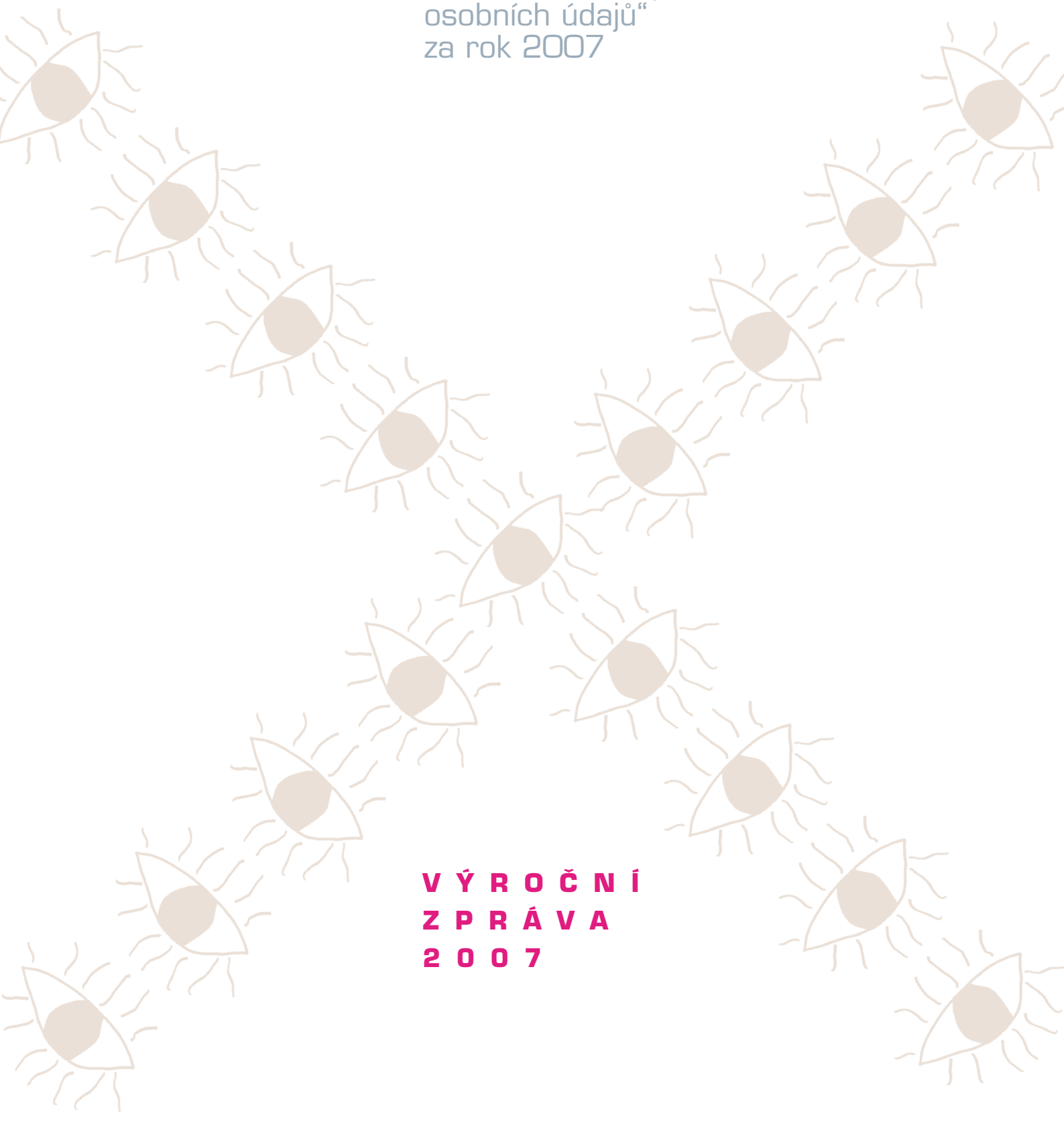
úřad
pro ochranu
osobních
údajů

Držitel „Evropské ceny za nejlepší službu veřejnosti v oblasti ochrany osobních údajů“ za rok 2007



VÝROČNÍ ZPRÁVA 2007

Rok 2007 z pohledu předsedy Úřadu

Když se ohlížím za uplynulým rokem, promítám si události, které se odehrávaly v souvislosti s ochranou osobních údajů, vrací se mi myšlenka, že na prahu 21. století jsme svědky upevňování demokracie, ale svoboda člověka jako by se stávala méně důležitou. Jakoby kolektivní problémy typu ochrany před globální změnou klimatu nebo kolektivní obrana před terorizmem byly prioritou na úkor osobní svobody. Začínají se prosazovat opatření bez ohledu na rizika, potíže a náklady, jaké to může přinést pro člověka, pro omezení jeho svobody, např. práva na soukromí.

Jsme svědky toho, že se kyvadlo vychyluje směrem ke kolektivní bezpečnosti, ale i pohodlí, na úkor práva na ochranu soukromí. A je to za málo vědomého souhlasu většiny společnosti. Je zřejmé, že i řada zodpovědných činitelů si neuvědomuje, že invazivní zásah do soukromí občanů v konečném důsledku může být jednou z cest, jak prolomit bezpečnost všech.

Jednou z institucí, která se snaží na tento fenomén upozorňovat je český Úřad pro ochranu osobních údajů. Nejsme tedy jenom úřadem vyřizujícím konkrétní stížnosti, podněty a následně ukládajícím sankce – i když to plníme jakožto zákonem nám uloženou povinnost – ale sami sebe vnímáme také jako preventivní orgán, který se snaží na problémy upozorňovat, a to nejen v rámci legislativní činnosti, ale také propagací ochrany osobních údajů směrem k veřejnosti.

Snad právě proto, že takto svoji roli chápeme, jsme za rok 2007 obdrželi Evropskou cenu za nejlepší službu veřejnosti v oblasti ochrany osobních údajů od Agentury na ochranu dat v Madridu. Cítíme prostě, že musíme upozorňovat na rizika, které přináší hromadné zpracování osobních dat ruku v ruce s raketovým rozvojem informačních technologií. Pozorně sledujeme ten vývoj u nás i v zahraničí a hovoříme o něm při každé sebemenší příležitosti, kdy máme možnost oslovit spoluobčany – poskytujeme konzultace, přednášíme, pořádáme semináře, ochotně věnujeme čas médiím. Časem nešetříme ani při našich interních odborných debatách. I ochránci osobních údajů jsou totiž neustále stavěni před nové problémy, které plynou především z už zmíněného překotného vývoje nových a nových technologií. Ty prakticky vždy sice pro člověka znamenají ve svém důsledku větší komfort, zároveň ale také větší ohrožení soukromého, ba nejintimnějšího života jednotlivce; proto hledání zákonem vyvažovaných možností pro jejich využití je natolik důležité. S uspokojením ale musím konstatovat, že naše kontakty se zákonodárci a jmenovitě se Stálou komisí pro ochranu soukromí Senátu Parlamentu ČR nabyly v roce 2007 na intenzitě a já do tohoto faktu vkládám i mnoho nadějí pro budoucí pozitivní kroky ve prospěch soukromí i svobody každého z nás.

Přirozeně bych proto uvítal, kdyby se podrobné pojmenování problémů s ochranou osobních údajů, jak se nám je za loňský rok podařilo v přehledu nastínit hned v úvodní kapitole této výroční zprávy, stalo inspirací také pro naše zákonodárce i moc výkonnou. Ten přehled vyplynul z velmi praktických a konkrétních poznatků inspektorů Úřadu, ale je zároveň reflexí toho, co je u nás aktuálně překážkou pro zabezpečení práva na soukromý a rodinný život každého občana a co naše soukromí ohrožuje. V tom také spatřuji nejen naplnění povinnosti dozorové autority, kterou nepochybně Úřad nepřestává být, ale také další pozitivní možnost rozvoje instituce, která je skutečnou službou veřejnosti.

Je to pro mne výzva a je mi ctí být tzv. „u toho“. Znám velmi podrobně vývoj problematiky v naší zemi. Byl jsem první, kdo o tomto tématu v ČR hovořil na mezinárodní konferenci, kterou pořádal v roce 1997 Úřad pro státní informační systém, jehož jsem byl předsedou. Dobře si pamatuji atmosféru ve společnosti, v parlamentu i v senátu. Po ochraně osobních dat nebyla poptávka. A nelze se divit. Řada informací vypadala jako ze světa sci-fi. Vždyť v té době se např. teprve začínaly u nás používat mobilní telefony. Nelze však nevidět, že od té doby se v souvislosti s rozvojem informačních technologií názory lidí změnily. Narostla řada otázek, ale i konkrétních problémů. V roce 2000 vznikl český zákon o ochraně osobních údajů i česká dozorová autorita – úřad, který byl koncipován tak, že jako jeden z mála má chránit občana v oblasti, kde občan sám si těžko pomůže a v řadě případů se ani o svém ohrožení nedozví.

Dnes je český Úřad pro ochranu osobních údajů pevně zakotven v systému veřejné správy. Jeho charakteristickým rysem je dynamičnost, jak v organizační struktuře, tak v kompetencích i komunikační strategii. Jeho snahu držet ruku na tepu vyvíjející se problematiky ochrany osobních údajů lze mj. dokumentovat novelami zákona o ochraně osobních údajů za 7 let jeho existence, ale i řadou reorganizací, které byly vyvolány změnou kompetencí Úřadu (nejnověji např. organizačními změnami vyvolanými přistoupením ČR do schengenského prostoru).

Jsem ovšem také rád, že se podařilo a daří problematiku diskutovat s veřejností, že naši občané si stále více uvědomují rizika spojená s laxním nakládáním se svým majetkem – osobními údaji, což se projevuje v nárůstu dotazů, stížností a registrací.

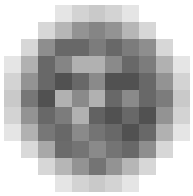
Velmi mě také těší, že jsme už něco ze získaných zkušeností mohli poskytnout v rámci twinningového programu, který jsme vedli v Bosně a Hercegovině.

Jsem také velmi nakloněn mezinárodním spolupracím, protože si jakožto člověk, který se část svého života pohyboval jako odborník-matematik v oblasti informačních technologií, dobře uvědomuji, nakolik žádná mezistátní hranice automaticky nechrání osobní údaje.

Především ale věřím, že společnými silami spolu se zákonodárci můžeme na poli ochrany osobních údajů udělat pro ochranu soukromí a svobody člověka mnoho užitečného.

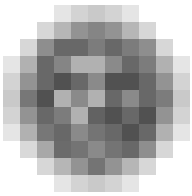
Igor Němec

Obsah



Činnost Úřadu v číslech – rok 2007

Dotazy	e-mailové dotazy	1 674
	Osobní konzultace	60
Stížnosti	Přijaté podněty dle zákona o ochraně osobních údajů	574
	Stížnosti předané ke kontrole	207
Nevyžádaná obchodní sdělení	Podnětů dle zákona o některých službách informační společnosti	1 569
	Uložené pokuty	71
Kontroly	Ukončeno	112
Správní trestání	Podnětů celkem	305
	Rozhodnutí o uložení pokuty	43
Registrace	Celkem podáno oznámení	30 806
	V roce 2007 podáno oznámení	2 215
	Celkem zaregistrováno zpracování	28 030
	V roce 2007 zaregistrováno zpracování	1 195
	V roce 2007 zrušeno registrací	904
	Celkem podáno oznámení o změně zpracování	1 597
	V roce 2007 podáno oznámení o změně zpracování	178
	Celkový počet žádostí o předání osobních údajů do zahraničí (§ 27 zákona č. 101/2000 Sb.)	51
	Rozhodnutí, která předání osobních údajů do zahraničí povolují	28
	Rozhodnutí, která předání osobních údajů do zahraničí zamítají	0
	Řízení zastaveno podle § 30 zák. č. 71/1967 Sb., na žádost účastníka řízení	1
Publikované materiály	Věstník Úřadu (počet částek)	4
	Bulletin Úřadu (počet čísel)	4
	Podkladové materiály pro média: Agenturní servis, tisk, rozhlas, TV, elektronická média	202
Tiskové konference	Pravidelné TK Úřadu	4



Činnost inspektorů

I. Poznatky inspektorů z kontrolní činnosti

ORGÁNY STÁTNÍ SPRÁVY

Rozsáhlá kontrola byla provedena v oblasti činnosti ústředního orgánu státní správy, do jehož působnosti patří výběr a příprava justičních čekatelů a dalších osob ucházejících se o výkon funkce soudce. Bylo zjištěno, že tento orgán v jím vedené personální dokumentaci držel osvědčení a čestná prohlášení podle lustračního zákona ohledně osob narozených po 1. prosinci 1971, v návrzích na jmenování soudcem prezentoval informace o rodinném stavu, počtu dětí a zaměstnavateli manžela uchazečů o výkon funkce soudce, uváděl národnost uchazečů a opatřoval si od nich čestné prohlášení o jejich dřívějším a stávajícím členství v politických stranách a hnutích. Uvedený orgán tak shromažďoval o uchazečích o výkon funkce soudce nadbytečné údaje včetně citlivých, aniž k tomu měl souhlas dotčených osob, a poskytl jim v této souvislosti informace stanovené zákonem. Je závažné, že uvedená kontrolní zjištění byla učiněna v praxi ústředního orgánu, který vykonává správu na úseku spravedlnosti.

Realizovaná kontrolní činnost ukazuje, že i nadále bude nezbytné věnovat zvýšenou pozornost působení orgánů státní správy a samosprávy. Z kontroly v úřadu jednoho z velkých měst, který zabezpečuje volbu přísedících příslušného soudu městským zastupitelstvem, vyplývá, že správce osobních údajů v předmětném případě zpracovával nepřesný údaj, opatřoval údaje o národnosti dotčených, jejich povolání, číslech občanských průkazů a telefonních číslech i informace o vedení trestního řízení proti kandidátům na funkci přísedících a jejich příbuzným, přestože to zákon neukládá. Jeho činností byly osobní údaje o soukromí kandidátů zveřejněny na webové stránce města, a to bez jejich souhlasu, a spisy s osobními údaji přísedících byly v městském úřadu uloženy po celé funkční období těchto osob. Kontrolou bylo také zjištěno, že nakládání členů volených orgánů města s podkladovými materiály pro jednání těchto orgánů, obsahujícími osobní údaje, zejména po ukončení jednání není žádným vnitřním předpisem upraveno. Shledané nedostatky nejsou výsledkem nedbalého vztahu příslušných pracovníků k jim svěřeným povinnostem, svědčí však často o nepochopení relevantních ustanovení zákona o ochraně osobních údajů a o pochybeních s tím souvisejících, jež byla mnohdy motivována snahou o maximální uspokojení oprávněných potřeb občanů.

Stejně tomu bylo i v praxi odborného útvaru jiného městského úřadu, když v zájmu urychlení řešení žádosti občanů zaslal jejich podání i s osobními údaji fyzické osobě k vyřízení, která jediná o něm mohla v souladu s příslušnými právními předpisy rozhodnout. Vzhledem k tomu, že k takovému předání neměl kontrolovaný subjekt právní titul (zmocnění či kompetenci vyplývající ze zvláštních předpisů) a jednal v rozporu se zákonem o ochraně osobních údajů, bylo nezbytné kontrolujícími konstatovat porušení tohoto zákona.

Další obecní úřad předal jinému subjektu k vyjádření petici občanů a tím neoprávněně zpřístupnil osobní údaje petentů. Uvedení se obrátili na Úřad s dotazem, zda se postupovalo v souladu ze zákonem o ochraně osobních údajů. Kontrolou

bylo zjištěno zpracování osobních údajů petentů v rozporu ze zvláštním právním předpisem a zákonem o ochraně osobních údajů. Obecní úřad porušil povinnosti správce při vyřizování peticí, nedbal práva občanů na ochranu soukromého a osobního života, a za to mu byla uložena pokuta.

POŠTOVNÍ SLUŽBY

V průběhu let 2005 až 2007 bylo opakovanými kontrolami dokumentováno, že poskytovatel poštovních služeb, jako zpracovatel osobních údajů pro jiné správce, ukládá svým pracovníkům pro nemalý počet situací vznikajících na jeho pobočkách pořizovat kopie občanských průkazů klientů či kopírovat jiné doklady nebo listiny těchto osob, obsahující jejich osobní údaje. Kontrolovaný subjekt byl seznámen s tím, že uvedená praxe je protiprávní. Na základě opatření, která přijal v důsledku kontrol na konci roku 2007, změnil příslušné vnitřní předpisy, ukládající provádění uvedených předpisů.

Dále byla u výše uvedeného subjektu zahájena kontrola na základě podnětu zaslaného Úřadu v souvislosti se zpracováním osobních údajů občanů, adresátů platby od správy sociálního zabezpečení. Stěžovatel dodal Úřadu nalezené personifikované poukázky typu B. Kontrolující tak zjišťovali a prověřovali skutečnosti u poskytovatele poštovních služeb při realizaci tisku a následné distribuci poštovních poukázek typu B. Kontrolou zpracování osobních údajů občanů při tisku poštovních poukázek bylo provozovateli poštovních služeb prokázáno porušení plnění povinností podle zákona o ochraně osobních údajů. Z hlediska svého postavení musí poskytovatel služeb poskytnout záruky o technickém a organizačním zabezpečení při zpracování osobních údajů a přijmout taková opatření, aby nemohlo dojít k nahodilému přístupu k těmto údajům. Na základě závěrů kontroly byla poskytovateli udělena sankce dle příslušného ustanovení zákona o ochraně osobních údajů.

STAVEBNÍ SPOŘITELNA

Na základě podnětu starosty obce byla zahájena kontrola, která byla zaměřena na plnění povinností správce, případně zpracovatelů (stavební spořitelny a jejích obchodních zástupců) při zpracování osobních údajů klientů. Z podnětu vyplývalo podezření na neoprávněný přístup k listinám s osobními údaji klientů uvedené stavební spořitelny při jejich nálezu v katastru obce. V kontrolovaném případě bylo nutno konstatovat, že úroveň nastavení práv a povinností správce umožnila v určité fázi zpracování osobních údajů klientů v rozporu se zákonem o ochraně osobních údajů. Správcem nebyla dostatečně přijata opatření k tomu, aby nedošlo k neoprávněnému přístupu k osobním údajům klientů této společnosti. V průběhu kontroly přijala stavební spořitelna opatření a provedla kroky, aby se napříště předešlo popsané situaci a nedošlo tak k neoprávněnému přístupu k osobním údajům. Kontrolovanému subjektu byla za porušení zákona udělena sankce.

SOUDNÍ EXEKUTOŘI

V roce 2007 kromě jiného Úřad zaznamenal také zvýšený počet podání občanů směřujících proti činnosti soudních exekutorů. Ne vždy se však ukázalo, že stížnosti, týkající se zpracování osobních údajů soudními exekutory, jsou oprávněné. Je zřejmé, že neznalost příslušné právní úpravy spolu s tím, že exekuce se povinných vždy negativně dotýká, způsobují ve vztazích exekutorů s dalšími účastníky exekučního řízení nejasnosti, na jejichž základě jsou posléze Úřadu doručovány podněty na údajně protiprávní postupy soudních exekutorů při zpracování osobních údajů. Přesto i v okruhu těchto osob, u nichž je vysokoškolské právnické vzdělání předpokladem jejich působení, bylo zjištěno vadné provedení úkonu, v jehož důsledku se neoprávněné osoby seznámily se závažnými osobními údaji jiných subjektů.

Při provádění zákona o ochraně osobních údajů se v dalším období jeví jako nezbytné pokračovat v seznamování jak laické, tak zejména i odborné veřejnosti s jeho obsahem. Zákon mnohdy není respektován, neboť jeho obsah není adresátům znám, případně znám je, ale zůstává nepochopen. Ani úředníci státní správy nebo samosprávy, pracující s mnoha osobními údaji, často nechápou fakt, že tato data jsou specificky chráněna, a není jim zřejmý důvod této ochrany. Zmíněnou skutečnost lze vysvětlit také dosud nedostatečným povědomím o možnostech zneužití osobních údajů.

Neoprávněné zpřístupnění osobních údajů bývá také zapříčiněno určitým dilematem mezi ochranou osobních údajů a právem občanů na svobodný přístup k informacím. Nedostatkům v této oblasti lze zamezit pouze osvětou zaměřenou na zvládnutí matérie zákona o ochraně osobních údajů a zákona o svobodném přístupu k informacím a objasněním jejich vzájemného vztahu.

Pomocí, zejména pro menší a malé podnikatelské subjekty, by bylo zpracování vzorového vnitřního předpisu, jenž by těmto subjektům pomohl k naplnění jejich povinností vyplývajících pro ně z ustanovení § 13 zákona o ochraně osobních údajů a zároveň by přispěl cestou objasnění mnohdy složitého znění tohoto zákona k jeho porozumění těmito subjekty a posléze k jeho důslednějšímu a kvalitnějšímu provádění v praxi. Přílohou takového předpisu by měl být vzor obsahu poskytnutí informace o zpracování osobních údajů povinným subjektem, vzor souhlasu se zpracováním osobních údajů v typických situacích a možná formulace pasáže, týkající se zpracování osobních údajů, jež bývá vepsána do obchodních podmínek, tvořících obvykle součást obchodních smluv.

Pro praxi by bylo rovněž vhodné jasným způsobem určit, jaké jsou důsledky registrace podle § 16 zákona o ochraně osobních údajů. Je to důležité zejména proto, že provedení registrace je povinnými subjekty převážně vnímáno jako faktický souhlas s realizací oznámené činnosti.

Ze závěrů kontrolní činnosti je možné dovodit, k jakým nejčastějším porušením povinností správce, případně zpracovatele dochází. Neustále přetrvává tendence správců shromažďovat osobní údaje subjektu údajů ve větším rozsahu, než je nezbytně nutné k naplnění stanoveného účelu. Uvedené zjištění bylo shledáno nejen v sektoru soukromém, ale i veřejném.

Správci (malé podnikatelské subjekty) se často potýkají s nepochopením ustanovení § 13 (plnění povinnosti osob při zabezpečení osobních údajů), a následkem toho nejsou dostatečně zhodnocena rizika při zpracování osobních údajů těmito subjekty a přijata taková opatření, aby nemohlo dojít k neoprávněnému či nahodilému přístupu k informacím.

Mezi další velmi časté porušení povinnosti správce, případně zpracovatele lze uvést neplnění informační povinnosti podle § 11 zákona o ochraně osobních údajů, který ukládá správci, aby při shromažďování osobních údajů byl 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 už známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i jeho o dalších právech. Jak bylo zjištěno kontrolní činností v roce 2007, uvedená povinnost bývá naplněna pouze částečně, nebo chybí úplně.

ZDRAVOTNICTVÍ

I.

Byla dokončena kontrola Ústavu zdravotnických informací a statistiky ČR (ÚZIS ČR), zahájená koncem roku 2006. Předmětem kontroly bylo dodržování zákona o ochraně osobních údajů při sběru a zpracování zdravotnických informací a při vedení národních zdravotních registrů.

Šlo o velmi závažnou kontrolu, neboť ÚZIS je co do rozsahu spravovaných dat zřejmě největším správcem citlivých údajů v České republice. Ve čtrnácti národních zdravotních registrech, které jsou součástí Národního zdravotnického informačního systému, vede ÚZIS ČR citlivé osobní údaje o značné části obyvatel České republiky.

Kontrola byla zaměřena zejména na zabezpečení a ochranu uchovávaných osobních údajů proti zneužití. V rámci kontroly bylo posouzeno technické řešení příslušných informačních systémů, technická a organizační opatření implementovaná v celém procesu zpracování dat, soulad těchto opatření s příslušnými normami pro bezpečnost informačních systémů, a rovněž byla ověřována aplikace interních bezpečnostních předpisů a jejich dodržování v praxi.

Kontrolou bylo zjištěno a konstatováno, že ÚZIS ČR v rámci sběru a zpracování zdravotnických informací a při vedení národních zdravotních registrů řádně plní všechny podmínky ochrany osobních údajů stanovené zákonem a že zpracovávané osobní údaje požívají řádné a úplné ochrany v takovém rozsahu, jaký lze při zpracování takového rozsahu citlivých údajů oprávněně očekávat.

II.

Byla dokončena kontrola nestátního zdravotnického zařízení – velké polikliniky, provedená na základě informace, že ve sběrném dvoře několik km od polikliniky se nacházejí zdravotní karty pacientů této polikliniky. Kontrolou bylo zjištěno, že jde o zdravotnickou dokumentaci zhruba 2000 osob, které byly skutečně pacienty uvedeného zdravotnického zařízení. K vývozu zdravotnické dokumentace došlo při stavebních úpravách budovy polikliniky, kdy zdravotnická dokumentace nebyla zabezpečena proti přístupu neoprávněných osob. Pozitivní byla skutečnost, že pracovníci sběrného dvora dokumentaci ihned zajistili a předali Policii ČR, čímž se zabránilo dalšímu případnému zneužití.

V následném správním řízení byla za spáchaný správní delikt poliklinice uložena pokuta ve výši 1,75 mil. Kč. Zohledněna byla zejména skutečnost, že šlo o citlivé údaje a že k úniku zdravotnické dokumentace došlo zcela nepochopitelnou nedbalostí při nakládání s ní. Míra této nedbalosti je zarážející vzhledem k tomu, že jde právě o zdravotnické zařízení a zdravotnické pracovníky, pro něž by měla být ochrana údajů o pacientech naprostou samozřejmostí, a to i bez zákonem stanovených zásad. Vyšší pokuta nebyla poliklinice uložena zejména na základě zohlednění skutečnosti, že značná část nalezené dokumentace se týkala již nežijících osob.

III.

Vzhledem k tomu, že velká zdravotnická zařízení nemocničního typu již byla v minulosti opakovaně kontrolována a stav ochrany osobních údajů pacientů byl v převážné většině případů vyhodnocen jako odpovídající požadavkům zákona, soustředila se kontrolní činnost v roce 2007 zejména na malá nestátní zdravotnická zařízení – ordinace soukromých lékařů. Důvodem byly i četné stížnosti občanů na nedostatečnou ochranu zdravotnické dokumentace v těchto zařízeních. Kontrolami byl skutečně zjištěn stav mnohdy nevyhovující.

Na základě poznatků z provedených kontrol lze shrnout, že většinově bylo zjišťováno velmi primitivní porušování zásad ochrany osobních údajů na základě elementární nedbalosti a spoléhání se na to, že „děláme to tak pořád a doposud se nic nestalo“. Jako demonstrativní příklady lze uvést následující kauzy:

■ Soukromý lékař smluvně zajišťující preventivní zdravotní péči pro strojírenskou firmu doporučil na základě lékařského vyšetření zaměstnancům firmy další odborná vyšetření. Doporučení na vyšetření (včetně diagnóz) předal nikoliv přímo svým pacientům, ale pro „urychlení“ hromadně jejich nadřízenému, aby ten předaná doporučení rozdal. Pacienti (zaměstnanci firmy) byli s takovým postupem oprávněně nespokojeni. V rámci kontroly bylo konstatováno porušení zákona, neboť lékař nepřijal taková opatření, aby nemohlo dojít ke zneužití citlivých údajů.

■ Soukromé lékařce byla na vlastní žádost krajským úřadem zrušena registrace její ordinace (nestátního zdravotnického zařízení). Lékařka měla povinnost předat zdravotnickou dokumentaci svých pacientů krajskému úřadu. Tuto povinnost nesplnila, protože majitel nebytových prostor, kde měla lékařka svou ordinaci, zdravotnickou dokumentaci z vyklizovaných místností nedopatřením odebral a spálil v kotli. V rámci kontroly pak bylo konstatováno porušení zákona tím, že lékařka řádně nezabezpečila citlivé údaje proti zničení.

■ Další soukromá lékařka hodlala předat zdravotnickou dokumentaci jinému lékaři (pacient změnil lékaře). K předání lékařka využila, tak jako obvykle, smluvní zásilkovou službu. Zdravotní dokumentace byla zásilkové službě předána takovým způsobem, že lékařka zdravotní karty položila na volně přístupný stůl na chodbě polikliniky, odkud si zásilková služba vždy zásilky odebírá. Zdravotní karty se však ze stolu ztratily. Dotčení pacienti si pak na postup lékařky oprávněně stěžovali. Zákon byl tedy i v tomto případě porušen, neboť lékařka nezabezpečila citlivé údaje pacientů proti ztrátě.

■ Jiná soukromá lékařka má kartotéku se zdravotními kartami svých pacientů v čekárně před ordinací. Jako kartotéka slouží dřevěná registrační skříň se samostatnými zásuvkami, každá opatřená zámkem. Pacienti si stěžovali, že v průběhu ordinačních hodin nejsou zámky zásuvek uzamčeny a že tedy hrozí reálná možnost, že do zdravotních karet mohou nahlížet nepovolané osoby, případně že hrozí odcizení zdravotnické dokumentace. Kontrolou bylo zjištěno, že stížnost je oprávněná a že lékařka porušila zákon, neboť nezabezpečila řádně citlivé údaje proti zneužití.

Výsledky kontrolních šetření a oprávněné poukazování občanů na nedostatky v činnosti malých nestátních zdravotnických zařízení prokazují, že mnozí soukromí lékaři si dosud neuvědomují nezbytné nároky na ochranu dat pacientů a odpovědnost za tuto ochranu, a to i přesto, že na základě principu zachování lékařského tajemství by pro ně měly být tyto věci zcela přirozené. Markantní je to zejména v případě údajů o zdravotním stavu pacientů, které jsou citlivými údaji, jejichž zneužití může mít hluboký dopad na soukromí každého člověka. Proto se bude pozornost inspektora v oblasti zdravotnictví soustředit na činnost soukromých lékařů i v dalším období.

KAMEROVÉ SYSTÉMY

I v roce 2007 se inspektoři zabývali značným množstvím podnětů směřujících proti provozovatelům kamerových systémů. Podněty jsou z nejrůznějších oblastí, zejména se týkají škol, větších zdravotnických zařízení (polikliniky, nemocnice), bytových domů a pracovišť zaměstnanců. Bylo zahájeno celkem 23 kontrol, z nichž 14 již bylo ukončeno.

V rámci kontrol se inspektoři opakovaně setkávají s kamerovými systémy, jejichž provozováním není respektováno základní lidské právo na ochranu soukromí, s obvyklým důsledkem porušení zákona o ochraně osobních údajů.

Naprostá většina kontrolovaných kamerových systémů se záznamem byla zřízena a provozována za účelem ochrany osob a majetku. Základním, většinově zjišťovaným nedostatkem takových kamerových systémů je skutečnost, že jsou provozovány nikoliv jako nezbytný prostředek pro dosažení stanoveného účelu, ale jako pouhé preventivní opatření. To by samozřejmě bylo možné, ovšem za předpokladu splnění některých nezbytných, zákonem stanovených podmínek. Vzhledem k tomu, že všechny kontrolované kamerové systému byly provozovány bez souhlasu monitorovaných osob, je nezbytné, aby byly provozovány buď na základě zvláštního zákona (takové oprávnění má např. Policie ČR), nebo na základě výjimky ze zákona o ochraně osobních údajů. Takovou výjimkou je právě možnost chránit své oprávněné zájmy, ovšem ochrana realizovaná tímto způsobem (tedy pořizováním kamerového záznamu) musí být pro provozovatele nezbytná a současně nesmí zasahovat do soukromého a osobního života sledovaných osob. Naplnění parametrů této výjimky se naprosté většině provozovatelů kamerových systémů nepodařilo dosáhnout a v takovém případě bylo vždy třeba označit shromažďování záznamů jako nezákonné. Nutno ale dodat, že v mnoha případech docházelo k excesům z důvodu nevhodného použití jen některých kamer, resp. nadbytečného rozsahu pořizovaných záznamů. Tento rozsah lze vždy ovlivnit počtem kamer, jejich umístěním a zaměřením, nastavením času a doby pořizování záznamu a nastavením rozlišovací schopnosti kamery. Jak však bylo kontrolami zjištěno, provozovatelé obvykle využívají maximálního rozsahu pořizovaných záznamů, zejména použitím co největšího (nejširšího) záběru a kontinuálního pořizování dat po celých 24 hodin denně ze všech kamer. Přitom je zřejmé, že např. ve škole není pro ochranu fasády budovy nezbytné pořizování záznamů z chodeb školy, že pro ochranu zaparkovaných aut v garážích bytového domu je třeba snímat především ona auta a ne schodiště domu, že v nemocnici je pro účel ochrany skladu léků vhodnější umístit kameru dovnitř skladu než sledovat zvenčí vstupní dveře včetně celé chodby. Jako příklad použití kamer v nesmyslném čase lze uvést kauzu městského úřadu, kde bylo „chráněno“ vybavení čekárny pořizováním záznamu v pracovní době, kdy celý prostor čekárny byl sledován 12 úředníky přes prosklené přepážky jejich pracovišť, avšak po pracovní době byl systém vypínán, takže případný zloděj by nebyl sledován ani úředníky, ani kamerami.

Při projednávání závěrů kontrolních protokolů se inspektoři neustále setkávají nejen s nepochopením a neznalostí principů ochrany osobních údajů, ale s neúctou k soukromí vůbec. Argumentace právy, zaručenými Listinou základních práv a svobod, zejména právem každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě, je obvykle ze strany provozovatelů (správců) zpochybňována argumenty ekonomickými.

Stále častější je také situace, kdy jednotlivé prvky kamerového systému jsou pouhými maketami, nebo některé technologické prvky kamerového systému (kamery, vodiče) jsou sice instalovány, avšak jsou nefunkční, a systém je tak využíván pouze pro „placebo-efekt“. Takový způsob ochrany může být samozřejmě velmi efektivní, vzhledem k jeho psychologickému účinku na případné pachatele nežádoucího chování. Inspektoři se však setkávají s případy, kdy i takový systém velmi výrazně zasahuje do soukromého a osobního života lidí a jeví se jako evidentně nežádoucí.

Jako skutečně odstrašující příklad, se zjevným dopadem do soukromí sledovaných osob, lze uvést provozování kamerového systému v domě s pečovatelskou službou (DPS), který je ve správě městské části statutárního města. Obyvatelé DPS si stěžovali, že kamerovým systémem je preventivně zaznamenáváno jejich chování v celém domě. Takové bezdůvodné monitorování pociťovali obyvatelé jako újmu a porušování základního práva na soukromí. Stížnost se jevila o to závažnější, že v domech s pečovatelskou službou jsou byty zvláštního určení pro osoby, které mají sní-

ženou soběstačnost z důvodu věku, chronického onemocnění nebo zdravotního postižení.

Při kontrole bylo zjištěno, že v domě je instalován funkční kamerový systém a provozovatelem je městská část statutárního města. Kamery zabírají chodby domu včetně vchodu do některých bytů. Systém je v nepřetržitém provozu, signál z kamer je přenášen na vrátnici objektu do technologických zařízení umožňujících záznam signálu. Záznamové zařízení (videorekordér) je standardně nastaveno na režim „pořizování záznamu“, obsluha (personál DPS) pravidelně po ukončení nahrávacího cyklu vyměňuje nahrané videokazety. Při podrobné prohlídce technického zařízení však bylo zjištěno, že záznam není pořizován, neboť chybí propojení jednotlivých komponent. Rovněž kontrolou videokazet se záznamem bylo zjištěno, že je pořizován záznam bez signálu, tedy nic. Tato skutečnost byla potvrzena i vedením radnice, které prokazatelně takovýto bezzáznamový režim nastavilo. O bezzáznamovém režimu však radnice obyvatele DPS úmyslně neinformovala. Informován nebyl ani obslužný personál DPS, který má zakázáno měnit nastavení systému a neví ani o tom, že ve skutečnosti se záznam nepořizuje.

Výsledkem je tedy stav, kdy obyvatelé DPS, jejich návštěvy i osoby zde zaměstnané se oprávněně domnívají, že jejich život v DPS je nahráván, soukromí ohrožováno, a trpí obavami, jak je s nahrávkami dále nakládáno.

V uvedeném případě bylo zjevné, že soukromí obyvatel DPS je bezdůvodně narušováno. Nedochází zde však ke zpracování osobních údajů, a tak možnost efektivního zásahu Úřadu, např. formou uložení nápravných opatření, je zde pro věcnou nepříslušnost nemožná. Inspektor doporučil vedení radnice, aby alespoň komunikací s obyvateli DPS situaci urovnalo. Stěžovatelům byly výsledky kontroly sděleny s radou, aby v případě přetrvávání nežádoucího stavu řešili věc občanskoprávní cestou. Celý případ, který ovšem zdaleka není ojedinělý, ukazuje na možné nežádoucí zneužívání monitorovacích systémů s významnými dopady do soukromí občanů a mohl by být impulsem pro řešení *de lege ferenda*.

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PRO NABÍZENÍ OBCHODU A SLUŽEB

V roce 2007 obdržel Úřad větší počet stížností směřujících proti marketingovým firmám. Standardním obsahem těchto stížností je poukazování na činnost marketingových firem, které zasílají občanům nevyžádané listovní zásilky s reklamními tiskovinami a s nabídkou obchodu a služeb. Občané si většinou stěžovali na to, že obdrželi zásilku, přestože vůči firmě uplatnili nesouhlas se zasíláním nabídek. Při kontrolách těchto firem se v rámci zákonem stanovené součinnosti prověřovaly i zdroje jejich osobních údajů, tedy firmy spolupracující s firmou kontrolovanou. V rámci každé kontroly je tak prověřena činnost většího počtu firem.

Na základě kontrol se zjistilo, že problematika takto opakovaně zasílaných nabídek se projevuje ve dvou rovinách.

Prvním a zásadním problémem je skutečnost, že občan (jak bylo v naprosté většině případů zjištěno) udělil souhlas se zasíláním nabídek. Je téměř pravidlem, že takový souhlas udělil jiné firmě nežli té, od níž zásilku obdržel a na jejíž postup si stěžuje. To však nemusí být nezákonným postupem. V takových případech se vždy zkoumá kvalita uděleného souhlasu, zejména to, zda udělený souhlas obsahuje ustanovení o právu předávání osobních údajů občana i dalším firmám. V rámci kontroly bývá většinou potvrzeno, že souhlas obsahuje klauzuli typu „zákazník svým podpisem uděluje souhlas s předáváním poskytnutých osobních údajů všem obchodním a marketingovým partnerům naší firmy“. Poté se prověřuje, zda mezi firmami je skutečně obchodní či marketingový vztah, což bylo doposud vždy potvrzeno. Skutkový stav je tak zjištěn a právní posouzení problému je již velmi jednoduché a v neprospěch stěžovatele. Vzhledem k tomu, že správce osobních údajů má zákonem stanoveno právo předávat osobní údaje (v rozsahu jméno, příjmení a adre-

sa) dalšímu správci za účelem nabízení obchodu a služeb, pokud subjekt údajů (tedy občan) byl o tomto postupu správce předem informován a nevyslovil s tímto postupem nesouhlas, je nutno v takových případech posoudit jednání správce, tedy zasilatelské firmy, jako oprávněné a porušení zákona konstatovat nelze.

Takové případy nechť jsou varováním pro občany, kteří dobrovolně (a obvykle s vidinou nějaké drobné výhody či slevy či možného zařazení do nějakého výherního slosování) podepíší v podstatě „bezbřehý" souhlas s předáváním svých osobních údajů, a pak jsou překvapeni, jaké množství firem je obesílá svými nabídkami.

Druhou problémovou rovinou je zasílání nabídek i přes nesouhlas občana s dalším zpracováním jeho osobních údajů za účelem nabízení obchodu nebo služeb. Podle zákona nesmí správce osobní údaje občana (které mohou být pouze v rozsahu jméno, příjmení a adresa) dále zpracovávat, pokud s tím občan vysloví nesouhlas. Takový nesouhlas musí být vysloven písemnou formou.

Jak bylo opakovaně zjištěno, stěžovatelé po obdržení zásilky uplatnili svůj nesouhlas se zasíláním dalších nabídek a požadovali vymazání svých osobních údajů z registru zasilatelské firmy. Po obdržení další zásilky pak žádali Úřad o nápravu. V rámci kontrolních šetření se prověřovalo, jakou formou byl nesouhlas uplatněn a po jaké době od vyslovení nesouhlasu obdrželi stěžovatelé další zásilky.

Velmi problematické bylo dodržení ustanovení zákona o nezbytnosti písemného vyjádření nesouhlasu. Stěžovatelé většinou nebyli schopni doložit, kdy a jakým způsobem vyjádřili svůj nesouhlas. Buď se odvolávali na telefonát, který vedli s nějakým pracovníkem zasilatelské firmy, nebo uváděli, že nesouhlas byl zaslán běžnou poštovní zásilkou nebo e-mailovou poštou. Pokud potom při místním kontrolním šetření v zasilatelské firmě nebylo možno zjistit, zda firma skutečně takový nesouhlas obdržela, a stěžovatel rovněž není schopen doklad dohledat, nelze v takovém případě konstatovat, že činnost zasilatelské firmy je v rozporu se zákonem. Ovšem stěžovatelé jsou v takových případech vždy informováni o tom, že svůj nesouhlas mají písemně vyjádřit znovu a doklad o jeho podání si uschovat. V případě, že by firma pokračovala v zasílání nabídek, mají možnost znovu podat stížnost Úřadu. Je třeba však konstatovat, že žádnou takovou opakovanou stížnost již inspektor ke kontrole neobdržel.

Prověřováno bylo rovněž několik podnětů, kdy stěžovatel řádně vyslovil nesouhlas se zpracováním osobních údajů, podání bylo stěžovatelem doloženo, a zasilatelská firma přesto pokračovala v zasílání nabídek. Ve všech těchto případech bylo zjištěno, že další zásilky obdrželi stěžovatelé vždy přibližně do tří týdnů ode dne vyslovení nesouhlasu, přičemž tyto další zásilky byly již zásilkami posledními, které stěžovatelé obdrželi. V těchto případech inspektor nekonstatoval rozpor se zákonem. Důvodem pro takový právní názor je skutečnost, že pro marketingové firmy je z organizačních a technologických důvodů již obvykle nemožné okamžitě reagovat na každý nesouhlas zákazníka se zpracováním jeho osobních údajů tak, aby mu již připravovaná další zásilka nebyla doručena. Osobní údaje zákazníka již objektivně nelze vyřadit ze zpracování, když jsou již v běhu automatizované technologicko-organizační procesy, zejména tisk, expedice a distribuce zásilek, navíc částečně zajišťované i dodavatelsky. Proto je inspektorem tolerována uvedená doba přibližně tří týdnů jako lhůta, po kterou ještě může zákazník následnou zásilku obdržet, přestože vyslovil nesouhlas.

K problematice činnosti marketingových firem je třeba dodat, že provedené kontroly se týkaly zejména nejvýznamnějších a nejčastěji prezentovaných firem na marketingovém trhu v ČR. V rámci kontrol těchto firem nebylo ani v jednom případě zjištěno, že by byly zasílány nabídky i přes nesouhlas zákazníka. Standardně mají tyto firmy nastavenou organizaci práce tak, aby k takovému zasílání naopak nemohlo

dojít. Vyplývá to i z logiky věci, kdy pro marketingovou firmu je zjevně nežádoucí zbytečně vynakládat finanční prostředky na zasílání nabídek nesouhlasícímu zákazníkovi a ještě k tomu riskovat právní problémy.

PŘÍSTUP SUBJEKTU ÚDAJŮ K INFORMACÍM O VYUŽÍVÁNÍ OSOBNÍCH ÚDAJŮ EVIDENCE OBYVATEL

Právo na přístup k informacím o zpracování osobních údajů, které je v obecné poloze zakotveno v ustanovení § 12 zákona o ochraně osobních údajů, se promítlo i do praxe poskytování osobních údajů z informačních systémů veřejné správy na základě zvláštního zákona. Na základě novelizovaného znění § 12 s účinností od 26. července 2004 doznala změn i praxe. To platí rovněž pro informační systém evidence obyvatel (dále jen „informační systém"). Informační systém obsahuje zákonem taxativně stanovené údaje o občanech a o cizincích s povolením k pobytu na území České republiky a o osobách, kterým byl udělen azyl na území České republiky. Právo na přístup k informacím upravuje § 8 zákona 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o evidenci obyvatel").

O poskytnutí údajů lze požádat Ministerstvo vnitra, krajský úřad nebo obecní úřad obce s rozšířenou působností. Vzor tiskopisu Žádost o poskytnutí údajů z informačního systému stanoví prováděcí vyhláška k zákonu o evidenci obyvatel: vyhláška č. 296/2004 Sb., kterou se provádí zákon o evidenci obyvatel a kterou se mění vyhláška č. 177/2000 Sb., kterou se provádí zákon o evidenci obyvatel, zákon o občanských průkazech a zákon o cestovních dokladech, ve znění pozdějších předpisů. Informace o tom, kdo a za jakých podmínek může o takové informace žádat, jsou zveřejněny také na webových stránkách Ministerstva vnitra. Na žádost se poskytují výpisy z informačního systému ve shodné obsahové struktuře a se shodnou formální úpravou. Takto lze požádat i o záznam o výdeji údajů. Žadatel obdrží přehled ve formě výpisu z datového souboru. Všechny výpisy mají stejnou formální strukturu a obsah. Obsahují záznam o datu a hodině výdeje a o tom, komu byly údaje poskytnuty. Údaj o příjemci osobních údajů se uvádí ve formě názvu státního orgánu nebo orgánu veřejné správy. Příjemcem se rozumí výhradně orgán, který požádal o přidělení uživatelského oprávnění.

Na základě takových výpisů podali v březnu, dubnu a červenci 2007 tři stěžovatelé Úřadu stížnost. Všichni se na základě přehledu informací o tom, komu byly jejich osobní údaje z informačního systému poskytnuty, domnívali, že jejich osobní údaje byly využívány neoprávněně. Někteří se domnívali, že na základě podané stížnosti jim bude poskytnut jmenný seznam lidí, kteří „zneužili" jejich osobní údaje.

Správnost a vypovídací hodnota výstupu, tedy poskytnutí osobních údajů z informačního systému, který vypracovalo vždy Ministerstvo vnitra, byly předmětem kontroly. Bylo zjištěno, že struktura, rozsah a věcný obsah informací uvedených ve zprávě, jímž je subjektu údajů na jeho žádost předávána informace o zpracování osobních údajů, neodpovídají v části *záznamy o výdeji údajů* obsahu ustanovení § 12 odst. 2 písm. d) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů"), v prvé řadě tím, že nedostojí legitimnímu očekávání úplnosti, a dále tím, že nejsou subjektu údajů srozumitelné, a nakonec tím, že nesplňují ani požadavky § 8 odst. 6 zákona o evidenci obyvatel.

Výpis pro stěžovatele Z. pokrývá období od 24. července 2000 do 20. března 2007, pro stěžovatelku T. od 20. července 1998 do 17. dubna 2007 a pro stěžovatelku J. podchycuje auditní záznamy od 6. ledna 1998 do 27. dubna 2007. U stěžovatelky T. výpis uvádí šest příjemců. Praha hl. město je uvedena jako příjemce ve dvou případech v roce 1999, tedy v době, kdy příjemcem nebyla. U stěžovatele

Z. jsou uvedeni tři příjemci, u stěžovatelky J. sedm příjemců. Městský úřad Havlíčkův Brod a Magistrát hlavního města Prahy jsou uvedeny také jako příjemci v době, kdy přístupem do informačního systému, jehož výrazem záznamy o výdeji jsou, nedisponovaly. U několika auditních záznamů byl zjištěn nesoulad s údajem poskytnutým žadateli: např. z deseti záznamů, kdy byly během jednoho dne automaticky zaznamenány dva a více vstupů, je uveden pouze první; v jiném případě byl uveden z šesti záznamů, kdy byly během jednoho dne automaticky zaznamenány dva a více vstupů, pouze první. Zjištěn byl dále rozdíl v označení příjemce. Jako příjemce je ve všech výpisech uvedeno samo Ministerstvo vnitra. Je tomu tak v případech, kdy osobní údaje stěžovatelů použilo k vyřízení *žádosti o poskytnutí údajů z informačního systému*. Ve výpisech poskytnutých stěžovatelům je uvedeno vyhledání Ministerstvem ještě v dalších 14 případech: ministerstvo tyto záznamy označilo jako chybně připsané. Doložilo ještě použití osobních údajů jednoho ze stěžovatelů k vyřízení žádosti o vystavení lustračního osvědčení.

Z informačního systému se informace o poskytnutí osobních údajů sdělují na základě záznamů, které Ministerstvo vede ve stejném rozsahu a ve shodné formě již od dob před nabytím účinnosti jak zákona o evidenci obyvatel, tak zákona o ochraně osobních údajů. To se jeví jako zdroj problémů pro subjekt údajů a posléze i ve vztahu k zákonu o ochraně osobních údajů. Záznamy o předání mohou být pro subjekt údajů nevysvětlitelné. Pro jejich správnou interpretaci je nutná znalost vývoje právní úpravy evidence obyvatel: *údaj o výdeji* je zaznamenán i při každém použití pro potřeby vedení datových souborů s osobními údaji, o nichž tak stanoví zákon, např. výkonu státní správy na úseku občanských průkazů nebo cestovních dokladů. Ministerstvo se ještě v době kontroly rozhodlo aplikovat názor, že výpis z informačního systému bude poskytován od data, k němuž nabyl účinnosti zákon o evidenci obyvatel. Naproti tomu auditní záznamy k informačnímu systému nepodchycují zpracování hromadných výdejů, uskutečňovaných na základě zákona. Objem takových sestav a rozsah v nich uvedených osobních údajů byl v předchozích letech značný. V době, kdy byla kontrola Úřadu prováděna, byly takové sestavy s osobními údaji zpracovávány pouze pro Všeobecnou zdravotní pojišťovnu. Ostatní příjemci osobních údajů z informačního systému již mají být uváděni adresně v auditních záznamech ve spojení s vlastním uživatelským oprávněním.

Na základě výsledků kontroly uložil Úřad opatření k nápravě. Každému stěžovateli byly zaslány doplněné a opravené záznamy o hodině a datu výdeje podle ustanovení § 8 odst. 6 zákona o evidenci obyvatel. Splnění ostatních uložených opatření přímo zaznamenávají všichni žadatelé o poskytnutí záznamu o výdeji údajů. Přesto je třeba počítat s tím, že přijímaná opatření směřují do budoucnosti a kompenzovat nedostatky minulého stavu je možné jen do určité míry. Záznamy o výdejích pořízené před 1. zářím 2006 nelze považovat za úplné. Žadatelé o takové informace z informačního systému by měli věnovat pozornost doprovodným informacím, poskytovaným Ministerstvem vnitra, nebo se seznámit podrobně s právní úpravou.

S účinností od 1. září 2006 se v informačním systému evidence obyvatel vedou podle § 3 odst. 8 záznamy o přístupech do informačního systému, které obsahují: přidělené uživatelské jméno zpracovatele údajů, den, měsíc, rok a čas zpracování, rodné číslo obyvatele, jehož údaje jsou poskytovány, nebo jiný údaj, který je pro vyhledání tohoto obyvatele rozhodující. Vyhledání příslušného obyvatele se přitom uskuteční prostřednictvím dalších obyvatel, pro něž je rozhodující údaj společný a důvod a konkrétní účel přístupu do informačního systému. Tyto záznamy jsou podkladem pro podání zprávy žadatelům. Lze tak předpokládat, že záznamy o poskytnutí osobních údajů jiným příjemcům, vypovídající o sdělení osobních údajů po tomto datu, již nebudou zdrojem podobných problémů.

Stížnosti, na jejichž základě byla tato kontrola provedena, spojovalo ještě očekávání, že úkolem Úřadu je prověřit veškeré souvislosti jimi napadeného nakládání

s osobními údaji a svá zjištění jim poskytnout. Tato očekávání nemají ovšem oporu v zákoně, a nemohou proto být naplněna. Informace o zpracování – v daném případě výpis z informačního systému – je přímým naplněním práva člověka jako subjektu údajů být informován o zpracování. Takto nabytý přehled za podmínek stanovených zvláštním zákonem je základem pro případné uplatnění práv vůči správci a zpracovateli postupem podle § 21 zákona o ochraně osobních údajů. Tento zákon dává člověku právo reagovat na nesrozumitelné nebo nepravdivé, či jen nepřesné, sdělení od správce a požádat o vysvětlení, případně o nápravu zjištěného nesprávného stavu, bez ohledu na to, zda postup při získání výchozích informací o zpracování je upraven zvláštním zákonem. Pokud žádost adresovaná správci nebo zpracovateli o vysvětlení nebo nápravu závadného stavu nevede k objasnění a popř. nápravě, vytváří důvodné podklady pro uplatnění dozorových povinností Úřadu.

Stížnosti na poskytování informací o zpracování osobních údajů v informačním systému evidence obyvatel tak na jedné straně nenaplnily očekávání stěžovatelů, na straně druhé přispěly k vytvoření podmínek pro lepší naplňování práva subjektu údajů ve zpracování, jež má význam pro všechny obyvatele České republiky.

INCIDENČNÍ KONTROLA ZAMĚŘENÁ NA DODRŽOVÁNÍ ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ SUBJEKTEM ČINNÝM V KOMUNÁLNÍ POLITICE PŘI ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ČLENŮ

(vůči subjektu činnému v komunální politice směřovaly dva podněty)

1. podnět:

Původce podnětu byl členem kontrolovaného. Řádný orgán kontrolovaného v místě A. (jehož byl původce podnětu řádným členem) projednal na řádném jednání anonymní dopis směřující vůči původci podnětu. Kontrolovaný, z toho pět jeho významných funkcionářů, dostali nezávisle na sobě poštou stejný anonymní dopis obsahující stejné přílohy, které obsahovaly kopie dokumentů dokazujících nepravdivost písemného závazku původce podnětu stvrzeného jeho podpisem na přihlášce o členství kontrolovaného. Řádný orgán kontrolovaného projednal na řádném jednání anonymní dopis směřující vůči původci podnětu. K dispozici měl přihlášku k členství kontrolovaného obsahující identifikační a kontaktní osobní údaje původce a již zmíněný anonymní dopis obsahující stejné přílohy, které obsahovaly kopie dokumentů dokazujících nepravdivost písemného závazku původce podnětu stvrzeného jeho podpisem na přihlášce o členství kontrolovaného. Rodné číslo se vyskytovalo na obou dokumentech a bylo to rodné číslo původce podnětu. Původce podnětu nepochybně poskytl své rodné číslo se souhlasem jak podle zákona o ochraně osobních údajů tak i podle zákona o evidenci obyvatel a rodných číslech a to jak kontrolovanému tak i subjektu, jemuž patřily kopie dokumentů dokazujících nepravdivost písemného závazku původce podnětu stvrzeného jeho podpisem na přihlášce k členství kontrolovaného.

Problém č. 1: Jak se dostali pisatelé anonymního dopisu k přihlášce k členství kontrolovaného původce podnětu obsahující jeho identifikační a kontaktní osobní údaje včetně rodného čísla? Pisatelé anonymního dopisu znali kontaktní osobní údaje pěti významných funkcionářů kontrolovaného (jejich adresy) v místě A.

Problém č. 2: Jak se dostali pisatelé anonymního dopisu ke kopiím příloh, které byly již šest let staré a pravděpodobně již dávno archivované? Tyto přílohy byly vytvořeny v lokalitě vzdálené cca 200 km od místa působení již zmíněného řádného orgánu kontrolovaného (jehož byl původce podnětu tehdy řádným členem), a to v místě B, jinou právnickou osobou. Tyto přílohy byly interní dokumenty, o jejichž existenci mohlo vědět pouze několik málo osob.

Kontrolní zjištění 1. podnětu:

Součinnost kontrolujících s orgány činnými v trestním řízení neodhalila identitu pisatelů anonymního dopisu. To jednak způsobilo, že nebyla bezezbytku vyřešena otázka „jak se dostali pisatelé anonymního dopisu k přihlášce původce podnětu k členství u kontrolovaného, obsahující jeho identifikační a kontaktní osobní údaje“ přesto, že kontrolovaný má fyzicky řádně zajištěny své místnosti, v nichž pracuje řádný orgán kontrolovaného v místě A. Přihlášky členů v písemné podobě jsou uloženy v uzamykatelné dřevěné skříni umístěné v malé zasedací místnosti, kde je i kopírovací přístroj. K evidenci aktuální členské základny v elektronické podobě a k evidenci svých bývalých členů používá kontrolovaný programový produkt „X“, vyvinutý pro podobné využití. Kontrolovaný v interních směrnicích stanovil povinnosti osob (zaměstnanců kontrolovaného) při zabezpečení osobních údajů tak, že pověřený zaměstnanec odpovídá za zamezení neoprávněnému přístupu k osobním údajům a svým pokynem určuje opatření používaná při jejich nakládání a zabezpečení, a dále, že pověřené osoby přicházející do styku s osobními údaji členů jsou vázány mlčenlivostí o osobních údajích a bezpečnostních opatřeních v rozsahu pokynu pověřeného zaměstnance. Nicméně kontrolující vypátrali a prokázali, že v inkriminovaném období, v případě přístupu k přihláškám uchazečů o členství u kontrolovaného, se k těmto přihláškám mohli snadno dostat i nepověření členové a dokonce i nečlenové kontrolovaného, kteří navštívili místnost kontrolovaného v místě A. a věděli o umístění přihlášek, aniž odpovědný zaměstnanec o tom věděl, a tím kontrolovaný vytvořil podmínky pro neoprávněný přístup k přihláškám uchazečů o členství u kontrolovaného. Tuto situaci však zákon o ochraně osobních údajů nepřipouští.

Dále neodhalení identity pisatelů anonymního dopisu nevyřešilo problém č. 2, a to „jak se dostali pisatelé anonymního dopisu ke kopiím příloh obsahujícím osobní údaje, které byly již šest let staré a pravděpodobně již dávno archivované“. Nevyřešením problému č. 2 paradoxně vznikly zákonné podmínky pro provedení kontroly zaměřené na dodržování zákona o ochraně osobních údajů u již zmíněné jiné právnické osoby působící mimo jiné i v místě B.

2. podnět:

Původce podnětu je členem kontrolovaného. Řádný orgán kontrolovaného v místě C. (jehož je původce podnětu řádným členem) projednal na řádném jednání dokumenty směřující vůči původci podnětu. Projednání probíhalo tak, že tehdejší předseda řádného orgánu kontrolovaného na zasedání tohoto orgánu měl při úvodním projevu k dispozici složku obsahující částečně osobní údaje původce podnětu a jeho rodiny a částečně informace o údajné trestné činnosti původce podnětu. Na jednání bylo přítomno okolo 160 členů. Původce podnětu byl označen za člověka „zlotřilého“, který před časem páchal trestnou činnost. Po skončení svého projevu vyzval tehdejší předseda řádného orgánu kontrolovaného přítomné, aby přišli nahlédnout do složky, mají-li zájem, že jim to umožní. Několik přítomných se šlo na výše zmíněné materiály podívat. Dle původce podnětu byla složka obsahující částečně osobní údaje původce podnětu a jeho rodiny a částečně údaje o jeho údajné trestné činnosti dále distribuována a on sám ji získal na již zmíněném řádném jednání. Součástí podnětu byla i složka obsahující částečně osobní údaje původce podnětu a jeho rodiny a částečně údaje o jeho údajné trestné činnosti.

Problém č. 3: Jakou cestou se dostala složka obsahující částečně osobní údaje původce podnětu a jeho rodiny a částečně údaje o údajné trestné činnosti původce podnětu a obsahující jeho identifikační a kontaktní osobní údaje k předsedovi řádného orgánu kontrolovaného působícího v místě C.?

Kontrolní zjištění 2. podnětu:

Tehdejší předseda řádného orgánu kontrolovaného působícího v místě C dostal složku obsahující částečně osobní údaje původce podnětu a jeho rodiny a částečně údaje o údajné trestné činnosti původce podnětu od jiného člena X, a to z titulu zastávané funkce. Člen X dostal poštou anonym, který obsahoval již zmíněnou složku. Později tehdejší předseda řádného orgánu kontrolovaného působícího v místě C. v rámci své výpovědi orgánům činným v trestním řízení jim výše zmíněnou složku předal. Kontrolující zahájili součinnost s orgány činnými v trestním řízení, pokud jde o podnět č. 2. V kopii dokumentu, označeného v záhlaví *Registr osob* a poskytnutém orgány činnými v trestním řízení, byly začerněny některé osobní údaje (např. rodná čísla). Kontrolujícími bylo prokázáno, že dokumenty označené v záhlaví *„Registr osob"* nebyly na jednání řádného orgánu kontrolovaného rozmnožovány. Dále kontrolující zjistili, že dokument označený původcem podnětu za materiál distribuovaný tehdejším předsedou řádného orgánu kontrolovaného působícího v místě C. neměl začerněny osobní údaje původce podnětu a jeho rodiny.

Další součinností s orgány činnými v trestním řízení ve věci složky obsahující částečně osobní údaje původce podnětu a jeho rodiny a částečně údaje o jeho údajné trestné činnosti a označené v záhlaví *„Registr osob"* bylo zjištěno, že:

- předmětný listinný materiál neobsahuje identifikační znaky, na jejichž základě by mohla být ustanovena doba lustrace v Informačním systému orgány činnými v trestním řízení k osobě poškozeného, tedy původce podnětu a osoba, která tuto lustraci vykonala;
- z výpisu sledování dotazů z Informačního systému orgánů činných v trestním řízení, opatřeného za období jednoho roku, je nemožné z objektivních důvodů (zejména s ohledem na četnost obecně zadaných dotazů do informačního systému a s ohledem na neznalost bližších okolností, za kterých byl podkladový materiál předán) ustanovit konkrétní lustraci, na jejímž základě mohl být předmětný listinný materiál vyhotoven;
- přístup do Informačního systému orgánů činných v trestním řízení bez zanechávání stop má umožněno ze zákona několik samostatných subjektů.

S výše uvedeným závěrem byla tato další součinnost s orgány činnými v trestním řízení ukončena (a další kontrola nebyla zahájena).

Jelikož se na kontrolovaného vztahuje ustanovení § 9 písm. e) zákona o ochraně osobních údajů, z něhož vyplývá, že je možné zpracovávat citlivé údaje bez souhlasu subjektu údajů podle ustanovení § 9 písm. a) zákona o ochraně osobních údajů, jestliže jde o zpracování, které sleduje politické, filosofické, náboženské nebo odborové cíle, prováděné v rámci oprávněné činnosti občanského sdružení, nadace nebo jiné právnické osoby nevýdělečné povahy (dále jen „sdružení"), a které se týká pouze členů sdružení nebo osob, se kterými je sdružení v opakujícím se kontaktu souvisejícím s oprávněnou činností sdružení, a osobní údaje nejsou zpřístupňovány bez souhlasu subjektu údajů, a o takové zpracování citlivého údaje, jímž je osobní údaj vypovídající o politických postojích těchto fyzických osob, se u kontrolovaného v daném případě jedná, je kontrolovaný oprávněn toto zpracování provádět bez souhlasu subjektu údajů podle ustanovení § 9 zákona o ochraně osobních údajů a neporušil tedy ustanovení § 9 písm. a) zákona o ochraně osobních údajů.

Kontrolou bylo zjištěno porušení ustanovení zákona o ochraně osobních údajů:
Kontrolovaný porušil ustanovení § 13 odst. 1 zákona o ochraně osobních údajů tím, že umožnil neoprávněný přístup k evidenci přihlášek fyzických osob.

Zaměstnavatel jako správce osobních údajů

Zaměstnavatel je bezpochyby správcem osobních údajů, a tudíž smí shromažďovat pouze takové osobní údaje, které jsou nezbytné pro naplnění stanoveného účelu, v daném případě plnění povinnosti zaměstnavatele. Tyto povinnosti spočívají ve výpočtu mzdy, hlášení na sociálním úřadě a odvodu sociálního a zdravotního pojištění. K tomu jsou nutné tyto osobní údaje: Příjmení, Jméno, Všechna dřívější příjmení, Datum a místo narození, Rodné číslo, Číslo občanského průkazu. V případě, že zaměstnanec pobírá slevu na daních na své děti, musí zaměstnavatel dodat, a tudíž zpracovávat, rodná čísla dětí zaměstnanců. V případě, že zaměstnavatel svým zaměstnancům také vyplňuje daňová přiznání, potřebuje navíc mít informace o manželovi / manželce. Pro výpočet mzdy bývá často potřebné znát předchozí zaměstnání. Otázku, zda je zaměstnanec kuřák či nekuřák, je rozumné vyřešit při přijímání: např. v provozovně společnosti není dovoleno kouřit. Další dovednosti, ke kterým se zaměstnanec sám hlásí, lze brát jako jeho přednosti pro případ hledání jeho lepšího využití zaměstnavatelem.

Pokusili jsme se proto zpracovat seznam osobních údajů, které jsou povinné pro plnění povinností zaměstnanců:

Při nástupu do zaměstnání uzavírá zaměstnavatel s budoucím zaměstnancem pracovní smlouvu, která podle zákoníku práce obsahuje identifikační údaje zaměstnance (podle správního řádu jméno, příjmení, datum, místo narození a místo trvalého pobytu)

Zaměstnavatel má právo zpracovávat tyto osobní údaje:

Pro evidenční listy důchodového pojištění zasílaných na PSSZ (Pražská správa sociálního zabezpečení – § 37 zákona o organizaci a provádění sociálního zabezpečení):

– datum a místo narození,
– všechna dřívější příjmení,
– rodné číslo,
– místo trvalého pobytu.

(Byl-li občan účasten důchodového pojištění v cizině a zaměstnavatel je jeho prvním zaměstnavatelem po ukončení důchodového pojištění v cizině, rovněž údaj o názvu a adrese cizozemského nositele pojištění a cizozemském čísle pojištění.)

Pro správný výpočet mzdy: vzdělání, předchozí praxe;
Pro správný výpočet měsíčních záloh na daně (podle zákona o správě daní a poplatků): druh pobíraného důchodu;
Pro zjištění přesného data nároku na odchod do starobního důchodu (podle zákona o organizaci a provádění sociálního zabezpečení): počet dětí (u žen);
Pro plnění povinného podílu osob se zdravotním postižením na celkovém počtu zaměstnanců (podle § 83 zákona o zaměstnanosti): zdravotní znevýhodnění;
Pro placení zdravotního pojištění (podle § 10 zákona o veřejném zdravotním pojištění): zdravotní pojišťovna;
Za účelem hlášení zaměstnávání cizinců: státní občanství.

Prohlášení poplatníka daně z příjmu (podle *zákona o správě daní poplatků*):
Pokud zaměstnanec uplatňuje daňové zvýhodnění a manžel/ka je zaměstnán/a: Příjmení a jméno manžela/ky, název a adresa zaměstnavatele;
Pokud zaměstnanec uplatňuje zvýhodnění na vyživované dítě: Jméno, příjmení a rodné číslo dítěte.

Zaměstnavatel ovšem k osobním údajům zaměstnanců musí přistupovat jako k vlastnictví zaměstnanců, které má pouze propůjčené k určitým, předem daným a zákonem stanoveným účelům (viz výše) a používat je výhradně pro tyto své účely: výpočet mzdy, komunikace se zaměstnancem, možnost povýšení. Speciálně ustanovení § 13 zákona o ochraně osobních údajů říká, že správce musí učinit taková opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům. A neoprávněnou osobou je každý, kdo nemá ze zákona povinnost s osobními údaji pracovat. Tudíž je třeba uchovávat personální spisy např. v uzamčených skříních, dostupné pouze oprávněným osobám. Možnost přistupovat do jejich elektronického zpracování musí být omezena pouze na úzký okruh zaměstnanců a podle novely ustanovení § 13 zákona o ochraně osobních údajů je nutné všechna zpracování osobních údajů logovat (vést o nich záznam), přičemž zpracováním se rozumí i nahlížení. Týká se to obzvláště velkých podniků, které zpracovávají statisíce osobních údajů (často velmi citlivých), a přesto není nijak zaznamenáno, kdo z možných, třeba 25 osob, do nich nahlížel.

U menších podniků, zvláště závodů, je problémem předávání výplatních listů zaměstnancům, což se často děje způsobem, při kterém si ostatní zaměstnanci mohou přečíst mzdu i odměny ostatních. Informace o mzdě a o odměnách jsou osobní údaje, které mohou souviset i se závistí ostatních, tudíž je nelze zpřístupňovat ostatním.

Osobní údaje pro sociologický výzkum

Sociologové často získávají data pro svůj sociologický výzkum pomocí dotazníků, které považují za anonymní, protože nežádají základní identifikační údaje. Je ovšem třeba pečlivě zvažovat anonymitu takovýchto dat. Podle definice zákona o ochraně osobních údajů je osobním údajem každá informace o určeném nebo určitelném subjektu údajů. Určitelným subjektem se může osoba stát třeba pouze větším rozsahem osobních údajů samostatně neidentifikujících, popř. špatně vyplněnou otázkou. Tento problém je zvlášť patrný v případě dětí, které na jedné straně ještě nemohou posoudit riziko a nemohou tedy samy poskytnout souhlas se zpracováním svých osobních údajů, na druhé straně však mohou špatně pochopit otázku a odpovědí se v podstatě identifikovat (například zaměstnání otce: prezident republiky). V současném světě investigativních žurnalistů je třeba zvažovat riziko toho, zda by při příliš citlivých otázkách (drogy, sexuální život) některému novináři nestálo za to zjišťovat z množiny osobních údajů dítě, které dotazník vyplnilo.

Cestovní kancelář

Rozhodnutí o udělení pokuty ve výši 400 tisíc Kč jedné soukromé cestovní kanceláři, vyvolalo řadu následných akcí, jejichž spojovacím článkem byla právě uložená výše pokuty. Kromě toho, že na základě provedeného kontrolního a správního řízení nepochybně došlo k nápravě nesprávného stavu a ke zvýšení ochrany osobních údajů statisíců občanů, došlo především k tomu, že si bezpochyby nejen majitelé, vedoucí, ale i všichni zaměstnanci této společnosti konečně uvědomili podstatu problematiky ochrany osobních údajů.

Je třeba si připomenout, že v rámci průmyslu cestovního ruchu dochází ke zpracování výrazně vysokého počtu osobních údajů. Že jsou zpracovávány osobní údaje nejen občanů České republiky, ale i osobní údaje občanů třetích zemí, že v rámci cestovního ruchu musí docházet k předávání osobních údajů nejen mezi jednotlivými poskytovateli služeb, ale rovněž do zahraničí. S některou z cestovních kanceláří vycestoval za posledních patnáct let alespoň jednou téměř každý občan. Doposud bohužel stále přetrvává pocit, že cestovní kanceláře mají o svých cestujících jen mi-

nimum informací, které vlastně nelze zneužít. Vždyť v cestovní smlouvě se uvádí „pouze jméno, příjmení, adresa bydliště, telefon“. Jenže k těmto identifikačním údajům se pak přiřazují další informace, bez nichž nelze služby cestovního ruchu zajistit, tedy informace o tom, s kým, kam a za kolik si klient zájezd pořizuje. Ale také informace o zaměstnavateli, který přispívá na úhradu zájezdu, informace o požadavcích na ubytování, stravování a cestování, které mohou vycházet třeba ze zdravotního stavu nebo z náboženských stravovacích zvyklostí. K tomu je však nutno připočítat také údaje, které cestovní kanceláře shromažďují v souvislosti se zprostředkováním víz, pojištění, letenek atd. a které pouze předávají pojišťovnám, konzulátům a dalším. Často pak dochází ke kumulaci všech těchto údajů u cestovní kanceláře a u některých klientů využívajících věrnostní programy také k opakování a k obnově jednotlivých dat. V případě kontrolované cestovní kanceláře, která ve své databázi eviduje osobní údaje všech svých klientů, tedy za posledních patnáct let, by u některých klientů bylo možné zjistit například změny bydliště, telefonního spojení, případně zaměstnavatele, případné narození dětí, ale třeba i rozvod či sňatek apod. Samotná kontrola ukázala, že tato cestovní kancelář podstatně podcenila nakládání s osobními údaji při jejich předávání do zahraničí, zejména do tzv. rizikových zemí.

Riziko zneužití tedy nelze vyloučit ani přes sebedokonalejší zabezpečení elektronických databází včetně omezení přístupu k uloženým informacím, přičemž tato hrozba roste úměrně s počtem zpracovávaných údajů i s růstem cestovní kanceláře. Vzdálený elektronický přístup do klientské databáze o klientech, přeposílání osobních údajů při zajišťování objednaných služeb mezi jednotlivými provozovnami, smluvními prodejci a jednotlivými dodavateli služeb, navíc bez jakéhokoliv šifrování nebo kryptování zasílaných zpráv, prostřednictvím běžné e-mailové korespondence, kdy nelze vyloučit třeba i osobní selhání jednotlivce nebo záměnu adres, může vést ke ztrátě kontroly nad spravovanými osobními údaji. V případě kontrolované cestovní kanceláře lze rovněž předpokládat, že informace o cestujících politicích nebo tzv. celebritách by mohly být v některých případech zneužitelné například bulvárním tiskem. Běžná informace o tom, že někdo bude s celou rodinou v daném období v zahraničí, by mohla být návodem pro bytové zloděje. Nehledě na dodatečnou informaci, že ten a ten si pořídil zájezd za vyšší částku, takže lze předpokládat i lepší kořist v jeho prázdném bytě. Tomu lze kromě zákonného zajištění zabránit i tím, že informace o klientech se nebudou uchovávat v tak velkém rozsahu. V tom spočívá prvotní úkol každého správce osobních údajů, aby si sám zodpověděl otázku, zda a k čemu bude jednotlivé osobní údaje uchovávat. Zda budou využívány například k oslovování klientů konkrétní obchodní nabídkou nebo zda budou využívány pro kontrolu splnění kritérií při poskytování věrnostních slev různých specifických nabídek apod. Ve svém souhrnu jsou cestovní kanceláře a agentury jedním z největších zpracovatelů osobních údajů v České republice, protože bez osobních údajů nelze služby cestovního ruchu vůbec poskytovat.

Samostatný problém představuje plnění informační povinnosti a zcela opomíjený nárok občana, aby se s jeho osobními údaji nakládalo pouze s jeho vědomím a souhlasem. V rámci kontroly cestovní kanceláře, ale i z ostatních kontrol lze zobecnit, že nejen soukromé společnosti, ale i státní a obecní instituce si stále dostatečně neuvědomují, že subjekt údajů, tedy konkrétní fyzická osoba, má právo rozhodovat o svých osobních údajích samostatně, že má přirozené právo vědět, kdo, kdy a jak s jeho osobními údaji zachází a proč a za jakým účelem je má ve své databázi. A že pouze zákon může toto jeho právo omezit. Správci se mnohdy domnívají, že pokud již jednou získali nějaké osobní údaje, je pouze na nich, jak s nimi budou nakládat. To, že neoprávněným zpracováním osobních údajů zasahují do soukromí konkrétního člověka, jim v podstatě nedochází. Druhou stránkou této mince je pak skutečnost, že ti, kdo přistupují k nakládání s osobními údaji z pozice

správce, si neuvědomují, že v mnoha dalších životních situacích jsou naopak v pozici subjektu údajů.

Druhým významným aspektem výsledků rozhodovací činnosti Úřadu se stala skutečnost, že rozhodnutí o udělení pokuty jedné cestovní kanceláři vyvolalo řadu jednání, dotazů a žádostí o konzultace a o informace ze strany dalších subjektů cestovního ruchu. Úřad byl osloven oběma asociacemi, které zastřešují převážnou většinu cestovních kanceláří a agentur působících v České republice. Úřad poskytl přímé konzultace největším cestovním kancelářím. Na přednášky a semináře byly vysláni zástupci Úřadu, aby vysvětlili zástupcům cestovních kanceláří základní povinnosti, které zákon při zpracování osobních údajů ukládá. Vzhledem k postoji představitelů obou asociací cestovních kanceláří a agentur se tak podařilo oslovit převážnou část podnikatelských subjektů v oblasti cestovních kanceláří a agentur. Bohužel je nutno konstatovat, že při jednáních se zástupci jednotlivých cestovních kanceláří bylo zjištěno minimální povědomí o povinnostech, které jim jako správcům osobních údajů zákon při jejich zpracování ukládá. Lze se tedy domnívat, že teprve pokuta uložená v řádu o desítku vyšším oproti původní pokutě přiměla jednotlivé subjekty v takto významném odvětví, jakým cestovní ruch je, zabývat se důrazně ochranou osobních údajů. Na základě této zkušenosti lze pro Úřad vyvodit závěr, že ke zvýšení právního vědomí v oblasti ochrany osobních údajů by stačilo významným způsobem zvýšit sazby ukládaných pokut. Je to sice také jedna z možností, nelze ovšem opomíjet skutečnost, že i jednání s představiteli profesních a obdobných asociací je jednou z cest, jak zavést ochranu osobních údajů do praxe jednotlivých firem a institucí. Že je tato forma působení správná, se ukázalo i při jednání s představiteli resortu školství při řešení problematiky využívání kamerových systémů ve školách.

Pokuta ve výši 400 tis. Kč nepatří k nejvyšším, které dosud Úřad při své rozhodovací praxi uložil. Ač nejde o částku nevýznamnou, její výše dosáhla 20 % horní hranice zákonné sazby, lze tedy hovořit o uložení pokuty při dolní hranici. Přesto výše pokuty vyvolala odezvu nejen u samotné cestovní kanceláře, ale i u dalších cestovních kanceláří. Je logické, že zástupcům cestovního ruchu, kteří nemají podrobnější informace, se může zdát částka vysoká, nepřiměřená. Ale v rozhodovací praxi Úřadu se jednalo pouze o logické vyústění činnosti v dozorové činnosti. Uložení relativně vysoké částky je výsledkem skutečnosti, že cestovní kancelář nesplnila všechna nápravná opatření, uložená jí předchozí kontrolou. Bez problémů uhradila dřívější uloženou pokutu ve výši 20 tis. Kč, aniž napravila protizákonný stav. Právě k tomu Úřad při svém rozhodování o výši pokuty přihlédl. Cílem bylo přinutit toho, kdo soustavně porušuje zákon, k pořádku. Bez důsledné kontroly a bez možnosti vymáhat naplnění ukládaných nápravných opatření by bylo provádění kontrolní činnosti zbytečné.

I na základě jedné kontroly a následného správního řízení lze konstatovat, že důkladně prováděný dozor ve formě kontroly, důsledné vyžadování plnění nápravných opatření k odstranění chyb při zpracování osobních údajů a také správně zvolený způsob prostředků k dosažení nápravy, včetně uplatnění vyšší částky při ukládání pokut, je cestou k nápravě nezákonného stavu a k rozšíření právní gramotnosti v oblasti osobních údajů.

RFID

Nové technologie umožňující efektivněji sledovat pohyb zboží i osob jsou stále dokonalejší. Jednou z nebouřlivěji se rozvíjejících technologií nacházejících nové a nové aplikace jsou i čipy RFID (Radiofrekvenční identifikace). Je to vlastně spojení radiofrekvenční technologie s miniaturizovaným počítačem, který může vysílat identifikační signál, případně další údaje, a může komunikovat se čtečkou, nebo s dalšími čipy. Jeho zásadní vlastností je i to, že nemusí mít vlastní zdroj energie a vystačí s energií, kterou mu dodá vysílaným signálem čtečka. Podle délky vlaso-

vé antény pak vyšle své informace na vzdálenost od několika centimetrů až, zatím „jenom“, po 50 metrů. Velikost RFID čipu může být jen několik milimetrů nebo i méně a s rozvojem technologie se bude dále zmenšovat, takže se už hovoří o tzv. „informačním prachu“.

Ekonomické využití čipů a jejich možností je obrovské. Není tak daleko doba, kdy takovým čipem může být opatřen, katalogizován a sledován každý výrobek, a možná se dočkáme vědeckých studií, které nás budou uklidňovat, že to nepatrné zrníčko v rohlíku nemůže lidskému organismu uškodit. Nebudete však muset u pokladny hlásit, kolik a jaké rohlíky máte v nákupní tašce, a čtečka na rohu ulice bude moci zájemci ohlásit, kolik jste jich měli k snídani. Ale nejen pro marketing lze RFID čipy využít. Hlavním zájemcem o zvyky a sledování svých občanů je stát. I Evropská unie za horlivého přikyvování vlád hodlá dát zelenou využívání RFID čipů jak v komerčním, tak i ve „státním zájmu“. Máme již příklady doma. Naše nové pasy již obsahují RFID čip, na kterém jsou zaznamenány nejen všechny identifikační osobní údaje, ale také fotografie a v budoucnu i vaše otisky prstů. Záměrem EU je také co nejdříve zavést i občanské průkazy s čipem, na kterém by měly být nejen dříve uvedené údaje, ale i zdravotní dokumentace. Tyto údaje by měly být prý ochráněny před neoprávněným přečtením kódy, šifrováním a tím, že lidé, kteří budou spravovat čtecí systémy, budou dbát, aby se údaje a kódovací systémy nedostaly do nesprávných rukou. A až budeme všichni v databázích potenciálních sledovaných zločinců, budou všechny informace o našich zvycích, pohybech, atd. skutečně účinně chráněny státními orgány před neoprávněným využitím v něčí prospěch? Je zřejmé, že pro RFID čipy platí skoro více než pro oheň známé přísloví, že jsou dobrý sluha, ale zlý pán. Oheň nás může připravit o majetek nebo i o život, ale RFID čipy o soukromí a lidskou důstojnost.

Orgány Evropské unie stále otálejí se stanovením závazných pravidel používání RFID čipů, zejména v otázkách ochrany soukromí a osobních údajů, i když mají odborná stanoviska od pracovní skupiny WP 29, Evropského ochránce osobních údajů a dalších, a zavázaly se, že do konce roku 2007 s těmito pravidly seznámí veřejnost. Měly také navrhnout doplňky do Direktivy ePrivacy pro využívání oblasti RFID. I když i u nás se již několik let geometrickou řadou zvyšuje počet aplikací RFID, teprve na konci roku 2008 se mají analyzovat ekonomické a sociální vlivy RFID technologií a začne se uvažovat, jak ochranu před riziky začlenit do legislativy.

Úřad se samozřejmě nespoléhá na to, až konečně bude vytvořena příslušná legislativa, snaží se s využitím zákona o ochraně osobních údajů při kontrolách stanovit zásady, aby osobní údaje občanů mohly být ochráněny před zneužíváním. A počty kontrol zaměřených na možné zneužívání možností a vlastností čipů stále stoupají. Úřad již kontroluje In karty Českých drah, čipové karty magistrátů, škol i komerčních subjektů. Zákon o ochraně osobních údajů je bohužel jeden z mála právních nástrojů v ochraně osobních údajů v oblastech nových technologií, jakými jsou RFID čipy, kamerové systémy a mobilní technologie.

Český úřad zeměměřický a katastrální

Kontrolou byl v roce 2007 posouzen soulad současné právní úpravy Katastru nemovitostí České republiky (dále jen „katastr nemovitostí“) s principy ochrany osobních údajů.

V prvé polovině devadesátých let minulého století byla na základě usnesení vlády přijata koncepce komplexní digitalizace katastru nemovitostí. Jejím záměrem bylo nejen doplnit datovou základnu katastru nemovitostí, ale vytvořit moderní zdokonalený informační systém katastru nemovitostí, který by odpovídal současným i perspektivním potřebám státu a byl srovnatelný s obdobnými systémy v zemích Evropské unie.

Přínosem zdokonaleného informačního systému katastru nemovitostí mělo být zejména:

a) zrychlení a zkvalitnění činnosti katastrálních úřadů při vedení katastru nemovitostí,
b) dostupnost údajů katastru nemovitostí pomocí dálkového přístupu k datům prostřednictvím internetu,
c) nezávislost získávání údajů na místě vznesení dotazu a místě uložení dat, kdy bude možné získat údaje z kteréhokoliv katastrálního území ČR na každém katastrálním úřadu, popř. získat v odůvodněných případech údaje o vlastnictví nemovitosti fyzickými i právnickými osobami z území celé ČR (pro potřebu soudů, ministerstva vnitra, ministerstva financí).

Podle názoru kontrolujícího však při zadání realizace schválené koncepce se mělo přihlédnout k tomu, že směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů, která představuje v EU obecný právní rámec pro aplikaci principů ochrany osobních údajů, musí být transponována v souvislosti se vstupem ČR do EU do českého právního řádu. Podle názoru kontrolujícího nejde o postup mimořádný, což dokládají některé veřejně dostupné informace z jiných členských států EU (Např. v SRN je ochrana osobních údajů hlavním důvodem, proč lze nahlížet do katastru nemovitostí pouze tehdy, jestliže se uplatňuje právní zájem; zdůvodnění, že se jedná o obchodní vztahy, není dostačující. Ve Francii a Španělsku se poskytují písemné informace z evidence nemovitostí se souhlasem vlastníka.)

Osoby požadující kopii ze sbírky listin, která obsahuje rozhodnutí státních orgánů, smlouvy a jiné listiny, na jejichž podkladě byl proveden zápis do katastru nemovitostí, nepředkládají žádost, pouze zaplatí příslušný správní poplatek za ověření kopie. Tímto postupem jsou zpřístupňovány jak osobní údaje osob ve vlastnickém nebo obdobném vztahu k nemovitosti, tak i osobní údaje osob, které nemusí mít k předmětné nemovitosti žádný vztah. Podle ustanovení § 10 zákona o ochraně osobních údajů (dále jen ZOOU) však má správce a zpracovatel při zpracování osobních údajů dbát, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.

Podle § 5 odst. 1 písm. d) ZOOU musí správce osobních údajů shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Jak vyplývá z ustanovení § 1 katastrálního zákona, má být katastr nemovitostí veden jako soubor údajů o nemovitostech, jehož součástí je evidence vlastnických a jiných práv k nemovitostem. Účely pro vedení katastru jsou však stanoveny velmi rozsáhle a obecně, což přispívá k jejich zneužívání pro zjišťování informací ryze soukromoprávního charakteru, jejichž zneužití je přísně chráněno jinými právními předpisy. Jako příklad takto stanoveného účelu slouží zejména účel „tvorba dalších informačních systémů“, který je jako samostatný účel z hlediska principů ochrany osobních údajů vedených v katastru zcela nepřijatelný a v rozporu i s evropskými předpisy, týkajícími se ochrany soukromí. V tomto směru se odkazuje zejména na článek 6 směrnice 95/46/ES, který stanoví (obdobně i ZOOU v § 5), že osobní údaje musejí být zpracovány korektně a přípustným způsobem; sbírány pro stanovené účely, výslovně vyjádřené a legitimní, a nesmí být dodatečně zpracovávány způsobem neslučitelným s těmito účely; osobní údaje musí být přiměřené, podstatné a nepřesahující míru s ohledem na účely, pro které jsou sbírány a pro které jsou dodatečně zpracovávány.

Pokud jde o plnění ohlašovací povinnosti fyzických osob o změně sdílených údajů, existence § 5 vyhlášky č. 111/2001 Sb., vytváří podle názoru kontrolujícího dostatečné právní podmínky pro naplnění ZOOU stanovené právní povinnosti správce tím, že „Pokud u fyzické osoby, která je evidována v evidenci obyvatel a zároveň

jako vlastník nebo jiný oprávněný v katastru, dojde ke změně sdílených údajů katastru, postačí, pokud tato osoba oznámí změnu ohlašovně evidence obyvatel. Tím se považuje za splněnou její ohlašovací povinnost ohledně změny těchto údajů vůči správci katastru."

Podle názoru kontrolujícího právě tento právní předpis má přispívat nejen ke snížení administrativní zátěže kontrolovaného spojené se změnami osobních údajů osob evidovaných v katastru nemovitostí, ale má také významně snížit množství osobních údajů uchovávaných ve sbírce listin.

Kontrolující tak dospěl k závěru, že katastr nemovitostí je sice veden v souladu se zvláštním zákonem o katastru nemovitostí, ale v rozporu s obecným zákonem upracujícím podmínky pro zpracovávání osobních údajů.

V tomto směru je dále nezbytné uvést, že zpřístupňování osobních údajů jednotlivým fyzickým osobám výlučně pro jejich potřebu v libovolném rozsahu není v rozporu se ZOOU, neboť v souladu se směrnicí č. 95/46/ES a v souladu s § 3 odst. 3) ZOOU se stanoví, že se ZOOU nevztahuje na zpracování osobních údajů fyzickou osobou výlučně pro její potřebu. Ve všech ostatních případech je však ZOOU třeba aplikovat.

Spam a nevyžádaná obchodní sdělení

Spamu se ve sdělovacích prostředcích, ale i v běžném lidském životě věnuje čím dál více prostoru a času. Pravidelně vycházejí různé statistiky o tom, kolik procent běžné elektronické pošty je spam. Údaje se liší zejména podle toho, co autor pokládá za spam a nakolik míní veřejnost „šokovat". Je to 80 % či 90 % nebo jiné číslo? Zvláštní skupina OECD, na jejíž práci se Úřad podílel, vytvořila přehlednou příručku popisující tento problém včetně možností nápravy. Jedno z témat, o němž se diskutovalo, bylo právě „měření" spamu, a to proto, že je třeba zjistit, zda přijatá opatření budou mít nějakou účinnost a jakou. První problém nastal už v okamžiku, kdy se mělo stanovit, co se vlastně má měřit. Je zřejmé, že pokud budeme považovat za spam veškerou nevyžádanou poštu, dostaneme se v procentech velmi vysoko, neboť většina všech e-mailů je nevyžádaná. Většina osobní pošty je také v podstatě nevyžádaná a málokdo disponuje prokazatelným souhlasem příjemce předtím, než mu zašle zprávu. Takto však spam nikdo nechápe. Pokud si jako kritérium vezmeme obtěžování, je to opět velmi individuální otázka.

Obdrželi jsme například stížnosti na „spam" ze serveru "Spolužáci": Jsou tedy lidé, které obtěžuje, když je bývalí spolužáci lákají do hostince, na druhé straně jsou lidé, kteří např. uvítají výhodnou nabídku levných tonerů, i když si tuto nabídku neobjednali. Jde tedy vždy o velmi subjektivní záležitost, kterou spamové filtry mohou jen těžko ve všech možných situacích zvládnout. Samotné spamové filtry navíc vlastně také porušují ochranu soukromí, neboť vyžadují od administrátorů, aby tuto mnohdy osobní poštu četli.

Z pohledu Úřadu je jeho kontrolní funkce v oblasti spamu jasná. Předmětem našeho postihu jsou obchodní nabídky či reklamní sdělení, a to od českých právních subjektů, zaslaná lidem, kteří nejsou zákazníky nabízejícího, či mu nedali předem souhlas k tomu, aby je oslovil s nabídkami. Je třeba tyto dvě kategorie zpráv jasně odlišit. NOS čili tzv. „nevyžádaná obchodní sdělení" mají v českých poměrech trochu jiný charakter a nelze na ně vztahovat obecná tzv. „spamová" kritéria. V případě obchodní nabídky zaslané českou firmou s možností odhlášení je třeba toto učinit, a teprve pokud to nepomůže a nabídky docházejí dále, je třeba tuto firmu náležitě „poučit". Před podáním stížnosti je však třeba si vzpomenout, zda jsme přece jenom něco nenakupovali, či něco někde nedostali „zdarma", či zda jsme se někde jenom nenechali nalákat na nějakou nabídku. Množství případů končí právě tím, že kontrolovaný předloží Úřadu doklady o registraci, o využívání nějakého produktu či o tom, že dotyčný je jejich dlouholetým zákazníkem. Jsou případy, kdy Úřad si-

ce dosáhne odstranění z databáze, ale dotyčný se vzápětí přihlásí znovu. Jsou lidé, kteří zapomněli své původní heslo, a tak se přihlásí znovu pod jiným heslem. Existují případy, kdy Úřad našel stěžovatele v jedné databázi šestkrát, pokaždé pod jiným přihlašovacím jménem, ale se stejnou elektronickou adresou. Samozřejmě trocha viny je na registračním softwaru té které firmy, ale je to právě Úřad, který firmy nabádá, aby na elektronickou adresu nehleděli, neboť lidé někdy mívají odlišnou přijímací a odesílací adresu, a tak je třeba opatřit e-mail zákaznickým kódem či jiným jednoznačně určujícím prvkem.

V okolních evropských zemích je legislativa sice odvozena ze stejné směrnice, pro řešení stížnosti je však podstatné, zda byla způsobena nějaká škoda či újma a zda jde o hromadné rozesílání. Úřady nezasahují, pokud počet stížností nedosáhne jisté hranice (např. v Nizozemí 40 atd.). To, že inspektoři Úřadu nemají možnost získávat přímé informace o rozesilateli od příslušných poskytovatelů připojení, je spolu s povinností řešit každou jednotlivou stížnost, staví do nezáviděníhodné situace. Přesto se však díky zvýšení počtu pracovníků inspektorátu, který je agendou NOS-nevyžádaných osobních údajů pověřen, podařilo snížit prodlevu mezi podáním stížnosti a jejím vyřízením z cca 16 na 3 měsíce. Vyřizování stížností pod tuto hranici už není v podstatě možné a ani rozumné, neboť nejprve je třeba vyčkat, zda nepřijde na téhož odesilatele více stížností; samotný kontrolní proces potom zabere téměř dva měsíce.

Způsob podání stížnosti je v podstatě anonymním webovým formulářem, který je snadno zfalšovatelný a jeho případná úprava by kladla vysoké technické nároky na stěžovatele. Vzorem by mohly být formuláře na podání stížnosti z okolních zemí. Jde o několikastránkové, velmi podrobné formuláře, obsahující vedle mnoha technických detailů i ověřenou identitu stěžovatele. Pro mnoho stěžovatelů případ vyplněním našeho formuláře končí a neuvědomují si nutnost předmět stížnosti, tedy příslušné NOS-nevyžádané obchodní sdělení, držet v nezměněné formě až do konečného uzavření případu, což se v případě soudní dohry může protáhnout i na několik let.

Na závěr uvádíme statistiku činnosti Úřadu v oblasti nevyžádaných obchodních sdělení: V roce 2007 Úřad obdržel 1569 podnětů na šíření nevyžádaných obchodních sdělení, z toho bylo vyřešeno 1012, které se týkaly 515 subjektů. 115 stížností bylo neoprávněných (65 nebylo obchodní sdělení, 50 pocházelo ze zahraničí), ve 13 případech se nepodařilo dohledat odesílatele. 466 subjektům bylo uloženo nápravné opatření, z toho se 71 subjekty bylo vedeno správní řízení a byla jim pravomocně uložena pokuta v celkové výši 437 000 Kč.

II. Poznatky inspektorů ze správního řízení

V roce 2007 dále inspektoři Úřady pokračovali v praxi roku 2006, kdy jim bylo umožněno vést správní řízení, při kterém mohou zohlednit poznatky z jimi provedených kontrolních akcí. V řadě z těchto správních řízení byl využit institut příkazního řízení. Tato praxe se ukázala jako účelná zejména proto, že umožňuje zkrátit proces správního řízení. Správní řízení vedená inspektory se osvědčila jako efektivní, protože při rozhodování o závažnosti skutku, a tedy i o výši pokuty, bylo možno vycházet z důkladné znalosti věci.

Správní řízení bylo inspektory zahajováno na základě jejich kontrolních zjištění; buď z kontrol prováděných na základě kontrolního plánu, nebo na základě podnětů třetích osob.

V roce 2007 bylo vedeno inspektory Úřadu celkem 108 správních řízení, z toho 96 formou příkazu podle § 150 správního řádu. V roce 2007 bylo pravomoc-

ně ukončeno 102 správních řízení. Celkově byly ve správních řízeních uloženy pokuty ve výši 4 668 500 Kč, z této částky povinné subjekty v roce 2007 zaplatily 1 563 500 Kč. Nejvyšší uložená pokuta uložená v roce 2007 byla pokuta ve výši 1 750 000 Kč, nejvyšší uložená a zaplacená pokuta v roce 2007 byla pokuta ve výši 400 000 Kč.

Správní řízení (71 z celkového počtu 108) byla vedena v případech zjištění porušení povinností stanovených zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů, v oblasti nevyžádaných obchodních sdělení. V 5 případech byly uloženy i značně vyšší pokuty za opakované porušení zákona.

V případech zjištění porušení povinností stanovených zákonem o ochraně osobních údajů byla správní řízení vedena zejména při zjištění porušení povinností stanovených v ustanovení:

- § 5 odst. 1 písm. c), kdy správce neaktualizoval nebo zpracovával nepřesné osobní údaje,
- § 5 odst. 1 písm. d), kdy správce případně zpracovatel shromažďoval osobní údaje subjektu údajů ve větším rozsahu, než je nezbytně nutný pro naplnění stanoveného účelu. Uvedené zjištění bylo shledáno nejen v sektoru soukromém, ale i veřejném,
- § 5 odst. 2, kdy správce zpracovával osobní údaje bez souhlasu subjektu údajů,
- § 11 odst. 1, kdy správce při shromažďování osobních údajů neinformoval subjekty údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny; neinformoval je o jejich právu přístupu k osobním údajům a právu na opravu osobních údajů a o dalších právech stanovených v § 21,
- § 11 odst. 2, kdy správce nepoučil subjekt údajů o tom, zda poskytnutí osobního údaje je povinné či dobrovolné,
- § 13 odst. 1, kdy správce nebo zpracovatel zanedbal povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Ve správním řízení byla i v 8 případech formou příkazu uložena pořádková pokuta za neposkytnutí součinnosti nutné k provedení kontroly ve smyslu ustanovení § 39 zákona o ochraně osobních údajů.

I.

Personalisté velkých společností už byli poučeni o nutnosti ochrany osobních údajů zaměstnanců, avšak malé společnosti, kde často bývá jedna zaměstnankyně zároveň mzdovou účetní i personalistkou, mnohdy málo dbají na ochranu osobních údajů. Správní pokuta byla proto uložena malé stavební společnosti, kde nebylo zpracováno žádné technicko-organizační opatření k zajištění ochrany osobních údajů a personální spisy byly volně položené v policích v průchozí místnosti, kudy běžně procházeli zaměstnanci a kde večer uklízela uklízečka.

Neustále přetrvává tendence správců shromažďovat osobní údaje subjektu údajů ve větším rozsahu, než je nezbytně nutné k naplnění stanoveného účelu. Uvedené zjištění bylo shledáno nejen v sektoru soukromém, ale i veřejném.

Správci (malé podnikatelské subjekty) se často potýkají s nepochopením ustanovení § 13 (plnění povinnosti osob při zabezpečení osobních údajů) a následkem toho nejsou dostatečně zhodnocena možná rizika při zpracování osobních údajů těmito subjekty a přijata taková opatření, aby nemohlo dojít k neoprávněnému či nahodilému přístupu k informacím.

Mezi další velmi časté porušení povinnosti správce, případně zpracovatele, lze uvést neplnění informační povinnosti podle dle § 11 zákona o ochraně osobních údajů, kdy správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace už známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech. Jak bylo zjištěno kontrolní činností v roce 2007 uvedená povinnost bývá naplněna pouze částečně, nebo chybí úplně.

II.

V průběhu roku 2007 byla využita forma jak zkráceného řízení formou příkazu, tak i vedení řádného správního řízení. O formě správního řízení bylo rozhodováno zejména podle závažnosti porušení zákona, ale i na základě zkušeností získaných o kontrolované osobě při průběhu kontroly. Pokud kontrolovaná osoba již v průběhu kontroly má zájem o napravení nezákonného stavu a jedná se o jednorázové a nedbalostní porušení zákona, ukázala se možnost vedení příkazního jednání jako více efektivní.

Zkušenosti získané v průběhu provádění kontrol se promítají i do úvahy o obligatorním ukládání pokut. Ne vždy je uložení finanční pokuty výrazem spravedlnosti, ale pouze aplikací zákonného ustanovení o správním trestání. Toto se projevilo při vedení dvou správních řízení, navazujících na předchozí kontrolu. V obou případech se prokázalo jednorázové, marginální porušení zákona, způsobené jeho nepochopením konkrétními pracovníky. V prvním případě šlo o vyvěšení fotografie zaměstnance v prostorách společnosti. Skutečností je, že k takovému zpracování zaměstnanec nedal souhlas, ale tím, že jej jako kolegu znali všichni pracovníci této společnosti, mu nenastala žádná újma. Ve druhém případě byli obesláni pracovníci nelékařských profesí ve zdravotnictví s nabídkou na odebírání odborného profesního časopisu, který se zabývá výhradně problematikou zdravotnictví. O tom, že adresní osobní údaje budou využity i pro tuto činnost, však nebyla podána informace předem. Ač jde o porušení povinností uložených zákonem, skutečností zůstává, že tento časopis je v praxi odebírán právě pouze osobami, které vykonávají nelékařské profese ve zdravotnictví.

V obou těchto případech bylo vedeno následné správní řízení, ve kterém byly uloženy pokuty. Bylo ovšem zřejmé, že jeden ze základních principů při ukládání pokut, a to výchovný, nebyl naplněn uložením pokuty, ale již předchozím projednáním porušení zákona v rámci kontroly.

Výše uvedené zkušenosti lze shrnout do jednoduchého konstatování. Vedení správního řízení inspektorem, tedy úřední osobou, která prováděla ve shodné věci kontrolní činnost, se projevilo jako účinné, zejména proto, že již v rámci kontrolního procesu jsou shromažďovány důkazy i s ohledem na následné správní řízení, a protože při posuzování závažnosti skutku, a tedy i výši pokuty, lze vycházet z důkladné znalosti věci.

Ze správních řízení vedených v rámci inspektorátu byla pozornost věnována řízení se společností, která provozovala kamerový systém na pracovišti svého zákaznického centra. Již v kontrole a následně i ve správním řízení bylo prokázáno, že prostřednictvím kamer byla dokumentována činnost vlastních zaměstnanců, kteří se na pracovišti zdržovali v pracovní době, aniž společnost disponovala jejich

souhlasy, a aniž to bylo nezbytné pro vlastní činnost této společnosti, a činila tak za účelem sledování jejich pracovní výkonnosti. Tato společnost používala kamerový systém pouze v pracovní době. Nesloužil vůbec k deklarovanému zabránění krádeží, ochraně majetku nebo ochraně zdraví vlastních zaměstnanců. Záznamy byly vyhodnocovány pouze z hlediska pracovní výkonnosti, sledování běžné činnosti zaměstnanců. A následně byly zneužívány k jejich šikanování. Takovéto „šmírování“ nemělo vůbec nic společného s ochranou práv a právem sledovaných zájmů zaměstnavatele, který nejen bez souhlasu svých zaměstnanců, ale i přes jejich protesty tímto hrubým způsobem zasahoval do jejich osobnostních práv. Tímto jednáním porušil nejen povinnosti uložené zákonem o ochraně osobních údajů, ale i zákoník práce, který umožňuje zaměstnavateli sledování zaměstnanců jen ve zcela výjimečných případech. Vedení společnosti se skutečností, že porušuje základní ústavní práva svých zaměstnanců vůbec nezabývalo, a stejně tak ani protesty svých zaměstnanců, požadujících odstranění kamer. V tomto případě bylo rozhodnuto o uložení pokuty ve výši 200 tis. Kč. Toto rozhodnutí bylo v následném rozkladovém řízení plně potvrzeno.

Dobrá znalost závěrů z provedené kontroly byla využita rovněž při vedení následných správních řízení u tří významných sesterských finančních společností. Tyto společnosti, v rámci tzv. obchodní skupiny, rozhodly, že budou prostřednictvím telefonního automatu identifikovat všechny osoby, které do těchto společností zavolaly. Tímto rozhodnutím došlo k situaci, kdy se bez identifikace volajícího hovor vůbec nemohl uskutečnit. V rámci správního řízení bylo prokázáno, že rozhodnutí vedení všech tří společností nevzalo v úvahu, že ne všichni volající mají zájem se nechat identifikovat a evidovat v jakési databázi a že ne všichni volající jsou nebo chtějí být potencionálními zákazníky. Současně s vynucenou identifikací volajících byly všechny telefonické rozhovory nahrávány. Každá ze společností tak porušila svým jednáním povinnosti stanovené zákonem o ochraně osobních údajů, protože zpracovávala osobní údaje pro účely, které nebyly nezbytné, zpracovávala osobní údaje volajících, aniž by jim umožnila vyjádřit svůj souhlas nebo nesouhlas a aniž jim poskytla zákonem předepsanou informaci o účelu a rozsahu zpracovávaných osobních údajů. Byly tak shromažďovány osobní údaje osob, které neměly žádný právní vztah k některé z těchto společností. I zde rozhodnutí o identifikování a monitorování volajících bylo ovlivněno tím, že získávání informací pro vlastní obchodní činnost bylo nadřazeno právu jednotlivce na ochranu jeho soukromí.

V roce 2007 bylo v návaznosti na předchozí kontrolní zjištění vedeno správní řízení s nestátním zdravotnickým zařízením, kterému bylo prokázáno, že jako správce osobních údajů dostatečně nezabezpečilo zdravotnickou dokumentaci cca 2 tisíc svých pacientů. Tato zdravotnická dokumentace byla v rozporu nejen se zákonem o ochraně osobních údajů, ale současně i v rozporu se zákonem o péči o zdraví lidu, který definuje povinnosti zdravotnických zařízení při nakládání se zdravotnickou dokumentací, vyhozena do sběrného dvora. Pokuta uložená za prokázaný správní delikt, ve výši 1.750.000 Kč, byla druhou nejvyšší pokutou uloženou Úřadem od jeho vzniku. Při stanovení výše sankce bylo přihlédnuto rovněž nejen k závažnosti porušení povinností ze strany zdravotnického zařízení, ale rovněž i celkovému liknavému přístupu vedení tohoto zařízení k ochraně dat a informací, uložených ve zdravotnické dokumentaci.

III.

Ve správních řízeních byly ukládány sankce za porušení povinností stanovených v zákoně o ochraně osobních údajů v § 5 odst. 1 písm. c) zákona o ochraně osobních údajů, když správce neaktualizoval nebo zpracovával nepřesné osobní údaje, a za porušení povinností stanovených v § 11 odst. 1, když správce neinformoval

subjekty údajů o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovávány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, a neinformoval je o právu na opravu osobních údajů a o dalších právech stanovených v § 21, a když správce nepoučil subjekty údajů ve smyslu ustanovení § 11 odst. 2, zda poskytnutí osobního údaje je povinné či dobrovolné. Dále byly ve správním řízení uloženy sankce za porušení povinností stanovených v § 13 odst. 1 zákona o ochraně osobních údajů, a to povinnost správce přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů.

Správní řízení v oblasti nevyžádaných obchodních sdělení

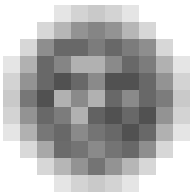
Pro oblast nevyžádaných obchodních sdělení se již v předchozím roce velice osvědčil institut příkazního řízení, který navazuje na ukončenou kontrolu. V tomto trendu bylo pokračováno i v roce 2007.

V roce 2007 provedl inspektorát IV celkem 71 správních řízení, z toho 70 bylo provedeno příkazem podle § 150 správního řádu. Odpor byl podán pouze proti 2 vydaným příkazům a v 1 případě bylo podáno odvolání. V 7 případech byla příkazem uložena pořádková pokuta za neposkytování součinnosti nutné k provedení kontroly, z nichž jen v jednom případě došlo k dodatečnému doložení potřebných dokladů, a kontrola tudíž mohla být ukončena. Úřad se setkává s případy, kdy některé subjekty porušují ustanovení zákona č. 480/2004 Sb., tedy šíří nevyžádaná obchodních sdělení opakovaně, i přes skutečnost, že jim byla uložena pokuta.

Nutno podotknout, že při opakovaném porušování se pokuty značně zvyšují. V případě 5 subjektů Úřad při rozhodování o výši uložené pokuty přihlížel právě k této skutečnosti.

Pravomocně tedy bylo v roce 2007 ukončeno 69 řízení, za něž byly uloženy pokuty v celkové výši 437 000 Kč.

Jeden ze subjektů i přes to, že mu již byla uložena pokuta podruhé (celková výše těchto dvou pokut činila 81 000 Kč), dále zasílá obchodní sdělení, přičemž adresáti k tomuto zasílání neposkytli ani souhlas, ani nebyli jeho zákazníky. Zákon č. 480/2004 Sb. nestanovuje jinou možnost zjednání nápravy než uložení sankce.



Výkon kontrolních, dozorových a správních kompetencí Úřadu

I. Obecně

Tato část výroční zprávy se zaměřuje na popis činnosti sekce dozorových činností Úřadu, která v sobě soustřeďuje následující agendy:

Příjem podání, stížností a oznámení směřujících proti porušení zákona o ochraně osobních údajů a jejich vyřizování zejména v první fázi jejich posouzení – tyto činnosti zajišťuje odbor stížností a konzultací;

Příjem oznámení o zpracování osobních údajů podle § 16 zákona o ochraně osobních údajů a vedení registračního řízení a příjem podání podle § 27 tohoto zákona týkajících se záměru předávat osobní údaje do jiných států a jejich posouzení včetně rozhodnutí o povolení či nepovolení tohoto záměru – tyto činnosti zajišťuje samostatné oddělení registračních činností;

Příjem a vyřizování žádostí o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále také „zákon o svobodném přístupu k informacím“) – tyto činnosti zajišťuje kancelář náměstkyně předsedy Úřadu;

Administrativní zajištění kontrolní činnosti Úřadu prováděné inspektory – tyto činnosti zajišťují inspektoráty;

Příjem stížností na postup úředníků Úřadu podávaných podle § 175 zákona č. 500/2006 Sb., správní řád, ve znění pozdějších předpisů (dále také „správní řád“) – tyto činnosti zajišťuje kancelář náměstkyně předsedy Úřadu;

Výkon správních činností souvisejících s ukládáním pokut při vedení správního a přestupkového řízení podle správního řádu a zákona o ochraně osobních údajů, případně zvláštních právních předpisů. Tyto činnosti zajišťuje v první instanci v úřadu několik k tomu úředně oprávněných osob, kterými jsou inspektoři úřadu zejména v případech, kdy sankční řízení má navazovat na výsledky řízení kontrolního; vedle případů řešených inspektory tyto agendy zajišťuje odbor správních činností.

Výkon legislativních činností probíhajících jak v rámci vnějšího meziresortního připomínkového řízení, tak i tvorba vlastních legislativních návrhů, a to i charakteru vnitřních předpisů – tuto činnost zajišťuje samostatné oddělení legislativních činností;

Výkon analyticko koncepčních činností podporujících další agendy a příprava druhoinstančních rozhodnutí vydávaných předsedou Úřadu a tvorba stanovisek a vyjádření, a to zejména v případě, kdy jsou rozhodnutí předsedy úřadu napadena cestou soudní – tuto agendu zajišťuje odbor právní podpory.

Dozor nad dodržováním principů ochrany osobních údajů v Schengenském informačním systému, do něhož se Česká republika zapojila dne 21. prosince 2007, vykonává nově zřízený odbor schengenské spolupráce. Ten rovněž zajišťuje a koordinuje spolupráci s dalšími orgány, které se na chodu Schengenského informačního systému podílejí.

S ohledem na výše uvedené se dá konstatovat, že činnost sekce dozorových činností (dále také „SDČ" nebo „sekce") je páteří Úřadu pro ochranu osobních údajů a přes její administrativně správní agendy prochází naprostá většina podání, sdělení, vyjádření, oznámení a stížností, kterými se Úřad ve své činnosti zabývá. Je proto velmi důležité, aby jednotlivé články sekce velmi úzce spolupracovaly, a to nejen mezi sebou, ale zejména s dalšími útvary Úřadu, které na jejich činnost navazují nebo které vůči nim činí podněty.

Tím hlavním iniciátorem aktivit SDČ je kromě veřejnosti samé zejména předseda Úřadu, který díky sledování zájmů společnosti v oblasti ochrany osobních údajů iniciuje nové aktivity, a to jak kontrolní, tak administrativně správní. V případě kontrolních aktivit se tak děje poměrně novou metodou podnětů předsedy Úřadu, kterými oslovuje přímo jednotlivé inspektory Úřadu a ukládá jim zahájit kontrolu ve společensky významných případech porušení soukromí při zpracování osobních údajů. Tato metoda se již v předchozím roce ukázala jako velmi účinná reakce Úřadu nejen na mediálně sledované případy porušování povinností při zpracovávání osobních údajů, ale zejména v situacích, kdy je třeba rychlým a efektivním způsobem dosáhnout zastavení nezákonného chování správce nebo zpracovatele a rychle dosáhnout nápravy nezákonného stavu. Tímto způsobem byly v roce 2007 zahájeny tyto kontrolní akce:

- Dne 22. května 2007 rozhodl předseda Úřadu prověřit podezření z nezákonného zpracovávání osobních údajů v souvislosti s medializovaným případem týraného Ondřeje M. v Kuřimi. Tento podnět byl na základě výsledků šetření inspektora odložen.
- Dne 19. června 2007 rozhodl předseda Úřadu prověřit způsob zpracovávání osobních údajů včetně genetických, a to společností Genomac International, s.r.o. Kontrola nebyla do konce roku 2007 ukončena.
- Dne 13. července 2007 rozhodl předseda Úřadu prověřit podezření z nezákonného zpracovávání osobních údajů občanským sdružením Fond ohrožených dětí. Kontrola nebyla do konce roku 2007 ukončena.
- Dne 17. října 2007 rozhodl předseda úřadu prověřit podezření z nezákonného zpracovávání osobních údajů Ministerstvem vnitra ČR, a to v souvislosti s realizací projektu zaměřeného na oblast prevence kriminality mladistvých osob. Kontrola nebyla do konce roku 2007 ukončena.

K těmto případům je nezbytné doplnit dosud neukončené kontroly zahájené na základě podnětů předsedy Úřadu v roce 2006. Jde o tyto kontrolní akce:

- *Kriminalistický ústav Praha, zpracování DNA databáze.*
  Kontrola Národní databáze DNA se soustředila na podmínky pro vedení tohoto registru v mezích zákona o Policii ČR a zákona o ochraně osobních údajů. V současné době jsou zpracovávána kontrolní zjištění.
- *České Aerolinie a.s., zpracování osobních údajů v souvislosti s předáváním osobních údajů cestujících osob do USA.*
  Kontrola se zaměřila na plnění povinnosti správce v souvislosti se zpracováním a předáváním osobních údajů cestujících. Kontrola nebyla do konce roku 2007 ukončena.

- *České dráhy, a.s., zpracování osobních údajů uživatelů služby In karta.*
  Kontrola se mj. na základě podnětů uživatelů, které Úřad obdržel, soustředila na zpracování osobních údajů cestujících osob v souvislosti s realizací projektu Českých drah s názvem „In Karta". Jde o technologicky náročný proces zpracovávání osobních údajů fyzických osob, uživatelů služeb spojený s držbou identifikační karty, ve které je využívána technologie RFID čipů, a to ve velkém rozsahu. Kontrola nebyla do konce roku 2007 ukončena.
- *Rádio Svobodná Evropa/Rádio Svoboda, zpracování osobních údajů v souvislosti s provozem kamerového systému.*
  Vzhledem ke skutečnosti, že v rámci kontroly je nakládáno s informacemi, které mají zásadní vliv na bezpečnost nejen objektu Rádia Svobodná Evropa/Rádia Svoboda, ale i na střed hlavního města Prahy, je kontrolní akce podrobena zvláštnímu režimu ze strany kontrolujících i ze strany kontrolovaného subjektu. Kontrola nebyla do konce roku 2007 ukončena.

Z podnětu předsedy Úřadu jsou často oslovovány jednotlivé resorty, se kterými je díky současnému stavu legislativy a některým krokům při aplikaci právních předpisů, které ne vždy zcela jednoznačně respektují principy ochrany osobních údajů, třeba vést dialog týkající se možnosti změny současných poměrů. Tyto aktivity se týkaly v roce 2007 zejména:

- Možné spolupráce Úřadu s Ministerstvem práce a sociálních věcí a se Státním úřadem inspekce práce v oblasti kontroly provozu kamerových systémů na pracovišti, kdy dochází k zásahům do soukromí zaměstnanců v souvislosti s aplikací ustanovení § 316 zákoníku práce.
- Spolupráce s Ministerstvem školství a s Českou školní inspekcí v oblasti provozu sledovacích systémů ve školách, které sice na jedné straně mají bránit nárůstu negativních jevů ve školách, jako je šikana, distribuce drog nebo drobné krádeže či poškozování věcí dětí či škol nebo školských zařízení, ale na druhé straně mohou svým působením negativně ovlivnit vývoj dětí a studentů trvale se pohybujících pod dozorem kamer ve školách.
- Spolupráce s Ministerstvem zdravotnictví v oblasti ochrany soukromí pacientů při zpracovávání jejich osobních údajů a sladění těchto zájmů se zájmem na co nejlepším zabezpečení zdravotní péče.
- Spolupráce s Exekutorskou komorou České republiky v oblasti postupů soudních exekutorů, kdy dochází k zabavování movitých věcí (mobilní telefony, osobní počítače), které obsahují osobní údaje.
- Spolupráce s Ministerstvem vnitra při realizaci záměru zpřístupnění veřejné správy jako služby občanovi pomocí projektu CzechPoint, který je součástí nové koncepce v oblasti e-governmentu a jeho služeb.
- Spolupráce s Ministerstvem spravedlnosti při postupu na záměru elektronizace provozu obchodního rejstříku a jeho služeb, s ohledem na ochranu soukromí fyzických osob, jejichž osobní údaje jsou veřejně dostupnými informacemi, a dále aktivní účast Úřadu při realizaci projektu E-justice.

K těmto aktivitám předsedy Úřadu přispívá i nová možnost přímo na jednání zvláštních odborných orgánů státu, mezi jejichž programové priority patří ochrana soukromí jednotlivce, přispívat k rozvoji společenských záměrů v této oblasti a navrhovat nové směry a impulsy. V roce 2007 se předseda úřadu stal členem těchto poradních orgánů vlády:

Rada vlády pro lidská práva

Na jednání tohoto poradního orgánu vlády má předseda Úřadu nebo další zástupce Úřadu možnost informovat tento vládní orgán o aktivitách Úřadu v oblasti ochrany soukromí jako jednoho ze základních lidských práv garantovaných Listinou základních práv a svobod a současně iniciovat zájem tohoto orgánu o aktuální otázky a problémy v této oblasti, které lze přenést i na jednání vlády jako vrcholného orgánu státní exekutivy.

Rada vlády pro informační společnost

V roce 2007 se předseda Úřadu měl možnost účastnit jednání tohoto významného vládního poradního sboru, jehož hlavním cílem je aktivně ovlivňovat vládní politiku v oblasti služeb informační společnosti v České republice.

Velmi významným subjektem a partnerem pro Úřad je stálá **Komise Senátu pro ochranu soukromí**.

Předseda Úřadu je pravidelně zván na jednání zvláštní stálé komise Senátu, která se zabývá aktuálními problémy v oblasti ochrany soukromí, a to nejen v souvislosti se zpracováváním osobních údajů.

V roce 2007 se uskutečnilo výjezdní zasedání komise přímo v budově Úřadu a členové komise tak měli příležitost k setkání s inspektory Úřadu a vedoucími pracovníky, kteří prezentovali své zkušenosti z aplikace zákona o ochraně osobních údajů v praxi.

II. Kontrolní činnosti

Jak se uvádí v předcházející části, SDČ v oblasti kontrolních činností aktivně spolupracuje zejména s inspektory Úřadu. Pro zabezpečení součinnosti je nezbytné, aby se podněty a impulsy zájmu veřejnosti a orgánů státu na výkonu dozorových činností v oblasti ochrany osobních údajů sladily se zájmy inspektorů Úřadu. Tento soulad se projevuje zejména při tvorbě Plánu kontrolní činnosti Úřadu, který každoročně schvaluje a podepisuje společně předseda a inspektoři Úřadu. Pro rok 2007 se kontrolní plán člení na obecnou a zvláštní neboli realizační část plánu.

Obecná část plánu kontrolní činnosti pro rok 2007 obsahuje tato témata pro zaměření kontrolní činnosti inspektorů Úřadu:

1. INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY:

Správce nebo také provozovatel každého informačního systému veřejné správy musí respektovat obecné principy ochrany soukromí fyzické osoby – subjektu údajů, jejíž osobní údaje jsou předmětem zpracování, a zajistit tak naplnění všech základních právních podmínek v oblasti ochrany osobních údajů. Jestliže je informační systém provozován v návaznosti na zvláštní právní podmínky, nesmí být tyto podmínky v rozporu s obecnými principy práv a povinností subjektů při zpracování osobních údajů. Proto se kontrolní aktivity zaměří zejména na systémy zpracovávající údaje a informace o majetkových poměrech osob (katastr nemovitostí).

2. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZA PODMÍNEK NASAZENÍ SLEDOVACÍCH SYSTÉMŮ:

Úřad po zkušenostech z uplynulého období a v návaznosti na nárůst tlaku na provozování monitorovacích systémů a jejich nasazování v různé úrovni společenského zájmu často zasahujícího do zájmu jednotlivce na ochranu svého soukromí a soukromí rodiny, která je součástí života společnosti i v roce 2007, hodlá v této oblasti uplatňovat své kontrolní aktivity a zaměřit se na dodržování povinností správců při zpracování osobních údajů v této oblasti. Kontrolní aktivity Úřadu se proto zaměří zejména do oblasti školství a zdravotnictví, ale také směrem k provozování městských nebo obecních kamerových systémů.

3. PŘIPRAVENOST ČESKÉ REPUBLIKY NA VSTUP DO SCHENGENSKÉHO INFORMAČNÍHO SYSTÉMU:

V návaznosti na výsledky evaluační mise v této oblasti, která v ČR proběhla v roce 2006, a v souladu s výzvou (závěrem) této mise Úřad ještě před vstupem ČR do SIS prověřil oblast ochrany osobních údajů a připravenost jednotlivých článků participujících na tomto informačním systému na jejich povinnosti ve vztahu k ochraně soukromí jednotlivce a dodržování jeho práv. Šlo zejména o kontroly některých zastupitelských úřadů České republiky.

4. DOPRAVNÍ SYSTÉMY V ČESKÉ REPUBLICE A ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PŘI JEJICH PROVOZOVÁNÍ:

V rámci provozování dopravních systémů v ČR, které jsou propojovány s některými státem provozovanými registry, vzniká obava, zda monitorování pohybu vozidel a následné zpracování osobních údajů v rámci dopravní obslužnosti a výběru poplatků nepřesahuje právní rámec podmínek pro zpracování osobních údajů v rámci nejen právního řádu ČR, ale také právních předpisů EU. Kontrolní aktivity Úřadu se proto zaměří zejména na způsob zpracování osobních údajů v souvislosti s výběrem mýtného.

5. OBLAST VÝKONU ČINNOSTI JUSTICE, STÁTNÍHO ZASTUPITELSTVÍ A PŘÍPADNĚ DALŠÍCH SUBJEKTŮ PŮSOBÍCÍCH NEBO SE PODÍLEJÍCÍCH NA PROCESU ZPRACOVÁVÁNÍ OSOBNÍCH ÚDAJŮ V TÉTO OBLASTI:

Při výkonu dozorové působnosti Úřadu pro ochranu osobních údajů byla oblast působnosti justice a působnosti státních zastupitelství při zpracovávání osobních údajů osob, které se účastní nebo podílejí na procesu zpracovávání osobních údajů, poněkud stranou zájmu Úřadu, avšak s nárůstem tlaku na prolínání různých druhů informací, které jsou v těchto procesech shromažďovány, a jejich další využívání v dalších informačních systémech se ukazuje nutnost prověřit dosavadní postupy při zpracovávání osobních údajů v této oblasti.

Zvláštní část plánu kontrolní činnosti obsahuje následující **přehled plánovaných konkrétních kontrolních akcí inspektorů Úřadu** v návaznosti na obecnou část kontrolního plánu pro rok 2007:

ZAMĚŘENÍ KONTROLY

■ Zpracování osobních údajů o držitelích vozidel a řidičů vozidel při provozování elektronického systému mýtného:

Kontrola se zaměřila na dodržování podmínek pro zpracování osobních údajů účastníků silničního provozu v souvislosti s výběrem poplatku na užívání dálnic a na skutečnost, zda zpracovávané osobní údaje jsou přiměřené co do rozsahu a účelu zpracování a zda nejsou zpřístupňovány jiným subjektům. Kontrola byla ukončena bez zjištění porušení povinnosti správce při zpracovávání osobních údajů.

■ Zpracování osobních údajů v souvislosti s vízovým řízením v zastupitelských úřadech ČR:

Kontrola proběhla na Velvyslanectví ČR v Kyjevě a zaměřila se na vízové řízení prováděné v zastupitelských úřadech. Předmět kontroly byl stanoven na základě doporučení expertní komise pro Schengenské hodnocení nových členských států na úseku ochrany osobních údajů.

V souvislosti s touto kontrolou bylo Ministerstvu zahraničních věcí jako odpovědnému subjektu za dodržování podmínek zpracování osobních údajů kontrolující inspektorkou navrženo upravit dosavadní postup při poskytování informací žadatelům o víza s ohledem na ustanovení § 11 odst. 1, věta druhá zákona o ochraně osobních údajů.

V souvislosti s doporučením expertní komise proběhla také kontrola na Generálním konzulátu v Sankt Peterburgu. Cílem bylo prověřit bezpečnost zpracovávaných údajů a prověřit toky údajů žádostí o udělení víz od konzulátů a zjistit, zda odpovídají zákonným předpisům a zároveň i požadavkům Schengenského katalogu a vyhovují „Best practices“ při udělování víz. Součástí ověření postupů při udělování víz byla i kontrola na Cizinecké policii.

■ Zpracování osobních údajů při provozu Registru silničních vozidel:

Kontrola byla provedena ve statutárním městě O., které vykonává při zpracování a využívání osobních údajů v registru silničních vozidel činnost státního orgánu. Při vedení elektronické a listinné části registru nebylo zjištěno porušení zákona o ochraně osobních údajů kontrolovaným.

■ Zpracování osobních údajů v souvislosti s čipovými kartami In-karta:

Jak je uvedeno výše, zaměřila se kontrola na zpracování osobních údajů cestujících osob v souvislosti s realizací projektu Českých drah. Vzhledem k záměru propojení uživatelských služeb určených pro cestující osoby v příměstské hromadné dopravě bude kontrola probíhat také v roce 2008.

■ Zpracování osobních údajů orgány činnými v trestním řízení:

Kontrola proběhla na jednom obvodním státním zastupitelství a zaměřila se na dodržování povinností při zpracování osobních údajů v trestním řízení a na jejich případné další využívání v jiných informačních systémech s ohledem na § 13 zákona o ochraně osobních údajů. Kontrolou nebylo zjištěno porušení povinností při zpracování osobních údajů podle zákona.

■ Zpracování osobních údajů za podmínek nasazení sledovacích systémů ve školách:

Úřad registruje stále častější používání kamerových a jiných sledovacích systémů, proto se na tuto oblast ve své kontrolní činnosti také zaměřuje. V oblasti školství pak považuje Úřad tuto problematiku za mimořádně citlivou. Probíhá kontrola kamerového systému jedné pražské základní školy.

Zpracování osobních údajů hostů Poslanecké sněmovny:

Kontrola Kanceláře Poslanecké sněmovny se soustředila na evidenci návštěvníků budov Poslanecké sněmovny, konkrétně na to, jaká osobní data návštěvníků jsou zpracovávána a po jakou dobu se tato data uchovávají. Kontrola byla ukončena vzhledem k tomu, že kontrolovaný podal proti kontrolnímu protokolu námitky.

Zpracování osobních údajů a dodržování podmínek jejich ochrany v souvislosti s vedením katastru nemovitostí:

Kontrola se zaměřila na určení mezí pro podmínky zpracovávání osobních údajů v rámci katastrálního zákona, který považuje katastr nemovitostí za veřejně přístupný registr, a pro podmínky zpracovávání osobních údajů podle obecného zákona o ochraně osobních údajů, který požaduje, aby zásahy do soukromí fyzických osob byly jasné a zřetelně vycházely z veřejného zájmu prosazovaného ve společnosti.

Zpracování osobních údajů za podmínek nasazení sledovacích systémů obecní policií:

Téma bylo součástí kontroly provedené ve statutárním městě O. se zaměřením na zpracování osobních údajů orgány obce v souvislosti se zpracováním a využíváním osobních údajů v registru silničních vozidel. Kontrolováno bylo vedení evidence paměťových karet vozidel, která jsou vybavena záznamovým zařízením; ve zpracování, které je jako součást registru silničních vozidel funkční od 1. 7. 2007, nebylo zjištěno porušení zákona o ochraně osobních údajů.

Zpracování osobních údajů orgány činnými v trestním řízení:

Byla provedena kontrola u obvodního soudu a zaměřila se zejména na realizaci práv a povinností upravených v ustanoveních §§ 5, 9, 11 a 13 zákona. Ze skutečností zjištěných při kontrole vyplynulo, že obvodní soud (správce) při zpracování osobních údajů postupoval v rozporu se zákonem, protože zpracovával citlivé údaje, aniž by subjekt údajů dal ke zpracování výslovný souhlas a aniž byl při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Kontrolou bylo prokázáno, že uvedeným jednáním obvodního soudo došlo k porušení zákona v jeho ustanovení § 9 písm. a).

Zpracování osobních údajů za podmínek nasazení sledovacích systémů ve zdravotnictví:

Rovněž v oblasti zdravotnictví Úřad zaznamenává rostoucí trend používání sledovacích systémů. Ve zdravotnictví je pak toto sledování rizikové proto, že se zde pracuje s citlivými osobními údaji o zdravotním stavu pacientů. Kontrola se zaměřením na sledovací systémy probíhá v jednom zdravotnickém zařízení.

Zpracování osobních údajů klientů Státního fondu rozvoje bydlení:

Zahájení kontroly se přesouvá do roku 2008.

Zpracování osobních údajů v souvislosti s provozem kamerového systému v umělecké galerii:

Účelem kontroly je prověření způsobu zpracovávání osobních údajů osob, pohybujících se v monitorovaných prostorách.

Sekce dozorových činností při spolupráci s inspektory Úřadu administrativně zajišťuje činnost poradního orgánu předsedy Úřadu pro vypořádání námitek kontrolovaných osob podaných proti výsledkům kontrol, obsažených v kontrolních protokolech, které se nazývá **„Námitkové kolegium inspektorů"**.

Při kontrole inspektoři Úřadu postupují podle zákona č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů. Tento zákon kontrolovaným umožňuje podat proti kontrolnímu protokolu, který je vyhotoven na konci kontroly a obsahuje zejména popis kontrolou zjištěných skutečností s uvedením případných nedostatků a označení ustanovení právních předpisů, které byly porušeny, námitky. Podle § 17 zákona o státní kontrole lze proti kontrolnímu protokolu podat písemné a zdůvodněné námitky do pěti dnů od seznámení se s ním. O námitkách pak dle § 18 zákona o státní kontrole rozhoduje předseda Úřadu.

V loňském roce došlo ke změně při projednávání námitek proti kontrolnímu protokolu. Podle nově vydané vnitřní směrnice námitky projednává a posuzuje kolegium inspektorů Úřadu, které předsedovi Úřadu také doporučuje jejich posouzení. Kolegium jako zvláštní orgán je poradním orgánem předsedy a kromě projednávání námitek proti kontrolnímu protokolu projednává i námitku podjatosti vznesenou proti některému z inspektorů Úřadu. Při své posuzovací činnosti pak kolegium má dbát a přispívat k jednotnému výkonu kontrolních činností Úřadu.

V roce 2007 se kolegium jako zvláštní orgán sešlo celkem v jedenácti případech a vždy projednávalo námitky vznesené kontrolovaným proti kontrolnímu protokolu. Celkem kolegium v roce 2007 projednalo a předsedovi Úřadu navrhlo vypořádání námitek třinácti kontrolovaných.

Posuzování a projednávání námitek proti kontrolnímu protokolu, ať už procesně nebo hmotně právních, kolegiem inspektorů, jehož zasedání se zúčastňují rovněž předseda Úřadu, náměstkyně sekce dozorových činností a ředitel odboru právní podpory (odbor právní podpory připravuje návrh na vypořádání námitek a následně na základě závěrů kolegia předsedovi předkládá návrh rozhodnutí o námitkách), přispívá i k dosažení výše uvedeného záměru, tedy ke sjednocování výkonu kontrolních činností Úřadu. Z detailního posuzování jednotlivých kontrol, jejich součástí, fází i postupů a námitek kontrolovaných vyplývá pro inspektory Úřadu nezanedbatelné množství poznatků jak o kontrolním procesu samotném, tak i o aplikaci zákona o ochraně osobních údajů, zákona o státní kontrole atd.

III. Poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím

Účelem zákona o svobodném přístupu k informacím je přispět k posílení principu publicity státní správy. Tento zákon umožňuje veřejnosti získávat informace o činnosti veřejné správy, tedy o jejím konání, jejích aktivitách, o jejím hospodaření atd.

I v roce 2007 se Úřad setkal se situacemi, kdy byl osloven se žádostí o konzultaci či o názor v oblasti ochrany osobních údajů s tím, že tato žádost byla žadatelem označena jako žádost o poskytnutí informace podle zákona o svobodném přístupu k informacím. Povinnost poskytovat konzultace týkající se zákonné úpravy ochrany osobních údajů Úřadu vyplývá z § 29 písm. h) zákona o ochraně osobních údajů a Úřad samozřejmě takovéto konzultace v souladu se zákonem poskytuje. V případě, kdy je žádost o konzultaci žadatelem označena jako žádost podle zákona o svobodném přístupu k informacím, tedy Úřad postupuje podle citovaného ustanovení zákona o ochraně osobních údajů.

Úřad v roce 2007 obdržel celkem čtyři žádosti o informace ve smyslu zákona o svobodném přístupu k informacím. Třem z nich Úřad v souladu s ustanovením § 15 zákona o svobodném přístupu k informacím nevyhověl. Jedné žádosti o informace Úřad vyhověl a následně v souladu s § 5 odst. 3 zákona o svobodném přístupu k informacím obsah poskytnuté informace v anonymizované podobě zveřejnil na svých internetových stránkách.

IV. Vyřizování stížností podle § 175 správního řádu

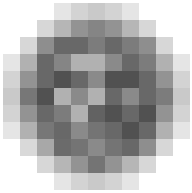
I v roce 2007 Úřad řešil stížnosti podle § 175 zákona č. 500/2004 Sb., správní řád. Toto ustanovení umožňuje dotčeným občanům obracet se na správní orgán, jestliže se domnívají, že v jejich případě správní orgán volil nesprávný úřední postup, nebo když namítají nevhodné chování úředních osob. Se stížností podle § 175 správního řádu se dotčené osoby na správní orgán mohou obracet v případě, že jim zákon neposkytuje jiný prostředek ochrany.

Institut stížnosti přinesl nový správní řád, který vstoupil v účinnost dne 1. ledna 2006. Od začátku loňského roku také začala platit vnitřní směrnice Úřadu, která postup při vyřizování stížností podle § 175 správního řádu upravuje. Postup, který byl vedením Úřadu zvolen, se osvědčil i v roce 2007. Stížnosti vyřizují pověření zaměstnanci kanceláře náměstků předsedy ve spolupráci s pověřeným zaměstnancem kanceláře předsedy Úřadu.

Úřad v roce 2007 obdržel celkem dvacet sedm podnětů, které vyhodnotil a následně řešil jako stížnost dle § 175 správního řádu. V porovnání s předchozím rokem jde o nárůst o devět případů, což také svědčí o tom, že tento nově upravený institut je veřejností více vnímám a využíván. Z dvaceti sedmi stížností byly celkem tři posouzeny jako důvodné, jedna jako částečně důvodná. V porovnání s rokem 2006 tedy poklesl poměr stížností, které byly jako důvodné či částečně důvodné vyhodnoceny.

Značná část stížností (celkem dvanáct) vyjadřovala nesouhlas s vyřízením předchozího podnětu, který stěžovatel zaslal Úřadu a ve kterém uvedl podezření na porušení zákona o ochraně osobních údajů. Ve dvou případech bylo po prošetření stížnosti konstatováno, že při posuzování předchozího podnětu stěžovatele skutečně Úřad nepostupoval správně, stížnosti byly posouzeny jako důvodné a byl dán podnět k provedení kontroly. Ve čtyřech případech stížnosti směřovaly proti kontrolním závěrům inspektorů Úřadu, ani jedna z těchto stížností nebyla posouzena jako důvodná. Šest stížností směřovalo proti vyřízení předchozí stížnosti dle § 175, kdy stěžovatelé nesouhlasili s vyřízením své předchozí stížnosti na nesprávný úřední postup či na chování úředních osob. Ani jedna z těchto stížností nebyla posouzena jako důvodná.

Z celkového počtu dvaceti sedmi stížností směřovala pouze jedna proti nevhodnému chování úředních osob. Takto malý počet podnětů upozorňujících na možné nevhodné chování zaměstnanců Úřadu je dobrým zjištěním, neboť vyřizování podnětů ve všech jeho fázích, od posouzení, přes kontrolu až po správní řízení, je spojeno s často intenzivní komunikací s veřejností, která nemusí být vždy snadná a bezproblémová. Stížnost proti nevhodnému chování úředních osob, kterou Úřad v roce 2006 obdržel, byla po prošetření vyhodnocena jako bezdůvodná.



Vyřizování stížností a poskytování konzultací

Prioritou činnosti odboru stížností a konzultací v roce 2007 bylo maximální přiblížení občanům s cílem komplexnosti poskytovaných služeb v rozsahu úkolů uložených Úřadu pro ochranu osobních údajů § 29 odst. 1 písm. c) a písm. h) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o ochraně osobních údajů“). Cílem byla účinná ochrana osobních údajů a citlivých osobních údajů fyzických osob před jejich zpracováním prováděným v rozporu s citovaným zákonem jakýmkoliv subjektem majícím postavení správce nebo zpracovatele osobních údajů.

V drtivé většině případů byl prvotním telefonický kontakt žadatele, kdy v průměru bylo denně odpovídáno na 35 dotazů. Ve složitějších případech následovala zpravidla písemná odpověď nebo osobní konzultace. Za osobní konzultace považujeme řešení požadovaného problému v celé šíři, ne pouhé jednorázové doplnění informací stěžovatelem. Z 60 osobních konzultací poskytnutých v letošním roce ústředním orgánům státní správy, veřejné správy i soukromému sektoru jen pro ilustraci uvádíme tyto subjekty: Ministerstva vnitra, spravedlnosti, obrany, financí, kultury, Generální ředitelství Celní správy, Policie České republiky, Vojenská policie Inspekce městské policie, Česká národní banka, Československá obchodní banka, Mesit holding, společnosti Siemens, Bosch, Hitachi, Škoda Auto, Auto Esa, obchodní řetězec Lidl, Centrum sociálních služeb Praha, Zemědělská vodohospodářská správa.

Prostřednictvím elektronické pošty bylo řešeno celkem 1 674 podání (v roce 2006 to bylo 1 413 podání). V počátečních měsících roku 2007 nastaly určité problémy s novým softwarem dodaným externí firmou. Za vzniklé potíže, převážně za prodlení v příjmu i odeslání pošty, se všem dotčeným ještě jednou i touto cestou Úřad omlouvá. V současné době je provoz elektronické pošty již bezproblémový, průměrná doba odpovědi odboru stížností a konzultací na takováto podání činila 10 dnů. Možnosti využívaného systému přispějí i k vyšší kvalitě analytických výstupů, což bude v konečném důsledku znamenat zkvalitnění celkové činnosti Úřadu.

Prakticky ve všech sledovaných ukazatelích dochází k permanentnímu nárůstu, který u dotazů činil 19%, u stížností 21% a osobních konzultací bylo poskytnuto o celých 50% více. Kromě kamerových systémů, jimž je věnována samostatná pasáž, byly nejčetnějšími problémy neoprávněné kopírování občanských průkazů a využívání rodného čísla správci nebo zpracovateli osobních údajů v rozporu se zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů. Samostatnou kapitolou bylo pokračující rozhořčení občanů nad uváděním rodného čísla, ale i dalších osobních údajů, ve veřejně dostupných seznamech, které je sice v souladu se zvláštní právní úpravou, ale podle názoru Úřadu již nikoli v souladu s obecnými principy ochrany osobních údajů. Úřad pokračoval i v roce 2007 ve svém úsilí přimět příslušné orgány k přijetí opatření měnících stávající právní stav. V nejbližší době lze očekávat konkrétní výsledky, co se týče katastru nemovitostí.

Statistika stížností vyřízených v roce 2007

– celkem ---------- 574
z toho
– předáno ke kontrole ---------- 207
– předáno na zahájení řízení ---------- 35
– postoupeno příslušným orgánům ---------- 5
– odloženo s vyrozuměním ---------- 327

K další analýze před případným zahájením kontroly bylo předáno 207 stížností. Největší podíl závadového jednání představovalo, stejně jako v roce 2006, nesprávné používání kamerových systémů se záznamovým zařízením. V souvislosti s nabytím účinnosti nového zákoníku práce k 1. lednu 2007, který v § 316 zakazuje, až na výjimky, přímé sledování zaměstnanců na pracovišti, došlo k posunu v této oblasti ve smyslu úbytku anonymních podání. Největší počet stížností se týkal právě pracovně právní oblasti. Dále se stížnosti týkaly námitek proti instalaci kamer v bytových domech, městských aglomeracích, ale i v soukromých obydlích. Úřad si je plně vědom složitosti této problematiky, která v sobě mimo jiné zahrnuje dvě ústavní práva – nedotknutelnost soukromého majetku, ale současně i nedotknutelnost soukromí, a snaží se v každém ad hoc případě důsledně zkoumat jejich vyváženost. Komplikované bývá v této souvislosti i posouzení hranice aplikovatelnosti zákona o ochraně osobních údajů, který se nevztahuje na zpracování prováděné fyzickou osobou výlučně pro osobní potřebu. Jako příklad uvádíme:

Mladý muž se telefonicky dotazoval, zda může zabezpečit svůj Mercedes a Audi svého přítele, parkující na veřejném parkovišti typického pražského sídliště ze sedmdesátých let minulého století, kamerovým systémem instalovaným ve svém bytě. Účelem bylo získat důkazní materiál ve formě nahrávky pachatele opakovaných krádeží z interiérů obou vozidel a jejich poškozování se škodou značného rozsahu.

Úřad zaujal následující stanovisko: Pokud bude minimalizován zásah do soukromí osob pohybujících se na tomto veřejném prostranství, čehož lze dosáhnout nastavením úhlu kamery, jejím zaostřením jen na vozidla a dalšími technickými parametry, při respektování dalších pravidel zpracování osobních údajů, zejména zabezpečení pořizovaných záznamů před nepovolanými osobami, jejich uchovávání v řádu několika dnů, využití jen k deklarovanému účelu, nelze takovémuto použití kamerového systému bránit s odkazem na zákon o ochraně osobních údajů. Vyloučit ovšem nelze stížnosti podle občanského zákoníku, neboť není naplněna zákonná licence k pořizování obrazových záznamů bez souhlasu dotčených osob. Tento právní názor lze uplatnit při řešení stále se množících dotazů i stížností na používání kamer při ochraně vlastního majetku, převážně soukromých domů a vil.

Přestože problematika kamerových systémů nadále představovala rozhodující podíl na celkovém počtu dotazů i stížností, objevil se, jednoznačně v přímé souvislosti se stále kvalitnějšími a dostupnějšími technickými prostředky a technologickými možnostmi, nový fenomén, a to zpracování biometrických údajů. Šlo především o daktyloskopické otisky.

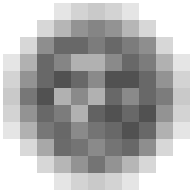
Zákonem č. 170/2007 Sb. provedená novela zákona o ochraně osobních údajů definovala jako citlivý údaj takový biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. Daktyloskopické otisky tedy citlivými osobními údaji, kterým zákon o ochraně osobních údajů přiznává přísnější režim ochrany, bezpochyby jsou.

Úřad považoval za nutné zaujmout k této problematice od počátku zásadní stanovisko. Použití systémů, v jejichž paměti dochází k uchovávání biometrických

údajů, nelze považovat za nezbytné pro jakoukoliv běžnou evidenci. Objevily se pokusy o jejich uplatnění např. pro evidenci odběru obědů žáky ve školní jídelně, evidenci vstupu pedagogických pracovníků a studentů do budovy školy, docházky zaměstnanců do běžného výrobního podniku. Takovéto zpracování biometrických údajů je nepřiměřené a dochází při něm k porušení povinnosti shromažďovat osobní údaje, které odpovídají stanovenému účelu, a pouze v rozsahu nezbytně nutném k jeho naplnění, a to i přes výslovný souhlas subjektů údajů, který je v tomto případě nezbytný. V podstatě neřešitelnou otázkou pro správce osobních údajů je jeho další postup po neposkytnutí prvotního otisku prstu, k němuž nemůže být, bez zákonného důvodu, nikdo nucen. Mělo by to snad znamenat, že dětem, jejichž zákonní zástupci nedali souhlas, nebude vydán školní oběd? To jistě ne – a proto lze na takovýto postup podat stížnost Úřadu. Jednání správce může být posouzeno jako správní delikt s obligatorně ukládanou sankcí, jejíž výše může činit až 10 milionů Kč.

Úřad připouští možnost využití systémů umožňujících s pomocí jednosměrné hashovací funkce vytvořit číselný údaj, jehož zpětná rekonstrukce na biometrický údaj není možná a který slouží jen k verifikaci vstupu oprávněné osoby do určitého, z nějakého smysluplného důvodu zvláštním režimem chráněného prostoru. Ani zde se však správce nevyhne získání výslovného, tedy písemného souhlasu subjektu údajů s prvotním zpracováním otisku prstu a pochopitelně musí plnit další povinnosti správce. Velký význam má zejména informační povinnost ve smyslu § 11 zákona o ochraně osobních údajů s důrazem na získání souhlasu všech dotčených subjektů, jinak by nasazení tohoto verifikačního systému ztrácelo význam.

Závěrem lze konstatovat, že povědomí občanů, a to nejen státních příslušníků České republiky, o existenci Úřadu a jeho dozorových kompetencích soustavně roste. Stále častěji řeší Úřad otázky předání osobních údajů do států Evropské unie i do třetích zemí. Poměrně složité bývají vazby mezi mateřskou společností s postavením správce osobních údajů sídlící kdekoliv ve světě a jejími organizačními součástmi působícími na území České republiky. V této oblasti je řada drobných nuancí, které je zapotřebí brát v úvahu a odpovídat tazatelům v jejich jazyce. Přestože jde převážně o angličtinu, přináší tato situace nové nároky na profesní způsobilost pracovníků Odboru stížností a konzultací. Další trend nárůstu vyřizované agendy lze očekávat i v příštím roce, což kromě stále se prohlubujícího právního vědomí společnosti v oblasti ochrany osobních údajů ovlivní i vstup České republiky do schengenského prostoru.



Správní řízení

Obecná část

Odbor správních činností je podle organizačního řádu Úřadu příslušný k projednávání správních deliktů (přestupků i jiných správních deliktů právnických osob a podnikajících fyzických osob). Při této činnosti dostává podněty z několika zdrojů; jejich nejrozsáhlejší část tvoří ty, které byly předány k vyřízení odborem stížností a konzultací. To jsou však pouze takové případy, kdy podnět nasvědčuje tomu, že nezákonné jednání již bylo ukončeno a závadný stav nelze kontrolou napravit (není-li tomu tak, podnět je předán k provedení kontroly). Druhou významnou část tvoří podněty, které postoupí Úřadu orgány činné v trestním řízení, případně jiný správní orgán, který se cítí k vyřízení věci nepříslušný, neboť došel k závěru, že jde o podezření z porušení právních předpisů upravujících oblast ochrany osobních údajů (obvykle jde o Policii České republiky a obecní úřady). Třetí skupinou jsou návrhy inspektorů Úřadu činěné na základě ukončené kontroly, a to pouze v případech, kdy se inspektor nerozhodne provést sankční řízení sám.

Výše uvedené tedy stojí na počátku správního řízení. Na jeho konci pak není jen samotné posouzení viny resp. zákonnosti jednání účastníka řízení a případné uložení pokuty, ale také vyhodnocení veškerých zjištění a rozhodnutí o tom, zda z podkladů nevyplývá, že správce či zpracovatel chybně nebo nedostatečně stanovil systémové parametry zpracování. V takových případech může být případ po ukončení správního řízení předán inspektorům Úřadu k provedení kontroly.

Zákon o ochraně osobních údajů umožňuje ukládat v řízeních o správních deliktech vysoké pokuty. Zatímco minimální sazba není zákonem výslovně stanovena, maximální výše sankce může dosáhnout až 10 miliónů korun, aniž bylo přesněji stanoveno (s výjimkou kvalifikované skutkové podstaty, kde vyšší závažnost vyplývá buď ze zpracování citlivých údajů, nebo z ohrožení soukromého a osobních života většího počtu osob), čím se Úřad při této činnosti řídí. Proto se objevují dotazy, co má vlastně pro Úřad při ukládání pokuty prvořadý význam.

Základními prvky, které ovlivňují stanovení výše sankce, jsou kritéria uvedená v § 46 odst. 2 zákona o ochraně osobních údajů, tj. povaha, závažnost, způsob jednání, míra zavinění, doba trvání a následky protiprávního jednání. K těm je nutno přihlédnout vždy. V jejich výkladu jsou však některé nejasnosti a tak lze upřesnit, že jde o: širší okolnosti protiprávního jednání, míru zavinění jednání (pouze u fyzických osob, protože u právnických osob se k zavinění zásadně nepřihlíží, jde o tzv. objektivní odpovědnost), délku trvání a rozsah a charakter způsobených následků (v souhrnu můžeme hovořit o závažnosti deliktního jednání).

Kromě těchto obecných kritérií je možno stanovit i zvláštní skupinu prvků, které vycházejí z dikce zákona o ochraně osobních údajů:

- zda jde o zveřejnění, zpřístupnění, neoprávněné zpracování, případně o „jiné ohrožení“ osobních údajů,
- jaký je počet dotčených subjektů údajů,
- zda jsou neoprávněným zpracováním dotčeny citlivé údaje nebo jiné osobní údaje,
- a zda došlo k zásahu do lidské důstojnosti, resp. zda porušitel měl nějaký další prospěch z neoprávněného zpracování.

Z praxe dozorové činnosti Úřadu lze shrnout, že zásadní je množství a kategorie osobních údajů, resp. počet subjektů údajů, jejichž osobní údaje byly neoprávněně zpracovávány, případně ohroženy. Počet ohrožených subjektů údajů má tedy nepochybně nejčastěji zásadní vliv na výši trestu.

Skutečnost, že od roku 2006 se správnímu řízení týkajícímu se deliktů podle zákona o ochraně osobních údajů věnují i inspektoři Úřadu, umožnila odboru správních činností soustředit pozornost v roce 2007 také na jiné typy správních řízení, které jsou mu (od 1. ledna 2007) podle organizačního řádu Úřadu svěřeny, tj. řízení podle § 17 odst. 1 zákona o ochraně osobních údajů, které vede na základě podnětu Samostatného oddělení registračního. Tato řízení jsou vedena z úřední povinnosti v případech, kdy z podaného oznámení o zpracování osobních údajů vznikne důvodná obava, že by při tomto zpracování mohlo dojít k porušení zákona. Že v jeho činnosti nejde o věc podružnou, vyplývá i z níže uvedených čísel.

V roce 2007 se v podstatě všechna tato správní řízení - jejichž výsledkem není uložení sankce, nýbrž rozhodnutí o nepovolení zpracování v případech, kdy je shledáno, že původní důvodná obava byla oprávněná, případně zastavení řízení, pokud je oznámené zpracování v souladu se zákonem - týkala oznámených nasazení kamerových systémů. Těm se Úřad celý rok intenzivně věnoval nejen v registrační a správní, ale též při kontrolní, konzultační a obecně osvětové činnosti.

Přitom možné porušení zákona o ochraně osobních údajů bylo nejčastěji spatřováno v oznámené době uchovávání pořízených záznamů, tj. době nikoli nezbytné k účelu zpracování [viz § 5 odst. 1 písm. e)], v plnění informační povinnosti (viz § 11) a dále v porušení ustanovení § 10, které se týká povinnosti dbát, aby subjekt údajů neutrpěl újmu na zachování lidské důstojnosti, a povinnosti dbát na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektů údajů.

Za prvotní je však třeba považovat plnění povinnosti zpracovávat osobní údaje pouze se souhlasem subjektů údajů, příp. při naplnění některé ze zákonem stanovených výjimek (viz v § 5 odst. 2). Kromě souhlasu subjektu údajů a poměrně nečetných případů, kde instalaci takových systémů zákon přímo nařizuje (např. kasina), je za nejčastější právní titul pro možnost nasazení kamerových systémů třeba považovat ochranu práv a právem chráněných zájmů [viz § 5 odst. 2 písm. e)], která však podle zákona o ochraně osobních údajů nesmějí být v rozporu s právem na ochranu soukromého a osobního života subjektu údajů.

Lze konstatovat, že zatímco jsou ve většině řízení odstraněny problémy s plněním informační povinnosti a s dobou uchovávání záznamů (v rámci vedených ústních jednání), u řady případů přetrvává problém nadměrného zasahování do soukromí, a zpracování je proto (s odkazem na porušování § 5 odst. 2, případně § 10 zákona o ochraně osobních údajů) nepovoleno.

Úřad se po svých zkušenostech při vedení správních řízení hodlá i nadále zaměřit na řešení problémů kamerových systémů, a to nejen s jednotlivci, ale i prostřednictvím různých zájmových a profesních skupin. Je totiž vhodné, aby se problémy řešily sektorově, tak, jak se o to Úřad snaží například u problematiky škol (viz např. text „Kamerové systémy instalované ve školách a školských zařízeních z pohledu Úřadu pro ochranu osobních údajů“).

Přestože rok 2007 byl v oblasti kamerových systémů spíše rokem informační kampaně a prevence, je třeba na závěr připomenout, že za instalaci systémů, které neodpovídají požadavkům zákona, bylo již také uloženo několik sankcí.

V průběhu posledních let se zvyšuje počet právních předpisů, které obsahují skutkové podstaty správních deliktů týkající se ochrany dat a ukládají Úřadu kompetenci k jejich projednání. Takové delikty pak v Úřadu (s ohledem na zmíněný obsah Organizačního řádu Úřadu) projednává Odbor správních činností. V roce 2006 Parlament České republiky rozhodl (s účinností od 1. ledna 2007) o nové právní úpravě podmínek týkajících se omezení některých činností veřejných funkcionářů a neslučitelnosti výkonu funkce veřejného funkcionáře s jinými funkcemi. Tato materie je provedena zákonem č. 159/2006 Sb., o střetu zájmů. V § 13 a 14 tohoto zákona jsou upraveny podmínky pro vedení registru oznámení o činnostech, oznámení o majetku a oznámení o příjmech, darech a závazcích, které zabezpečují orgány zde uvedené, a právo každého do registru nahlížet (a to i prostřednictvím veřejné datové sítě) a pořizovat si z něj výpisy a opisy. Fyzická osoba, která informace z registru použije nebo dále zpracuje k jinému účelu než ke zjištění případného střetu zájmů při výkonu funkce veřejného funkcionáře [§ 23 písm. a)] nebo poruší povinnost mlčenlivosti o skutečnostech, o nichž se dozvěděla z údajů v registru, nebo o osobách, které sdělily skutečnosti nasvědčující o nepravdivosti nebo neúplnosti údajů [§ 23 písm. b)], spáchá přestupek, k jehož projednání je dána pravomoc Úřadu a za nějž lze uložit pokutu až do výše 100 000 Kč. O porušení povinností veřejných funkcionářů, které ze zákona vyplývají, rozhoduje nikoli Úřad, ale soud ve správním soudnictví.

V průběhu roku 2007 Úřad projednával pouze jeden přestupek dle zákona o střetu zájmů; informace o obsahu rozhodnutí Úřadu v tomto řízení jsou uvedeny níže.

Zvláštní část

V této části uvádíme informace z několika oblastí, které odbor správních činností považuje na základě své činnosti v roce 2007 za aktuální.

K zajímavým sankčním řízením podle zákona o ochraně osobních údajů a zákona o některých službách informační společnosti

■ Provádění exekucí

Porušení zákona o ochraně osobních údajů bylo shledáno v činnosti osoby pověřené provedením exekuce v souvislosti se zpracováním osobních údajů povinného při vedení exekuce. V rozporu se zákonem o ochraně osobních údajů tento exekutor uvedl ve výroku rozhodnutí o ceně (které následně umístil na svých internetových stránkách) rodné číslo povinného, přitom žádný právní předpis neukládá soudnímu exekutorovi usnesení o ceně tímto způsobem zveřejnit.

Podle § 13 odst. 7 zákona o evidenci obyvatel je oprávněna užívat nebo rozhodovat o jeho využívání výlučně fyzická osoba, které bylo rodné číslo přiděleno, nebo její zákonný zástupce; jinak lze rodné číslo využívat jen v případech stanovených v § 13c zákona o evidenci obyvatel. Podle § 13c odst. 1 písm. a) zákona o evidenci obyvatel lze rodné číslo využívat pouze tehdy, jde-li o činnost ministerstev, jiných správních úřadů, orgánů pověřených výkonem státní správy, soudů, a vyplývá-li to z jejich zákonem stanovené působnosti, nebo notářů – pro potřebu vedení Centrální evidence závětí. Podle § 28 zákona č. 120/2001 Sb., o soudních exekutorech a exekuční činnosti (exekuční řád) a o změně dalších zákonů, se úkony exekutora při provádění exekuce považují za úkony soudu: Proto lze konstatovat, že soudní

exekutor je oprávněn využívat při své činnosti rodná čísla. Současně je však třeba konstatovat, že ačkoliv mají správní orgány a soudy obecné zmocnění k využívání rodných čísel, nelze je vykládat tak, že by s rodným číslem mohly neomezeně nakládat, ale musejí při jeho používání současně respektovat ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, podle něhož je správce povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly při výkonu jeho činnosti shromážděny. Žádný právní předpis přitom nepředpokládá, že by rodné číslo bylo zpracováváno za účelem zveřejnění. Současně ani žádný právní předpis, konkrétně zákon č. 99/1963 Sb., občanský soudní řád, nestanoví, že by usnesení nebo rozsudek měly obsahovat v označení účastníků jejich rodné číslo.

V předmětné věci bylo rodné číslo povinného uvedeno v usnesení o ceně nemovitosti. Náležitosti usnesení jsou stanoveny v § 169 odst. 1 zákona č. 99/1963 Sb., podle kterého se v usnesení uvede mimo jiné označení účastníků. V souladu s ustanovením § 167 odst. 2 zákona č. 99/1963 Sb. lze poté na usnesení užít ustanovení o rozsudku; § 157 odst. 1 zákona č. 99/1963 Sb. vyžaduje „přesné označení účastníků". Podle věty poslední tohoto ustanovení se, je-li to možné, uvede v označení účastníků též jejich datum narození (identifikační číslo). Logickým výkladem lze poté dospět k jednoznačnému závěru, že požadavek na uvedení data narození vedle požadavku na „přesné označení účastníků" v rozsudku (a tedy i v usnesení) znamená, že ono „přesné označení účastníků" nezahrnuje uvedení jejich rodného čísla, neboť pak by uvádění data narození účastníků řízení bylo zcela nadbytečné.

Lze odkázat také na komentář k občanskému soudnímu řádu (Bureš J. a kol.: Občanský soudní řád: komentář, C.H. Beck, 6. vydání, Praha 2003), který v případě označení účastníků řízení v rozsudku odkazuje na označení účastníků v žalobě; zde se uvádí, že fyzickou osobu jako účastníka řízení je třeba označit jménem, příjmením a bydlištěm. Je-li to potřebné nebo nutné (ten, kdo podává návrh, například nezná bydliště, nebo účastník se v místě bydliště nezdržuje, ve stejném místě bydlí více osob, které mají stejné jméno a příjmení apod.), je potřebné uvést i další údaje (datum narození, rodné číslo, místo, kde se zdržuje, místo podnikání). K tomuto je nutno dodat, že rodné číslo, jakožto obecný identifikátor fyzické osoby požívající zvláštní právní ochrany podle zákona o evidenci obyvatel lze použít až jako poslední možnost, přičemž v naprosté většině případů bude postačovat identifikace účastníka řízení prostřednictvím jména, příjmení, bydliště a data narození.

Argumentaci, že v exekučním řízení je nutné, či snad dokonce jedině možné, naprosto přesně identifikovat povinného prostřednictvím rodného čísla, je s ohledem na výše uvedené v rozporu se současnou platnou právní úpravou, kromě jiného také proto, že požadavek na identifikaci účastníka řízení před soudem je vždy stejný, bez ohledu na to, zda jde o běžné civilní nalézací řízení, trestní řízení nebo o exekuční řízení, přičemž v prvních dvou případech není v rozsudku rodné číslo účastníků běžně uváděno. Současně by totiž ad absurdum bylo možné dospět k závěru, že nelze nařídit exekuci na základě rozsudku, který neobsahuje rodné číslo účastníků, neboť soud by neměl jistotu, že exekuce bude nařízena skutečně proti povinnému, který má povinnost uloženou rozsudkem plnit, neboť by nebyl v rozsudku dostatečně přesně identifikován.

Obdobně nelze oprávnění k využívání rodných čísel pro identifikaci žalovaných vyvozovat ani ze skutečnosti, že jak katastr nemovitostí, jenž je veřejnou evidencí dostupnou i ve formě dálkového přístupu, tak i list vlastnictví, jako veřejná listina, rodná čísla obsahují a zpřístupňují je tak široké veřejnosti. Zpracování rodných čísel v souvislosti s vedením katastru nemovitostí je v souladu s § 13c odst. 1 písm. a) zákona o evidenci obyvatel. Avšak ani zákon č. 344/1992 Sb., o katastru nemovitostí České republiky (katastrální zákon), ani jiný právní předpis neobsahuje oprávnění uživatelů této evidence volně disponovat se zde uvedenými rodnými čísly.

K uveřejnění usnesení o ceně na internetových stránkách exekutorského úřadu lze konstatovat, že i tento způsob zpracování osobních údajů povinného je v rozporu s § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, neboť žádný právní předpis neukládá soudnímu exekutorovi zveřejnit tímto způsobem usnesení o ceně. Podle § 336a odst. 4 zákona č. 99/1963 Sb. se usnesení o ceně doručí oprávněnému, těm, kdo do řízení přistoupili jako další oprávnění, povinnému a osobám, o nichž je známo, že pro ně váznou na nemovitosti práva nebo závady. Toto usnesení se proto nijak dále veřejně nepublikuje. Proto Úřad ve smyslu čl. 2 odst. 3 Ústavy České republiky, podle kterého lze státní moc uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon, považuje uveřejnění usnesení o ceně na internetových stránkách účastníka řízení za zpracování osobních údajů, které není v souladu s účelem, pro který byly údaje shromážděny.

Za uvedené porušení povinnosti podle § 5 odst. 1 písm. f) zákona o ochraně osobních údajů byla Úřadem udělena pokuta ve výši 8 000 Kč, která byla na základě podaného rozkladu potvrzena rozhodnutím předsedy Úřadu, jež bylo následně napadeno správní žalobou.

Vymáhání pohledávek

Další pokuta za porušení zákona o ochraně osobních údajů byla udělena (ve dvou samostatných řízeních) dvěma osobám, které v souvislosti s vymáháním pohledávek obchodní společnosti uvedly v tiskovém prohlášení, že po fyzické osobě (bylo uvedeno jméno, příjmení a rodné příjmení) byly vymáhány pohledávky, a to včetně uvedení dlužné částky, příslušného soudu a spisové značky případu a data uhrazení částky. Uvedeným jednáním tyto osoby porušily povinnost stanovenou v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, tedy povinnost zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny.

Zveřejnění osobních údajů je jedním ze způsobů zpracování ve smyslu ustanovení § 4 písm. e) zákona o ochraně osobních údajů. V dodatku mandátní smlouvy, na jejímž základě svou činnost účastníci řízení prováděli, je sice uvedeno, že na informace, které jim obchodní společnost předává pro účely vymáhání pohledávek, se režim stanovený zákonem o ochraně osobních údajů v žádném případě nevztahuje; tento zákon však obsahuje i kogentní normy veřejného práva, jejichž aplikaci strany nemohou smluvně vyloučit a vyhnout se tak povinnostem z nich vyplývajících.

Obchodní společnost shromažďuje osobní údaje osob, vůči nimž má pohledávku, a je správcem těchto osobních údajů. K tomuto účelu také provádí další zpracování osobních údajů těchto osob, např. osobní údaje uchovává, třídí nebo předává. Účastníci řízení mají s obchodní společností uzavřenu mandátní smlouvu a podle ní vymáhají její pohledávky vůči těmto osobám, jestliže je nezaplatily řádně a včas, a to ani poté, co v souvislosti s tímto zjištěním byly k zaplacení vyzvány. Na základě pověření v této smlouvě proto účastníci řízení zpracovávají osobní údaje osob, vůči nimž vymáhají pohledávky.

V daném případě je jednoznačné, že tito účastníci provádějí zpracování těchto osobních údajů ve smyslu § 4 písm. e) zákona o ochraně osobních údajů, neboť tyto osobní údaje např. používají, předávají, uchovávají či třídí. Současně je naplněna i druhá podmínka definice zpracování, a to požadavek, aby shora uvedené operace s osobními údaji byly prováděny systematicky. Prvek systematičnosti je dán tím, že některá z operací charakterizujících pojem zpracování je prováděna s určitým záměrem. V tomto případě je také prvek systematičnosti obsažen v samotném způsobu, jakým jsou osobní údaje obchodní společností vedeny a účastníkům řízení předávány, kdy jde o společnou počítačovou síť. Dále lze uvést, že účastníci řízení se v mandátní smlouvě zavazují, že povedou evidenci všech převzatých pohledávek, a to jednak ve formě dokumentace a jednak ve formě počítačové doku-

mentace (vedení evidence pohledávek nepochybně odpovídá pojmu uchovávání v definici zpracování), přičemž nejpodstatnější složkou vedení každé dokumentace je prvek systematičnosti.

Obchodní společnost zpracovávala osobní údaje fyzické osoby za účelem vymáhání svých pohledávek, přičemž účastníky řízení pověřila v mandátní smlouvě zpracováním těchto osobních údajů za totožným účelem. Podle ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů je správce (resp. zpracovatel) povinen zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Účastníci řízení přesto zpracovávali osobní údaje fyzické osoby i po zaplacení dlužné částky, kdy z celkové evidence pohledávek vybrali ty, které se jí týkají, a poté je zveřejnili v tiskovém prohlášení; zveřejnění je přitom jedním ze způsobů zpracování ve smyslu ustanovení § 4 písm. e) zákona o ochraně osobních údajů. Toto zpracování osobních údajů neodpovídá žádnému z účelů, pro který jsou účastníci řízení na základě mandátní smlouvy oprávněni osobní údaje dlužníků zpracovávat. Současně lze konstatovat, že neodpovídá ani účelu, pro který obchodní společnost osobní údaje zpracovává. Za porušení povinnosti stanovené v § 5 odst. 1, písm. f) zákona o ochraně osobních údajů byla Úřadem udělena pokuta ve výši 25 000 Kč každému z účastníků řízení. Tyto pokuty byly, stejně jako v předchozím případě, napadeny správní žalobou.

■ Zasílání obchodních sdělení

Porušení zákona bylo shledáno i v případě obchodní společnosti, která zasílala obchodní sdělení bez prokazatelného souhlasu adresátů, čímž byla porušena povinnost stanovená v § 7 odst. 2 zákona o některých službách informační společnosti, podle kterého lze podrobnosti elektronického kontaktu za účelem šíření obchodních sdělení elektronickými prostředky využít pouze ve vztahu k takovým uživatelům, kteří k tomu dali předchozí souhlas.

Obchodní společnost byla na základě smlouvy o poskytování informačních služeb Evropské databanky účastníkem Evropské databanky a tvrdila, že možnost zasílat obchodní sdělení ostatním účastníkům této databáze vyplývá ze smluvního vztahu k ní. Naopak společnosti, které se podílejí na správě a provozu databáze, tj. na poskytování jejích služeb, sdělily, že není pravdou, že všichni účastníci databáze Evropské databanky jsou si vědomi, že na základě zařazení do ní mohou být adresáty obchodních sdělení ze strany ostatních subjektů databáze, neboť mohou být pouze adresáty poptávek na jejich výrobky nebo služby. Dále uvedly, že všeobecné obchodní podmínky smluv o poskytování informačních služeb Evropské databanky, uzavíraných s účastníky databáze, neobsahují prvek souhlasu jejích účastníků s tím, že jejich elektronická adresa slouží pro vzájemnou komunikaci mezi účastníky databáze.

Souhlas účastníka řízení se zařazením do databáze Evropské databanky byl podle výše uvedené smlouvy udělen za účelem zveřejnění a poskytnutí informací prostřednictvím poskytovatele pro účely propagace činnosti, reklamy a pro marketingové účely, za účelem možnosti zaslání poptávky po zboží nebo službě takto prezentované, a nikoli pro rozesílání vlastních propagačních materiálů, a zjevně tak nebyl souhlasem pro šíření obchodních sdělení elektronickými prostředky.

Na webovém portálu Evropské databanky je každému účastníkovi automaticky vytvořena jeho vlastní webová stránka, na které je uvedena poznámka, že zpráva účastníka (poptávka) bude doručena zprostředkovaně a že systémem nebude doručena, pokud by měla charakter nabídky.

Za porušení § 7 odst. 2 zákona o některých službách informační společnosti byla prvoinstančním orgánem Úřadu uložena pokuta ve výši 10 000 Kč. Na základě podaného rozkladu poté v odvolacím řízení předseda Úřadu napadené rozhodnutí zrušil a věc vrátil správnímu orgánu prvního stupně k novému projednání. Orgán

prvního stupně spisový materiál doplnil na základě závěrů obsažených v odůvodnění druhoinstančního rozhodnutí a uložil pokutu v původní výši, která byla po podaném rozkladu předsedou Úřadu potvrzena.

K řízením podle § 17 zákona o ochraně osobních údajů

Tato část se pro lepší představu a informaci o prováděných řízeních zaměřuje na sektorové dělení, ze kterého oznámení o zpracování, ze kterých vyplynula obava o jeho zákonnost, pocházejí:

školy (mateřské, základní, střední, vysoké i umělecké)	37
průmyslové podniky	22
nemocnice	6
bytové domy	8
orgány veřejné správy	6

Z rozhodnutí Úřadu o přestupku podle zákona o střetu zájmů

Podstatou jednání obviněného bylo zveřejnění údajů z majetkových přiznání členů vlády v jednom z českých deníků, aniž se přitom autor věnoval konkrétnímu střetu zájmů u některé z osob, jejíž údaje byly zveřejněny. Článek se pouze zabýval kontrolou majetkových přiznání českých politiků, tj. shrnul obsah údajů o majetku a závazcích, tak jak je uvedli ve článku zmínění politici ve svých oznámeních podaných podle zákona o střetu zájmů. Tento zákon přitom stanoví, že veškeré údaje vedené v registru mohou být použity a dále zpracovávány pouze za účelem zjištění případného střetu zájmů při výkonu funkce veřejného funkcionáře, a porušením této povinnosti se fyzická osoba dopustí přestupku.

Úřad dospěl k závěru, že samotné zveřejnění údajů z registru, aniž bylo dáno do souvislosti s jinou skutečností nebo informací, která by mohla nebo měla vést ke zjištění případného střetu zájmů, nesplňuje podmínku oprávněného použití údajů. Na základě této úvahy pak dospěl k závěru, že obviněný svým jednáním naplnil formální znaky skutkové podstaty přestupku podle § 23 písm. a) zákona o střetu zájmů, neboť údaje použil k jinému účelu než ke zjištění případného střetu zájmů.

Současně se však Úřad zabýval i otázkou materiálního znaku jednání, tedy otázkou, zda lze jednání obviněného posoudit jako jednání, které porušuje nebo ohrožuje zájem společnosti. Není-li přitom naplněn tento znak, nelze dané jednání považovat za přestupek.

Zákon o střetu zájmů vymezuje okruh veřejných funkcionářů velmi široce, neboť sem zařazuje osoby od členů vlády, poslanců a senátorů přes vrcholné státní úředníky, soudce, členy obecních a krajských zastupitelstev až po policisty a běžné vedoucí státní zaměstnance. Pravidla pro nakládání s jejich osobními údaji v registru zpracování jsou přitom vymezena stejným způsobem, ačkoliv je zřejmé, že tyto osoby mají ve společnosti z hlediska svého postavení velmi rozdílnou roli. V daném případě je zřejmé, že i míru ochrany jejich soukromí a soukromého života bude nutno posuzovat rozdílně. Úřad se v této souvislosti shodně s judikaturou Ústavního soudu a Evropského soudu pro lidská práva domnívá, že je třeba vytvořit určitou hierarchii veřejně činných osob; na vrcholu tohoto žebříčku stojí členové vlády následováni řadovými politiky na celostátní nebo lokální úrovni, dalšími veřejně činnými osobami jako jsou celebrity, ale i úředníci, soudci, advokáti, až po běžné občany nezastávající ve společnosti žádnou funkci nebo významnou roli.

Úřad v této věci posuzoval také konflikt ústavního práva na ochranu soukromí (čl. 10 Listiny základních práv a svobod, resp. čl. 8 Úmluvy o ochraně lidských práv a základních svobod) a práva na svobodu projevu (čl. 17 Listiny základních práv a svobod, čl. 10 Úmluvy o ochraně lidských práv a základních svobod). Jak vyplývá z omezení způsobu použití údajů získaných z registru oznámení v zákoně o stře-

tu zájmů, upravil zákonodárce s ohledem na vyvážení obou zmíněných ústavních práv pravidla pro přístup k informacím a pro použití informací z registrů. Zákonné omezení tak umožňuje naplnit účel tohoto zákona, tedy zjištění a zabránění střetu zájmů, a současně nemá představovat významný zásah do soukromí povinných osob (veřejných funkcionářů), tj. nekontrolované nakládání s údaji o jejich majetku. Současně ovšem zákon nijak nezohledňuje rozdílnou roli těchto osob jako „veřejných osobností".

Přesto, nebo právě proto, se Úřad domnívá, že v případě členů vlády, tedy osob stojících na vrcholu výkonné moci, lze ústavně konformním výkladem dospět k závěru, že prosté zveřejnění informací o jejich majetku prostřednictvím novin neporušuje ani neohrožuje zájem společnosti. V případě členů vlády je zřejmé, že se v jejich rukou koncentruje rozsáhlá pravomoc rozhodovat o nejpodstatnějších otázkách týkajících se nakládání s veřejnými prostředky, o vnitropolitickém i zahraničním směřování České republiky apod. S touto pravomocí je nepochybně spojen také vyšší zájem veřejnosti na transparentnosti a kontrole jejich rozhodování, kromě jiného také z hlediska, zda není ovlivněno možným střetem zájmů. Současně je také třeba dle Úřadu přihlédnout ke skutečnosti, že jedním z úkolů tisku ve svobodné a demokratické společnosti je plnit úlohu tzv. „veřejného hlídacího psa".

Uložené sankce

V této části se zaměříme na tři nejzávažnější případy porušení povinností při zpracování osobních údajů – měřeno kritériem výše uložené sankce.
(Pozn. Jde pouze o taková řízení o správních deliktech, která byla v roce 2007 pravomocně ukončena.)

Jedna z nejvyšších pokut v minulém roce byla uložena ministerstvu, které v souvislosti s vedením informačního systému Evidence obyvatel (ISEO) jako správce osobních údajů zpracovávalo osobní údaje osob zemřelých před rokem 1956, ačkoliv dle § 9 odst. 1 zákona (zákon o evidenci obyvatel), je tato lhůta taxativně stanovena na dobu 50 let od úmrtí osoby nebo od prohlášení osoby za mrtvou, dále vytvářelo pomocné datové položky (osobní údaje), které nejsou obsaženy v zákonném taxativním výčtu v tomto informačním systému, a umožňovalo jejich zpřístupnění příjemcům údajů z ISEO. Také se dopustilo porušení zákona tím, že subjektům údajů neposkytlo požadované informace a poučení o jejich právech souvisejících se zpracováním osobních údajů, a také tím, že umožňovalo provádět operace, a zejména testování pro vývojové účely, na „ostrých" datech, které představovaly zvýšené riziko neoprávněného zpracování, změny či dokonce ztráty osobních údajů v ISEO, a to pouze na základě neformálního zajištění bezpečnosti v podobě ústního nebo konkludentního pokynu oprávněného zaměstnance. Výše popsaným jednáním došlo ze strany ministerstva k porušení § 5 odst. 1 písm. e) a f), § 11 odst. 1 a 2 a § 13 odst. 1 zákona o ochraně osobních údajů, za což mu byla příkazem uložena pokuta ve výši 1 000 000 Kč. Na základě podaného odporu bylo přihlédnuto k tomu, že plnění povinností při zpracování osobních údajů v ISEO je stanoveno v několika právních předpisech, které je třeba splnit současně, a dále ke skutečnosti, že nebylo prokázáno, že by došlo k zásahu do práva na ochranu osobních údajů nebo práva na ochranu soukromého a rodinného života. Proto byla následně pravomocně uložena pokuta ve výši 400 000 Kč. V současnosti je věc napadena správní žalobou, o které nebylo dosud rozhodnuto.

Další sankce byla Úřadem uložena odborovému sdružení, které v souvislosti s provozem kamerového monitorovacího systému, instalovaného v kancelářích předsedy a sekretariátu, shromažďovalo v druhé polovině roku 2004 osobní údaje všech

osob, které se v uvedených prostorách zdržovaly v pracovní době, aniž disponovalo jejich souhlasem se zpracováním osobních údajů, ačkoliv na dané zpracování se nevztahovala žádná z výjimek umožňujících zpracování osobních údajů bez souhlasu subjektů údajů. Dále porušilo povinnost informovat subjekty údajů o podmínkách tohoto zpracování, tedy o tom, v jakém rozsahu a pro jaký účel budou osobní údaje shromažďovány, kdo a jakým způsobem bude údaje zpracovávat a komu mohou být zpřístupněny, přičemž je ani nepoučilo o jejich právu přístupu k osobním údajům, právu na opravu údajů a o dalších právech podle § 21 zákona o ochraně osobních údajů. Současně nesplnilo další z povinností, která ukládá přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo k nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům a k jinému neoprávněnému zpracování. Následkem těchto pochybení došlo v tomto případě k odcizení pevného disku osobního počítače obsahujícího záznamy z kamerového systému a k následnému zveřejnění těchto záznamů v televizním vysílání. Výše popsaným jednáním tak došlo k porušení § 5 odst. 2, § 11 odst. 1 a § 13 odst. 1 zákona o ochraně osobních údajů, za které byla odborovému sdružení příkazem uložena pokuta ve výši 200 000 Kč. Sankce ve stejné výši byla po podaném odporu uložena odborovému sdružení i prvoinstančním rozhodnutím a následně potvrzena rozhodnutím předsedy Úřadu. Tento případ je, stejně jako případy předchozí, předmětem správní žaloby.

Při výkonu pravomocí Úřadu ukládat sankce podle zákona o ochraně osobních údajů byla v minulém roce jedna z pokut uložena též společnosti poskytující služby elektronických komunikací, která prostřednictvím svého dealera, který měl postavení zpracovatele, uzavírala smlouvy o připojení a poskytování veřejných služeb retransmise a o koupi a prodeji. Přílohou každé této smlouvy byla kopie občanského průkazu, kterou byl smluvní partner povinen vyžadovat při uzavírání smluv na základě přílohy k mandátní smlouvě. Dále byla u některých smluv také kopie cestovního pasu nebo řidičského průkazu a také kopie rozpisu bezhotovostní platby SIPO, které daný zpracovatel shromažďoval již zcela nad rámec svých povinností. Došlo tak ke shromažďování nadbytečných osobních údajů získaných z kopií obou stran občanského průkazu v rozsahu rodinný stav, rodné příjmení, místo narození, údaje získaného prostřednictvím fotografie, případně jména, příjmení a rodného čísla manžela/manželky a dětí. Tím došlo i k porušení několika ustanovení zákona o ochraně osobních údajů. Jednalo se konkrétně o shromažďování osobních údajů společností, a to v rozporu se stanoveným účelem a v rozsahu nikoliv nezbytném pro naplnění tohoto účelu, kterým je uzavíraní a plnění smluv, u nichž jsou v zákoně o elektronických komunikacích taxativně stanoveny jejich náležitosti. Podle názoru Úřadu je tedy v souladu s příslušnými ustanoveními speciálních právních předpisů pro identifikaci smluvní strany v případě smlouvy o výpůjčce postačující uvést jméno, příjmení, adresu a datum narození fyzické osoby. Společnost dále nesplnila úplně svoji informační povinnost tím, že neinformovala své klienty o jejich právu přístupu k osobním údajům, právu na opravu osobních údajů a o jejich dalších právech stanovených v § 21 zákona o ochraně osobních údajů. Nepřenesla rovněž tuto povinnost na své zpracovatele a ani neinformovala klienty, zda je poskytnutí osobních údajů povinné či dobrovolné. Popsaným jednáním tak došlo k porušení § 5 odst. 1 písm. d), § 11 odst. 1 a 2 zákona o ochraně osobních údajů, za které byla společnosti uložena pokuta ve výši 57 000 Kč.

Počet podnětů a provedených řízení:

Počet podnětů ve věci sankčních řízení podle zákona o ochraně osobních údajů, zákona o evidenci obyvatel, zákona o střetu zájmů a zákona o některých službách informační společnosti

celkem ---------- 82

z toho

– podnětem fyzických a právnických osob ---------- 41

– postoupením orgány činnými v trestním řízení a přestupkovými orgány ---------- 25

– na základě kontrolní činnosti Úřadu ---------- 16

Vyřízeno:

(obsahuje i vyřízení podnětů jejichž projednávání bylo započato v roce 2006)

– odložením před zahájením řízení, postoupením příslušnému orgánu ---------- 21

– rozhodnutím o uložení sankce celkem ---------- 43

– z toho pravomocně ---------- 32

– zastavením řízení, rozhodnutím o nespáchání deliktu ---------- 18

Počet podnětů při vzniku důvodných pochybností o zákonnosti oznámeného zpracování (řízení podle § 17 odst. 1 zákona o ochraně osobních údajů)

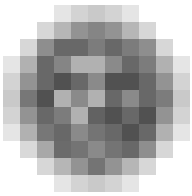
Celkem ---------- 115

Vyřízeno:

nepovolením zpracování ---------- 16

zastavením řízení (správce neporušuje podmínky stanovené zákonem) ----- 76

zastavením řízení (nedochází ke zpracování osobních údajů) ---------- 4



Legislativa v roce 2007

SCHENGENSKÁ NOVELA ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ

V legislativní oblasti v roce 2007 se Úřad zaměřil na zpětné promítnutí zkušeností při aplikaci pravidel ochrany a zpracování osobních údajů do zákona o ochraně osobních údajů. Ačkoliv v konečné fázi nerealizoval vlastní novelu tohoto zákona, některé výsledky své práce využil při přípravě novely zákona o ochraně osobních údajů. Novelizace zákona o ochraně osobních údajů byla jednou z klíčových částí implementace schengenského acquis a její provedení se stalo nezbytným krokem pro bezproblémový vstup České republiky do schengenského prostoru. Změna zákona byla společně s novelami dalších předpisů jako jeden změnový zákon projednána bez připomínek a pozměňovacích návrhů Parlamentem (viz sněmovní tisk č. 187) a vyhlášena pod č. 170/2007 Sb.

Na první pohled se „schengenská" novelizace úzce dotýká pouze policejní práce, avšak je třeba si uvědomit, že v oblasti zpracování osobních údajů v rámci schengenského prostoru umožňuje využívání a sdružování řady informací vedených v jednotlivých státních, a to nejen v čistě bezpečnostních agendách, navíc v rámci „nadnárodní" (tj. přeshraniční) spolupráce. Tento stav klade zvýšené nároky na dosud samostatně provozované databáze i nově zřizované přenosy dat, jak z pohledu pravidel pro jejich využívání, tak z pohledu zabezpečení údajů před zneužitím.

OBSAH NOVELY

Úřad v této souvislosti uvítal doporučení expertů v rámci provedeného hodnocení připravenosti ČR na vstup do schengenského prostoru, současně však při tvorbě novely zákona přihlížel k aktuálním dokumentům a v nich obsaženým požadavkům tak, aby formulovaná pravidla nebyla v rozporu s téměř dokončenými návrhy dokumentů pro novou verzi Schengenského informačního systému (SIS II). Výše uvedené pak promítnul do následujících oblastí: 1) došlo ke zpřesnění dozorové kompetence Úřadu, 2) byly provedeny drobné změny v oblasti zpracování citlivých údajů a 3) podrobně byla rozvedena pravidla týkající se zabezpečení osobních údajů. Pro úplnost je třeba dodat, že mimo rámec zákona o ochraně osobních údajů, ve zvláštních předpisech týkajících se zejména policie a celní správy, byla více či méně úspěšně zapracována doporučení expertů např. v oblasti přístupu občanů k údajům, které jsou o nich vedeny, v právu na opravu těchto údajů i v povinnosti úřadů a bezpečnostních složek informovat o zpracování těchto údajů (o „schengenské agendě" blíže v samostatné části výroční zprávy).

PŘESNĚJŠÍ KOMPETENCE ÚŘADU

Předně bylo úpravou § 2 odst. 2 zákona ochraně osobních údajů jednoznačně zakotveno, že Úřadu je svěřena působnost ústředního správního úřadu pro oblast ochrany osobních údajů, ať už je tato oblast upravena v zákoně o ochraně osobních údajů anebo v jiných zákonech či v mezinárodních smlouvách, které jsou součástí právního řádu (včetně schengenských úmluv), a že tento úřad je v ČR kompetent-

ní plnit v nich stanovené úkoly. Uvedená změna odráží skutečnost, že kompetence dozorových úřadů jsou již dnes vymezeny také prostřednictvím mezinárodních předpisů a předpisů Evropských společenství, jejichž dodržení je závazkem České republiky vůči Evropské unii.

Souběžně byla doplněním § 2 odst. 3 zákona o ochraně osobních údajů jednoznačněji zakotvena pozice Úřadu pro ochranu osobních údajů jakožto dozorového úřadu ve smyslu mezinárodních smluv, které jsou součástí právního řádu ČR a v nichž je výslovně zakotven závazek smluvních stran určit dozorový orgán pro oblast ochrany osobních údajů. Stanovení takového orgánu s nezpochybnitelnou kompetencí vůči údajům zpracovávaným v SIS byla jednou ze základních otázek posuzovaných v rámci připravenosti České republiky na vstup do schengenského prostoru. Ustanovení přitom zohledňuje dosavadní působnost Úřadu vyplývající i z jiných mezinárodních smluv, např. o Europolu.

Další úpravy napravily nejasnosti konstatované v schengenské hodnotící zprávě, které v minulosti vedly nebo by mohly vést ke zpochybnění dozorové kompetence Úřadu. Předně se v § 29 zákona o ochraně osobních údajů výslovně stanoví, že Úřad je oprávněn provádět dozor nejen nad dodržováním povinností stanovených zákonem o ochraně osobních údajů, ale i podle zvláštních zákonů, v nichž jsou upraveny postupy při zpracování osobních údajů. Současně se výslovně zakotvuje kompetence Úřadu přijímat podněty a stížnosti na porušení povinností pro zpracování osobních údajů stanovených jak v zákoně o ochraně osobních údajů, tak ve zvláštních zákonech.

ZÁSADNÍ VĚCNOU ZMĚNOU JE ÚPRAVA MNOŽINY CITLIVÝCH ÚDAJŮ

Podle do novely platné definice citlivých údajů by byly na veškeré biometrické údaje kladeny nepřiměřené požadavky, mj. odlišné od praxe v Evropské unii. Z tohoto důvodu došlo k upřesnění definice citlivého údaje, a tím i k omezení povinnosti správce a zpracovatele na užší množinu biometrických údajů. Důvodem pro zpřesnění definice biometrického údaje jako citlivého údaje je skutečnost, že nikoliv každý biometrický údaj sám o sobě umožňuje přímo identifikovat nebo autentizovat subjekt údajů, tyto biometrické údaje nemohou být citlivými údaji. Proto podle navrhované právní úpravy je citlivým údajem pouze takový biometrický údaj, který umožňuje bezprostřední identifikaci nebo autentizaci subjektu údajů bez spojení s jinými údaji, tj. takový údaj, který svou kvalitou obvykle slouží k zajištění bezpečnosti či stanovení určité míry důvěry spojených s nositeli těchto údajů. Použití takových údajů v úředních agendách (např. v souvislosti s cestovními pasy) již v současnosti upravují některé předpisy Evropských společenství. Na místo technické definice vymezující biometriku podle aktuálního způsobu jejího využití byla zvolena definice, která by do budoucna měla umožnit, aby byla zohledněna vždy pouze skutečně „citlivá“ množina údajů.

ZPRACOVÁNÍ CITLIVÝCH ÚDAJŮ V BEZPEČNOSTNÍ OBLASTI

Doposud byly některé postupy týkající se zpracování citlivých údajů v bezpečnostních agendách předmětem dílčích právních úprav (např. v zákonu o Policii ČR a trestním řádu). Svou systematikou se však množina takových jednání nepochybně řadí do oblasti obecné úpravy zpracování citlivých údajů (§ 9 zákona o ochraně osobních údajů). Doplněním § 9 byla výslovně stanovena výjimka pro zpracování citlivých údajů pro ucelenou agendu předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách, a to s ohledem na povahu této agendy i bez souhlasu subjektu údajů. Úprava současně vychází vstříc expertním doporučením, tedy požadavku podřadit SIS, v jehož rámci budou zpracovávány i citlivé údaje, nikoli pod režim výjimek, ale pod režim obecné úpravy ochrany osobních

údajů (viz odůvodnění k čl. I bodu 2 a 3). Podobně jako v případě stávajících podmínek pro zpracování citlivých údajů podle § 9 zákona o ochraně osobních údajů však nové ustanovení nestanoví blíže jednotlivé fáze zpracování citlivých údajů, neboť v oblasti veřejné moci jsou detailní postupy (včetně oprávnění vyžadovat informace a osobní údaje) upravovány vždy příslušnými zvláštními zákony.

UPŘESNĚNÍ PODMÍNEK PRO ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Jak již bylo zmíněno ve výroční zprávě za rok 2006, dosavadní vyjádření konkrétních povinností správců a zpracovatelů k zabezpečení údajů bylo již od počátku vzniku zákona považováno za příliš obecné a v mnoha případech obtížně realizovatelné. Odborná veřejnost aplikující předmětné ustanovení v praxi požadovala podrobněji vysvětlit, v právních předpisech zakotvit a alespoň rámcově vymezit náležitosti technicko-organizačních opatření k zajištění ochrany osobních údajů, příp. podrobněji stanovit povinnosti v oblasti automatizovaného zpracování osobních údajů. Stručná formulace § 13 zákona o ochraně osobních údajů nepodávala jasnou představu naplnění povinnosti u správců a zpracovatelů pracujících s malým množstvím dat, ani v případech rozsáhlých databází a přenosů osobních údajů (SIS). Do § 13 byly proto novelou přidány nové odstavce 3 a 4, jimiž se stanoví přesný obsah opatření v rámci plnění povinnosti správců (a zpracovatelů) při zabezpečení osobních údajů. Nová ustanovení konkretizují opatření požadovaná již do novely platným odstavcem 1 citovaného paragrafu, kterých si každý správce a zpracovatel osobních údajů musí být vědom a které musí vyhodnotit obvykle předem i v průběhu plnění jednotlivých povinností při zpracování osobních údajů. Pokud při zpracování osobních údajů hrozí některá z rizik neoprávněného nebo nahodilého přístupu k osobním údajům, jejich změny, zničení či ztráty, neoprávněných přenosů, zneužití apod., je tedy na místě přijmout příslušný postup uvedený v § 13 odst. 3 nebo 4. Jednou z podmínek upřesnění zákona bylo, aby detailněji upravené předcházení rizikům nepřinášelo nové povinnosti ani další byrokratickou zátěž, proto se mj. vztahuje výslovně k § 13 odst. 1. Případná dokumentace relevantních opatření (§ 13 odst. 2) je tedy vedena v nezměněném rozsahu. Lze doufat, že toto ustanovení vnese více právní jistoty do oblasti zpracování osobních údajů i souvisejících problematik. Zcela určitě ovšem nemůže dlouhodobě nahradit pravidla pro informační bezpečnost, která v roce 2007 jako doplnění stávajících formálních předpisů slibovalo Ministerstvo informatiky.

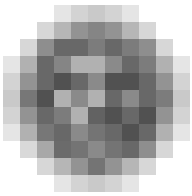
V oblasti vnější legislativy se Úřad v uplynulém roce nejčastěji vyjadřoval k legislativním návrhům i k souvisejícím materiálům nelegislativní povahy týkajícím se elektronizace veřejné správy. V této souvislosti Úřad opakovaně upozorňoval, že nové elektronické evidence a komunikační toky nemohou být v právu jednoduše upraveny, a de facto vzniknout, pouhým okopírováním pravidel pro manuální nebo částečně automatizovaný způsob zpracování dat. Z pohledu ochrany osobních údajů mohou elektronické komunikace přinést účelnější nakládání s osobními údaji, současně však vyžadují přísnější podmínky zejména pro zabezpečení evidencí a přenosu osobních údajů. Takové podmínky však obvykle s ohledem na požadavek, aby právní předpisy nebyly závislé na konkrétní technologii, často v zákonu nejsou vůbec obsaženy. Skutečným základem pro elektronickou komunikaci a e-government bude revize základních registrů státní správy plánovaná na rok 2008, kdy je nezbytné očekávat i rozpracování principů zpracování osobních údajů (např. při uchovávání údajů, ale i v oblasti přístupu občanů ke svým údajům, jak je již naznačeno v projektu CzechPoint).

Také v roce 2007 lze najít negativní případy, kdy předkladatel právního předpisu neprojevil ochotu vyhodnotit navrhovaný text z pohledu ochrany soukromí a osobních údajů. Tak tomu bylo např. v případě novely týkající se měření rychlosti na

silnicích, navržené bez projednání s Úřadem po dohodě ministrů (!) prostřednictvím poslanecké iniciativy (!). Lze se jen domnívat, že v pozadí tohoto kroku byla neznalost a nedůvěra k ochraně soukromí jako prostředku bránícího rychlému dosažení cíle na úkor všech spoluobčanů (zbývá dodat: nejen nezdárných a tímto návrhem postihovaných). Není zřejmé, proč se nenašel čas na drobné, z hlediska ochrany soukromí občanů však nezbytné formulační úpravy a na případné doplnění odůvodnění o přesný popis, jak bude nakládáno se záznamy o měření rychlosti (viz sněmovní tisk č. 185).

Případem, který by si zasloužil pečlivější přípravu zákonných pravidel zpracování osobních údajů, je návrh nového zákona o Policii ČR. Podle vyjádření zpracovatelů bude tento předpis považován mj. za pomůcku policistů, a z tohoto důvodu byl zpracovatelem požadován podrobný popis činností policie nebo alespoň návodnost jednotlivých postupů. Zde by Úřad uvítal, kdyby o návrhu komplexní úpravy zvláštního zpracování osobních údajů byl vyrozuměn s dostatečným časovým předstihem a mohl se např. v rámci expertních skupin k problematice vyjádřit. V připomínkovém řízení lze totiž jen velmi těžko projednávat a měnit systematiku navrhovaného zákona.

Za zdárné zohlednění pravidel pro zpracování osobních údajů v legislativě lze v roce 2007 považovat novelu zákona o péči o zdraví lidu, kterou Úřad od počátku podporoval. Přínosné bylo i jednání s resorty, které v poslední době navrhovaly, z pohledu Úřadu často nadbytečné, úpravy zpracování osobních údajů. Ukončeno již bylo jednání s Ministerstvem školství, mládeže a tělovýchovy, jehož zástupcům byla poskytnuta možnost seznámit se s pravidly ochrany soukromí i s poněkud odlišným názorem Úřadu na centralizovaná uchovávání údajů od občanů v době, kdy stát prostřednictvím veřejnoprávních předpisů přenáší stále více konkrétních úkolů na obce a jiné subjekty.



Schengenská spolupráce

1. PŘÍPRAVA A HODNOCENÍ

Vstup České republiky do Evropské unie dne 1. května 2004 automaticky znamenal pro naši republiku také splnění některých povinností, resp. zahájení přípravy na jejich plnění, které vyplývaly ze vstupu ČR do schengenského prostoru (tj. území států, na jejichž společných hranicích nejsou vykonávány hraniční kontroly). ČR tak již od roku 2004 prováděla část schengenských, resp. unijních pravidel týkajících se bezpečnosti a ochrany hranic nebo policejní spolupráce a na převzetí zbývající části se začala intenzivně připravovat.

Připravenost České republiky na převzetí schengenských předpisů (souvisejících především s ukončením kontroly na společných hranicích) byla zkoumána od roku 2005 v rámci schengenského hodnotícího procesu, v jehož průběhu do naší země postupně přijížděly skupiny zahraničních expertů a ověřovaly plnění schengenských pravidel v praxi. Jednou z hodnocených oblastí byla, vedle ochrany hranic, policejní a justiční spolupráce, vízové a konzulární spolupráce a Schengenského informačního systému, také úroveň ochrany osobních údajů včetně funkční kontroly prováděné nezávislým dozorovým úřadem a uplatňování standardů ochrany dat v praxi všech zainteresovaných rezortů.

Hodnocení v oblasti ochrany osobních údajů vyvrcholilo návštěvou expertní mise na jaře roku 2006 (7. až 9. března 2006). Závěrečná fáze hodnocení proběhla koncem září 2007, kdy byly prověřovány podmínky provozu Schengenského informačního systému (SIS), který byl z důvodu nezbytných technických příprav v ČR zprovozněn již k 1. září 2007. Od tohoto data tak mohou příslušné orgány (zejména policejní a celní) využívat všechny údaje, které byly do SIS vloženy v ostatních zemí, a také některé informace, pocházející z jejich činnosti, vkládat. Z pohledu terminologie zákona o ochraně osobních údajů tak od počátku školního roku dochází na našem území ke zpracování osobních údajů obsažených v SIS, a to se všemi z toho plynoucími důsledky včetně aplikace zákona o ochraně osobních údajů.

Vzhledem k tomu, že ČR byla vcelku pozitivně hodnocena ve všech uvedených oblastech a případné nedostatky byly postupně řešeny v rámci tzv. „follow-up“ procesu, byla dne 8. listopadu na jednání Rady EU pro spravedlnost a justici potvrzena připravenost ČR i dalších 8 států EU na zrušení hraničních kontrol ke dni 21. prosince 2007 v případě vnitřních pozemních a mořských hranic a ke dni 30. března 2008 na mezinárodních letištích u letů uvnitř Schengenu. Finální rozhodnutí o rozšíření Schengenu bylo poté přijato na jednání Rady ve dnech 6. a 7. prosince 2007.

2. SCHENGENSKÝ INFORMAČNÍ SYSTÉM

Schengenský informační systém byl vytvořen jako vyrovnávací opatření přispívající k udržení vysokého stupně bezpečnosti v rámci společného prostoru. Sdílení určitých informací tak představuje kompenzaci za odstranění hraničních kontrol, které s sebou přináší volný pohyb všem osobám, tedy včetně pachatelů nejrůznější trestné činnosti, a SIS je tak v současné době již neodmyslitelným prostředkem spolupráce policejních a justičních orgánů v rámci Schengenu.

SIS je fakticky společná databáze, sdílená všemi členskými státy, která obsahuje velké množství nejrůznějších informací, včetně osobních údajů (tj. informací, které jsou, popř. mohou být, vztaženy ke konkrétním fyzickým osobám). Jde např. o záznamy o osobách hledaných za účelem zatčení, o pohřešovaných osobách či o státních příslušnících třetích zemí, kterým má být odepřen vstup a pobyt na území schengenského prostoru. Další skupinu záznamů tvoří údaje o hledaných věcech, jako jsou např. odcizené či ztracené doklady, automobily, střelné zbraně nebo padělané bankovky. Pro ilustraci rozsahu tohoto systému lze uvést, že počet záznamů uložených v SIS dosahuje přibližně 18 milionů.

Využívání těchto informací je omezeno na provádění hraničních kontrol, policejních a celních kontrol ve vnitrozemí, při řízení o udělování víz a vydávání povolení k pobytu. Vzhledem k tomu, že SIS je rozsáhlou databází osobních údajů, uplatní se na zpracování dat zde vložených striktní pravidla ochrany osobních údajů. Tyto principy jsou v současné době upraveny jednak v tzv. Schengenské prováděcí úmluvě (mezinárodní dohoda z roku 1985, kterou byl mj. vytvořen SIS), jednak v národní právní úpravě ochrany dat v jednotlivých členských zemích. V ČR jde o obecný zákon o ochraně osobních údajů a o dílčí úpravy ve zvláštních právních předpisech, např. v zákoně o Policii České republiky.

3. KOMPETENCE ÚŘADU VE VZTAHU K SIS

Úřad se podílí, ve spolupráci s příslušnými resorty, na přípravě na zapojení ČR do schengenského prostoru již od roku 2005, neboť jednou z podmínek vstupu do Schengenu je existence nezávislého dozorového orgánu příslušného provádět kontrolu nad zpracováním osobních údajů.

Úkolem Úřadu v oblasti schengenské spolupráce je tedy dozor nad dodržováním principů ochrany osobních údajů zpracovávaných zejména v rámci SIS (ale také při jiných formách spolupráce příslušných orgánů) a garance práv osob, kterých se zde zpracovávaná data týkají. S ohledem na účel zpracování dat v SIS, kterým je především zajištění bezpečnosti v rámci společného prostoru, a vzhledem k charakteru opatření, která mohou být přijata na základě existence záznamu v SIS (např. zabránění vstupu nežádoucích osob na území schengenského prostoru nebo zadržení hledaných osob) je zřejmé, že zpracování osobních údajů v SIS může mít pro dotčenou osobu dalekosáhlé následky. Důsledné dodržování principů ochrany osobních údajů je proto neodmyslitelnou součástí schengenské spolupráce.

Mezi základní práva subjektů údajů ve vztahu k SIS, jejichž garantování je úkolem Úřadu, patří zejména právo být informován o údajích, které se k němu vztahují, právo na opravu chybných údajů nebo na výmaz údajů neoprávněně vložených. Nedílnou součástí tohoto práva je také možnost obrátit se, a to v kterékoli členské zemi, na národní dozorový orgán pro ochranu osobních údajů s požadavkem na prověření zpracování údajů v SIS. Dále je zaručeno právo obrátit se na soud nebo na jiný příslušný úřad a domáhat se opravy či výmazu dat vedených v SIS, nebo požadovat poskytnutí informací, případně náhrady škody.

Úřad postupuje při vyřizování žádostí či stížností týkajících se zpracování osobních údajů v SIS obdobně jako v případě ostatních podnětů, tj. uplatňuje veškeré své kompetence podle zákona o ochraně osobních údajů, včetně kontrolních a sankčních pravomocí. Úřad je oprávněn prověřovat zpracování dat jak na základě jednotlivých stížností, tak i na základě vlastního uvážení (podle plánu kontrol). Při těchto inspekcích se uplatní tytéž procesní předpisy jako při kontrolách čistě vnitrostátních informačních systémů, tedy správní řád a zákon o státní kontrole.

4. SOUVISEJÍCÍ PROBLEMATIKA

Kromě SIS, který je nejrozsáhlejším a také zřejmě nejznámějším nadnárodním informačním systémem, existuje několik dalších databází, v nichž dochází ke zpracování osobních údajů, a které obvykle tak či onak souvisejí se schengenskou spoluprací, resp. se spoluprací v rámci tzv. III. pilíře EU (jde o policejní a justiční spolupráci, tj. o agendy, které se neřídí komunitárním principem většiny, ale jsou ponechány suverénnímu rozhodování členských států).

Pro zajištění jednotné vízové politiky členských států EU je zřízen Vízový informační systém (VIS). Dále byl vybudován systém EURODAC pro porovnávání daktyloskopických otisků prstů žadatelů o azyl, za účelem určení státu příslušného k vyřízení žádosti a ve snaze zabránit zneužívání azylového řízení v EU. Dalším společným informačním systémem je Celní informační systém (CIS). V současné době je také budován Schengenský informační systém druhé generace (tzv. SIS II), který by měl od roku 2009 nahradit stávající SIS a který bude již obsahovat tzv. biometrické údaje (fotografie, otisky prstů) a umožní sdílet a využívat vložené záznamy širšímu počtu subjektů.

Zavádění biometrických údajů do národních i nadnárodních databází je ostatně trvalým trendem, který představuje (i přes své deklarované přínosy) z hlediska ochrany osobních údajů a potažmo ochrany soukromí osob velké riziko, kterému je proto ze strany Úřadu nutno věnovat zvýšenou pozornost.

Dohled nad řádným zpracováváním osobních údajů v uvedených informačních systémech, z hlediska činnosti příslušných orgánů na území ČR, spadá také do kompetence Úřadu.

5. ODBOR SCHENGENSKÉ SPOLUPRÁCE

Pro splnění všech úkolů vyplývajících z nových kompetencí Úřadu v oblasti schengenské spolupráce, ale také v rámci zmíněné související agendy, byl k 1. červenci 2007 zřízen nový útvar Úřadu – odbor schengenské spolupráce a III. pilíře (dále jen „odbor“). V souvislosti s neustále rostoucí agendou v této oblasti bylo vyhodnoceno, že toto koncepční řešení, kdy se příbuzné agendy vyřizují v rámci jednoho útvaru, je z hlediska činnosti Úřadu (dovnitř i navenek) nejpřínosnější.

Mezi základní oblast činnosti odboru patří přijímání a vyřizování podnětů a stížností od občanů na neoprávněné zpracování údajů v SIS a zodpovídání dotazů týkajících se zpracování osobních údajů v tomto systému. Především prostřednictvím analýz došlých podnětů (a z nich vyplývající koncepční činnosti) bude odbor zapojen také do provádění dozoru nad zpracováním osobních údajů v národní části Schengenského informačního systému. V případě, kdy bude zjištěno porušení povinností při zpracování osobních údajů v SIS českými orgány, povede odbor řízení o správních deliktech, které může vyústit v uložení sankce (pokuty).

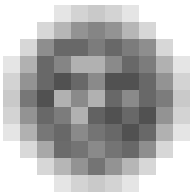
Nedílnou součástí práce odboru při vyřizování podnětů a stížností ve věci zpracování osobních údajů v SIS je úzká spolupráce s obdobnými dozorovými úřady v zahraničí, neboť efektivní kontrola mezinárodního systému jakým je SIS, je možná opět pouze za předpokladu účinné mezinárodní spolupráce.

Důležitou součástí práce odboru je poskytování informací o podmínkách zpracování osobních údajů v SIS veřejnosti, s důrazem na práva osob, jejichž osobní údaje mohou být v SIS zpracovávány. Děje se tak zejména prostřednictvím informací na webové stránce Úřadu, v Bulletinu a ve Věstníku Úřadu. Na webových stránkách Úřadu byla za tímto účelem vytvořena zvláštní sekce „Schengen“, v níž návštěvníci najdou nejen základní informace o schengenské spolupráci, ale také informace o aktuálním dění v Schengenu či právní předpisy týkající se dané problematiky. Velký důraz se zde klade na zpracování osobních údajů v SIS, zvláště na ozřejmění práv subjektů údajů. Součástí těchto stránek jsou také odkazy na dal-

ší zdroje informací o Schengenu a odkazy na národní dozorové orgány členských a přidružených států.

Pracovní náplň odboru zahrnuje také spolupráci s ostatními resorty, které se v ČR podílejí na zpracování osobních údajů v SIS. Jedná se primárně o konzultační činnost, případně účast na tvorbě nezbytných legislativních opatření (jako byl zákon č. 170/2007 Sb., kterým se mění některé zákony v souvislosti se vstupem České republiky do schengenského prostoru) anebo na realizaci společných informační kampaní.

Odbor dále zajišťuje účast Úřadu na jednání společného dozorového orgánu pro SIS (tzv. Joint Supervisory Authority – JSA Schengen) a dalších orgánů či pracovních skupin, tuzemských i zahraničních, zabývajících se souvisejícími tématy (např. Visa&Biometrics, EURODAC, JSA Customs nebo pracovní skupina pro informační kampaň k SIS II).



Registrační činnost

Hlavní náplň činnosti Registračního oddělení lze rozdělit do dvou hlavních skupin. Je to vedení registru zpracování osobních údajů, které spočívá zejména v přijímání registračních oznámení, jejich přezkoumání a evidenci, a dále vyřizování agendy spojené s předáváním osobních údajů do zahraničí, tj. vedení řízení o povolení k předání osobních údajů do třetích zemí a vydávání rozhodnutí Úřadu v této věci. V roce 2007 byl zaznamenán rovněž zvýšený zájem správců, kteří se obracejí na registrační oddělení s žádostí o konzultaci ještě dříve, než přistoupí k písemnému oznámení zpracování. Dotazy se týkaly zejména okolností spuštění kamerových systémů, podmínek předávání osobních údajů do zahraničí, povinností správce při zpracování osobních údajů apod. Konzultační činnost se tak v roce 2007 stala významnou součástí náplně práce registračního oddělení.

Rok 2007 přinesl do činnosti a postupů Registračního oddělení několik zásadních změn. Na konci roku 2006 došlo k úpravě registračních formulářů a zároveň byl zaveden elektronický způsob přijímání registračních oznámení. Cílem nové úpravy bylo celý registrační proces zpřesnit a současně zjednodušit pro správce plnění registrační povinnosti. Jednoletá zkušenost s „novou" registrací vyzněla jednoznačně pozitivně. Správci osobních údajů elektronický registrační formulář plně využívají bez větších problémů. Během této doby byly provedeny některé dílčí úpravy resp. upřesnění, které měly spíše technický charakter a reagovaly na dotazy či upozornění samotných správců na funkčnost systému. Pro Úřad znamenala tato změna zpřesnění a zefektivnění celého registračního procesu.

REGISTRAČNÍ PROCES

Z reakcí a dotazů správců je zřejmé, že smysl a účel registračního procesu není stále vnímán ze strany správců zcela přesně. Předně je nutné zdůraznit, že povinnost vést registr zpracování ukládá Úřadu zákon (§ 29 odst. 1 písm. b). Jedním z důvodů vzniku tohoto registru byl záměr, aby se mohl kdokoli a kdykoli seznámit s tím, kdo a za jakých podmínek zpracovává jeho osobní údaje. Z toho důvodu je také registr zpracování veřejně přístupný, a to i dálkovým přístupem prostřednictvím webových stránek Úřadu. V registru lze vyhledávat podle názvu subjektu, přiděleného registračního čísla nebo IČ, a lze zde nalézt informace nejen o tom, kdo, kde a jaké údaje zpracovává, ale také např. v jakém rozsahu a za jakých podmínek tak činí. V této souvislosti je nutno upozornit na skutečnost, že do registru nejsou zapisována taková zpracování, jejichž vedení správci ukládá zvláštní zákon, a o jejichž existenci je tedy subjekt údajů informován jejich prostřednictvím (jde o veřejně přístupné evidence, např. obchodní rejstřík, živnostenský rejstřík apod.), nebo taková zpracování, jejichž existenci lze alespoň předpokládat (zpracování osobních údajů, jichž je třeba k uplatnění práv a povinností, vyplývajících ze zvláštních zákonů, např. zpracování osobních údajů zaměstnanců pro vedení personální a mzdové agendy apod.). Ve vztahu k výše uvedenému je však třeba zdůraznit, že výjimka z oznamovací povinnosti nezbavuje správce žádné další povinnosti vyplývající ze zákona.

Dalším velmi častým dotazem jsou okolnosti zahájení oznámeného zpracování. Správce je oprávněn zahájit zpracování osobních údajů dnem zápisu do registru nebo po uplynutí zákonné lhůty, tj. po 30 dnech ode dne, kdy bylo oznámení o tomto zpracování doručeno Úřadu. V praxi to znamená, že správce má možnost nahlédnout do registru kdykoli před uplynutím třicetidenní zákonné lhůty, a pokud je jeho zpracování v registru zapsáno, může zahájit zpracování ještě před vypršením této lhůty. Z výše uvedeného tedy vyplývá, že Úřad, v případě, že neshledá nedostatky podaného oznámení, provede zápis do registru a oznamovatele o této skutečnosti již neinformuje. Pouze na žádost oznamovatele vydá Úřad osvědčení o provedené registraci.

Osvědčení o registraci považuje stále mnoho správců za důkaz toho, že jejich zpracování bylo Úřadem povoleno. To je ovšem velký omyl, který může vést a vede k častým nedorozuměním mezi správci a Úřadem. Je pravda, že např. některé dozorové úřady spolkových zemí v Německu vydávají osvědčení o provedeném auditu (např. Zemský úřad na ochranu dat ve spolkové zemi Šlesvicko-Holštýnsko – ULD). Zde mohou všechny orgány státní správy požádat ULD o provedení auditu, buď pro veškeré zpracování osobních údajů, nebo jejich části. Postup je takový, že na základě písemné dohody mezi ULD a příslušným státním orgánem jsou stanoveny cíle auditu, následně ULD vypracuje posudek a udělí osvědčení o provedení auditu, a to nejdéle na 3 roky. V roce 2006 provedl ULD 15 takových auditů. Osvědčení o registraci vydané Úřadem má ovšem zcela jinou dimenzi. Je pouze dokladem skutečnosti, že správce splnil svou zákonnou povinnost oznámit předem Úřadu zamýšlené zpracování a že takové zpracování bylo Úřadem zapsáno do registru. V tomto smyslu můžeme hovořit o registraci založené na „evidenčním principu“.

Jiná situace nastává v případě, že z oznámeného zpracování vznikne důvodná obava, že při zpracování osobních údajů by mohlo dojít k porušení zákona. V takovém případě má Úřad povinnost zahájit z vlastního podnětu řízení. Takové řízení má de facto naplňovat potřeby a cíle předběžné kontroly ve smyslu čl. 20 Směrnice. Vychází z předpokladu existence zpracovatelských operací, které mohou představovat zvláštní rizika pro práva a svobody subjektů údajů, a záměru, aby taková zpracování byla ze strany orgánu dozoru kontrolována ještě před jejich uskutečněním.

V plné míře se řízení podle § 17 osvědčila při posuzování záměru instalovat kamerové systémy, které bezesporu pod rizikové okruhy zpracování patří. Předmětem tohoto řízení je tedy posouzení zákonnosti oznámeného zpracování. V případě, že Úřad zjistí, že oznámeným zpracováním správce neporušuje podmínky stanovené zákonem, řízení zastaví a takové zpracování je zapsáno do registru. Pokud dojde Úřad k závěru, že na základě skutečností uvedených v oznámeném zpracování by mohlo dojít k porušení zákona, vydá rozhodnutí o nepovolení (dále viz kapitola správní rozhodování).

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ KAMEROVÝMI SYSTÉMY

Ještě ve větší míře než v loňském roce zasáhl do činnosti registračního oddělení neustávající nárůst kamerových sledovacích systémů v naší společnosti. Zatímco v loňském roce oznámilo Úřadu záměr provozovat kamerové systémy 390 správců, v letošním roce jejich počet vzrostl na 790. Podobně se zvýšil i počet dotazů a konzultací týkající se podmínek instalace kamerových systémů.

Důvody vzrůstajícího počtu kamer v naší společnosti lze hledat jednak v jejich finanční dostupnosti a velké nabídce na trhu, a jednak ve stále dokonalejších a širších možnostech jejich využití (tzv. inteligentní kamery, „mluvící kamery“ apod.). Bohužel však je iluzí, že kamery vyřeší všechny problémy spojené s vandalstvím, kriminalitou a s dalšími negativními jevy v naší společnosti. Nasazení kamerového

systému může být jistě v mnoha případech vhodným technickým prostředkem, směřujícím k prevenci páchání trestné činnosti či k odhalení případného pachatele. Je však zapotřebí, aby byly provozovány v souladu se zákonem a s respektem k ochraně soukromí. Jedním z hlavních oznamovaných účelů instalace kamer je ochrana majetku. V souvislosti s instalací a provozováním kamerových systémů je třeba zdůraznit, že ochraně majetku nemůže být obecně dávána přednost před ochranou soukromí, jak se velmi často stává. V České republice stojí ochrana soukromí a lidské důstojnosti velmi vysoko v žebříčku hodnot základních lidských práv a ochranu vlastnictví lze upřednostnit jen ve velmi specifických případech, a proto by správci provozující kamerové systémy měli vždy pečlivě zvážit, zda je skutečně tak nezbytně nutné použít sledovací kameru, která může citelným způsobem zasáhnout do soukromého a osobního života jednotlivců.

Z podaných registračních oznámení, oznamujících úmysl provozovat kamerové systémy, z reakcí správců a na základě dotazů lze konstatovat, že aspekt ochrany soukromí jednotlivců je ze strany provozovatelů kamerových systémů velmi podceňován, mnohdy zcela přehlížen, a to buď z neznalosti nebo i záměrně. Někteří si stále nedostatečně uvědomují fakt, že soukromí, osobní a rodinný život, jakož i soukromí samotné neznamená pouze prostory určené ryze k soukromým účelům jako jsou toalety, sprchy, šatny apod. Soukromí, které zahrnuje osobní a rodinný život, totiž znamená jistou sféru integrity jednotlivce a jeho blízkých, která obklopuje jednotlivce samého, ať se nachází kdekoli, a která posiluje na významu v bezprostřední blízkosti prostor, jako je bytový dům, pracoviště apod., adekvátním způsobem.

Úřad došel dále k poznatku, že v mnoha případech je možné se kamerovému sledování jednoduše vyhnout a nahradit ho jinými, méně invazivními, avšak stejně účinnými technickými prostředky. Jinými slovy kamerové systémy nejsou v mnoha případech instalovány jako poslední možnost, kdy již nelze jinak, ale jako první možnost, což je nejen v rozporu s dikcí zákona o nezbytnosti, ale rovněž v rozporu se základním principem ochrany dat, principem přiměřenosti. K velmi smutným případům, nikoli však ojedinělým, dochází, když ani sám správce nedokáže odůvodnit skutečnou potřebu kamer a jejich instalaci hodlá uskutečnit pouze na základě doporučení výrobce či prodejce kamerových systémů.

Dalším velmi často uváděným účelem instalace kamerového systému je ochrana zdraví a života. Tento účel lze ovšem považovat za irelevantní k ospravedlnění instalace kamerového systému. Jelikož v případě, že by došlo k ohrožení nebo porušení zdraví nebo života, by totiž jediným významem a přínosem systému byla pomoc orgánům činným v trestním řízení, což je jistě neodmyslitelná pozitivní vlastnost, ale s podstatou účelu zpracování osobních údajů nemá v této souvislosti nic společného. Proto je nutno vzhledem k řečenému konstatovat, že ochranu života a zdraví lze zajistit i jinými prostředky a že kamerový systém nemůže fakticky tomuto účelu posloužit, a jeho instalace je tedy v tomto případě pro dosažení zamýšleného účelu deklarovaného správcem nevhodná.

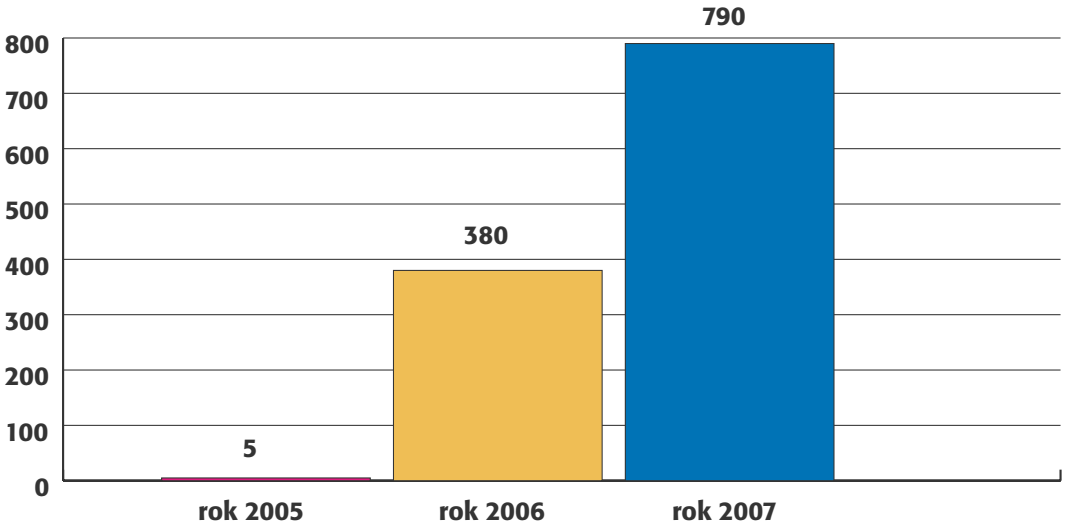
Jedním z nejčastějších míst, kde jsou kamery používány, jsou pracoviště. Kamerové systémy instalují zaměstnavatelé a jsou jimi monitorováni zejména zaměstnanci. Z registračních oznámení vyplývá, že nejčastějším důvodem je ochrana majetku, kontrola technologických postupů, kontrola dodržování bezpečnosti práce nebo kontrola výkonu práce zaměstnance. Dále, že záměrem správců je instalovat kamery ve výrobních halách, skladech, na recepcích, v administrativních budovách, firemních parkovištích a dalších venkovních prostorách, ale také v jídelnách, kantýnách, šatnách, kancelářích apod.

Princip účelnosti zpracování osobních údajů je v pracovněprávních vztazích prohlouben v § 316 odst. 2 a 3 zákoníku práce. Zákon pro sledování zaměstnanců klade přísné podmínky: Kamery (se záznamem i bez záznamu) a ostatní prostředky sledování zaměstnanců jsou zcela zakázány, pokud zde není závažný důvod

spočívající ve zvláštní povaze činnosti zaměstnavatele. Stanovení hranice závažnosti důvodů ve vztahu ke zvláštní povaze činnosti zaměstnavatele a vyjádření, v čem a proč je tato činnost zvláštní, aby mohlo být zasahováno do soukromí zaměstnanců, je často velmi obtížné. V zásadě se může jednat o prostředí, kde je třeba dbát zvýšených nároků na chování zaměstnanců (činnost peněžních ústavů, činnosti pracující s různými stupni utajení a zvláštních režimů apod.)

Nicméně je nutné striktně odmítnout snahy některých zaměstnavatelů zahájit provozování kamerového sledování v prostorách své firmy, z důvodu zabránění méně závažným disciplinárním pochybením, jako např. zamezení kouření nebo nepořádku v kantýně, zajištění používání bezpečnostních pomůcek apod.

Celkový počet registrovaných správců provozujících kamerové systémy v jednotlivých letech



Je také nutné zdůraznit, že zaměstnavatelé často vůbec nevnímají skutečnost, že pro zaměstnance, který tráví většinu svého aktivního času během dne v práci, představuje pracoviště po bydlišti významný prostor, kde probíhají jeho sociální interakce a kde se sbližuje s dalšími lidmi, a hlavně představuje prostor, který je po jeho domově většinou prostorem, kde očekává a objektivně se mu má dostávat většího soukromí než na jiných místech.

ZPRACOVÁVÁNÍ CITLIVÝCH ÚDAJŮ

V roce 2006 zaznamenal Úřad i nárůst počtu zpracování citlivých údajů. Zákon definuje citlivé údaje jako osobní údaje vypovídající o národnostním, rasovém nebo etnickém původu, náboženství a filozofickém přesvědčení, členství v odborových organizacích, odsouzení za trestný čin, zdravotním stavu a sexuálním životě, dále genetický údaj a biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů.

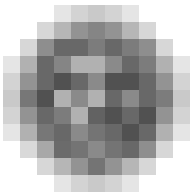
Poměrně velké množství správců v registračním oznámení uvedlo, že hodlají zpracovávat biometrické údaje. Z registračních oznámení vyplývá, že velká část správců oznamuje zpracování biometrických údajů z důvodu provozování kamerového systému, jehož prostřednictvím lze detektovat pohyb a vzhled osob. Dalším uváděným účelem zpracování biometrických údajů je vedení databáze lidí s jejich fotografiemi, sloužící zpravidla k účelům seznamovacích agentur, vyhledávání nových talentů, prezentaci vlastní osoby, nabídnutí pracovní činnosti. Jde zejména o castingové agentury nebo seznamovací servery. Zpracování biometrických úda-

jů je rovněž oznamováno z důvodu bezpečnosti a k jednoznačnému určení osoby, která vstupuje do chráněných prostor, a probíhá na základě odebrání otisku prstu. Klinické studie a lékařské účely jsou spolu s poskytováním sociálních služeb a zdravotní péče uváděny jako třetí skupina důvodů.

V souvislosti s množstvím subjektů, které zpracovávají údaje o sexuálním životě, je nutné si položit otázku, k jakým účelům jim tyto údaje slouží. Jde zejména o poskytování sociálních služeb a poradenskou činnost v sociální oblasti a v oblasti rozvoje osobnosti, o psychoterapii o lékařské účely či o vytváření jiných databází, např. studentů nebo dárců krve. V ojedinělých případech informace o sexuálním životě lidé dobrovolně vyplňují na webových seznamovacích serverech za účelem vyhledání vhodného partnera. Někdy také dochází k omylu, například v případě, kdy oznamovatel za údaj o sexuálním životě považuje údaj o počtu dětí nebo o rodinném stavu, ze kterého se dá sexuální orientace pravděpodobně odvodit.

Důvody pro sběr informací o náboženském a filozofickém přesvědčení jsou (stejně jako u údajů o sexuálním životě) především poradenská činnost, programy na opětovné začlenění různých typů lidí do společnosti nebo různé formy terapie a poskytování sociálních služeb. Vědecký výzkum a dokumentačně-badatelská činnost spojená s tvorbou databází a statistikou jsou dalšími možnostmi. Opět je zde možnost dobrovolného vyplnění příslušných formulářů na internetových stránkách seznamovacích agentur.

Největší podíl na zpracování citlivých údajů má evidence zdravotního stavu. Nejzávažnějším argumentem pro zpracování jsou lékařské účely jako např. nutnost posouzení zdravotního stavu kvůli správnému poskytnutí péče, evidence komplexních informací o pacientovi pro potřeby léčby a vedení statistiky, zvýšení bezpečnosti při vydávání léčiv nebo zpracování lékových záznamů pacienta. V oblasti medicíny se dále vytvářejí databáze a registry dárců, probíhá vědecko-výzkumná činnost, aby se zjistily vedlejší účinky léků a zhodnotila se jejich účinnost. Dalšími důvody jsou poradenská činnost v sociální oblasti a v oblasti rozvoje osobnosti, poskytování sociálních služeb, sběr dat v souvislosti s opatrovnictvím a pečovatelskou službou, diagnostika a psychoterapie. Podobně jako v předešlých případech se zpracovává údaj o zdravotním stavu na stránkách seznamovacích agentur.



Předávání osobních údajů do zahraničí

Velká většina žádostí dle ustanovení § 27 odst. 4 zákona č. 101/2000 Sb., o ochraně osobních údajů, se v roce 2007 (stejně jako v předchozích letech) týkala předání osobních údajů do Spojených států amerických. Jako příjemci těchto údajů byly nejčastěji uváděny společnosti, se kterými jsou žadatelé kapitálově propojeni, a dále pak obchodní partneři žadatelů. Vzhledem k tomu proto mezi deklarovanými účely převládaly takové, které bezprostředně souvisejí s personální a mzdovou politikou a s obchodní a výrobní činností (např. správa databáze volných pracovních míst, vedení evidence uchazečů o zaměstnání, plánování profesního rozvoje zaměstnanců, stanovení a vyhodnocení pracovních cílů, plánování služebních cest, optimalizace výrobních postupů atd.).

Nejvýznamnější události, které se v roce 2007 dotýkaly problematiky předání osobních údajů do třetích zemí, souvisely s leteckou dopravou. Úřad obdržel několik žádostí akciové společnosti České aerolinie, které se týkaly předání údajů jejích klientů (pasažérů), případně také jejích zaměstnanců (posádek letadel) příslušným úřadům v cílových destinacích. V souvislosti s rostoucími bezpečnostními opatřeními, která jsou zaváděna kvůli rizikům, která s sebou přináší sílící globalizace lidské společnosti, začínají být v některých destinacích vyžadovány po všech leteckých dopravcích velmi podrobné údaje o přepravovaných pasažérech.

Například v souvislosti s lety do Kuvajtu jsou údaje pasažérů předávány prostřednictvím systému APP (Advance Passenger Processing), který je zvláštním druhem systému APIS. Jedná se o interaktivní systém, umožňující jednotlivým národním autoritám ověřit informace o cestujících ještě před jejich vstupem na území daného státu. Osobní údaje pasažérů jsou předávány vládě Kuvajtu, resp. příslušným kuvajtským státním orgánům. Tyto státní orgány, které vyžadují údaje o pasažérech všech leteckých přepravců, chtějí takové údaje využívat k tomu, aby mohly jednotlivé pasažéry prověřit a kvalifikovaně posoudit, zda někteří z nich nepředstavují pro danou zemi bezpečnostní riziko. Jelikož jsou údaje předávány prostřednictvím interaktivního systému APP, dozví se letecká společnost v podstatě ihned, zda může konkrétní pasažér nastoupit na palubu jeho letadla, či nikoliv. Pokud by letecký dopravce přepravoval pasažéra ve svém letadle, přestože by mu jeho přílet příslušné státní orgány v Kuvajtu nepovolily, hrozila by mu vysoká finanční pokuta, nebo by mu vůbec nebylo umožněno přistání jeho letadla.

Obdobná situace je i v případě letů na Kubu. Osobní údaje pasažérů a posádek letadel jsou předávány prostřednictvím systému APIS, který však na rozdíl od systému APP není interaktivní. Po odeslání údajů prostřednictvím zmíněného systému se letecký dopravce přibližně za týden dozví, zda byly údaje předány v požadovaném rozsahu a zda jsou pro příslušné úřady dostatečné. V případě Kuby jsou osobní údaje pasažérů a posádek letadel předávány příslušným státním úřadům (Cuban Custome Office), které je vyžadují od všech leteckých společností. Účel předání těchto údajů a případné sankce jsou obdobné jako v případě Kuvajtu.

Velmi významná změna nastala v souvislosti s předáním osobních údajů cestujících (pasažérů) do Spojených států amerických. Problematika tohoto specifického předání byla původně upravena rozhodnutím Komise č. 2004/535/ES ze dne

14. května 2004, o odpovídající úrovni ochrany osobních údajů obsažených v záznamech o knihování cestujících v letecké dopravě, které se předávají Úřadu pro cla a kontrolu hranic Ministerstva vnitřní bezpečnosti USA. Zásadní obrat nastal v roce 2006, kdy Evropský soudní dvůr v Lucemburku zrušil svým rozsudkem ze dne 30. května 2006 výše uvedené rozhodnutí, na jehož základě letecké společnosti poskytovaly americkým orgánům v rámci boje proti terorismu osobní údaje všech cestujících (pasažérů). Vzniklé „právní vakuum" bylo třeba co nejrychleji odstranit. Dne 19. října 2006 proto byla uzavřena dohoda mezi Evropskou unií a Spojenými státy americkými o zpracovávání údajů jmenné evidence cestujících (PNR) leteckými dopravci a jejich předávání Ministerstvu vnitřní bezpečnosti Spojených států. Ta byla letos v červenci nahrazena dohodou novou (Dohoda PNR 2007).

Tuto novou dohodu však Úřad považuje z hlediska záruk pro úroveň ochrany osobních údajů za nedostatečnou. Poskytované záruky jsou totiž ještě nižší než ty, které byly obsaženy v předchozí dohodě z října 2006, ačkoliv ani ty plně neodpovídaly požadavkům a kritériím stanoveným směrnicí 95/46/ES Evropského parlamentu a Rady ze dne 24. října 1995, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, případně Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat (Rada Evropy, ETS 108/1981). Z pohledu Úřadu mohou být údaje podle této nové dohody zpracovány pro nedostatečně vymezené účely, mohou být zpřístupněny příliš širokému a nedostatečně vymezenému okruhu institucí a osob, mohou být uchovány po neadekvátně dlouhé období a ve výjimečných případech mohou být předány i citlivé údaje o jednotlivých cestujících (pasažérech).

Podobně jako v roce 2006 i v roce 2007 byly Úřadu předloženy k připomínkám celkem dvě závazná podniková pravidla (Binding Corporate Rules – BCR). BCR představují jednu z možností, jak vyhovět požadavku směrnice pro případy, kdy třetí země, do které mají být předávány osobní údaje, neposkytuje odpovídající úroveň ochrany. Možnost použití BCR jako jedné ze záruk dostatečných ochranných opatření poskytnutých správcem osobních údajů, který se zaručí za ochranu soukromí a základních práv, vyplývá z článku 26 odst. 2 směrnice. K BCR by se měl vyjádřit každý dozorový úřad, z jehož země jsou osobní údaje předávány, případně předložit vlastní připomínky, pokud se mu jeví některá ustanovení v rozporu s národním právem upravujícím ochranu osobních údajů.

Na rozdíl od například standardních smluvních doložek, které představují jednu z alternativ k BCR a které byly závazně upraveny rozhodnutím Komise, nebyly BCR prozatím upraveny obecně závazným dokumentem. Problematice BCR se však ve svých pracovních dokumentech věnovala a stále věnuje pracovní skupina zřízená na základě článku 29 Směrnice (dále jen „WP 29"). Hlavními a nejvýznamnějšími dokumenty pracovní skupiny WP 29 ve vztahu k BCR jsou pracovní dokumenty WP 74, WP 107, WP 108 a WP 133.

V obou případech bylo ze strany Úřadu konstatováno, že předložená závazná podniková pravidla společnosti Akzo Nobel NV a Accenture Ltd. představují vysoký a prověřený standard ochrany osobních údajů a jako takové je lze doporučit ke schválení. Shodně ovšem v obou případech Úřad uplatnil některé připomínky upozorňující na drobná úskalí, která by mohla při předávání osobních údajů do třetích zemí z České republiky vzniknout v souvislosti s platnými právními předpisy na území České republiky a jejich aplikací. Především bylo konstatováno, že schválení BCR udělené tímto vyjádřením nevylučuje povinnost poboček společností usazených v ČR požádat Úřad o povolení předávání osobních údajů do třetích zemí ve smyslu § 27 zákona, kdy bude opětovně (a tentokrát nikoli jen v obecné rovině) zkoumáno, zda BCR v modifikaci pro Českou republiku splňují podmínky uložené § 27 odst. 3 písm. b) zákona pro bezpečné předávání osobních údajů do třetích zemí.

V poslední době se Úřad stále častěji setkává s činností (zatím výhradně v neoficiální rovině, zejména v telefonických dotazech), pro kterou se vžil název „Whisteblowing“. Tento pojem označuje činnost, vyvíjenou ze strany amerických obchodních společností vůči jejich dceřiným společnostem, sídlícím v některém z členských států EU.

Důvodem této činnosti je existence zákona, známého pod názvem „Sarbanes-Oxley Act“ (dále jen „zákon SOX“), který platí na území Spojených států amerických. Ten upravuje oznamování podezření z porušení právních předpisů v oblasti účetnictví, vnitřních účetních kontrol a otázek auditu.

Nejčastěji byli zaměstnanci Úřadu pro ochranu osobních údajů prostřednictvím telefonu dotazováni na to, zda je taková činnost opravdu legální a zda ji mateřská společnost ve Spojených státech amerických může po zaměstnancích dceřiných společností v Evropě vůbec požadovat.

Důvodem pro přijetí zákona SOX bylo zajištění stability amerických finančních trhů a ochrana oprávněných zájmů investorů. Podle jeho znění musí americké veřejné společnosti (a také jejich dceřiné společnosti sídlící EU) zavést v rámci svého auditorského výboru postupy k přijímání stížnosti předložených emitentovi v souvislosti s účetnictvím, kontrolami nebo otázkami auditu, jakož i možnost důvěrného oznámení zaměstnanci emitenta o sporných otázkách účetnictví. Vnitřní postupy oznamování se zavádějí v zájmu uplatnění zásad řádné správy a řízení společností při jejich běžném fungování. Jestliže společnost neprokáže, že dodržuje předpisy, které upravují oznamování podezření z protiprávního jednání, hrozí jí přísné sankce a pokuty. Tento zákon obsahuje navíc ustanovení, podle něhož mají zaměstnanci těchto společností povinnost oznámit podezření z možného protiprávního jednání (podezření na finanční či účetní podvody) a případně také předložit získané důkazy.

Uplatňování některých ustanovení zákona SOX na evropské dceřiné společnosti (organizační složky) amerických společností (a na evropské společnosti kotované na amerických burzách cenných papírů) je v současné době předmětem soudního přezkumu ve Spojených státech amerických. Odvolací soud USA (1. obvod) totiž dne 5. ledna 2006 rozhodl, že ustanovení zákona SOX o ochraně osob, které podávají oznámení o podezření z protiprávního jednání, se nevztahují na cizí státní příslušníky, pracující mimo území USA v zahraničních organizačních složkách společností, jež se jinak řídí příslušnými ustanoveními zákona SOX.

Dalším častým dotazem, se kterým se v telefonických hovorech zaměstnanci Úřadu pro ochranu osobních údajů setkávali, bylo zjištění, zda se v takových případech bude skutečně jednat o předání osobních údajů do zahraničí či nikoliv. Na tuto otázku nebylo vždy snadné najít jednoznačnou odpověď, protože sami volající často přesně nevěděli, jak by takové oznámení pro podezření z možného protiprávního jednání mělo v praxi probíhat. Jestliže by tyto informace do Spojených států amerických předávala dceřiná společnost a šlo by o trvalou a systematickou činnost, o předání osobních údajů by se s největší pravděpodobností jednalo.

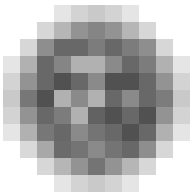
Takový postup předpokládá i stanovisko ze dne 1. února 2006, které vydala Pracovní skupina na ochranu údajů, vytvořená podle článku 29 směrnice 95/46/ES (dále jen „WP 29“). To obsahuje pokyny k provádění vnitřních postupů oznamování podezření z protiprávního jednání v souladu s právními předpisy EU o ochraně údajů.

WP 29, která představuje nezávislý evropský poradní orgán v oblasti ochrany údajů a soukromí, dospěla ve výše citovaném stanovisku k názoru, že postupy oznamování mohou představovat užitečný prostředek, s jehož pomocí může společnost nebo organizace monitorovat dodržování obecných právních předpisů i předpisů týkajících se správy a řízení společností, zejména pak účetnictví, vnitřních účetních kontrol a auditu, jakož i boje proti úplatkářství a trestné činnosti v bankovním a finančním sektoru i proti jiným porušením práva. Tyto postupy také mohou spo-

lečnostem napomoci při řádném provádění zásad správy a řízení společností a při odhalovaní skutečností, které by mohly mít vliv na postavení společnosti.

WP 29 však zdůraznila, že tyto postupy je třeba zavádět v souladu se zásadami ochrany osobních údajů zakotvenými ve směrnici 95/46/ES. Zastává názor, že dodržování těchto zásad přispívá k řádnému fungování uvedených postupů. Zajištění základního práva na ochranu osobních údajů, ať již jde o oznamovatele nebo osobu označenou za podezřelou, má v průběhu celého řízení o oznámení s využitím postupu oznamování zásadní význam.

Z některých telefonických dotazů však vyplynulo, že by oznámení o podezření z možného protiprávního jednání mohl podávat mateřské společnosti ve Spojených státech amerických jakýkoliv zaměstnanec, a to bez vědomí svého zaměstnavatele. Oznámení by pravděpodobně bylo uskutečňováno prostřednictvím elektronické pošty, popř. zvláštní telefonické linky. Takový postup by však s největší pravděpodobností byl v rozporu nejen se zákonem SOX, směrnicí č. 95/46/ES, ale i s výše uvedeným stanoviskem ze dne 1. února 2006.



Styky se zahraničím a zapojení Úřadu do mezinárodní spolupráce

Náplň a organizování styků se zahraničím, včetně zapojení do mezinárodní spolupráce, se legislativně opírá především o ustanovení zákona o ochraně osobních údajů v § 29 odst. 1 písm. g), podle kterého Úřad zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána, a z přímo použitelných předpisů Evropských společenství. Dalším výchozím ustanovením zákona je § 29 odst. 1 písm. i), kterým se Úřadu ukládá spolupracovat s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů; v souladu s právem Evropských společenství kromě toho musí plnit oznamovací povinnost vůči orgánům EU.

Výraznou prioritu pro rozvoj styků se zahraničím představuje Evropská unie, v jejímž rámci Úřad spolupracuje jak s mezinárodními orgány, především s Evropskou komisí, tak s partnerskými úřady na národní úrovni. V obecné rovině proto tvoří hlavní mezinárodní smluvní základnu, ze které vychází činnost Úřadu, smlouvy zakládající Evropská společenství a Evropskou unii, a tedy i veškeré sekundární právo zahrnující závazné právní akty v oblasti ochrany osobních údajů, které jsou součástí tzv. acquis communautaire. Zásadní význam mají dvě směrnice Evropského parlamentu a Rady, několik návazných rozhodnutí Evropské komise a úmluva převzatá od Rady Evropy pro III. pilíř EU.

Výchozí principy ochrany osobních údajů kodifikuje především směrnice 95/46/ES o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Zákon o ochraně osobních údajů se s ní zcela vyrovnal v roce vstupu ČR do EU novelizačním zákonem č. 439/2004 Sb., i když transpozice ustanovení této směrnice do národního práva byla rozhodujícím způsobem zajištěna již od původního vstupu zmíněného zákona v platnost v r. 2000, jak s uznáním konstatovaly všechny evaluační dokumenty orgánů Evropské komise v období před vstupem.

Důležitým právním aktem je také směrnice 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí a elektronických komunikacích). Ta byla částečně implementována zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, a to z hlediska některých ustanovení týkajících se nevyžádaných obchodních sdělení (tzv. NOS, nebo též tzv. marketingový spam). Transpozice pak byla dovršena zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, kterým se ovšem implementuje ještě celá řada dalších směrnic ve sféře telekomunikací a elektronických komunikací a sítí. Celkovou gesci k oběma zákonům mělo až do svého zrušení Ministerstvo informatiky ČR, s nímž Úřad spolupracoval při přípravě příslušných ustanovení zaměřených na ochranu osobních údajů. Totéž platí i o dílčí novele zákona č. 480/2004 Sb., reagující na kritické připomínky Evropské komise; návrh novely byl připravován na přelomu let 2005 a 2006 a uskutečněn zákonem č. 214/2006, s účinností k 1. 8. 2006 s výjimkou některých ustanovení s účinností od 1. 1. 2007.

Relevantní rozhodnutí Evropské komise se většinou týkají adekvátnosti ochrany osobních údajů v některých „třetích“ zemích; mimo hranice EU a země tvořící

s EU Evropský hospodářský prostor (Norsko, Island a Lichtenštejnsko) Evropská komise uznává jako přiměřenou legislativu ochrany osobních údajů ve Švýcarsku, Kanadě, Argentině a v legislativně autonomních regionech Guernsey a Ostrov Man. Na základě doporučení nezávislého poradního orgánu Evropské komise se obdobné rozhodnutí očekává v nejbližší době i pro Jersey a Faerské ostrovy.

Při výčtu základních právních aktů s mezinárodní účinností v oblasti ochrany osobních údajů je třeba připomenout rovněž Úmluvu o ochraně osob se zřetelem na automatizované zpracování osobních dat ETS 108 z roku 1981, která je sice produktem Rady Evropy, byla však Evropskou unií převzata pro sféru spravedlnosti a vnitra, tedy pro tzv. III. pilíř. ČR tuto úmluvu ratifikovala v roce 2001 s rozšířením v roce 2003 i na neautomatizované zpracování dat a se současnou ratifikací Dodatkového protokolu o orgánech dozoru a toku údajů přes hranice. Úmluva 108 tvoří podstatu legislativy uplatňované ve spolupráci ČR a Europolu a při přípravě na spolupráci v schengenském prostoru, jichž se Úřad velmi intenzivně účastní, jak bude ještě dále zmíněno. Pro mezinárodní spolupráci v EU ve III. pilíři již ovšem Úmluva 108 delší dobu neposkytuje dostatečnou právní základnu ochrany osobních údajů a jednotlivé aktivity se opírají o vlastní specifická ustanovení, včetně příslušných ustanovení pro spolupráci bilaterální povahy. Proto se již delší dobu volá po právním aktu, který by principy ochrany osobních údajů v celé sféře spravedlnosti a vnitra sjednotil a náležitě rozpracoval obdobným způsobem, jakým je tomu v I. pilíři uplatněním směrnice 95/46/ES, o ochraně fyzických osob v souvislosti s ochranou osobních údajů a s volným pohybem těchto údajů. Zdá se, že více než dva roky trvající diskuse v pracovních orgánech Rady EU/Coreperu k návrhu příslušného rámcového rozhodnutí vypracovanému Evropskou komisí se blíží k závěru. Přispělo k tomu německé předsednictví v první polovině roku 2007, ovšem za cenu značných ústupků z hlediska úrovně ochrany osobních údajů a zúžení aplikační oblasti připravovaného dokumentu. Současná a zřejmě již téměř definitivní verze (stav koncem listopadu 2007) „Návrhu rámcového rozhodnutí o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech“ byla podrobena kritice ochránců osobních údajů na mezinárodní úrovni a rovněž Úřad k ní při pracovních jednáních vyslovil své výhrady.

Nejvýznamnější pracovní platformou pro styk a spolupráci jak s Evropskou komisí, tak s partnerskými orgány dozoru v ostatních státech EU byla i v roce 2007 Pracovní skupina podle článku 29 směrnice 95/46/ES pro ochranu osobních údajů (tzv. WP 29). Jde o prestižní orgán Evropské komise s poradním a nezávislým statutem, jehož členy jsou přímo předsedové nezávislých orgánů dozoru z členských států EU, kteří se také většiny jeho zasedání osobně účastní. V roce 2007 se konalo celkem 5 zasedání WP 29. Mezi důležitými projednávanými dokumenty a náměty opět, stejně jako v předchozím roce, figuroval již zmíněný návrh rámcového rozhodnutí. Dlouhodobě na programu také přetrvávají témata spojená s předáváním osobních údajů do tzv. „třetích zemí“, zejména (avšak nikoliv výlučně) do USA.

Přední místo zaujímá pokračování „kauzy Swift“ spočívající v původně tajném předávání údajů o mezibankovních transakcích obsahujících i osobní údaje společností SWIFT nejprve pro zálohovací účely do jejího technického střediska v USA a návazně pak ve velkém množství úřadům v USA v souvislosti s bojem proti terorismu. K určitému pozitivnímu posunu došlo formálním vstupem společnosti Swift do systému „Bezpečného přístavu“ (Safe Harbour) kontrolovaného z hlediska dohodnutých principů ochrany osobních údajů Ministerstvem obchodu USA (FTC – Federal Trade Commission) a dále jednostranným prohlášením Ministerstva financí USA (US Treasury). K zásadnímu řešení by mohlo dojít pouze geografickou restrukturalizací činnosti a zařízení společnosti Swift, která je sice v horizontu několika let slíbena, zůstává zde však stále ještě velký otazník z hlediska rozsahu dat, která by měla být zpracovávána v budoucím technickém centru ve Švýcarsku.

V programu jednání WP 29 pokračuje i letitý námět předávání osobních údajů ze jmenné evidence cestujících v systémech leteckých dopravců (tzv. PNR data) úřadům v USA pro potřeby boje proti terorismu a závažné kriminalitě. Po zrušení původní dohody mezi EU a USA Evropským soudním dvorem – z formálních právních důvodů – a s účinností od 1. října 2006, byla uzavřena nová, prozatímní dohoda do poloviny roku 2007. Současná (tedy již třetí) dohoda s předpokládanou dlouhodobou platností se vyznačuje zjevným oslabením záruk pro ochranu osobních údajů a byla kritizována pracovní skupinou WP 29 i v Evropském parlamentu. Pro úplnost je třeba dodat, že dohodu o předávání PNR dat má EU také s Kanadou a chystá se jednání o obdobné dohodě s Austrálií. Mnohem závažnější je ovšem případ Jižní Koreje (s obdobnými signály i z jiných států), která od prosince 2007 začne od evropských dopravců PNR data vyžadovat, aniž se připravovalo uzavření nějaké mezinárodní dohody, a k předávání by tedy mělo docházet bez náležitého právního základu a bez byť jen minimálních garancí pro řádné zacházení s daty. Evropská komise k dovršení všeho oznámila, že přichází s návrhem závazného rámcového rozhodnutí Rady o využívání PNR dat pro prosazování práva v zemích EU. WP 29 v této souvislosti přijala k tomuto postupu ostře kritické stanovisko.

Mezi četnými dalšími tématy projednávanými na zasedáních WP 29 zmiňme sjednocení interpretace definice osobních údajů, přípravu materiálu o dětech a jejich soukromí, návrh alternativních standardních smluvních doložek pro předávání osobních údajů do „třetích zemí“, zlepšení implementace směrnice 95/46/ES aj.

Pracovní skupina WP 29 má i řadu pracovních podskupin, přičemž v některých z nich je Úřad zastoupen svými experty. Úřad se účastní činnosti pracovní podskupiny pro záležitosti internetu (Internet Task Force), pro víza a biometrii, pro technologie RFID, pro spravedlnost, svobodu a bezpečnost a pro řízení identity a e-government.

Příležitost pro těsný kontakt a společné řešení problémů Úřadu s příslušným pracovištěm ochrany dat (C-5 Unit) Generálního ředitelství pro spravedlnost, svobodu a bezpečnost (DG Justice, Freedom and Security) Evropské komise se kromě platformy WP 29 nabízí také prostřednictvím účasti na zasedáních Výboru pro ochranu osobních údajů podle článku 31 směrnice 95/46/ES (tzv. Výbor 31). S tímto výborem Evropská komise konzultuje všechna zásadní rozhodnutí a opatření v oblasti ochrany osobních údajů. Pokud přijímaná opatření nejsou v souladu se stanoviskem Výboru 31, musí o tom být informována Rada, která pak může přijmout odlišné rozhodnutí. V roce 2007 Výbor 31 svolán nebyl. Na rozdíl od skupiny WP 29 však jde o orgán spíše politický, kde převažuje zastoupení vládních orgánů jednotlivých zemí.

Zcela jednoznačně politickým orgánem je Pracovní skupina pro ochranu dat (G09) Rady EU. Její činnost byla po několikaleté přestávce obnovena počátkem roku 2006 zásluhou rakouského předsednictví. ČR je zastupována pracovníkem Stálého zastoupení ČR při EU v Bruselu a zástupce Úřadu se v pozici přizvaného experta aktivně účastnil dvou zasedání. Mezi hlavní věcné náměty jednání patřila informace Evropské komise o záměru podpořit rozvoj technologie RFID, založit pro tento účel pracovní skupinu a koncem roku zveřejnit doporučení EK. Zahájena byla rovněž dlouhodobá diskuse o lepší implementaci, případně novelizaci směrnice 95/46/ES.

Úřad ovšem spolupracuje s orgány Rady EU / Coreper také nepřímo, začleněním do mezirezortní spolupráce v ČR. Velmi pozitivně je třeba hodnotit zejména součinnost s Ministerstvem informatiky ČR před jeho zrušením k 1. 6. 2007, a to v široké problematice rozvoje informační společnosti („e-Europe“, „e-government“ aj.), otázek bezpečnosti dat a elektronických komunikací, regulace či deregulace služeb spojených s veřejnými komunikačními sítěmi apod. Způsob spolupráce s ministerstvy průmyslu a obchodu a vnitra, která tuto problematiku převzala, se teprve hle-

dá. V otázkách bezpečnosti s dopadem do ochrany dat a soukromí se Ministerstvo vnitra ČR při sestavování instrukcí pro jednání v orgánech Rady EU / Coreper občas obrací na Úřad se žádostí o stanovisko. Lze si však představit systémovější spolupráci; uplatnění hledisek Úřadu bývá totiž složitější vzhledem k rozdílným názorům obou institucí v celé řadě aspektů při hledání vyváženého přístupu k posilování bezpečnosti se současným respektováním práv jednotlivců, včetně práva na soukromí a na adekvátní ochranu osobních údajů. Velmi pozitivně naproti tomu Úřad hodnotí spolupráci s MV ČR při přípravě na přistoupení k Úmluvě o Schengenu a určitý příslib do budoucna představuje také zahájení spolupráce v přípravě na předsednictví ČR v oblasti justice a vnitřních věcí. Otázkám přípravy na schengenskou spolupráci je věnována zvláštní kapitola.

Ohledně přípravy na předsednictví ČR v první polovině roku 2009 Úřad hodlá prosadit hledisko ochrany osobních údajů při stanovení priorit. Jak již bylo naznačeno, příslibem je přizvání Úřadu k účasti na „Mezirezortní expertní skupině pro rozpracování priorit CZ PRES v oblasti justice a vnitřních věcí". Zde se podařilo do prvních materiálů sektorové agendy začlenit alespoň zmínku o významu ochrany osobních údajů v souvislosti s prioritou rozvoje prostoru svobody, bezpečí a práva s jejím mottem „Evropa bez bariér". Rovněž v úsilí ČR při dokončování implementace Haagského programu se u jednotlivých iniciativ deklaruje potřeba prosazovat adekvátní dimenzi ochrany základních lidských práv a svobod, včetně ochrany osobních údajů. Při definování oné „adekvátnosti" je ovšem třeba na základě dosavadních zkušeností očekávat tvrdou diskusi.

Naproti tomu při formulování celkových priorit ČR pro předsednictví v obecné rovině přesahující sektorové agendy zatím Úřad neuspěl ve své snaze dosáhnout toho, aby problematika ochrany dat a soukromí byla pojímána jako průřezové téma, které v menší či větší míře se týká většiny úkolů a administrativních nebo právních počinů. Tuto nezbytnost umocňuje současné prostředí masivního uplatňování nových informačních technologií, moderních komunikačních prostředků a bezpečnostních opatření prostupující každodenní život občanů, s rostoucím tlakem právě na soukromí a ochranu osobních údajů. Tento pohled se do základních materiálů zatím nepodařilo promítnout. Předseda Úřadu se proto osobním dopisem obrátil na místopředsedu vlády pro evropské záležitosti. Vzhledem ke vstřícné odezvě očekáváme první výsledky v roce 2008, při etapě rozpracovávání priorit.

V rámci III. pilíře EU je mimořádně aktivní spolupráce se Společným kontrolním orgánem pro EUROPOL (Joint Supervisory Body of Europol – „JSB Europol"). Zástupkyně Úřadu, inspektorka PhDr. Miroslava Matoušová, jako místopředsedkyně tohoto orgánu byla opět koordinátorkou kontrolního týmu, který provedl v březnu 2007 pravidelnou kontrolu zpracování osobních údajů Europolem v sídle tohoto orgánu. Současně se inspektorka Matoušová ve stejné pozici podílela na kontrole centrální části Celního informačního systému – III. pilíř v sídle OLAF. Zprávy z obou kontrol schválily příslušné společné dozorové orgány: JSA Customs a JSB Europol.

Během roku se konaly čtyři schůze JSB Europol a tři zasedání Odvolacího výboru Europolu, který projednává a řeší stížnosti subjektů údajů. Klíčové činnosti a úkoly, které JSB Europol projednával, byly mj. analýza a stanovisko k úmluvám mezi Europolem a třetími zeměmi (Austrálie, Kanada, USA), zhodnocení stanovisek k návrhu nové právní úpravy a nové projekty.

Výrazem uznání úrovně kontrolní činnosti Úřadu v Policii ČR a dalších orgánech činných v trestním řízení je skutečnost, že inspektorka Úřadu byla přizvána do kontrolního týmu inspekce Společného dozorového orgánu EUROJUSTu, která proběhla v listopadu 2007 v sídle EUROJUSTu. Další položkou ve výčtu významných pozic Úřadu v oblasti III. pilíře je účast na práci Pracovní skupiny pro policii a justici, zřízené Konferencí evropských orgánů ochrany osobních údajů, a pořádající každoročně svá jarní zasedání.

Specifickým příkladem rozvoje bilaterálních styků v rámci EU je spolupráce s partnerským polským úřadem v programu Leonardo da Vinci. V rámci programu získal polský Úřad generálního inspektora pro ochranu osobních údajů tzv. projekt mobility, což jsou obecně projekty poskytující účastníkům možnost získat odborné pracovní zkušenosti v zahraničí. Jednou z forem jsou krátkodobé studijní návštěvy. Projekt, jehož partnerem se Úřad stal, nese název „Nové schopnosti pracovníků pověřených prosazováním ochrany dat". Vybraným odborníkům z partnerského úřadu v Polsku umožní rozšířit si znalosti a získat nové zkušenosti během studijních návštěv (stáží) u partnerských institucí v Evropské unii. Kromě českého Úřadu se partnery staly obdobné úřady ve Francii, Irsku, Německu a Velké Británii.

Podle uzavřené dohody mají přijet polští kolegové do Prahy na týdenní stáž ve třech termínech (listopad 2007, leden 2008, březen 2008). První stáž se uskutečnila ve dnech 22. – 29. listopadu 2007, kdy navštívila Úřad tisková mluvčí z varšavského Úřadu generálního inspektora pro ochranu osobních údajů. Během svého pobytu se podrobně seznámila s prací našeho tiskového oddělení a s celkovou strukturou činností Úřadu. Její návštěva byla i vítanou příležitostí k diskusím o možné budoucí spolupráci na poli propagace ochrany dat mezi občany.

Dne 31. března 2007 byl úspěšně zakončen projekt EU „Podpora Komisi ochrany dat Bosny a Hercegoviny" v programu CARDS zaměřeném na stabilizaci situace v zemích západního Balkánu. Projektové aktivity byly zahájeny již 1. 2. 2006, a činnost v roce 2007 se proto soustředila pouze na dokončení již rozpracovaných úkolů především v oblasti legislativní a na závěrečnou propagační kampaň. Celý projekt pak byl dovršen tiskovou konferencí pořádanou v budově vlády a parlamentu Bosny a Hercegoviny, s poměrně hojnou účastí zástupců místních sdělovacích prostředků. Projekt se ve státě příjemce zjevně setkal s pozitivním ohlasem a byla rovněž vyslovena neoficiální žádost o pokračování v navázané spolupráci. To však bude záviset spíše na řešení velmi závažných nahromaděných problémů politického charakteru, s nimiž se v současné době Bosna a Hercegovina potýká. Dále projekt prokázal, že český Úřad náleží ke špičkovým evropským institucím v oblasti ochrany osobních údajů a že je schopen své zkušenosti dále šířit. Z hlediska dalšího možného zapojení do podpůrných programů Evropské unie však bude z obecného pohledu třeba s naléhavostí řešit ekonomickou stránku účasti našich institucí jakožto poskytovatelů pomoci, což je nyní velmi důležitý úkol pro Ministerstvo financí.

Úřad obdržel „Evropskou cenu za nejlepší projekt služby veřejnosti v oblasti ochrany osobních údajů", kterou udílí dozorová autorita pro ochranu osobních údajů v Madridu. Vítězný projekt byl vybrán mezinárodní porotou z 15 nominací a oceněn dne 11.12. 2007 na slavnostním shromáždění v Madridu. Úřad byl na cenu nominován společností Iuridicum Remedium za projekt soutěže pro děti a mládež „Moje soukromí! Nedívat se, nešťourat!" a za projekt „Ochrana osobních údajů ve vzdělávání", který je akreditován Ministerstvem školství, mládeže a tělovýchovy na dobu tří let v rámci dalšího vzdělávání pedagogických pracovníků. Společnost Iuridicum Remedium byla kolektivním členem poroty, která vyhodnocovala soutěžní práce dětí a mladých lidí. O této záležitosti informujeme také v kapitole „Úřad, sdělovací prostředky a komunikační nástroje".

S plněním požadavků mezinárodních smluv souvisí i pokračující účast Úřadu na aktivitách vyplývajících ze závazků České republiky jakožto členské země Rady Evropy a OECD. V Radě Evropy byl Úřad po řadu let v projektové skupině pro ochranu dat (CJ-PD) a koordinačním výboru (CJ-PD/CG). Aktivní účast pokračovala i ve Výboru pro ochranu dat, zřízeném podle Úmluvy č. 108 (T-PD), který je nejvyšším orgánem Rady Evropy zabývajícím se ochranou dat. Úřad je zastoupen v řídícím by-

ru Výboru PhDr. Hanou Štěpánkovou, tiskovou mluvčí úřadu. V průběhu roku 2007 byro připravovalo expertní vyjádření ke kompatibilitě s Úmluvou 108 (např. v souvislosti s problematičnosti Swift, s otázkami spojenými s předáváním osobních údajů leteckých pasažérů či s předáváním osobních údajů vrcholových sportovců do databáze ADAMS, vedené v Kanadě, otevřena byla otázka právního zakotvení spojeného s profilováním aj.). Z pověření uvedeného orgánu přednášela H. Štěpánková o evropských principech ochrany osobních údajů v Tiraně (Albánie připravuje zákon o ochraně osobních údajů) a v Ženevě na konferenci skupiny Asie-Evropa, ustavené UNHCR k problematice migrantů a uprchlíků v daném regionu. Rada Evropy vyhlásila v loňském roce 28. leden – den, kdy byla roku 1981 otevřena k podpisu Úmluva 108 – Dnem ochrany osobních údajů. V roce 2008 u příležitosti Dne ochrany osobních údajů se bude konat v Paláci Evropy , sídle RE, výstava prací českých dětí, které byly zaslány do soutěže „Moje soukromí! Nedívat se, nešťourat!“, vyhlášené roku 2007 českým Úřadem, a bude zde promítána rovněž vzdělávací série Neznalost neomlouvá aneb Každý máme tajemství, natočená za spolupráce Úřadu pro Českou televizi.

Na půdě OECD pokračuje součinnost s Pracovní skupinou pro bezpečnost informací a soukromí (WPISP při výboru ICCP). Zvláštní význam platformy OECD a jí organizovaných akcí spočívá v získávání cenných informací o mimoevropských přístupech k ochraně dat a možnostech uplatnění seberegulačních nástrojů v dané oblasti, jako jsou etické kodexy, alternativní řešení sporů, technologie podporující ochranu soukromí apod. Významný přínos OECD se očekává ve velmi citlivé a aktuální otázce hledání vyváženého přístupu k legitimním snahám o posílení bezpečnosti v souvislosti s růstem terorismu na jedné straně a k ochraně demokratických hodnot jako je právo na soukromí na straně druhé, podle principů tzv. „kultury bezpečnosti“. Mezi aktuální témata z hlediska ochrany soukromí patřila spolupráce při vymáhání práva, otázky řízení digitální identity a také technologie RFID. Hledisko informační bezpečnosti se zaměřilo na škodlivé technologie používané pro útoky v komunikačních sítích (tzv. malware).

Kromě výše uvedených aktivit v rámci pravidelné spolupráce ve zmíněných mezinárodních pracovních orgánech, platformách a projektech se odborníci Úřadu účastnili řady jednorázových i opakovaných akcí typu konferencí, seminářů a setkání nejrůznějšího druhu. Šlo například o následující významné akce:

Pracovní setkání „Ochrana osobních údajů a dopravní prostředky“

(Belgie, Brusel, 13. 2. 2007)

Tématem byla telematika v dopravních prostředcích a její možné dopady na soukromí uživatelů.

„Londýnská iniciativa“ – 1. pracovní setkání na téma komunikace

(Francie, Paříž, 18. – 19. 2. 2007)

Pracovní setkání, které bylo organizováno francouzským úřadem pro ochranu osobních údajů (CNIL) ve spolupráci s evropským insektorem ochrany údajů (EDPS). Cílem bylo konzultovat komunikační strategie, uplatňované jednotlivými orgány dozoru v oblasti ochrany dat; zvláštní pozornost byla věnována informačním kampaním zaměřeným na děti a mládež.

„Evaluační mise pro Schengen"

(Estonsko, Talin, Slovensko, Bratislava, Kypr, Nicosie, 18. 3. – 23. 3. 2007)

Ing. Jan Zapletal, inspektor Úřadu, byl přizván do expertního týmu pověřeného hodnocením příprav uvedených zemí na vstup do schengenského prostoru, a to ve státech, které neuspěly v předchozím hodnocení.

15. a 16. pracovní setkání k řešení případů („Case Handling Workshop")

(Finsko, Helsinky, 23. – 24. 4. 2007 a Portugalsko, Lisabon, 19. – 20. 11 2007)

Jedná se o pravidelná pracovní setkání expertů úřadů pro ochranu osobních údajů zaměřená na sdílení praktických poznatků z výkonu dozorové činnosti, s důrazem na rozbor konkrétních případů. Hlavními tématy workshopů byla ochrana osobních údajů v souvislosti s internetem, ochrana autorských práv, přímý marketing, problematika sledování osob prostřednictvím kamerových systémů, zpracování osobních údajů ve finančním sektoru, zpracování citlivých údajů v elektronických zdravotnických záznamech a tématika přístupu k dokumentům veřejné správy.

Jarní konference komisařů na ochranu údajů

(Kypr, Larnaka, 10. – 11. 5. 2007)

Úřad je akreditovaným členem Konference evropských orgánů ochrany osobních údajů, která každoročně pořádá svá jarní setkání. Konference v Larnace se zaměřila na elektronickou zdravotnickou dokumentaci a na ochranu osobních údajů ve 3. pilíři a v institucích EU. Byly přijaty tři závěrečné dokumenty – k problematice principu dostupnosti (availability) při prosazování práva, k návrhu rámcového rozhodnutí o ochraně osobních údajů ve III. pilíři a k budoucnosti Policejní pracovní skupiny (s jejím přejmenováním na Pracovní skupinu pro policii a justici).

Kontrola v konzulárním oddělení Velvyslanectví ČR v Kyjevě a na Generálním konzulátu ČR v Petrohradu

(Ukrajina, Kyjev, 15. – 16. 5. 2007 a Rusko, Petrohrad, 18. – 19. 7. 2007)

Na základě doporučení expertní komise pro schengenské hodnocení nových členských států na úseku ochrany osobních údajů byly provedeny kontroly zaměřené na vízové řízení v zastupitelských úřadech.

9. zasedání úřadů pro ochranu údajů střední a východní Evropy

(Chorvatsko, Zadar, 4. – 6. 6. 2007)

Každoroční zasedání konferenčního typu byla založena z iniciativy polského a českého úřadu pro ochranu osobních údajů. Konference v Zadaru se zúčastnili jak zástupci úřadů z členských států EU ze střední a východní Evropy (baltské státy, Bulharsko, Česká republika, Maďarsko, Polsko, Rumunsko, Slovensko a Slovinsko), tak i země o členství usilující – Chorvatsko, Makedonie, Bosna a Hercegovina.
Mezi hlavní témata patřil např. vztah a možný konflikt práva na ochranu osobních údajů s právem na informace, zkušenosti s přípravou na vstup do schengenského prostoru, význam zkušeností s totalitními režimy ve státech střední a východní Evropy pro ochranu soukromí v současnosti aj.

Návštěva polského Úřadu generálního inspektora ochrany osobních údajů

(Polsko, Varšava, 10. – 11. 7. 2007)

Cílem jednání bylo prodiskutovat a sjednotit přístupy k některým problémům v oblasti ochrany osobních údajů, a to jak legislativního charakteru (zpracování osobních údajů ve zdravotnictví, zpřístupnění materiálů tajných služeb komunistického režimu) tak i organizačního charakteru (problematika uplatňování pravomocí dozorových úřadu, možnost jejich inherence do legislativních záležitostí, postoje k některým problémům v rámci EU, organizace dalších akcí).

Mezinárodní sympozium „Soukromí v digitální televizi“

(Německo, Berlín, 3. 9. 2007)

Sympozium, které bylo součástí mezinárodního veletrhu audiovizuální techniky IFA, se věnovalo novému, rychle se rozšiřujícímu fenoménu digitální televize, který při ochraně soukromí přináší některé problémy.

Setkání k informační kampani Schengenského informačního systému II

(Belgie, Brusel, 20. – 21. 9. 2007)

První jednání zástupců dozorových orgánů působících v oblasti ochrany osobních údajů členských států Schengenského prostoru a kandidátských zemí zaměřené na otázky přípravy informační kampaně, která má provázet zprovoznění Schengenského informačního systému druhé generace.

29. mezinárodní konference komisařů pro ochranu dat a soukromí

(Kanada, Montreal, 24. – 28. 9. 2007)

Nejprestižnější mezinárodní konference předsedů a dalších zástupců vedení úřadů pro ochranu osobních údajů hostil kanadský partnerský úřad. Veřejné části zasedání se zúčastnila široká škála vládních, soudních, občansko-společenských i soukromých organizací. Program byl zaměřen na nejnovější vývoj v oblasti ochrany soukromí v souvislosti s globalizací a novými sledovacími technologiemi. Závěry byly shrnuty v „Usnesení o mezinárodní spolupráci“, v „Usnesení o rozvoji mezinárodních standardů“ a v „Usnesení o naléhavé potřebě celosvětových standardů pro ochranu dat cestujících“, které by vlády uplatňovaly pro účely vymáhání práva a zabezpečení hranic.

Seminář „Státní majetek – správa, pořizování a obnova“

(Německo, Berlín, 11. – 13. 10. 2007)

Akce navazovala na cyklus přednášek zaměřených na vzdělávání a výměnu zkušeností veřejné správy a profesních organizací při pořizování, správě a obnově veřejného majetku.

Mezinárodní konference „Právo na soukromí ve sledované společnosti“

(Polsko, Varšava, 22. – 23. 10. 2007)

Vystoupení se zabývala trendy založenými na vývoji nových sledovacích technologií a informačních systémů, směřujícími k všestrannému sledování osob. Zdůrazněn byl význam rostoucí naléhavosti ochrany osobních údajů ve společnosti.

Seminář „Dopad boje proti terorismu na legislativu EU“

(Irsko, Dublin, 2. 11. 2007)

Předmětem semináře nebyl jen dopad opatření v boji proti terorismu na společnou legislativu EU, ale i na problémy transpozice právních úprav této legislativy do národního práva.

Konference „Trendy ochrany dat v informační společnosti“

(Litva, Vilnius, 13. – 14. 11. 2007)

Zástupci evropských struktur se na konferenci zabývali zvyšujícím se nebezpečím omezování soukromí vlivem nových technologií. Zdůrazněn byl význam dohledu nad implementací směrnice 2006/24/ES (uchovávání dat poskytovateli telekomunikačních služeb, tzv. „dataretention“) z hlediska omezení účelu jen na terorismus a nejzávažnější trestnou činnost. Setkání uspořádal litevský úřad pro ochranu osobních údajů k desátému výročí svého vzniku.

4. ročník udílení cen za nejlepší postupy v oblasti ochrany osobních údajů v rámci evropských veřejných služeb

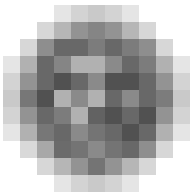
(Španělsko, Madrid, 11. – 12. 12. 2007)

Proběhlo vyhodnocení 4. ročníku soutěže „Nejlepší postupy evropských úřadů pro ochranu dat". Cenu získal Úřad pro ochranu osobních údajů (viz výše).

„Londýnská iniciativa" – Pracovní setkání na téma efektivních strategií komisařů ochrany dat

(Velká Británie, Londýn, 12. – 13. 12. 2007)

Výměna zkušeností a poznatků a hledání efektivní strategie činnosti komisařů pro ochranu dat (předsedů úřadů pro ochranu osobních údajů).



Úřad, sdělovací prostředky a komunikační nástroje

Jako mimořádnou událost v životě Úřadu je třeba uvést udělení Evropské ceny za nejlepší službu veřejnosti v rámci ochrany osobních údajů. Tuto cenu udělila českému Úřadu Agentura pro ochranu osobních údajů města Madridu za projekt zvyšování znalosti ochrany osobních údajů – konkrétně za soutěž pro děti a mládež „Moje soukromí! Nedívat se, nešťourat!“, kterou Úřad vyhlásil u příležitosti Dne ochrany osobních údajů 2007, a za projekt Ochrana osobních údajů ve vzdělávání, na nějž Úřad získal na 3 roky akreditaci MŠMT ČR v rámci DVPP (další vzdělávání pedagogických pracovníků). Cenu Úřad získal v mezinárodní konkurenci 15 projektů a převzal ji 11. prosince 2007 v Madridu.

Mimořádného uznání se výsledkům soutěže dostalo i na půdě Rady Evropy ve Štrasburku, kde práce dětí z uvedené soutěže budou vystavené od 28. 1., Dne ochrany osobních údajů 2008.

Ilustrativně stávající výroční zprávu provázejí v tištěné podobě reprodukce prací dětí z uvedené soutěže.

VYHLÁŠENÍ SOUTĚŽE

Úkolem soutěžících bylo literární či výtvarnou formou zpracovat téma ochrany soukromí. Jako inspiraci mohli soutěžící použít již existující umělecká díla, z nichž jako příklad v samotném formuláři přihlášky byl uveden text ze známé knihy George Orwella „1984“. Přišlo jich z celé republiky na 200. Poté se jejich hodnocení ujala odborná porota, složená ze zástupců Úřadu, Ministerstva školství, mládeže a tělovýchovy České republiky, Českého rozhlasu, stanice Praha, Vysoké školy uměleckoprůmyslové a občanského sdružení Iuridicum Remedium. Vítězové byli vyhlášeni na Mezinárodním filmovém festivalu pro děti a mládež ve Zlíně, kam byli spolu s jedním z rodičů Úřadem pozváni a kde jako hosté filmového festivalu strávili dva dny. Vítězové byli také pozváni předsedou Úřadu s celou svou třídou do Prahy, kde navštívili nejen Úřad pro ochranu osobních údajů, ale také studio Českého rozhlasu a na závěr je čekala noční návštěva ZOO. Partnery soutěže byli Ministerstvo školství, mládeže a tělovýchovy, Mezinárodní festival filmů pro děti a mládež Zlín, Český rozhlas Praha.

úřad pro ochranu osobních údajů
the office for personal data procession

Úřad pro ochranu osobních údajů vyhlašuje
soutěž

„Moje soukromí.

Nedívat se, nešťourat!“

ve věkových kategoriích 12-15 let a 16-20 let

U příležitosti „Dne ochrany osobních údajů“ 28. ledna 2007 se na vás obracíme s několika otázkami:

Co chápete pod pojmem soukromí? Je pro vás důležité – proč ano, proč ne? Měli bychom si soukromí vážit? V čem se o ně obáváte? Jaké máte zkušenosti s jeho respektováním? Jaké vidíte problémy s jeho dodržováním ve vztahu k vám i k druhým? Co by se podle vás mělo zlepšit v jeho zabezpečení?

Mezi nejslavnější knihy, kde můžete nalézt jako ústřední téma soukromí, patří slavná kniha George Orwella „1984“. I jinde v literatuře ale můžete objevit text, který o tématu soukromí hovoří. Čtenáři si to často ani neuvědomí. Pokud takový text najdete, můžete ho zpracovat literárně nebo výtvarně a poslat do soutěže. Můžete ale samozřejmě zaslat i své ryze vlastní texty či obrázky.
Příspěvky nám pošlete do 20. dubna 2007 na níže uvedenou adresu poštou nebo elektronicky. Na poštovní obálce nebo v případě elektronického odeslání v předmětu e-mailové zprávy uveďte označení „Soutěž“ a připojte také souhlas rodičů s využitím Vašeho příspěvku pro potřeby Úřadu.
Nezapomeňte uvést u příspěvku svůj věk a adresu, abychom mohli oslovit ty z Vás, jejichž výtvory ocení porota! Zaslané příspěvky se nevrací!
Vítěze pozveme na dva dny na Mezinárodní festival filmů pro děti a mládež do Zlína (děti v kategorii 12-15 let v doprovodu rodičů), kde jim budou ocenění slavnostně předána a jejich výtvory vystaveny. Cenou bude kromě uměleckého předmětu také moderní pomůcka pro komunikaci.
Vítěze spolu s jejich spolužáky a třídními učiteli pozveme na výlet do Prahy: Navštíví při té příležitosti studio Českého rozhlasu, aby uviděli při práci některého z „neviditelných herců“, poznají soukromí zvířat na noční návštěvě pražské ZOO a samozřejmě budou také hosty na Úřadě pro ochranu osobních údajů.
Bližší informace o soutěži najdete na webových stránkách Úřadu pro ochranu osobních údajů na adrese http://www.uoou.cz v sekci Pro mládež. Zde je také umístěno číslo Bulletinu Úřadu, které bylo celé věnováno právě vám, dětem. Takže čtěte, pište, malujte, na vaše výtvory se již moc těšíme !

Úřad pro ochranu osobních údajů
Pplk. Sochora 27
170 00 Praha 7
soutez@uoou.cz

partneři soutěže:

FILM FESTIVAL ZLÍN

PRAHA ČESKÝ ROZHLAS 2

Alík

hey!

un novinky učitelské

OCHRANA OSOBNÍCH ÚDAJŮ VE VZDĚLÁVÁNÍ
VZDĚLÁVACÍ PROGRAM V RÁMCI DVPP

1. Realizace programu:

Uvedený vzdělávací program byl akreditován Ministerstvem školství, mládeže a tělovýchovy ČR v prosinci 2006. Jeho první seminář se uskutečnil ve Zlíně v rámci MFF v prostorách, kde se konala výstava „Moje soukromí! Nedívat se, nešťourat!" Druhý seminář Úřad uspořádal v Praze pro Českou školní inspekci v prosinci 2007.

Účastníci seminářů na základě vyplněných testů získávají certifikát. V roce 2008 semináře budou pokračovat v dalších oblastech České republiky.

2. Obsah – podrobný přehled témat výuky:

1 vyučovací hodina bude věnována právu na ochranu osobních údajů v kontextu lidských práv a českého právního řádu

Mezi základní práva garantovaná jak Ústavou, tak Listinou základních práv a svobod náleží právo na ochranu soukromého a rodinného života. V tomto kontextu bude vysvětleno, proč je třeba chránit osobní údaje a jak je to zabezpečeno, jaký je vztah zákona o ochraně osobních údajů k evropským právním normám (tj. jak a proč je český právní řád harmonizován s právem evropským). Především jde o vysvětlení faktu, že osobní údaje jsou klíčem k našemu soukromí, které je jednou ze základních hodnot našeho civilizačního okruhu.

Vysvětleny budou principy ochrany osobních údajů mj. tzv. balanční princip zajišťující vyvážený postoj k ochraně osobních údajů a bezpečnosti (otázka závažná zejména v kontextu aktuálního problému terorismu) i vztah obecného zákona o ochraně osobních údajů ke zvláštním zákonům, v nichž je rovněž ochrana osobních údajů zakotvena. V zájmu dobrého fungování demokratického státu je třeba podporovat kultivaci právního povědomí a pro občany je čím dál důležitější umět se svého práva domáhat a znát základní právní ustanovení, na jejichž základě tak lze činit.

1 vyučovací hodina bude věnována problematice ochrany osobních údajů speciálně ve školství

Zkušenosti Úřadu s problémy ochrany osobních údajů vycházejí z mnoha oblastí, v nichž dochází ke zpracování osobních údajů. Děje se tak i ve školství. Jaké principy by zde měly být z hlediska zákona o ochraně osobních údajů i z hlediska práva na ochranu soukromí respektovány - takové bude východisko výkladu. Praktické zkušenosti nabídnou pedagogům také možnost klást dotazy na řešení situací, s nimiž se musí ve svém pedagogickém působení vyrovnávat.

2 vyučovací hodiny budou věnovány možnostem aplikace ochrany osobních údajů a soukromí v rámci konkrétních vyučovacích předmětů

(blíže srv. bod 6.).

3. Forma:

Přednáška, na kterou naváže diskuse s přednášejícími o konkrétních situacích či problémech.

4. Vzdělávací cíl:

V souvislosti se schválením zákona o ochraně osobních údajů č. 101/2000 Sb. a zřízením Úřadu pro ochranu osobních údajů (dále jen Úřad) v roce 2000 se v médiích začala ve stále větší míře objevovat problematika ochrany osobních údajů jako nesmírně důležitá součást práv každého jednotlivce. Přestože obecné povědomí o této problematice dosáhlo v ČR i díky činnosti Úřadu poměrně vysoké úrovně, stále je možné identifikovat sociální skupiny, kterým nebyla v minulosti věnována téměř žádná či jen velmi malá pozornost. Mezi ně nepochybně patří i děti a mládež. Dnešní žáci základních škol a studenti středních škol však budou v průběhu příš-

tích let postupně vstupovat do řad dospělých a ponesou tomu odpovídající politickou i ekonomickou odpovědnost. Proto je třeba začít již v této době pracovat na zlepšení jejich znalostí o ochraně osobních údajů, aby v okamžiku, kdy budou ovlivňovat osudy celé společnosti, nezůstala tato otázka mimo zřetel jejich zájmu.
Jedním z nejdůležitějších informačních kanálů, jehož prostřednictvím je možné žáky a studenty základních či středních škol seznámit s problematikou ochrany osobních údajů, je prostředí školy. Informace, které budou žáci, resp. studenti získávat v rámci předmětů základy společenských věd, dějepis, informační a výpočetní technika, však musí být obsahově správné a zároveň provázané s konkrétními příklady možných situací, ve kterých se objevuje otázka ochrany soukromí a osobních údajů. Proto přistoupil Úřad pro ochranu osobních údajů k vytvoření vzdělávacího programu v rámci DVPP, jehož cílem je připravit pedagogy základních a středních škol na témata z oblasti ochrany osobních údajů a umožnit jejich zapojení do vzdělávacích programů jednotlivých škol.

5. Hodinová dotace:

přednáška v délce 4 vyučovacích hodin

6. Počet účastníků a upřesnění cílové skupiny pedagogů:

V průběhu školního roku budou uskutečněny 4 semináře, max. kapacita každého semináře činí 40 osob.
Primární cílovou skupinu pedagogů tvoří vyučující následujících předmětů:

předmět	**specifický vzdělávací cíl ve vazbě na konkrétní předmět**
český jazyk a literatura	schopnost na základě literárního textu, eventuálně uměleckého díla vnímat pojetí soukromí a ochrany osobních údajů v rozdílných časových obdobích
základy společenských věd	ochrana osobních údajů, potažmo soukromí v kontextu lidských práv, výkladu práva a psychologie
dějepis	vývoj názoru na lidské soukromí, jeho hodnotu a vznik ochrany osobních údajů v různých časových etapách vývoje evropské civilizace, vliv totalitních režimů na vnímání problematiky ochrany soukromí
matematika, informační a výpočetní technika	ochrana osobních údajů, jejich zabezpečení při automatizovaném zpracování – bezpečnost při pohybu na Internetu, zásady správy výpočetní techniky s ohledem na ochranu údajů, nebezpečí krádeže identity, moderní technologie při ochraně osobních údajů (odposlechy, RFID, databázové systémy), princip elektronického podpisu
biologie	možnosti odběru DNA, její následné zpracování pro verifikační či identifikační účely, rozdílný přístup k databázím DNA ve světě, vytváření databází otisků prstů a dalších osobních identifikátorů, citlivé údaje ve zdravotnictví; soukromí člověka – soukromí zvířat

7. Plánové místo konání:

Úřad pro ochranu osobníchú dajů
Pplk.Sochora 27
Praha 7
V případě většího zájmu ze strany pedagogů z krajů více vzdálených od Prahy je Úřad schopen zajistit přednášky i v rámci příslušného krajského města.

8. Odborný garant:

RNDr. Igor Němec
předseda Úřadu pro ochranu osobních údajů

9. Materiální a technické zabezpečení:

Úřad poskytne své přednáškové prostory včetně potřebné audiovizuální techniky. Jednotlivým účastníkům semináře budou poskytnuty informační materiály.

10. Způsob vyhodnocení akce:

Po skončení přednášky bude účastníkům dána možnost vyjádřit se k přednesené problematice a položit doplňující dotazy; frekventantům semináře bude předložen test a dotazník, jehož úspěšné doplnění bude podkladem pro udělení certifikátu o absolvování kurzu.

11. Kalkulace předpokládaných nákladů:

Předpokládaná cena na 1 účastníka představuje 300 Kč. V případě konání přednášky mimo sídlo Úřadu (viz. bod 7) bude účastnický poplatek kalkulován vždy s ohledem na konkrétní situaci. Uvedená částka vychází z následujících předpokladů:

a. V případě seminářů probíhajících na Úřadě pro ochranu osobních údajů bude propůjčena zasedací místnost a technika bezplatně. V případě pořádání semináře mimo sídlo Úřadu bude třeba uhradit pronájem přednáškové místnosti a potřebné techniky.

b. Kalkulovány jsou ceny za DVD, VHS a tištěné materiály, které budou poskytnuty účastníkům semináře.

Přihlášku je možné zaslat poštou (Pplk. Sochora 27, 170 00 Praha 7) nebo elektronicky na adresu Úřadu. Současně s potvrzením přihlášky Vám zašleme i potřebné informace pro platbu účastnického poplatku.

TISKOVÉ KONFERENCE

Obraz instituce, která je otevřená vůči veřejnosti a usiluje v rámci tohoto zavedeného obrazu poskytovat o své práci pravidelně informace, byl vytvářen i v roce 2007:

Pravidelné čtvrtletní konference předně bilancují práci Úřadu za uplynulé období a podávají informaci o kontrolní činnosti instituce, která je její prvořadou zákonnou povinností, podávají ale také přehled o kauzách, jež v souvislosti s ochranou osobních údajů byly otevřeny za přispění médií či konkrétních novinářů. Každá z tiskových konferencí však věnuje také pozornost jednomu aktuálnímu tématu ochrany osobních údajů. Jde tedy o prohlubování informovanosti veřejnosti o problematice ochrany osobních údajů na základě problémů, s nimiž se občané setkávají a které ovlivňují kvalitu jejich soukromého života: V roce 2007 je z těchto témat obzvlášť třeba jmenovat využívání kamerových systémů a šíření znalostí o ochraně osobních údajů v schengenském informačním systému (SIS) v kontextu procesu přístupu České republiky do schengenského prostoru.

Úřad plnil i v roce 2007 vůči médiím konzultační povinnost. Dotazy novinářů se často dotýkají podstatně složitějších problémů, než tomu bylo v počátcích jeho existence. S důvěrou se novináři obracejí na Úřad i s telefonickými dotazy v otázkách, s nimiž se na média obrací veřejnost, případně samozřejmě očekávají informaci o dalších zdrojích, které by jim pomohly najít řešení, jež od nich tazatelé očekávají.

Zavedené pravidelné tiskové konference znamenají také opakovaný nárůst počtu příspěvků v médiích, někdy ve skutečně významném rozsahu.

Tiskové zprávy a materiály poskytované na tiskových konferencích jsou trvale dostupné v příslušné rubrice na webových stránkách Úřadu.

PUBLIKAČNÍ ČINNOST – ŠÍŘENÍ NOVÝCH EVROPSKÝCH A SVĚTOVÝCH POZNATKŮ

V roce 2007 vydal Úřad čtyři částky Věstníku. Zůstává tak u stejného počtu vydaných částek jako v roce předcházejícím.

Stanoviska vydávaná Úřadem, přehledy zobecnění z jeho rozhodovací činnosti, překlady dokumentů týkající se ochrany osobních údajů s celoevropskou platností – stále častěji také přímo přebírané a přetiskované z Úředního věstníku EU – jsou následně publikovány také na webových stránkách Úřadu. Tuto komunikační provázanost považuje Úřad za výhodnou, protože se tak rozšiřuje počet příjemců, k nimž se příslušné informace dostávají.

Informační bulletin Úřadu je čtvrtletníkem, určeným širší veřejnosti, než je tomu u Věstníku. Klade si za cíl prohlubovat znalosti o ochraně osobních údajů a informovat o nejzávažnějších událostech dotýkajících se ochrany soukromí, které se odehrávají ve světě, a paralelně ukázat i zahraniční kontakty a pozici Úřadu.

V rámci kampaně koordinované MV ČR v souvislosti se vstupem České republiky do schengenského prostoru zpracoval Úřad text letáku týkající se ochrany osobních údajů v SIS (Schengenském informačním systému). V období před přistoupením ČR do Schengenu se na problematiku ochrany osobních údajů v SIS a další problémy spojené s danou tématikou Úřad soustředil na informování o ní jak na tiskových konferencích, tak ve svých periodicích – Věstníku (zde především publikoval právní dokumenty) i Informačním bulletinu (zde zejména zveřejnil řadu obecných informací o schengenském prostoru, historii jeho vzniku i pravidlech jeho fungování). Úřad touto informační cestou provázel novou dozorovou kompetenci, kterou získal v rámci vstupu státu do schengenského prostoru.

DALŠÍ KOMUNIKAČNÍ NÁSTROJE

Webové stránky Úřadu byly obohaceny v roce 2007 zejména rozšířením rubriky věnované mládeži – včetně zábavné herní složky.

Rozšíření stránek o zvláštní rubriku „Schengen“ přirozeně provázelo aktivity Úřadu spojené s jeho novou dozorovou povinností vůči Schengenskému informačnímu systému.

Už v roce 2006 realizoval Úřad rozsáhlý informační projekt pro občany: Ve spolupráci se společností BENY TV připravil 13 dílů seriálu „Neznalost neomlouvá aneb Každý máme tajemství“, který byl odvysílán ČT na konci roku 2006. Série byla Českou televizí reprizována v létě roku 2007. Je nesporné, že tímto vysílacím rozložením se dostaly informace o zákoně o ochraně osobních údajů k velmi širokému okruhu veřejnosti. Úřad získal rovněž anglickou verzi této série, kterou využívá k prezentaci svých aktivit také v zahraničí, a setkává se při tom s živým zájmem svých partnerů. Anglická verze série je zapůjčena sekretariátu T-PD Rady Evropy na výstavu prací českých dětí (viz výše), kde má být ve smyčce promítána v týdnu 28.1.– 1.2. 2008.

Soutěž pro děti a mládež „Moje soukromí! Nedívat se, nešťourat!“ byla vyhlášena na lednové tiskové konferenci a po dobu čtyř měsíců podporována ČRo2 Praha, Ministerstvem školství, mládeže a tělovýchovy, serverem Alík.cz, s Rádiem Hey a Mezinárodním festivalem filmů pro děti a mládež Zlín. V kontextu této soutěže byl využíván již dříve vydaný Informační bulletin č. 2/2006 určený dětem a jejich rodičům.

Práce dětí a mladých lidí zaslané do soutěže byly vystaveny na Mezinárodním festivalu filmů pro děti a mládež Zlín (dále MFF Zlín) a byli zde oceněni vítězové soutěže. Třídy vítězných dětí byly hosty na Úřadu pro ochranu osobních údajů, kde se s nimi setkal předseda úřadu a uskutečnila beseda, v jejímž rámci bylo zdůraz-

něno nejen právo na soukromí, k němuž jsou osobní údaje klíčem, ale také potřeba respektu k soukromí druhých, což symbolicky vyjadřovalo i pozvání přátel vítězů soutěže.

V průběhu MFF Zlín se uskutečnil také seminář dalšího vzdělávání pedagogických pracovníků. Seminář byl uspořádán rovněž v prosinci pro Českou školní inspekci.

Jako každoročně poskytovali právníci Úřadu přednášky v rámci svých smluvních závazků.

Specializovaný seminář poskytlo tiskové oddělení seniorům, kteří se v říjnu účastnili na semináři pořádaném 3. lékařskou fakultou UK. Je zřejmé, že generaci seniorů bude třeba věnovat pozornost i v příštím roce. V kontextu semináře na 3. LF UK vznikl projekt spolupráce Úřadu v průběhu aktivit pořádaných pro seniory v roce 2008.

Úřad v rámci svých kompetencí i omezení spolupracuje s občanským sdružením Iuridicum Remedium, které Úřad jmenovalo na Evropské ceny za nejlepší službu veřejnosti. Tradičně jsou pracovníci tiskového oddělení přítomni i na udílení anticen Big Brother, udělovaných občanským sdružením Iuridicum Remedium, a přispěli rovněž svou účastí na filmu Oči Velkého bratra o využívání kamerových systémů.

KNIHOVNA JAKO ODBORNÉ ZÁZEMÍ

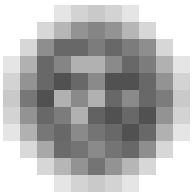
Odborná knihovna Úřadu poskytuje zázemí pro vlastní pracovníky, slouží ovšem trvale i studentům středních a vysokých škol a odborné veřejnosti. Doplňovaný fond knih i periodik se v roce 2007 rozšířil o 96 knih, z toho nákupem 51. Knihovna opakovaně slouží také studentům, kteří hledají specializované knihy či periodika o ochraně osobních údajů. V tomto ohledu knihovna nabízí unikátní knižní fond.

Úřad rovněž archivuje veškeré vstupy elektronických médií do oblasti ochrany osobních údajů – zejména však se soustřeďuje na archivaci vyjádření Úřadu ke kauzám, jimiž se média zabývají. I tímto prostřednictvím vysvětluje principy ochrany osobních údajů a šíří znalost zákona o ochraně osobních údajů.

KOMUNIKACE ÚŘADU S MÉDII V ČÍSLECH:

Období: leden – prosinec 2007

agenturní servis	22
tisk celkem	73
z toho:	
denní tisk	47
ostatní periodika	26
televize	66
rozhlas	29
servery	12
média celkem	**202**



Informatika

Odbor informatiky se v oblasti rozvoje informačního systému se v roce 2007 zaměřil na několik hlavních oblastí:

1. Bezpečnost informačního systému
2. Centrální úložiště dokumentů
3. Dokončení výměny personální výpočetní techniky
4. Změna databázové platformy

Jako součást upgradu celého informačního systému, který proběhl v minulých dvou letech, byla v roce 2007 modernizována bezpečnostní struktura připojení informačního systému k internetu. Tato struktura byla navíc z bezpečnostních důvodů doplněna o filtr webového provozu, který umožňuje tento provoz řídit.

Dlouhodobá snaha o řádné zabezpečení informačního systému dospěla v roce 2007 do stadia rutinní činnosti. Nastavená funkce interního bezpečnostního správce spolu s funkcí externího bezpečnostního správce (outsourcing) představuje základní autoritu, dohlížející na dodržování celkové bezpečnostní politiky a systémové bezpečnostní politiky, které byly Úřadem přijaty. Podle ročního plánu byly prováděny prověrky logů různých zařízení (servery, uživatelské stanice, bezpečnostní prvky), technická prověrka síťového prostředí a bezpečnostní školení uživatelů. Na základě rozboru těchto logů pak byla přijímána příslušná opatření.

Velká pozornost byla věnována také antivirové a antispamové ochraně informačního systému. Tato ochrana se skládá z vnější antivirové a antispamové ochrany a z vnitřní antivirové ochrany. Vnitřní linie obrany byla letos doplněna o modul ochrany proti tzv. "malwaru" (tedy škodícímu softwaru). Také logy antivirové ochrany pravidelně kontrolouje bezpečnostní správce a na základě jejich rozboru se opět provádějí příslušná opatření k nápravě.

V letošním roce byl rovněž vytvořen základní havarijní plán, a dále byli vedoucí zaměstnanci a jejich zástupci vybaveni elektronickým podpisem s kvalifikovaným certifikátem pro využití v agendě pořizování služeb a majetku.

V roce 2007 odstartoval projekt vytvoření centrálního úložiště dokumentů. Toto úložiště je postaveno na produktu MS SharePoint Server 2007 a obsahuje (nebo bude obsahovat) jednak dokumenty spisové služby, jednak společné dokumenty jednotlivých oddělení a odborů Úřadu. Současně je na SharePoint Serveru vytvořen intranetový portál Úřadu, který by měl představovat pro zaměstnance hlavní vstupní bod do informačního systému. V prostředí portálu je připraven i systém pro schvalování dokumentů.

Tento rok byla dokončena i výměna zastaralé personální výpočetní techniky a dále se rozšířila kapacita diskového pole. Tím byl dokončen cyklus obměny hardware celého informačního systému tak, aby po další zhruba 4 roky nepožadoval z hlediska hardwaru zásadní investice.

Dalším velkým projektem tohoto roku byl přechod z databázového prostředí Oracle na prostředí MS SQL. Během roku byly jednotlivé aplikace upravovány, testovány a připravovány na ostrý přechod. Přechod na nové databázové prostředí bude dokončen v prvním čtvrtletí roku 2008.

V roce 2007 rovněž proběhla veřejná zakázka na výběr systémové integrátora informačního systému Úřadu. Vítězem tohoto řízení se stala firma TESCO SW, a.s.

Služby e-governmentu v podmínkách Úřadu

1. ÚVOD

Pokud se podíváme na vládu, respektive na vládnutí, jako na procesy, které jsou vykonávány na straně jedné státními institucemi a na straně druhé občany respektive firmami, pak úspěch realizace těchto procesů je založen na efektivní komunikaci a vzájemné interakci. Na tyto procesy lze v zásadě pohlížet jako na poskytování služeb vlády svým občanům a lze je rozdělit do těchto okruhů:

1) Poskytování informací druhému subjektu (například na základě zákona o svobodném přístupu k informacím)
2) Poskytování osvědčení o splnění podmínek daných zákonem (Rejstřík trestů, řidičská oprávnění apod.)
3) Úhrada předepsaných poplatků (daně, sociální dávky apod.)

Komunikace probíhá oběma směry a je zřejmé, že je časově náročná a ekonomicky nákladná. Pro její efektivní vedení a plnění povinností státu a jeho občanů se tudíž nabízí s výhodou využít efektivní možnosti moderních informačních a komunikačních technologií propojené Internetem, tzn. e-government.

Pojmem e-government označujeme elektronickou formu komunikace mezi občanem, respektive ekonomickým subjektem, a institucemi veřejné správy, jejíž pomocí stát nebo občan plní povinnosti dané mu zákonem. E-government rovněž představuje zásadní transformaci vnitřních a vnějších vztahů veřejné správy prostřednictvím informačních a komunikačních technologií s cílem optimalizovat interní procesy.

Elektronická komunikace občan – veřejná správa nejenže přiblíží úřad k občanovi, ale i zefektivní jejich vzájemnou komunikaci.

2. HODNOCENÍ E-GOVERNMENTU V RÁMCI EU

Základní směry rozvoje jsou v současnosti dány strategickým dokumentem Evropské komise „i2010 - Evropská informační společnost pro růst a zaměstnanost“, který byl přijat 1. června 2005. Dokument mimo jiné definuje tyto cíle:

- Dobudovat jednotný evropský informační prostor, který podpoří otevřený, soutěžní a obsahově bohatý vnitřní trh pro elektronické komunikace a digitální obsah. V rámci této priority se Evropská komise zaměří na interoperabilitu, bezpečnost, zvyšování rychlosti připojení k internetu a na bohatství nabízeného obsahu.
- Posílit inovace a investice do výzkumu v oblasti ICT. Kromě podpory výzkumu jde také o rozvoj podnikání v ICT a reorganizaci podnikatelských procesů s využitím ICT.
- Rozvíjet všem přístupnou informační společnost podporující růst a vytváření nových pracovních míst, lepší veřejné služby a kvalitu života. Jde o rozvoj takové informační společnosti, která nebude nikoho vynechávat či vylučovat a prostřednictvím použití uživatelsky příjemných informačních a komunikačních technologií bude nabízet vysoce kvalitní a dostupné veřejné služby.

Materiál také konkretizoval soubor služeb státu, které jsou svojí povahou důležité pro rozvoj e-governmentu:

Veřejné služby pro občany

– Daně z příjmu
– Služby hledání zaměstnání
– Výhody sociálního zabezpečení

– Osobní dokumenty (pasy / řidičské průkazy)
– Registrace vozidel
– Žádost o stavební povolení
– Oznámení pro policii
– Veřejné knihovny
– Certifikáty
– Zápis do vyššího vzdělání
– Oznámení o stěhování
– Zdravotnické služby

VeFřejné služby pro podnikání

– Sociální přídavky
– Daně
– DPH
– Registrace nové společnosti
– Odevzdání dat pro statistické úřady
– Celní deklarace
– Povolení týkající se životního prostředí
– Veřejné zprostředkování

Rozvoj e-governmentu v jednotlivých zemích EU je na různé úrovni, která je odvozena zejména od kvality legislativy dané země. Je zřejmé, že smysluplné fungování e-governmentu je založeno na zákonech, které nebrání používání moderních informačních technologií, respektive užití těchto technologií předvídá. Pro potřeby Evropské komise je každoročně zpracováno hodnocení e-governmentu (online veřejných služeb) ve 27 členských státech. Hodnocení je založeno na 5 stupňové škále tzv. sofistikovanosti elektronických služeb (viz obrázek *Sofistikovanost online služeb e-governmentu*), jinými slovy na tom, zda komunikace probíhá jednosměrně nebo oběma směry, zda informace lze zaslat elektroniky nebo pouze klasickou poštou nebo zda občan při komunikaci s úřadem má svoji personalizovanou stránku, podobně jako je tomu při komunikaci s bankou v rámci elektronického bankovnictví.

1. stupeň sofistikovanosti – informace znamená, že komunikace občana s úřadem je pouze jednosměrná, značnou výhodu představuje obrovská disponibilita informací a občan má daleko vyšší nároky na aktuálnost informace (např. ve srovnání s tištěnou informací), přístup k obecným informacím není nutno chránit.

2. stupeň sofistikovanosti – jednocestná interakce znamená, že komunikace občana s úřadem je stále jednosměrná, avšak již existuje nabídka formulářů ke stažení, který si pak občan vytiskne, vyplní a zašle poštou příslušnému úřadu. Je-li nutná také identifikace občana, provádí se při osobní návštěvě úřadu ověřením průkazu s fotografií. Standardní papírové formuláře musí stále existovat, úřady však šetří část nákladů na tisk na úkor občana.

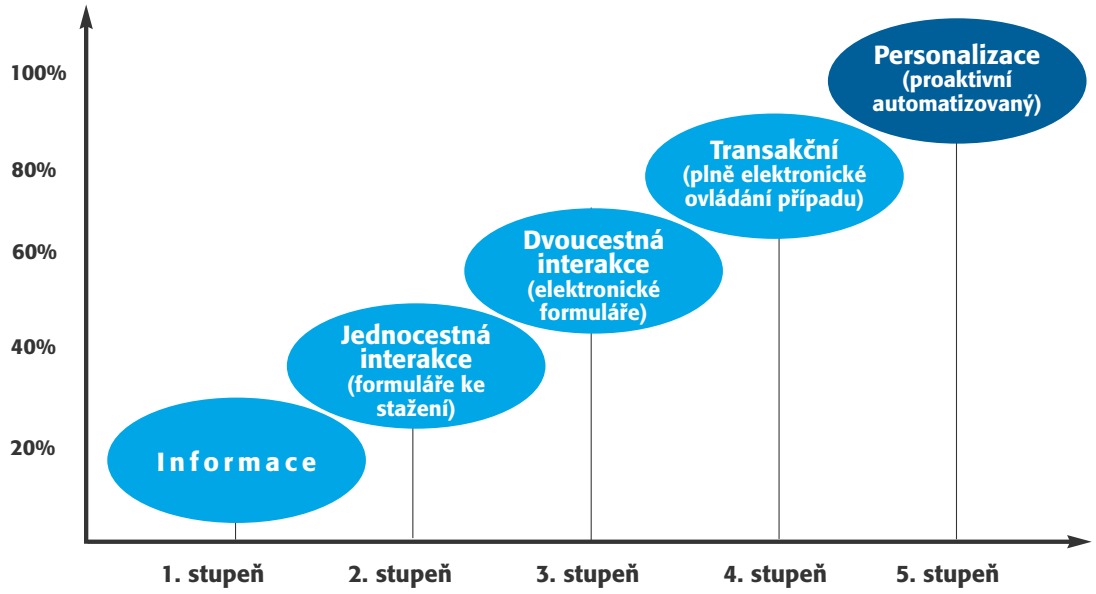
3. stupeň sofistikovanosti – dvoucestná interakce znamená, že komunikace občana s úřadem je již dvousměrná, přičemž existuje nabídka elektronického formuláře, který občan vyplní online, nebo na uživatelském počítači, a pak jej vytiskne a zašle poštou úřadu. Je-li nutná identifikace občana, provádí se při osobní návštěvě úřadu ověřením průkazu s fotografií. Standardní papírové formuláře musí stále existovat, úřady však šetří část nákladů na tisk na úkor občana.

4. stupeň sofistikovanosti – transakční služba znamená, že občan svoji žádost vyplní online a zašle ji elektronicky úřadu, a to buď prostřednictvím e-mailu, nebo webového formuláře. Rozhodnutí úřadu je občanovi doručeno elektronicky, což mu přináší výhodu časové a místní nezávislosti na úřadu. Problémem je právní relevance komunikace občan- úřad a proto je nutno zajistit identifikaci odesilatele, integritu dokumentu a neodmítnutelnost zodpovědnosti pomocí elektronického podpisu.

5. stupeň sofistikovanosti – proaktivní personalizace znamená, že jsou opakovaně využívána dostupná data a dodávka veřejných služeb je proaktivní. Úřad tedy předem upozorní občana, že bude něco vyžadovat, nebo mu přímo vyplní příslušná data ve formuláři žádosti (v povoleném rozsahu). Veřejná služba je dodávána občanovi automaticky, na základě jeho sociálních a ekonomických práv, aniž by občan musel o tyto služby žádat.

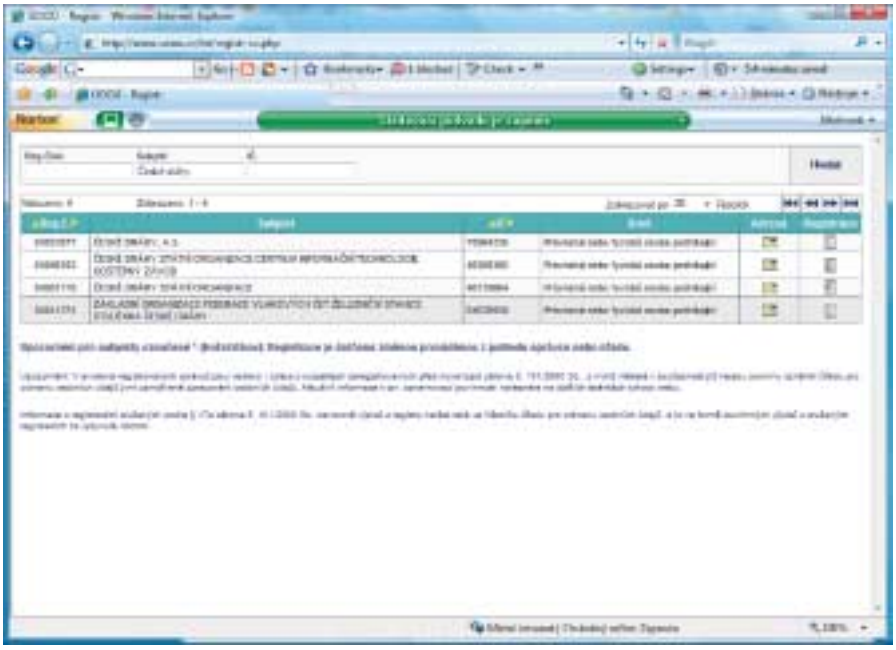
První až třetí stupeň sofistikovanosti pak znamená neúplnou online dostupnost elektronické služby, zatím co plnou online dostupnost služby představuje čtvrtý až pátý stupeň sofistikovanosti.

V návaznosti na výše uvedenou evropskou strategii i2010 reagovala vláda ČR zpracováním národní strategie „Efektivní veřejná správa a přátelské veřejné služby", přijaté usnesením vlády ČR č. 757/2007 a zpracované v dokumentu „Strategie realizace Smart Administration v období 2007-2015". Cílem této strategie je podpora socio-ekonomického růstu ČR a zvýšení kvality života občanů prostřednictvím zefektivnění fungování veřejné správy a veřejných služeb.



3. ÚŘAD A JEHO SLUŽBY V RÁMCI E-GOVERNMENTU ČR

Z hlediska sofistikovanosti on-line služeb Úřad pro ochranu osobních údajů provozuje 3 základní služby e-governmentu – na webových stránkách úřadu je veden registr správců osobních údajů spolu s on-line formulářem pro podání oznámení o zpracování osobních údajů, dále je zde možno podat stížnost na tzv. nevyžádané obchodní sdělení (NOS – marketingový spam) a rovněž je zde možno získat informace podle zákona o svobodném přístupu k informacím.



Dle zákona č. 101/2000 Sb., o ochraně osobních údajů, je Úřad povinen vést registr zpracování osobních údajů a rovněž učinit registr veřejně přístupným.

Oznámené zpracování zapsané do registru obsahuje: identifikační údaje správce, účel nebo účely zpracování, kategorie subjektů údajů a osobních údajů, které se těchto subjektů týkají, zdroje osobních údajů, místo nebo místa zpracování osobních údajů, příjemce nebo kategorie příjemců a předpokládaná předání osobních údajů do jiných států.

Registr mj. umožňuje přesvědčit se, zda určitá právnická nebo fyzická osoba zpracovává osobní údaje, a zda splnila svou zákonnou povinnost takové zpracování oznámit Úřadu obvyklým postupem. V registru lze vyhledávat podle názvu subjektu, přiděleného registračního čísla nebo IČ.

Správce může plnit svoji oznamovací povinnost vůči Úřadu také elektronicky, prostřednictvím webového formuláře, což pro něj znamená snazší a jednodušší plnění této povinnosti.

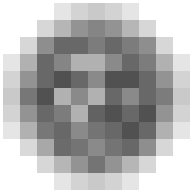
Pro Úřad představuje transakční vyřízení oznamovací povinnosti možnost omezit zpracování papírových dokumentů a automatickou dokumentaci spisů, což může znamenat úsporu nákladů.

Transakční elektronická služba představuje čtvrtý stupeň sofistikovanosti, což je z pohledu současné reality e-governmentu v ČR velmi dobrý výsledek hodnocení předmětné služby.

Dle zákona č. 480/2004 Sb., o některých službách informační společnosti je Úřad povinen vykonávat dozor nad šířením obchodních sdělení, jehož součástí je prověřování stížností na nevyžádaná obchodní sdělení. Stížnosti je možno podávat též elektronicky prostřednictvím webového formuláře, Úřad odpovídá rovněž elektronicky na udanou adresu. Jde tedy opět o transakční elektronickou službu s vysokým stupněm hodnocení – 4. stupeň sofistikovanosti služeb.

Dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím má Úřad povinnost poskytovat informace, vztahující se k jeho působnosti. Kromě klasické papírové podoby, poskytuje Úřad tyto informace též v elektronické podobě, prostřednictvím svých webových stránek, což značně podporuje dostupnost informací Úřadu pro občana. Občan má k dispozici relevantní a přehledně uspořádané informace, jako např.: právní předpisy, judikatura, předávání osobních údajů do zahraničí, Schengen, média, publikace a informace pro mládež.

Informace představuje první stupeň sofistikovanosti a komunikace občan – Úřad je pouze jednosměrná.



Personální zabezpečení Úřadu

Ke 31. 12. 2006 měl Úřad pro ochranu osobních údajů 88 zaměstnanců, pro rok 2007 byl státním rozpočtem stanoven plán počtu zaměstnanců na 90.

Na zabezpečení úkolů vyplývajících z výkonu předsednictví ČR v Radě Evropské unie schválila vláda ČR přechodné posílení Úřadu o 1 funkční místo na období od 1. 4. 2007 do 30. 9. 2009.

Vzhledem k naléhavé potřebě dokončit přípravy na plné zapojení do schengenské spolupráce a zajistit podmínky pro výkon kontrolních a dozorových činností, a to jak po stránce teoretické a koncepční, tak po stránce organizační, byl usnesením vlády ČR č. 633, ze dne 11. června 2007, zvýšen počet funkčních míst Úřadu od 1. července 2007 o 5, v polovině roku 2007 tak měl Úřad 96 funkčních míst.

Nábor nových zaměstnanců byl zaměřen jednak na nahrazení odcházejících pracovníků (v průběhu roku 2007 ukončilo pracovní poměr 16 zaměstnanců), jednak na získání specialistů, kteří budou zajišťovat dozor Úřadu jako nezávislého dozorového orgánu nad zpracováním osobních údajů v rámci III. pilíře (tj. Schengen, Europol, Eurojust, Eurodac apod.).

Splnění vysokých požadavků kladených na zaměstnance především v oblasti odborných a jazykových znalostí se Úřad snaží zajistit umožněním zvyšování, případně soustavného prohlubování jejich kvalifikace a také organizací jazykové výuky, které se zúčastní většina zaměstnanců Úřadu.

K 31.12. 2007 měl Úřad pro ochranu osobních údajů 92 zaměstnanců.

Členění zaměstnanců ÚOOÚ podle věku a pohlaví – stav k 31. 12. 2007

Věk	muži	ženy	celkem	%
18 - 20 let	1	0	1	1,1%
21 - 30 let	6	11	17	18,5%
31 - 40 let	5	5	10	10,9%
41 - 50 let	6	12	18	19,6%
51 - 60 let	24	15	39	42,4%
61 let a více	6	1	7	7,6%
Celkem	48	44	92	100,0%
%	52,2%	47,8%	100,0%	

Členění zaměstnanců ÚOOÚ podle vzdělání a pohlaví – stav k 31. 12. 2007

Vzdělání	muži	ženy	celkem	%
Základní	0	0	0	0,0%
Vyučen	0	0	0	0,0%
střední odborné	1	1	2	2,2%
úplné střední všeobecné	3	8	11	12,0%
úplné střední odborné	6	16	22	23,9%
vyšší odborné	0	1	1	1,1%
Bakalářské	1	0	1	1,1%
Vysokoškolské	36	17	53	57,6%
VŠ + vyšší kvalifikace	1	1	2	2,2%
Celkem	48	44	92	100,0%

Hospodaření Úřadu

Rozpočet Úřadu byl schválen zákonem č. 622/2006 Sb., o státním rozpočtu České republiky na rok 2007.

Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

v tisících Kč

Souhrnné ukazatele

Příjmy celkem	4 592,72
Výdaje celkem	89 555,25

Specifické ukazatele – příjmy

Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	4 592,72
v tom: příjmy z rozpočtu EU bez SZP-program. období 2004–2006	2 742,84
ostatní nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	1 849,88

Specifické ukazatele – výdaje

Výdaje na zabezpečení plnění úkolů Úřadu	89 555,25
v tom: výdaje spojené s výkonem předsednictví ČR v Radě EU	1 879,00
ostatní výdaje na zabezpečení plnění úkolů Úřadu	87 676,23

Průřezové ukazatele výdajů

Platy zaměstnanců a ostatní platby za provedenou práci	39 402,36
v tom: platy zaměstnanců	37 069,05
ostatní platby za provedenou práci	2 333,31
Povinné pojistné placené zaměstnavatelem?)	13 732,20
Převod fondu kulturních a sociálních potřeb	740,75
Platy zaměstnanců odvozené od platů ústavních činitelů	8 972,00
Výdaje na programy spolufinancované z prostředků EU bez SZP – programovací období 2004–2006 celkem	1 252,81
v tom: ze státního rozpočtu	0,00
kryté příjmem z rozpočtu EU	1 252,81

Dílčí ukazatele

Výdaje na financování programů podle přílohy č. 5	22 324,33
v tom: kapitálové výdaje	7 993,52
neinvestiční výdaje sledované v ISPROFIN	14 330,81
Běžné ostatní výdaje	14 096,36
Převod do rezervního fondu	4 450,00

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

Příjmy

Příjmy byly pro rok 2007 rozpočtem rozepsány ve výši 420 tisíc Kč. Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů, byl naplněn částku 4 592,72 tisíc Kč.

Šlo zejména o refundace zahraničních cest zaměstnanců Úřadu Radou Evropy a Evropskou komisí, o sankce uložené podle zákona č. 480/2004 Sb. o některých službách informační společnosti, o náhrady nákladů řízení, o úroky za finanční prostředky uložené na účtech u ČNB, o pojistnou náhradu, o převody z vlastních fondů, o příjmy vztahující se k roku 2006 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2006) a hlavně o refundace čerpaných prostředků z projektu Twinning Out – Pomoc Komisi pro ochranu dat v Bosně a Hercegovině, ve výši 1 272,45 tisíc Kč.

Na příjmovém účtu se projevilo použití finančních prostředků z rezervního fondu v celkové výši 2 505,70 tisíc Kč na akce sledované v ISPROFIN „Údržba zařízení a DHIM“, „Nájemné a služby“, investiční akci „Upgrade serverů Microsoft a OS pracovních stanic“ a projekt Twinning out.

Úroky z finančních prostředků uložené na účtech u ČNB činily 4,82 tisíc Kč.
Přijaté sankční platby byly ve výši 261,50 tisíc Kč, pojistné náhrady ve výši 242,71 tisíc Kč a náklady řízení, refundace týkající se minulých let ve výši 261,25 tisíc Kč.
Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

1. Běžné výdaje

Čerpání běžných výdajů ve výši 14 096,36 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, údržby a o výdaje související s neinvestičními nákupy.
Výdaje za vodu, plyn a elektrickou energii činily v roce 2007 865,38 tisíc Kč.
Výše uvedené částky odpovídají požadavku na účelný a hospodárný provoz Úřadu.

2. Platy zaměstnanců a ostatní platby za provedenou práci

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

Stav k 31. 12. 2007 byl 92 zaměstnanců.

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

V souladu se schválenou dokumentací programu 243 010 „Rozvoj a obnova materiálně-technické základny Úřadu pro ochranu osobních údajů“ bylo celkem vyčerpáno 22 324,33 tisíc Kč.
Z toho na investiční výdaje bylo čerpáno 7 993,52 tisíc Kč (z toho 454,56 tisíc převod do rezervního fondu).

Šlo zejména v programu 243010 „Rozvoj a obnova materiálně technické základny“ o:
podprogram 243 011 „Pořízení, obnova a provozování ICT Úřadu“, kde byly v roce 2007 čerpány investiční systémově určené výdaje SR na:

v tis.Kč

akci 243011 0014 „Upgrade serverů Microsoft a OS pracovních stanic“ 1 660,84
akci 243011 0016 „Pořizování majetku a služeb“ - - - - - - - - - - - - - - - - - - 345,10
akci 243011 0027 „Upgrade systému spisové služby“ - - - - - - - - - - - - - - - 959,33
akci 243011 0028 „Rozšíření diskového pole“ - - - - - - - - - - - - - - - - - - - 1 120,10
akci 243011 0032 „Reprodukce výpočetních sítí – internet“ - - - - - - - - - - - 765,43
akci 243011 0033 „Intranetový portál (Share Point)“ - - - - - - - - - - - - - - - 373,66
akci 243011 0034 „Rozvoj aplikace pro podporu nákupu majetku
a služeb – PMS“ - 547,40
akci 243011 0035 „GIS WORKS“ - 260,61
akci 243011 0036 „Ochrana webového provozu“ - - - - - - - - - - - - - - - - - - 402,07
akci 2430 11 0037 „Pořízení projektoru pro zasedací místnost“ - - - - - - - - 55,34
akci 243011 0038 „Terminál pro inventarizaci majetku“ - - - - - - - - - - - - - 45,15

neinvestiční systémově určené výdaje SR na:
akci 243011 0021 „Tiskové a kopírovací služby“ - - - - - - - - - - - - - - - - - 657,11
akci 243011 0024 „Zaměstnanecké certifikáty“ - - - - - - - - - - - - - - - - - - - 4,39
akci 243011 0029 „Obnova monitorů a notebooků“ - - - - - - - - - - - - - - - 1 080,59
akci 243011 0032 „Reprodukce výpočetních sítí – internet“ - - - - - - - - - - 64,92
akci 243011 0038 „Terminál pro inventarizaci majetku s čárovým kódem“ - 7,26
akci 243011 P200 „Provozování ICT Úřadu“ - - - - - - - - - - - - - - - - - - - 5 951,62

podprogram 243 012 „Reprodukce majetku Úřadu“ – kde byly čerpány investiční systémově určené výdaje SR na:
akci 243012 0123 „Bezpečnost objektu“ - 129,69
akci 243012 0127 „Modernizace výtahu“ - 435,30
akci 243012 0128 „Drobné úpravy budovy“ - 90,75
akci 243012 0129 „Pořízení osobního vozidla“ - - - - - - - - - - - - - - - - - - 348,19

Neinvestiční systémově určené výdaje SR na:
akci 243012 5501 „Nájemné a služby“ - 2 839,21
akci 243012 5502 „Údržba zařízení a DHIM“ - - - - - - - - - - - - - - - - - - - 1 480,27

Investiční systémově určené výdaje byly čerpány celkem ve výši 7 993,52 tisíc Kč, z toho čerpání na investiční akce v podprogramu 243 011 „Pořízení, obnova a provozování ICT Úřadu“ 6 535,03 tisíc Kč, v podprogramu 243 012 „Reprodukce majetku Úřadu“ 1 003,93 tisíc Kč a převod do rezervního fondu ve výši 454,56 tis. Kč. Neinvestiční systémově určené výdaje byly čerpány celkem ve výši 14 330,81 tis. Kč (v tom převod do rezervního fondu ve výši 2 245,44 tisíc Kč) a byly použity na úhradu provozních nákladů ICT, služeb a údržby zařízení a drobného hmotného dlouhodobého majetku.

4. Interní audit a vnitřní kontrola

Funkce vnitřního auditu je personálně zajištěna od roku 2006.
V květnu roku 2007 byl proveden v souladu s plánem audit správnosti čerpání rozpočtových prostředků EU poskytnutých v rámci programu CARDS s kladným hodnocením.

5. Použití rezervního fondu

Část prostředků, uložená v rezervním fondu, byla použita na částečné financování investiční akce 2430 11 0014 „Upgrade serverů Microsoft a OS pracovních stanic" ve výši 652,51 tisíc Kč a na neinvestiční akce 2430 12 5501 „Nájemné a služby" 61,99 tisíc Kč a 2430 12 5502 „Údržba zařízení a DHIM" 320,81 tisíc Kč. Na základě usnesení vlády č. 629/2007 byla část prostředků ve výši 1 915 tisíc Kč převedena z rezervního fondu ÚOOÚ do státního rozpočtu kapitoly VPS.

6. Projekt Twinning out

Projekt Twinning Out-Pomoc Komisi pro ochranu dat v Bosně a Hercegovině skončil definitivně dne 26.9.2007, kdy Evropská komise ukončila kontrakt jako naplněný. Nevyčerpané finanční prostředky z rezervního fondu ve výši 398,18 tisíc Kč byly po skončení projektu vráceny do státního rozpočtu.

Podseskupení, položka – název	Schválený rozpočet	Stav RF k 1. 1. 2007	Čerpání
501 – Platy		519,54	495,58
502 – Ostatní platby za prov.práci	300	98,71	159,31
503 – Povinné pojistné placené zaměstnavatelem		195,69	173,45
5031/11/16 – Povinné pojistné na soc. zabezp. a přísp. na stát. pol. zam.		144,74	128,85
5032/11/16 – Povinné pojistné na veřejné zdravotní pojištění		50,95	44,6
513 – Nákup materiálu		29,8	0
516 – Nákup služeb	120	181,5	155,88
517 – Ostatní nákupy		424,93	258,67
519 – Výdaje související s neinv. nákupy, příspěvky, náhrady a věcné dary		10	0
534 – Převody vlastním fondům		10,21	9,91
5342/11/16 – Převody FKSP		10,21	9,91
VÝDAJE CELKEM	**420**	**1470,38**	**1252,8**

Přehled čerpání rozpočtu v roce 2006

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2007 v tisících Kč	Upravený rozpočet 2007 v tisících Kč	Skutečnost dle účetních výkazů k 31.12. 2007 v tis. Kč	Skutečnost / Upravený rozpočet v %
	PŘÍJMY CELKEM	**0**	**0**	**41 052,29**	**0**
501	Platy	34 718	36 607	37 069,05	101,26
5011	Platy zaměstnanců	26 314	27 635	28 097,05	101,67
5014	Platy zaměstnanců odvozované od platů ústavních činitelů	8 404	8 972	8 972,00	100,00
502	Ostatní platby za provedenou práci	2 474	2 474	2 333,31	94,31
5021	Ostatní osobní výdaje	2 174	2 169	2 028,31	93,51
5024	Odstupné	300	305	305,00	100,00
5026	Odchodné	0,00	0,00	0,00	0,00
503	Povinné pojistné placené zaměstnavatelem	12 912	13 574	13 732,20	101,17
5031	Povinné pojistné na sociální zabezpečení	9 592	10 084	10 203,12	101,18
5032	Povinné pojistné na veřejné zdravotní pojištění	3 320	3 490	3 529,08	101,12
513	Nákup materiálu	5 758	4 920	2 846,83	57,86
514	Úroky a ostatní finanční výdaje	0	55	10,07	18,31
515	Nákup vody, paliv a energie	1 910	1 925	1 158,04	60,16
516	Nákup služeb	18 040	18 927	12 942,74	68,38
5167	Školení a vzdělávání	1 550	2 452	1 787,33	72,89
517	Ostatní nákupy	6 251	6 803	4 542,39	66,77
5171	Opravy a udržování	2 360	2 240	1 003,03	44,78
5173	Cestovné	2 500	3 134	2 815,51	89,84
518	Poskytnuté zálohy	0	0	0	0
519	Výdaje související s neinvestičními nákupy	2 280	2 390	2 182,60	91,32
5342	Převody FKSP	694	732	740,75	101,20
5346	Neinv. převody do RF			3 995,44	
536	Ostatní neinvestiční transfery jiných veřejných rozpočtů	25	25	8,31	33,24
542	Náhrady placené obyvatelstvu	60	60	0	0
5429	Ostatní náhrady placené obyvatelstvu	60	60	0	0
	BĚŽNÉ VÝDAJE CELKEM	85 122	88 492	81 561,73	92,17

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2007 v tisících Kč	Upravený rozpočet 2007 v tisících Kč	Skutečnost dle účetních výkazů k 31.12. 2007 v tis. Kč	Skutečnost / Upravený rozpočet v %
611	Pořízení dlouhodobého nehmotného majetku	3 420	3 908	4 146,94	106,11
612	Pořízení dlouhodobého hmotného majetku	4 320	3 832	3 392,02	88,52
6361	Investiční převody do RF			454,56	
	KAPITÁLOVÉ VÝDAJE CELKEM	7 740	7 740	7 993,52	103,28
	V Ý D A J E C E L K E M	**92 862**	**96 232**	**89 555,25**	**93,06**
	z toho: použití rezerv. fondu			2 505,70	

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 1. 2008

Přehled výdajů spojených s výkonem předsednictví ČR v Radě EU v roce 2007

Položka-název	Schválený rozpočet	Upravený rozpočet	Čerpání
5011/15 Platy	0,00	233,00	197,20
5031/15 – povinné pojistné na SZ	0,00	61,00	51,27
5032/15 – povinné pojistné na ZP	0,00	21,00	17,75
5342/15 FKSP	0,00	5,00	3,45
5142/15 Realizované kurz.ztráty	0,00	5,00	3,83
5167/15 Školení tuzemské	0,00	10,00	6,70
5167/2/15 Školení zahraniční	0,00	892,00	592,43
5176/1/15 Účast.popl. na konference	0,00	18,00	17,20
5173/2/15 Cestovné	0,00	634,00	400,49
5342 15 převody do RF			588,68
Celkem	**0,00**	**1 879,00**	**1 879,00**