za uplynulé období, ale také hovořit o ochraně osobních údajů v obecnější rovině v kontextu práva na soukromí jakožto základního lidského práva. V roce 2011 Úřad v České republice už popáté vyhlásil soutěž pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!“. V rámci šíření znalostí o ochraně osobních údajů (která je stavěna mezi důležité úkoly úřadů pro ochranu osobních údajů ve všech státech, v nichž tyto instituce působí) považuje český Úřad za stěžejní pracovat s mladou generací, protože její život se bude už cele odvíjet ve společnosti využívající stále dokonalejší nové informační technologie, které by rozhodně člověku měly pomáhat, ale nedestruovat hodnotu soukromí v jeho životě. V roce 2011 spolupracoval Úřad na tomto svém poslání tradičně s Českým rozhlasem Praha, MFF pro děti a mládež Zlín (kde předával ceny vítězům) a nově také se Svazem knihovníků a informačních pracovníků (SKIP). Ve více než 100 knihovnách po celé České republice soutěžily děti ve věku od 7 do 10 let s využitím hry Webowou diwočinou, která je zábavnou formou učí, jak se chovat bezpečně a ohleduplně na internetu. Na přípravě české verze hry spolupracoval Úřad s Radou Evropy, která tuto zábavnou formu výuky, jak se bezpečně pohybovat v internetovém prostředí, připravila.

Velmi rozsáhlá byla účast Úřadu na konferencích a seminářích. Ve spolupráci se společností F.S.C. uspořádal Úřad dvě konference o bezpečnosti dat. Problematice používání kamerových systémů ve školách byl věnován seminář pořádaný společností Wolters Kluwer ČR za účasti předsedy Úřadu a referenta registračního oddělení. Dále bylo uskutečněno 40 akcí a zaměstnanci Úřadu přednášeli pro: Jazykové centrum Ulita při SŠ a MŠ pro sluchově postižené, Institute for International Research, GmbH, Ministerstvo vnitra, IDG Czech, a. s., Pražská teplárenská, a. s., Česká správa sociálního zabezpečení, Jaroslava Šebestová, účetní a poradenská firma, F.S.C. Bezpečnostní poradenství, a. s., Regionservis, s. r. o., Pražská teplárenská, a. s., Clifford Chance, Služby škole Mladá Boleslav, Sokolovská uhelná, a. s., Fakta, s. r. o. vzdělávací zařízení, Městský úřad Kojetín, Asociace poskytovatelů sociálních služeb ČR, Úřad práce v Pardubicích, Svaz českých a moravských spotřebních družstev (COOP), Justiční akademie, ČSOB, SmithNovak, s.r.o., Institut pro veřejnou správu, Městský soud v Praze, D & D Health s.r.o., InBIT ČR, s. r. o., Agentura BOVA, Gordic spol. s. r. o., WEDOS, a. s.,

Ing. Jana Müllerová daňová poradkyně, Truconnexion, a. s., Česká zemědělská univerzita v Praze 6 a Právnická fakulta Univerzity Karlovy.

Speciálním seminářem mj. za účasti Americké obchodní komory byla představena příručka pro podnikatele zpracovaná ve spolupráci s maďarskými a polskými kolegy (bližší informace viz kapitola Styky se zahraničím a mezinárodní spolupráce v této VZ).

Příspěvkem o ochraně osobních údajů obohatil zaměstnanec Úřadu publikaci věnovanou problematice ochrany osobních údajů v práci školních psychologů, kterou pro rok 2012 připravuje k publikování nakladatelství Wolters Kluwer ČR a. s.

## KNIHOVNA A PUBLIKACE ÚŘADU

Knihovna nadále slouží jako odborné zázemí pro pracovníky Úřadu, ale je otevřena na individuální vyžádání též odborné veřejnosti. Využívají ji studenti pro své seminární a diplomové práce dotýkající se ochrany osobních údajů. V roce 2011 poskytla svůj fond šesti studentům a získala jednu diplomovou práci, která těžila z jejího fondu. Fond knihovny se rozrostl o 46 svazků.

V roce 2011 Úřad publikoval už 60. částku svého Věstníku. Zde publikovaná stanoviska Úřadu jsou určena odborným pracovištím a státním institucím, stejně jako závažné zahraniční dokumenty věnované ochraně osobních údajů. Trvale jsou tyto dokumenty s malým časovým odstupem od vydání Věstníku dostupné rovněž na webových stránkách Úřadu.

Dvě tematicky uspořádaná čísla Informačního bulletinu byla věnována zpracování genetických údajů spojených s využíváním vzorků DNA a legislativním problémům s tématem spojeným a využívání kamerových systémů a legislativním problémům. Zejména číslo věnované využívání kamer se setkalo s velkou odezvou v médiích.

## WEBOVÉ STRÁNKY ÚŘADU

Rozsah informací, který přinášejí stránky, bývá po obsahové stránce pozitivně hodnocen veřejností odbornou i laickou. Vzhledem k tomu, že od doby vzniku stránek uplynula už delší doba, rozhodl se Úřad provést inovaci stránek z hlediska jejich technické modernizace, která také umožní rychlejší vyhledávání v dnes již značně rozsáhlém obsahu, který stránky mohou nabídnout. První kroky k inovaci webových stránek, včetně využití diskusního fóra, které dávalo možnost vyjádření také široké veřejnosti, bylo učiněno na sklonku roku 2011. Předpokládáme, že webové stránky budou v uživatelsky přátelštější inovované podobě dostupné v polovině roku 2012.

# Informační systém ORG

Rok 2011 byl ve znamení budování projektu „Informační systém ORG“.

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

Financování investiční části požadovaného systému bylo zajištěno usnesením vlády č. 1019/2009 a systém 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 nejsou uložena žádná jména fyzických osob, takže ani znalost všech identifikátorů neumožňuje Úřadu zjistit jejich přiřazení jednotlivým fyzickým osobám. Touto cestou by měla realizace projektu základních registrů výrazně přispět k ochraně osobních údajů občanů.

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

- Registr obyvatel,
- Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (registr osob),
- Registr územní identifikace, adres a nemovitostí (registr územní identifikace),
- Registr agend orgánů veřejné moci a některých práv a povinností (registr práv a povinností),

- Informační systém základních registrů (jde o informační systém veřejné správy, jehož prostřednictvím je zajišťováno sdílení dat mezi jednotlivými základními registry navzájem a základními registry a agendovými informačními systémy, správa oprávnění přístupu k datům a další činnosti /ISZR/),
- Informační systém pro přidělování a tvorbu zdrojových identifikátorů fyzických osob, agendových identifikátorů fyzických osob a vedení jejich seznamů (ORG),

Smyslem začlenění Informačního systému ORG do systému základních registrů je ochrana identity občanů před zneužitím jejich osobních údajů. Dá se říci, že jednotlivé registry jsou od sebe odděleny, ale přes ORG je lze pomocí ISZR propojit.

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.

Po průtazích o dodání Informačního systému ORG v roce 2010 a odvolání na ÚOHS v roce 2011 bylo výběrové řízení na dodávku Informačního systému ORG dokončeno a dne 9. 2. 2011 byla podepsána smlouva s vítěznou firmou TESCO SW a.s. v ceně 131 802 000 Kč včetně DPH. Slavnostní zahájení („kick-off“) tohoto projektu se pak uskutečnilo 9. 3. 2011 v prostorách Úřadu.

Obsahem celé dodávky je:

- vypracování komplexní implementační dokumentace architektury IS ORG – architektura aplikační infrastruktury, model matematického aparátu, architektura systémové a komunikační infrastruktury, architektura integračních služeb, architektura Back-End aplikací,
- dodání SW i HW – dodání všech potřebných částí včetně poskytnutí uživatelských práv nutných pro provoz, servis a dlouhodobý rozvoj ke všem částím IS ORG,
- implementace IS ORG – realizace všech nezbytných prací souvisejících s instalací, konfigurací a propojením všech částí IS ORG do jednoho integrovaného plně funkčního celku,
- dokumentace a školení IS ORG – vypracování dokumentace skutečného provedení IS ke dni předání systému do provozu v etapách ORG Advanced a ORG Full.

Projekt je rozdělen na tři etapy:

Etapa BASE 9. 2. 2011 – 30. 9. 2011

V této etapě byla vybudována základní funkcionality (generování ZIFO, AIFO, transformace AIFO x AIFO) a zahájeno napojení ostatních komponent ZR. Informační systém má omezený výkon a provoz je veden pouze v jedné lokalitě. Datové centrum je umístěno v Olomouci.

Etapa ADVANCED 1. 10. 2011 – 31. 12. 2011

V etapě ADVANCED přibýly další funkcionality a IS byl odladěn v návaznosti na požadavky ostatních komponent ZR. Provoz probíhá stále v jedné lokalitě, navýšení výkonu je v souladu s náběhem celého Informačního systému základních registrů (ISZR).

Etapa FULL 1. 1. 2011 – 30. 5. 2012

V etapě Full bude již plná funkcionality celého systému, 100% výkon a redundantní provoz v primární a záložní lokalitě (z důvodu poskytování bezvýpadkových služeb).

Ostrý provoz celého projektu je plánován na 1. 7. 2012.

Podpisem smlouvy se mohly začít uskutečňovat i další aktivity, potřebné pro úspěšné budování.

V budově Úřadu bylo vybudováno řídicí pracoviště. Na jaře a v létě 2011 probíhaly stavební práce spojené s přestavbou dvou místností a zpevněním podlahy tak, aby zde mohly být umístěny servery řídicího pracoviště. Dodávka technického vybavení místností – klimatizace místností, instalace záložního zdroje, připojení místnosti na bezpečnostní pult – byla realizována v první etapě projektu (BASE IS ORG) na konci září 2011.

Dne 24. 1. 2011 byla podepsána smlouva s vítěznou firmou na projekt „Administrativní řízení projektu IS ORG v systému základních registrů“. Předmětem smlouvy je administrativní zajištění projektu a souvisejících poradenských a administrativních činností. Vítězem výběrového řízení se stala firma EUNICE Consulting a. s. s projektem v ceně 588 000 Kč včetně DPH.

Dne 12. 4. 2011 byla podepsána smlouva s firmou AEC, spol. r. o. o bezpečnostním auditu IS ORG v ceně 1 035 000 Kč včetně DPH. Obsahem této smlouvy je:

- analýza a definice bezpečnostních požadavků informačního systému ORG;
- hodnocení plnění bezpečnostních požadavků informačního systému ORG v průběhu jeho implementace;
- vyhodnocení splnění bezpečnostních požadavků informačního systému ORG po jeho implementaci.

Dne 3. 6. 2011 bylo vyhlášeno výběrové řízení Publicita projektu „Informační systém ORG v systému základních registrů“ a 15. 9. 2011 byla podepsána smlouva s vítěznou firmou Tristan promotion, s. r. o. Cena projektu je 414 240 Kč včetně DPH. Publicita je povinnou součástí každého projektu Evropské unie.

V červnu 2011 bylo podáno Hlášení o pokroku č. 3 dle pravidel strukturálních fondů EU.

Dne 2. 7. 2011 byla podepsána Dohoda o centrálním zadávání s Ministerstvem vnitra na poskytování služeb KIVS.

Byly vybudovány datové linky mezi Prahou a Olomoucí, které jsou nutné k přenosu zabezpečených dat mezi řídicím pracovištěm a datovým centrem. K 30. 9. 2011, po úspěšném dovršení etapy BASE IS ORG, byla na odbor strukturálních fondů Úřadu podána první žádost o platbu ve výši 74 328 901 Kč. Tato žádost byla přijata a finanční prostředky byly z Ministerstva pro místní rozvoj, ve výši 85 % celkových výdajů, Úřadu vyplaceny.

Dne 21. 11. 2011 byla podepsána smlouva s Corpus Solutions a. s. o zachování mlčenlivosti. Tato firma bude provozovat všechny registry pro správu základních registrů.

Projekt byl prezentován na odborné konferenci eGovernment v Mikulově ve dnech 6.–7. 9. 2011, byly publikovány články v odborném tisku. Celý projekt základních registrů byl představen v mimořádné příloze časopisu Veřejná správa.

S rostoucími aktivitami odboru základních identifikátorů bylo třeba rozšířit stávající tým odboru ORG. Po výběrovém řízení v únoru 2011 se tým k 1. 6. 2011 rozrostl o jednoho pracovníka, referenta HW. K 1. 1. 2012 dojde k rozšíření týmu ORG o dva nové spolupracovníky. K tomuto datu bude mít odbor celkem pět zaměstnanců.



# Projekt „Optimalizace procesů ÚOOÚ“

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

V květnu 2011 podepsal Úřad smlouvu se společností DYNATECH, která zvítězila ve výběrovém řízení na dodavatele služeb potřebných pro realizaci aktivit projektu. Projekt je zaměřen na analýzu a optimalizaci procesů v ekonomické, provozní a personální oblasti a jeho úkolem je zefektivnění činností v uvedených oblastech díky implementaci jednotného informačního systému, ve kterém bude možno tyto procesy řídit, sledovat a sdílet. V průběhu roku 2011 byly vytvořeny diagramy a detailní popisy procesů za účelem odhalení nedostatků. Detailní analýza posloužila jako podklad k provedení optimalizace neefektivních procesů. Prozatím byly předloženy konkrétní návrhy možných změn a chystá se testování modifikovaných procesů. Optimalizace bude probíhat ještě v roce 2012, kdy již budou schválené změny postupně implementovány do chodu Úřadu.

Součástí projektu je také nastavení systému projektového řízení, které zajistí bezchybnou a bezproblémovou realizaci projektů jak na domácím poli, tak i v rámci přeshraniční spolupráce s úřady stejného zaměření a znásobí šanci Úřadu na čerpání prostředků ze strukturálních fondů EU. Pro úspěšné řešení projektů byla vytvořena speciální metodika, která vychází z principů mezinárodně uznávané projektové metodiky PRINCE2®. Administrace a realizace projektů bude také usnadněna díky implementaci softwarového nástroje, který byl během podzimu 2011 úspěšně otestován.

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

# Personální obsazení Úřadu

Úřad měl pro rok 2011 státním rozpočtem stanoveny 102 funkčních míst.

K 1. lednu 2011 byl fyzický počet zaměstnanců v Úřadu 101, z toho 96 zaměstnanců bylo v evidenčním stavu a 5 zaměstnanců v mimoevidenčním stavu.

K 31. prosinci 2011 měl Úřad 104 zaměstnanců, z toho 99 zaměstnanců v evidenčním stavu a 5 zaměstnanců v mimoevidenčním stavu.

V průběhu roku do Úřadu nastoupilo 8 nových zaměstnanců a 6 zaměstnanců pracovní poměr ukončilo.

Průměrný evidenční počet zaměstnanců za rok 2011 činil 98,17.

Z 8 nových zaměstnanců 3 nastoupili po jmenování prezidentem republiky do funkce inspektora místo 3 inspektorů, kterým v roce 2011 skončilo desetileté funkční období. Jeden zaměstnanec nastoupil do nově vznikajícího útvaru – odboru základních identifikátorů.

V roce 2011 Úřad zahájil druhé desetiletí své činnosti, což se projevuje ve vyšší věkové struktuře zaměstnanců, z nichž 20 % pracuje v Úřadu od jeho vzniku.

Vysoké procento vysokoškolsky (65 %) a středoškolsky (32 %) vzdělaných zaměstnanců odpovídá stanoveným požadavkům na pracovní místa v Úřadu a je předpokladem pro úspěšné plnění činností a nových úkolů v Úřadu.

**Členění zaměstnanců Úřadu podle věku a pohlaví – stav k 31. prosinci 2011**

Věk	muži	ženy	celkem	%
do 20 let	0	0	0	0,0 %
od 21 do 30 let	6	8	14	14,1 %
od 31 do 40 let	6	11	17	17,2 %
od 41 do 50 let	8	7	15	15,2 %
od 51 do 60 let	16	20	36	36,4 %
61 a více	12	5	17	17,2 %
<b>Celkem</b>	<b>48</b>	<b>51</b>	<b>99</b>	<b>100,0 %</b>
<b>%</b>	<b>48,5 %</b>	<b>51,5 %</b>	<b>100,0 %</b>	

**Členění zaměstnanců Úřadu podle vzdělání a pohlaví – stav k 31. prosinci 2011**

Vzdělání	muži	ženy	celkem	%
Střední odborné + VL	1	1	2	2,0 %
Střední odborné	0	1	1	1,0 %
Úplné střední všeobecné	3	5	8	8,1 %
Úplné střední odborné + VL	1	1	2	2,0 %
Úplné střední odborné	4	16	20	20 %
Vyšší odborné vzdělání	0	2	2	2,0 %
Vysokoškolské	39	23	62	62,6 %
VŠ + vyšší kvalifikace	1	1	2	2,0 %
<b>Celkem</b>	<b>49</b>	<b>50</b>	<b>99</b>	<b>100,0 %</b>

**Celkový údaj o vzniku a skončení pracovních poměrů zaměstnanců v roce 2011**

	Počet
nástupy	8
odchody	6

# Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 433/2010 Sb., o státním rozpočtu České republiky na rok 2011.

## Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

Souhrnné ukazatele	v tisících Kč
Příjmy celkem	63 888,70
Výdaje celkem	166 689,66
<b>Specifické ukazatele – příjmy</b>	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	63 888,70
v tom: příjmy z rozpočtu Evropské unie bez SZP celkem	63 482,65
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	406,05
<b>Specifické ukazatele – výdaje</b>	
Výdaje na zabezpečení plnění úkolů Úřadu pro ochranu osobních údajů	166 689,66
<b>Průřezové ukazatele výdajů</b>	
Platy zaměstnanců a ostatní platby za provedenou práci	44 211,59
Povinné pojistné placené zaměstnavatelem)*	15 609,10
Převod fondu kulturních a sociálních potřeb	424,46
Platy zaměstnanců v pracovním poměru	34 289,54
Platy zaměstnanců v prac. poměru odvozané od platů ústav. činitelů	8 165,00
Výdaje spolufinancované z rozpočtu Evropské unie bez SZP celkem	76 863,09
v tom: ze státního rozpočtu	11 488,02
podíl rozpočtu Evropské unie	65 375,08
Výdaje vedené v informačním systému program. financování celkem	82 454,37

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

## 1. PŘÍJMY

Příjmy pro rok 2011 byly schváleným rozpočtem stanoveny ve výši 65 448 tisíc Kč, a to v souvislosti s projekty spolufinancovanými z rozpočtu EU – IOP „Informační systém ORG v systému základních registrů“, projektem OP LZZ „Optimalizace řídicích procesů Ú00Ú“ a projektem Komunitárního programu 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 63 888,70 tisíc Kč.

Jednalo se zejména o refundace zahraničních cest zaměstnanců Úřadu Evroplem, Evropskou komisí a Ministerstvem financí ČR, o sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti, o sankce uložené podle zákona č. 101/2000 Sb., o ochraně osobních údajů a jiných zákonů, o náhrady nákladů řízení, o úroky z finančních prostředků uložených na bankovních účtech, o refundace výdajů týkající se komunitárního programu Leonardo da Vinci, o příjmy vztahující se k roku 2010 (odvod zůstatku depozitního účtu po vyplacení platů a přidělu do FKSP za prosinec 2010).

Úroky z finančních prostředků uložené na účtech u ČNB činily 0,35 tisíc Kč.

Přijaté sankční platby byly ve výši – 716,88 tisíc Kč, investiční a neinvestiční dotace z EU ve výši 63 482,65 tisíc Kč, přijaté dary ve výši 20 tisíc Kč, pojistné náhrady ve výši 43,21 tisíc Kč, přijaté nekap. příspěvky a náhrady týkající se minulých let ve výši 785,10 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

## 2. OSTATNÍ BĚŽNÉ VÝDAJE

Čerpání běžných výdajů ve výši 27 240,45 tisíc Kč odpovídá běžným provozním výdajům, které vyplývají z hlavní činnosti Úřadu; jde zejména o položky spojené s nákupem drobného hmotného majetku, materiálu, služeb, cestovného, vzdělávání, údržby a o výdaje související s neinvestičními nákupy.

Výdaje za vodu, plyn, el. energii a PHM činily v roce 2011 1 808,32 tisíc Kč.

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

Jsou zde rovněž zahrnuty běžné výdaje na projekty, spolufinancované z rozpočtu EU v celkové výši 3 211,07 tis. Kč.

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

Čerpání rozpočtu na platy zaměstnanců, ostatních výdajů za provedenou práci a souvisejících výdajů, vč. projektů, ve výši 60 245,14 tisíc Kč odpovídá kvalifikační struktuře a plnění plánu pracovníků.

Stav k 31. 12. 2011 byl 99 zaměstnanců.

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

V souladu se schválenou dokumentací programu 143V01 „Rozvoj a obnova materiálně-technické základny Úřadu pro ochranu osobních údajů – od r. 2007“ bylo celkem vyčerpáno 82 454,37 tisíc Kč.

V podprogramu 143V01100 „Pořízení, obnova a provozování ICT Ú00Ú“ bylo v roce 2011 čerpáno celkem 82 068,83 tis. Kč v investičních *systémově určených výdajích SR na následující akce:*

	v tis. Kč
akci 143V011000037 „Prodloužení smlouvy Enterprise na používání produktů Microsoft“	1 706,91
akci 143V011000033 „Inform. systém Ú00Ú – NOS“	96,43
akci 143V011000034 „Upgrade bezpečnostní brány Firewall“	543,38
akci 143V011000035 „Technolog. a technická obnova prvků SI IT“	2 498,60
akci 143V011000036 „SW licence Veritas Storage Foundation“	119,84
akci 143V011000038 „IS Ú00Ú – úpravy modulů NOS, eKLEP, Registr“	207,20
akci 143V011000039 „Rozšíření kapacity páteřní části datové sítě LAN“	309,71
akci 143V011000019 „Informační systém ORG v systému základních registrů“ – projekt IOP spolufinancovaný z rozpočtu EU	74 318,68
Finanční prostředky na tento projekt byly čerpány z nároků z nepotřebovaných výdajů roku 2009 a 2010.	
akci 143V011000027 „Optimalizace procesů Ú00Ú“ projekt OP LZZ spolufinancovaný z rozpočtu EU	2 268,08

V podprogramu 143V01200 „Reprodukce majetku Ú00Ú“ byla uskutečněna akce 143V012000014 „Drobné úpravy budovy“ v souvislosti se zřízením Řídicího pracoviště ORG ve výši 385,54 tis. Kč.

#### Přehled čerpání rozpočtu v roce 2011

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2011 v tis. Kč	Konečný rozpočet 2011 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2011 v tis. Kč	Skut./konečný rozpočet v %
4118	Neinvestiční převody z Národního fondu	10 268	10 268	871,82	8,49
4153 2141,2211, 2212,2322, 2324,4132, 4135	Neinvestiční transfery přijaté od EU	129	129	275,33	213,43
	Ostatní nedaňové příjmy	0	0	406,05	
4218	Investiční převody z Národního fondu	55 051	55 051	62 335,51	113,23
	<b>PŘÍJMY CELKEM</b>	65 448	65 448	63 888,71	97,62

501	Platy	42 409	42 454,54	42 454,54	100,00
5011	Platy zaměstnanců	34 244	34 289,54	34 289,54	100,00
5014	Platy zaměst. odvozov. od platů úst. činitelů	8 165	8 165,00	8 165,00	100,00
502	Ostatní platby za provedenou práci	3 889	4 140,00	1 757,05	42,44
5021	Ostatní osobní výdaje	3 289	3 540,00	1 688,47	47,70
5024	Odstupné	600	600,00	68,58	11,43
503	Povin. pojist. plac. zaměstnavatelem	15 742	16 239,48	15 609,09	96,12
5031	Povin. pojist. na sociál. zabezp.	11 576	11 941,38	11 477,00	96,11
5032	Povin. pojist. na veřej. zdr. pojišť.	4 166	4 298,10	4 132,10	96,14
513	Nákup materiálu	5 059	5 126,00	1 962,15	38,28
514	Úroky a ost. fin. výdaje	16	15,00	8,68	57,88
515	Nákup vody, paliv a energie	2 045	2 111,00	1 808,32	85,66
516	Nákup služeb	38 786	39 436,73	17 216,77	43,66
517	Ostatní nákupy	5 761	5 299,36	4 079,75	76,99
5171	Opravy a udržování	2 600	2 047,00	1 595,33	77,94
5173	Cestovné	2 217	2 238,37	1 866,45	83,38
519	Výdaje souvis. s neinv. nákupy	2 390	2 424,00	1 990,49	82,12
5342	Převody FKSP	424	424,46	424,46	100,00
536	Ost. neinv. transf. jin. veřej. rozp.	12	12,00	4,33	36,11
542	Náhrady plac. obyvatelstvu	300	300,00	169,95	56,65
5424	Náhrady v době nemoci	300	300,00	169,96	56,65
590	Ostatní neinv. výdaje jinde nezařazené	0	0,00	0,00	0,00
	<b>Běžné výdaje celkem</b>	<b>116 833</b>	<b>117 982,58</b>	<b>87 485,59</b>	<b>74,15</b>
611	Pořízení dlouh. nehmot. majetku	31 296	75 678,36	46 612,74	61,59
612	Pořízení dlouh. hmot. majetku	39 560	68 514,10	32 591,33	47,57
	<b>Kapitálové výdaje celkem</b>	<b>70 856</b>	<b>144 192,46</b>	<b>79 204,06</b>	<b>54,93</b>
	<b>VÝDAJE CELKEM</b>	<b>187 689</b>	<b>262 175,04</b>	<b>166 689,66</b>	<b>63,58</b>

Číselné údaje jsou použity z výkazů zpracovaných ke dni 30. 12. 2011

## Přehled výdajů na projekty spolufinancované z rozpočtu EU v roce 2011

v tis. Kč

Název projektu	Schválený rozpočet 2011	Konečný rozpočet 2011	Skutečnost dle účetních výkazů k 31. 12. 2011	Skutečnost/konečný rozpočet v %
„Informační systém ORG v systému základních registrů“ – projekt IOP	71 120,00	145 438,68	74 318,68	51,10
„Optimalizace procesů Ú00Ú“	5 725,00	5 725,00	2 268,08	39,62
„Zvyšování povědomí o ochraně dat mezi podnikateli působícími v EU“ – projekt partnerství Leonardo da Vinci	129,00	276,36	276,33	99,99
<b>Celkem za projekty spolufinancované z EU</b>	<b>76 974,00</b>	<b>151 440,04</b>	<b>76 863,09</b>	<b>50,75</b>



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

Úřad v roce 2011 obdržel celkem dvacet tři žádosti o poskytnutí informace podle zákona o svobodném přístupu k informacím. V kontextu předešlých let lze konstatovat, že počet žádostí o informace stále narůstá.

Z celkového počtu žádostí o informace Úřad v roce 2011 zcela vyhověl sedmnácti z nich, ve čtyřech případech žádost částečně odmítl a informace poskytl v omezeném rozsahu a ve dvou případech zamítl žádost o poskytnutí informací jako celek. 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.

Stejně jako v předchozím roce žadatelé nejčastěji požadovali zaslání konkrétních správních aktů či jiných úředních písemností Úřadu, další dokumenty Úřadu, např. kontrolní plán pro rok 2011, informace o výsledcích řízení vedených Úřadem atd.

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



VÝROČNÍ ZPRÁVA

2011

**Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2011**

Úřad pro ochranu osobních údajů

Pplk. Sochora 27, 170 00 Praha 7

E-mail: [posta@uouu.cz](mailto:posta@uouu.cz)

Internetová adresa: [www.uouu.cz](http://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 2012 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. ÚOÚ a Mgr. Eva Strnadová

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

Pro Úřad pro ochranu osobních údajů vydalo Nakladatelství MU Brno, 2012

ISBN 978-80-210-5787-6