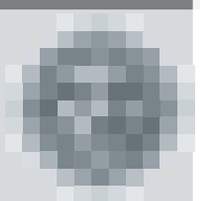
VÝROČNÍ ZPRÁVA

2009



úřad pro ochranu osobních údajů
the office for personal data protection

ISBN 978-80-210-5130-0

Ohlédnutí předsedy Úřadu za rokem 2009

Předkládaná výroční zpráva přináší především podrobný přehled o kontrolní činnosti Úřadu. Může se však svým pojetím stát nejen bilancí, ale namnoze také detailním poučením o rozhodování Úřadu a jeho výkladu zákona o ochraně osobních údajů, jehož dodržování dozoruje. S jistou nadsázkou si troufám říci, že jde o svého druhu judikaturu, dosti dobře pochopitelnou i pro laiky. Považuji to za důležité zejména proto, že Úřad soustavně vyvíjí úsilí, aby zákonu o ochraně osobních údajů a jeho souvislostem s ochranou soukromí dobře rozuměl co nejširší okruh občanů. Soukromí je pro mne jednou z hodnot naší civilizace a jednou ze zásadních podmínek toho, aby byla zachována i pro příští generace.

S uvedeným úsilím souvisí i přednášková činnost Úřadu a v roce 2009 ukončený tříletý vzdělávací projekt Ochrana osobních údajů ve vzdělávání, který byl na sklonku roku 2006 akreditován Ministerstvem školství, mládeže a tělovýchovy. Semináři, které pořádal Úřad v jeho rámci, prošlo 211 pedagogů – někteří se dokonce vraceli s novými dotazy, z některých školských zařízení se zúčastnilo a odneslo si osvědčení o absolvování několik pracovníků. Jejich postoje a ocenění nám dávají pocit, že jsme odvedli nezanedbatelný kus práce.

Úřad se úspěšně zhostil v loňském roce i těch aktivit, které souvisely s českým předsednictvím v EU v první polovině roku 2009. Podrobně se jimi zabývá část výroční zprávy věnovaná zahraničním aktivitám Úřadu. A v roce 2010 bude Úřad na řadu získaných kontaktů i podnětů navazovat.

Přestože jsme se museli v průběhu roku vyrovnat s velkým množstvím problematických případů zpracování osobních údajů, o čemž rovněž přinášejí důkaz kapitoly věnované kontrolní a správní činnosti Úřadu, za obzvlášť významné považuji, že jsme dokázali pokročit přinejmenším ve dvou oblastech, které činnost Úřadu výrazně profilovaly už v loňském roce. Především jde o posun v legislativním uchopení problematiky užívání kamerových systémů, které by se mělo završit v roce 2010. Věřím také, že velmi obsažný seminář věnovaný pohledu na problémy právní úpravy nakládání s DNA profily, který se uskutečnil na půdě Senátu a byl zaštítěn jeho místopředsedou i předsedkyní jeho Stálé komise pro ochranu soukromí, započal cestu k lepší legislativní ochraně jednoho z nejintimnějších a vůči narušení soukromí přímo fatálního osobního údaje. Zcela realisticky neočekávám, že cesta k lepší legislativě bude snadná a krátká (ostatně o její náročnosti svědčí i kapitola této výroční zprávy

věnovaná speciálně legislativní činnosti Úřadu); jsem ale přesvědčen, že jsme na ni už dobře vyzbrojeni množstvím poznatků, o něž jsme se v roce 2009 obohatili.

Tím nemám na mysli jen praktické a odborně zobecnitelné poznatky Úřadu. Rok 2009 nepochybně prokazoval i podstatně hlubší znalost zákona mezi veřejností. Soudím tak jednak z kvality dotazů, které nám kladli novináři a které byly jak detailnější, tak svým způsobem poučenější, jednak z agendy podání a stížností, kde dotazy byly podstatně kvalifikovanější. Především se to však projevilo a je to prokazatelné na žádostech o konzultace. Na odborné zaměstnance Úřadu ovšem agenda konzultací kladla také větší nároky po stránce časové i profesionální. Mohu být zajisté potěšen tím, že je Úřad chápán jako skutečně referenční a arbitrární instance. Na druhé straně si dobře uvědomuji, že se často jeho poznatky proměňují v kapitál advokátních kanceláří. Tedy si nemohu neklást otázku rozsahu konzultační činnosti, která je Úřadu zákonem uložena, a potažmo i dostatečnosti personálního zabezpečení.

Je sice pravda, že nová kompetence, která je svěřena Úřadu zákonem č. 111/2009 Sb., o základních registrech, byla provázena určitým navýšením počtu pracovníků Úřadu, přesto i v této oblasti je zatím nejisté, nakolik bude snadné plnění úkolů plynoucích z uvedeného zákona naplňovat. I finanční zabezpečení nové kompetence Úřadu bylo stanoveno na základě odhadů náročnosti zajištění nové agendy po stránce technické i po stránce personální. Nicméně považuji za úspěch, že jsme pro tento účel dokázali efektivně čerpat z evropských strukturálních fondů, a jsem si jist, že kooperativní duch instituce je dobrým předpokladem, že se s novými povinnostmi dokážeme úspěšně vyrovnat.

Ochota spolupracovat, které si na instituci, v jejímž čele stojím, upřímně cením, se doufám projeví také v mezinárodním měřítku – při organizaci Jarní konference komisařů pro ochranu osobních údajů 2010, kteří se z celé Evropy sjedou na konci dubna 2010 na Pražský hrad. Rozhodně není maličkost stát se jednou za sedmadvacet let pořadatelem takové události. Zároveň je však ctí, že českému úřadu byla dána důvěra ostatních členských úřadů EU, aby konferenci zorganizoval. Tomu úkolu ale jdu vstříc s dobrou nadějí, neboť jsem na předvánočním setkání 2009 s upřímným přesvědčením říkal zaměstnancům Úřadu: Těší mne, že jsme jeden tým.

Igor Němec

OBSAH

ÚŘAD V ČÍSLECH 2009

Dotazy a konzultace	dotazy ČR	2 215
	zahraničí	111
	konzultace	
	státní správě	45
	samosprávě	5
	právnickým osobám	42
	fyzickým osobám podnikajícím	9
	fyzickým osobám	13
Podání a stížnosti	přijaté podněty dle zákona o ochraně osobních údajů	879
	stížnosti předané ke kontrole	129
Nevyžádaná obchodní sdělení (kompetence podle zákona č. 480/2004 Sb.)	podnětů celkem	2 261
	vyřešených podnětů	1 678
	zahájených kontrol	145
	ukončených kontrol	131
	správních rozhodnutí o pokutě	112
Kontroly (vyjma kontrol týkajících se zákona č. 480/2004 Sb.)	zahájeno	143
	ukončeno	131
	předáno jiným státním úřadům	3
	napadeno námitkami	38
	námitkám vyhověno	5
	nevyhověno	27
	převážně vyhověno	0
	převážně nevyhověno	2
Správní trestání	správní řízení o porušení zákona č. 101/2000 Sb. a č. 133/2000 Sb.	89
	přestupková řízení podle zákona č. 101/2000 Sb.	10
	přestupková řízení o porušení zákona č. 159/2006 Sb., o střetu zájmů	1
	rozklady napadená rozhodnutí o porušení zákona	43
	zamítnutých rozkladů	23
	zrušeno a vráceno k novému projednání	7
	zrušených rozhodnutí a zastavená řízení	2
	změna rozhodnutí	3
Soudní přezkum	podaných žalob k soudu	17
	zamítnutých žalob soudem	5
	zrušených rozhodnutí soudem	1
	postoupení k vydání rozhodnutí (podle § 21 zákona č. 101/2000 Sb.)	3
	ukončených/neukončených soudních řízení	1/16

Registrace	přijatá oznámení (podle § 16 zákona č. 101/2000 Sb.)	3 278
	zaregistrovaná zpracování	2 841
	dosud v řízení	437
	zrušené registrace	139
	oznámení o změně zpracování	817
	řízení podle § 17 (zákona č. 101/2000 Sb.)	
	zastaveno (nedochází k porušení zákona)	49
	zastaveno z procesních důvodů (např. oznámení vzato zpět)	3
	nepovoleno	1
Povolení k předávání osobních údajů do zahraničí	Počet přijatých žádostí o předávání osobních údajů do zahraničí (podle § 27 zákona č. 101/2000 Sb.)	30
	rozhodnutí o povolení předávání	21
	rozhodnutí o nepovolení	0
	zastavená řízení z procesních důvodů	9
Stížnosti podle § 175 správního řádu	přijatých stížností	
	vyřízených jako důvodné	2
	vyřízených jako částečně důvodné	5
	vyřízených jako bezdůvodné	22
Stížnosti a jiné podněty na postup Úřadu, které nebyly řešeny podle § 175 správního řádu	došlých podnětů	0
	vyřízených jako oprávněné	
	vyřízených jako neoprávněné	
Žádosti podle zákona č. 106/1999 Sb.	přijatých žádostí	10
	vyřízených žádostí	8
	odmítnutých žádostí	2
Publikované materiály	Věstník Úřadu (počet částek)	4
	Informační bulletin Úřadu (počet čísel)	4
Tiskové konference	pravidelné	2
	mimořádné	1
Připomínkované legislativní návrhy	zákony	62
	prováděcí předpisy	
	návrhy nařízení vlády	11
	návrhy vyhlášek	101
	ostatní	94
	zahraniční materiály	14

KONTROLNÍ ČINNOST ÚŘADU

V souladu s ustanovením § 31 zákona o ochraně osobních údajů se kontrolní činnost Úřadu pro ochranu osobních údajů provádí na základě kontrolního plánu nebo na základě podnětů a stížností.

Kontrolní plán, jehož obecná část se dále uvádí, se zpracovává jako společný dokument předsedy a inspektorů Úřadu, který je závazný a jehož plnění se pravidelně vyhodnocuje na zasedání kolegia inspektorů, které je společným poradním orgánem této skupiny.

KONTROLNÍ PLÁN PRO ROK 2009

Úřad v návaznosti na své dosavadní zkušenosti z výsledků kontrolních, správních a registračních procesů a v souladu se zájmem společnosti zaměřovat své kontrolní aktivity při plánování kontrolní činnosti na takové způsoby zpracování osobních údajů, které postihují data velké části fyzických osob, nebo na situace, kdy se zájem správců a zpracovatelů soustřeďuje na tzv. citlivé skupiny osobních údajů společnosti, případně zaměřit tyto aktivity na nové požadavky zpracování osobních údajů v souladu s nově platnou právní úpravou, vyjadřuje tento svůj záměr prostřednictvím kontrolního plánu, který v souladu s ustanovením § 31 zákona č. 101/2000 Sb. vydával předseda Úřadu po projednání s inspektory Úřadu pro rok 2009:

I. OBECNÁ TÉMATA PRO ZAMĚŘENÍ KONTROLNÍ ČINNOSTI INSPEKTORŮ ÚŘADU

1. INFORMAČNÍ SYSTÉMY VEŘEJNÉ SPRÁVY

Již standardní součástí kontrolního plánu je plnění povinností správce nebo zpracovatele v oblasti eGovernment. Proto v souladu s očekávaným vývojem této oblasti a záměrů vlády soustředil Úřad své aktivity do těch oblastí veřejné správy, které shromažďují velké množství osobních údajů.

2. INFORMAČNÍ SYSTÉMY V OBLASTI III. PILÍŘE

V souladu s novelizací právní úpravy podmínek pro zpracování osobních údajů v oblasti boje proti legalizaci výnosů z trestné činnosti, provedené zákonem č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, a v návaznosti na zkušenosti, které Úřad získal z kontrolních činností prováděných v této oblasti v minulém období, také v tomto roce pokračoval v dozorové činnosti se zaměřením na realizaci povinností identifikace a kontroly klienta podle tohoto zákona a s tím související zpracování osobních údajů.

3. VÝKON POVINNOSTÍ SPRÁVCE V SOUVISLOSTI S POVOLOVACÍ ČINNOSTÍ PODLE § 16 ZÁKONA Č. 101/2000 SB.

V dosavadní registrační a povolovací činnosti Úřadu je zřejmé, že v řadě případů, kdy je Úřadu předložen záměr správce zpracovávat určité skupiny osobních údajů a toto zpracování není v očekávaném rozsahu záměru správce povoleno, chybí následná informace, zda bylo rozhodnutí Úřadu o nepovolení zpracování osobních údajů zcela respektováno. Proto se kontrolní aktivity inspektorů Úřadu zaměřily na vytipované skupiny správců s cílem prosazovat politiku Úřadu v dané oblasti.

4. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZA PODMÍNEK JEJICH PŘENOSU DO TŘETÍCH ZEMÍ

Záměrem kontrolní činnosti v roce 2009 je mimo jiné poznání, jakým způsobem jsou realizována doporučení v oblasti přenosů osobních údajů do jiných zemí, zejména za situace, kdy mají být osobní data přenášena za podmínek existence tzv. „binding corporate rules“ nebo jiných společných opatření nebo rozhodnutí přijatých v evropském právním rámci s ohledem na podmínky přenosu. Úřad po zkušenostech z uplynulého období a v návaznosti na nárůst požadavků na schválení podmínek přenosu dat zejména u velkých nadnárodních společností často řeší individuální problémy jednotlivců, ale tato oblast nebyla zatím v historii Úřadu podrobena větší kontrole.

5. OCHRANA OSOBNÍCH ÚDAJŮ A NEZISKOVÝ SEKTOR

V návaznosti na rostoucí počet projektů realizovaných v této oblasti, které jsou často finančně dotovány, a s ohledem na počet klientů, kterým jsou služby neziskových organizací nabízeny, vzniká potřeba a zájem Úřadu monitorovat rozsáhlejší zpracování osobních údajů s přihlédnutím k povinnostem správce vyplývajícím ze zákona o ochraně osobních údajů. Samotné prostředí poskytování služeb klientům (bezdomovci, zavlékané osoby, osoby podléhající návykovým látkám, osoby ocitnuvší se v krizové osobní či rodinné situaci) musí mít garantovány stejné podmínky pro ochranu svého soukromí v souvislosti se zpracováváním osobních údajů, jak to očekává příslušná právní úprava.

6. DALŠÍ KONTROLNÍ AKTIVITY, NAVAZUJÍCÍ NA ÚŘADEM AKCEPTOVANÉ POTŘEBY A POŽADAVKY V URČITÉ OBLASTI

Do plánu kontrolní činnosti se zařazují kontrolní záměry vycházející z aktuálních poznatků či společensky žádoucích témat nebo na ně navazující.

Transpozice směrnice 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí.

II. PLÁNOVANÉ A UKONČENÉ KONTROLY V ROCE 2009

1. KONTROLA PLNĚNÍ POVINNOSTÍ VYPLÝVAJÍCÍCH ZE ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ SPOLEČNOSTÍ, KTERÁ ZAMĚSTNÁVÁ I CIZÍ STÁTNÍ PŘÍSLUŠNÍKY

Kontrola byla zaměřena na zpracování osobních údajů nejen zaměstnanců, ale i uchazečů o zaměstnání ve společnosti, která zaměstnává 3 500 pracovníků, mezi nimiž je 2 800 občanů České republiky, 120 agenturních zaměstnanců a asi 30 osob, které sice působí v závodě společnosti, ale jsou zaměstnanci mateřských firem.

O práci ve společnosti lze požádat jednak prostřednictvím internetu, kde na webových stránkách společnosti v sekci Volná místa je možné vyplnit příslušný dotazník či lze zaslat životopis elektronickou poštou na e-mailovou adresu společnosti, případně je též možné se písemně nebo telefonicky obrátit na náborové centrum společnosti. Výběrové řízení je obsahově diferencováno pro uchazeče o místa ve výrobě a pro uchazeče o pozice specialistů a inženýrů. Při získávání nových pracovníků společnost používá tři typy souborů písemností. Dva z nich odpovídají výše zmíněným kategoriím uchazečů o práci, třetí soubor písemností je společný pro obě skupiny uchazečů. Tyto dokumenty společnost

používá ve vztahu ke kandidátům před nástupem do zaměstnání a v době nástupu do zaměstnání. Pokud je uchazeč přijat, dokumenty určené pro výběrové řízení společnost dále uchovává, jestliže však uchazeč přijat není, jsou tyto dokumenty skartovány, neboť se dále nepoužívají. V případě, že uchazeč požádá o vydání dokumentů opatřených v průběhu výběrového řízení, je mu vyhověno. Uchazeči o práci, kteří společnost kontaktují prostřednictvím jejích webových stránek, poskytují souhlas s tím, aby společnost zpracovávala jimi poskytnuté osobní údaje pro účely výběrového řízení a personální potřeby, a to až do odvolání. Některé nové zaměstnance společnost získává prostřednictvím personálních agentur. Těm sdělí příslušné požadavky a nezbytnou inzerci poté zajišťují zmíněné agentury, které také provádějí prvotní výběr z řad uchazečů a doporučují společnosti vhodné kandidáty. Navržené osoby jsou posléze podrobeny stejnému výběru jako ti uchazeči, jež společnost oslovila vlastní náborovou kampaní. Další personál poskytují společnosti agentury práce. O osobách poskytnutých agenturami práce společnost nevede žádné dokumenty, neboť agenturní pracovníci nejsou zaměstnanci společnosti. Ohledně nich společnost nezakládá žádné spisy, pouze je eviduje ve svém docházkovém systému, aby byla schopná vysílající agentuře prokázat, kolik hodin pracovníci agentury ve společnosti odpracovali, což je dokladem pro fakturaci. Společnost se snaží, aby o těchto osobách neměla žádné údaje, které mít nemusí.

Kontrolující se zaměřili zejména na rozsah zpracovávaných údajů v osobních spisech zaměstnanců, na právní titul opravňující společnost ke zpracování osobních údajů, dobu uchování a naplnění informační povinnosti společnosti jako správce.

Kontrolou bylo zjištěno, že v osobních spisech některých zaměstnanců je písemně zpracováván údaj o tom, zda jsou vojáky, přičemž se jedná o údaj, jenž není nezbytný pro výkon práce v pracovněprávním vztahu a toto zpracování je v rozporu s ustanovením věty druhé § 312 odst. 1 zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů (dále jen „zákoník práce“) a jedná se o zpracování osobního údaje v rozsahu větším než nezbytném pro naplnění stanoveného účelu. Stejně tak při zpracování osobních údajů manželky v rozsahu jméno, příjmení (i rodné), rodné číslo v osobním spisu zaměstnance (přičemž se nejedná o vyživovanou osobu dle zvláštního právního předpisu) jde o zpracování osobních údajů ve větším rozsahu než nezbytném pro naplnění stanoveného účelu. Uvedené zpracování osobních údajů bylo v rozporu s § 5 odst. 1 písm. d) zákona o ochraně osobních údajů, podle kterého je společnost jako správce povinna shromažďovat osobní údaje v rozsahu nezbytném pro naplnění stanoveného účelu. Jestliže společnost zpracovává u svých zaměstnanců informace o jejich členství v odborové organizaci, porušuje zákaz stanovený v § 316 odst. 4 písm. e) zákoníku práce. Protože zmíněná informace je podle uvedeného ustanovení nepřípustná, její opatřování nemůže být nezbytné ani ve smyslu zákona a taktéž odporuje § 5 odst. 1 písm. d) zákona o ochraně osobních údajů.

Zpracování jména a příjmení kontaktní osoby včetně čísla jejího telefonu v osobním spisu zaměstnance, jehož pracovní poměr ke společnosti skončil, je uchováváním osobních údajů nejen po dobu, která je nezbytná k účelu jejich zpracování, a tudíž neodpovídá ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů.

Ustanovení § 5 odst. 2 zákona společnost porušila, když v osobních spisech zaměstnanců v průběhu jejich zaměstnávání ve společnosti drží listiny s přijímacími testy a jejich vyhodnocením pořízenými při přijímání do pracovního poměru ve společnosti za situace, kdy tito zaměstnanci souhlasili se zpracováním těchto osobních údajů pouze pro účely výběrových řízení.

Když společnost ve spisech zaměstnanců evidovala údaj o jejich národnosti, přičemž k dispozici není jejich souhlasné stanovisko s tímto opatřením ani není naplněna žádná z dalších zákonných podmínek, jedná se o zpracování citlivých údajů, aniž by subjekty údajů daly ke zpracování výslovný souhlas, a tedy o nerespektování příkazu stanoveného v § 9 zákona o ochraně osobních údajů. Stejně tak dochází k porušení uvedeného ustanovení zákona, když společnost zpracovává osobní údaj týkající se členství v odborové organizaci, aniž by disponovala výslovným souhlasem s tímto zpracováním.

Vzhledem k tomu, že společnost jako správce nepoučuje uchazeče o zaměstnání ani zaměstnance o tom, zda je poskytnutí požadovaných osobních údajů povinné či dobrovolné, a dále chybí poučení o skutečnosti, kdy je subjekt údajů povinen podle zvláštního zákona osobní údaje pro zpracování poskytnout,

jakož i o následcích odmítnutí poskytnutí osobních údajů správci údajů, neplní tak povinnost dle hlavy II zákona o ochraně osobních údajů a porušuje ustanovení § 11 odst. 2 zákona o ochraně osobních údajů.

Společnost (správce) při zpracování osobních údajů uchazečů o zaměstnání ve společnosti a zaměstnanců společnosti postupovala v rozporu se zákonem o ochraně osobních údajů, protože jako správce shromažďovala osobní údaje v rozsahu větším než nezbytném pro naplnění stanoveného účelu, neuchovávala osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování, dále zpracovávala osobní údaje bez souhlasu subjektů údajů, aniž by byla splněna kterákoliv z podmínek umožňujících zpracovávání osobních údajů bez souhlasu těchto subjektů, dále zpracovávala citlivé údaje bez splnění kterékoliv z podmínek, jež toto zpracování umožňují, a dále nepoučila subjekt údajů o tom, zda je poskytnutí osobního údaje povinné, či dobrovolné, a o následcích odmítnutí poskytnutí osobních údajů. Za prokázané porušení zákona o ochraně osobních údajů byla společnosti uložena pokuta.

2. KONTROLA PLNĚNÍ POVINNOSTÍ SPRÁVCE PŘI ZPRACOVÁNÍ DNA V SOUKROMÉM SEKTORU

Byla kontrolována společnost, která je zapsána v obchodním rejstříku, přičemž jejími předměty podnikání jsou mimo jiné výzkum a vývoj v oblasti přírodních a forenzních věd a činnost technických poradců v oblasti přírodních věd, molekulární biologie, forenzní genetiky a správné laboratorní praxe i molekulárně biologické a forenzně genetické analýzy, tedy genetické analýzy zpracované pro soudní potřeby související s vyšetřováním a soudním dokazováním zejména v trestních záležitostech. Společnost se ve své činnosti zaměřuje především na vědu a výzkum, DNA servis, publikační činnost, poradenství a prodej specializovaných produktů pro forenzní laboratoře.

Zákazníci od společnosti zpravidla objednávají genetické určení původu předků, určení otcovství, identifikaci odesílatele anonymních dopisů, specifický průkaz spermatu nebo určování příbuzenského vztahu, včetně stanovení vaječnosti dvojčat. V současnosti je těžištěm aktivit společnosti identifikace kosterních pozůstatků, jež zahrnuje i historické nálezy.

Při genetickém určení původu předků společnost na základě požadavku objednatele uplatněného osobně, telefonicky, e-mailem, faxem nebo vyplněním elektronického objednávkového formuláře provádí genetickou analýzu biologického materiálu, jehož vzorek objednatel společnosti předává v zabezpečené a řádně označené odběrové soupravě DNA Collector. Výstupem této analýzy je certifikát o analýze a text vysvětlující základy genetické genealogie, případně porovnání zjištěného výsledku s veřejně dostupnými databázemi.

Také určení otcovství je realizováno pouze na objednávku zákazníka. Výstupem testu otcovství je expertní posudek konstatující existenci či neexistenci genetické shody v přímé příbuzenské linii mezi otcem a osobou, jež má být jeho potomkem. Zmíněný posudek rovněž obsahuje prohlášení jeho zpracovatele, podle kterého při všech operacích bylo se zpracovávaným biologickým materiálem nakládáno jako s citlivými údaji, a ujištění, že sekundární vzorky pocházející z předaného biologického materiálu budou protokolárně dezintegrovány, což se děje po skončení zákonem stanovené záruční doby. Nespotřebované primární vzorky jsou klientům odevzdávány zpět spolu s expertizními posudky. Informace o zpracování nestandardních vzorků, nacházejících se na zubních kartáčcích, nedopalcích cigaret, žvýkačkách, věcech osobní potřeby apod., která je uvedena v ceníku služeb společnosti v souvislosti s testy paternity, je toliko reprezentativním výčtem služeb, provedeným z marketingových důvodů. Potenciálním zákazníkům společnosti se tímto způsobem prezentuje odborná kvalifikace a erudice společnosti.

Při identifikaci odesílatele anonymních dopisů společnost zpracovává obvykle popis DNA vzorku ze slin. Detekce spermatu či krve je postup, jehož cílem je zjištění, zda dodaný biologický materiál je sperma nebo krev či cokoliv jiného. Specifickým průkazem spermatu se prokazuje, jestli například na prostěradle je sperma, zda zkoumané sperma je lidské, nebo zvířecí, a opatřuje se standardní popis vzorku, nedochází však k určení konkrétního jedince. Popisem zachyceného vzorku z dodaného materiálu společnost zajistí důkaz, který je poté předán objednateli, jenž jím dále disponuje. Postupy používané při

testování jsou specifikovány příručkou kvality, jež je ve společnosti zavedena. Uvedených testů společnost provedla v letech 2007 až 2008 asi sto ročně, což činí zhruba pět procent objemu její činnosti.

Určování příbuzenského vztahu, včetně stanovení vaječnosti dvojčat, je realizováno stejnými postupy jako určování otcovství, ale získané DNA profily jsou vyhodnocovány podle odlišných statistických vzorců.

Kontrolující se zaměřili na dodržování povinností při zpracovávání osobních údajů v souvislosti s předáváním biologických vzorků společnosti objednateli analýz DNA. Objednatelé objednávkou zároveň stanoví, v jakém rozsahu budou vzorky nesoucí osobní údaje zpracovány. Objednávka zákazníka je dokumentována v knize zakázek, která je jednou ze základních dokumentačních pomůcek společnosti. Ohledně každé zakázky zpracovávané společností se v ní eviduje číslo jednací, datum, kdy byla zakázka doručena do společnosti, popis objednávky, jméno a příjmení objednatele, určení zpracovatele zakázky, datum skončení zakázky, předání zakázky a termín provedení příslušné platby objednatelem. V knize zakázek se případně také uvádějí poznámky, které zakázku blíže charakterizují. Záznamy v knize zakázek je povinností v souladu s pravidly stanovenými příručkou kvality provádět ručně, nesmí být sepisovány na počítači. Subjekt osobních údajů podepisuje požadavkový formulář, čímž vydává souhlas s objednaným rozsahem zpracování osobních údajů nebo oznamuje společnosti, že příslušný souhlas se zpracováním osobních údajů byl dán. Zpracovávané osobní údaje jsou ve společnosti uchovávány v tištěné a elektronické podobě pouze po nezbytně nutnou dobu, kterou je lhůta šesti měsíců a tří týdnů. Tři týdny je doba pro zpracování biologického vzorku podle příslušné smlouvy o dílo, šest měsíců je lhůta, v níž společnost drží biologický vzorek po předání díla z důvodů možné reklamace v průběhu šestiměsíční záruční doby.

Před každým z výše zmíněných zpracování genetických vzorků objednatel od společnosti obdrží požadavkový formulář, informaci pro zákazníky, zálohovou fakturu, odběrovou soupravu a návod k jejímu použití. Mezi nimi je významná zejména „Informace pro zadavatele analýzy DNA za účelem testu otcovství, geneticko-genealogického zkoumání či jiného podobného úkonu“. Jejím prostřednictvím jsou subjekty údajů vyrozuměny o nakládání se vzorky DNA a jinými osobními údaji ve společnosti. Subjekty údajů jsou mimo jiné informovány, jaké osobní údaje společnost zpracovává, jakými způsoby se tak děje, jak jsou testované vzorky označovány, v jakém právním režimu zpracování probíhá, včetně poučení o tom, že odebrané vzorky DNA lze zpracovávat pouze se souhlasem dotčených osob, po jakou dobu budou testované vzorky ve společnosti uchovány, a též je jim sděleno, že po uplynutí záruční doby budou zpracovávané údaje zlikvidovány nebo jejich likvidace bude provedena dříve, pokud o to objednatel požádá. Objednatelům je uvedenou informací poskytnuto také úplné poučení ve smyslu §§ 12 a 21 zákona o ochraně osobních údajů. Všichni zaměstnanci společnosti jsou povinni zachovávat mlčenlivost o skutečnostech týkajících se činnosti firmy, včetně zpracování osobních údajů. Případné neoprávněné nakládání s dokumenty vytvořenými v rámci firmy by bylo považováno za hrubé porušení pracovní kázně. Dokumenty, které se odesílají zákazníkům, musí být před odesláním převedeny do formátu PDF. Data na firemních osobních počítačích se zálohují, přičemž obvyklým cyklem zálohování je jeden týden. S cílem zpracovávat jenom přesné osobní údaje společnost jako preventivní opatření zavedla a udržuje systém kvality podle normy ISO 9001:2000.

Společnost odebrané biologické vzorky v průběhu jejich zpracování důsledně eviduje a označuje, což se projevuje již při odběru srovnávacích vzorků pro DNA analýzu, kdy zákazník musí krabičku obsahující tampony se srovnávacími vzorky opatřit přelepkami zabraňujícími neoprávněným manipulacím a jednoznačně ji označit, přičemž toto označení zároveň uvede do formuláře „Požadavek na analýzu DNA“. Po skončení analýzy se ústní stěry (primární vzorky) zaslané na expertizu vracejí objednateli spolu s písemným vyhotovením expertizy. Vzorky, které jsou ve společnosti uchovávány po nezbytně nutnou dobu, jsou poté protokolárně likvidovány. Informace o průběhu a výsledcích zkoumání se předávají pouze objednatelům nebo osobám, které jsou objednateli k takovému převzetí písemně pověřeny. Po ukončení testů je zakázáno provádět dodatečné úpravy v záznamech o jejich průběhu. Doplňky a změny chybně napsaných údajů se provádějí přeškrtnutím původního údaje tak, aby zůstal čitelný, a doplněním správného údaje se šifrou pracovníka, jenž údaj opravil, a datem.

Společnost zpracovává základní identifikační údaje svých zákazníků za účelem splnění povinnosti průkaznosti účetních dokladů. K tomu vytvořila formuláře objednávek s určitými předepsanými údaji, které však objednatelé nemusí vyplňovat. Tyto údaje jsou uchovávány po dobu stanovenou příslušnými zákony. K ochraně osobních údajů ve společnosti přispívá rozsáhlá vnitřní normotvorba, která upravuje veškeré postupy pracovníků při zpracování osobních údajů objednatelů.

V době zahájení kontroly nebylo zpracování osobních údajů, které společnost provádí v rámci svých komerčních aktivit, písemně oznámeno Úřadu.

Kontrolou bylo zjištěno porušení zákona o ochraně osobních údajů pouze z důvodu, že společnost jako správce zpracovávala osobní údaje, aniž by tuto skutečnost písemně oznámila Úřadu před zpracováváním osobních údajů, čímž nerespektovala ustanovení § 16 odst. 1 tohoto zákona, a byla jí tak Úřadem uložena pokuta ve správním řízení.

3. KONTROLA PLNĚNÍ POVINNOSTÍ ODPOVĚDNÝCH SUBJEKTŮ VYPLÝVAJÍCÍCH Z NOVÝCH PRÁVNÍCH PŘEDPISŮ NAVAZUJÍCÍCH NA TRANSPOZICI MEZINÁRODNÍCH DOKUMENTŮ ZÁVAZNÝCH PRO ČESKOU REPUBLIKU

Kontroly plnění povinností správce při zpracování provozních a lokalizačních údajů (zákon č. 127/2005 Sb.) se zaměřily na zpracování provozních a lokalizačních údajů z veřejně dostupných služeb elektronických komunikací a veřejných komunikačních sítí, včetně uchovávání pro účely vyšetřování, odhalování a stíhání závažných trestných činů.

V termínu stanoveném kontrolním plánem byly provedeny kontroly ve čtyřech obchodních společnostech, dodatečně ve 4. čtvrtletí byla ještě provedena další kontrola. Dodatečná kontrola byla provedena v zájmu získání dostatečné vypovídací hodnoty kontrolních zjištění. Prověřeny tak byly všechny druhy služeb, u nichž je ze zákona povinnost uchovávat provozní a lokalizační údaje, s výjimkou služeb mobilní telefonie.

Všechny kontroly byly provedeny jako kontroly dodržování všech relevantních povinností stanovených zákonem o ochraně osobních údajů a zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, ve znění pozdějších předpisů, při zpracování osobních údajů podle § 97 odst. 3 zákona o elektronických komunikacích.

V žádné z kontrol nebylo zjištěno porušení zákonem stanovené povinnosti. Provozní a lokalizační údaje odpovídající povaze služeb poskytovaných kontrolovanými jsou uchovávány v souladu se zákonem, tj. logicky odděleně od jiných a po dobu stanovenou zákonem o elektronických komunikacích, i když tři z kontrolovaných stanovili dobu uchování na dolní hranici zákonného rozpětí a dva na horní. Dále bylo u čtyř kontrolovaných zjištěno, že se na ně s žádostmi podle § 97 odst. 3 zákona o elektronických komunikacích obrací Policie České republiky; u pátého taková žádost zjištěna ke dni ukončení kontroly nebyla.

4. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V SCHENGENSKÉM INFORMAČNÍM SYSTÉMU

V období od 22. října 2009 do 3. prosince 2009 proběhla státní kontrola zpracování osobních údajů v Schengenském informačním systému. Podnět k zařazení této kontroly do plánu kontrol na rok 2009 vzešel z jednání společných dozorových orgánů (JSA Schengen), které se uskutečnilo v prosinci roku 2007. Česká republika k Schengenskému informačnímu systému přistoupila dnem 1. září 2007, a proto se Úřad na této koordinované inspekci podílel.

V souladu s doporučením expertní komise pro Schengenské hodnocení členských států na úseku ochrany osobních údajů proběhla rovněž kontrola Ministerstva zahraničních věcí, a to v termínu od 30. června 2009 do 16. prosince 2009. Předmětem kontroly bylo dodržování povinností stanovených zákonem č. 101/2000 Sb. při zpracování osobních údajů v souvislosti s vízovým řízením v zastupitelských úřadech České republiky. Kontrolou bylo zjištěno porušení zákona.

III. VÝSLEDKY KONTROL Z KONTROLNÍCH PLÁNŮ Z PŘEDCHOZÍCH LET UKONČENÝCH V ROCE 2009

1. KONTROLA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ NÁVŠTĚVNÍKŮ POSLANECKÉ SNĚMOVNY PARLAMENTU ČESKÉ REPUBLIKY KANCELÁŘÍ POSLANECKÉ SNĚMOVNY PČR

Kontrola proběhla v roce 2007 a bylo konstatováno porušení ustanovení § 5 odst. 1 písm. e) zákona o ochraně osobních údajů. Kancelář se odvolala s poukazem na výjimku vzhledem k ochraně utajovaných skutečností. Předseda námitku uznal a předal věc k došetření. Kontrolující pokračovali v kontrole, při které byla dohodnuta změna režimu a zavedení dvou databází, neboť původní databáze byla používána k různým účelům, a tudíž i doba uchovávání údajů byla u každé z nich různá. Kontrola byla ukončena v únoru roku 2009 a závěrem nebylo konstatováno porušení zákona.

2. ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ ZA PODMÍNEK NASAZENÍ SLEDOVACÍCH SYSTÉMŮ

V roce 2008 Úřad, po zkušenostech z předchozích období a v návaznosti na nárůst tlaku na provozování monitorovacích systémů a jejich nasazování v různé úrovni, často způsobem zasahujícím do zájmu jednotlivce na ochranu jeho soukromí, zaměřil své kontrolní aktivity i do této oblasti.

V období od 5. prosince 2008 do 5. března 2009 byla provedena kontrola soukromé společnosti, která byla náhodně vybrána (šlo o významnou reklamní agenturu). Při kontrole bylo zjištěno, že společnost žádnou databázi hostů nevede, protože zaměstnanci si pro své návštěvy sami přicházejí a za jejich bezpečnost odpovídají.

3. OCHRANA SPOTŘEBITELE

V návaznosti na rostoucí zájem dodavatelů i uživatelů technologií umožňujících rychlou a bezpečnou identifikaci subjektu údajů Úřad registruje celospolečenský zájem po vytvoření pravidel, která by omezila zásah do soukromí fyzické osoby na nezbytné minimum při zpracování osobních údajů v souvislosti s používáním čipových karet a karet vybavených RFID technologií.

V období od 16. července 2008 do 2. června 2009 proto Úřad prováděl kontrolu dopravního podniku středočeského města, který technologii čipových zákaznických karet využívá.

4. KONTROLA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ OBYVATEL BYTOVÉHO DOMU

V době od 10. ledna 2008 do 4. prosince 2009 probíhala kontrola stavebního bytového družstva. Kontrola se zaměřila na plnění povinností správce, případně zpracovatele, při zpracování osobních údajů členů družstva, nájemníků bytů, vlastníků bytů a podnájemníků. Kontrola probíhala i se zřetelem na novelu zákona o ochraně osobních údajů č. 170/2007 Sb. účinnou od 1. září 2007.

IV. KONTROLY ZAHÁJENÉ V ROCE 2009 NA POKYN PŘEDSEDY

Praxe zahajování kontrol na základě rozhodnutí předsedy se osvědčuje u závažných aktuálních kauz už od roku 2007. K takovým rozhodnutím předsedy Úřadu docházelo i v roce 2009.

1. KONTROLA PLNĚNÍ POVINNOSTÍ STÁTNÍHO ÚSTAVU PRO KONTROLU LÉČIV, a to na základě závažnosti podnětu České lékárnické komory v tom směru, zda činností SÚKL nebo v souvislosti s ní nedochází k porušení povinností správce, případně zpracovatele, podle zákona č.101/2000 Sb. v souvislosti s provozem centrálního úložiště elektronických receptů a vzhledem k předpokladu, že vzniká mimořádně rozsáhlá databáze citlivých údajů.
Kontrola byla ukončena v srpnu roku 2009 a shledala porušení zákona o ochraně osobních údajů.

2. KONTROLA POSTUPŮ MINISTERSTVA VNITRA ČR A MINISTERSTVA SPRAVEDLNOSTI ČR

Dne 5. února 2009 předseda vydal pokyn k zahájení kontroly zpracování osobních údajů v rámci plnění povinností podle zákona o ochraně osobních údajů na Ministerstvu vnitra a Ministerstvu spravedlnosti při vedení a využívání informačního systému evidence obyvatel.
Bezprostředně na základě tohoto pokynu byly provedeny 3 kontroly:
– kontrolovaný subjekt: Ministerstvo vnitra: 18. června 2009 – 27. července 2009,
– kontrolovaný subjekt: Obvodní soud pro Prahu 4: 11. března 2009 – 9. června 2009,
– kontrolovaný subjekt: Ministerstvo spravedlnosti: 12. srpna 2009 – 22. října 2009.

Na Ministerstvu vnitra nebylo zjištěno porušení povinnosti při zpracování údajů o osvojení. V resortu Ministerstva spravedlnosti bylo zjištěno porušení povinnosti podle § 5 odst. 1 písm. c) a podle § 13 odst. 1, 2 a 3 zákona o ochraně osobních údajů při využívání osobních údajů informačního systému evidence obyvatel.

Na základě těchto kontrol a několika dalších byla v roce 2009 zahájena dvě správní řízení.

3. KONTROLA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ V RÁMCI PLNĚNÍ POVINNOSTÍ SPRÁVCE V SOUVISLOSTI S PROVOZEM KAMEROVÉHO SYSTÉMU

podle zákona č. 101/2000 Sb., o ochraně osobních údajů, který provozoval subjekt Prácheňské sanatorium, o. p. s. Kontrola proběhla na základě podnětu veřejného ochránce práv JUDr. Otakara Motejla. Sanatorium se specializuje na klienty s Alzheimerovou chorobou. Vzhledem k tomu, že se v sanatoriu neuchovávají záznamy z kamer a kamery pracují pouze v on-line provozu, nejsou provozovány v režimu, na nějž je aplikovatelný zákon o ochraně osobních údajů. Při kontrole bylo zjištěno, že vedení sanatoria o pořizování a uchovávání záznamu uvažuje, proto s ním byl tento záměr v rámci kontroly konzultován a bylo upozorněno na povinnosti, které by z toho pro sanatorium vyplynuly.

4. KONTROLA DODRŽOVÁNÍ POVINNOSTÍ KANCELÁŘE VICEPREMIÉRA PRO EVROPSKÉ ZÁLEŽITOSTI

při zpracovávání osobních údajů účastníků summitu EU–USA, který se konal dne 5. dubna 2009 v Praze.

V médiích se opakovaně objevily informace o úniku osobních údajů účastníků pražského summitu EU–USA, který se konal dne 5. dubna 2009. Podle některých zdrojů mělo být možné se na veřejně přístupném počítači v pražském hotelu dostat k osobním údajům přibližně 200 účastníků tohoto summitu. Podnět neoznačil žádný subjekt odpovědný za zpracování osobních údajů.
– První kontrolovaný subjekt: Gestin Holding, a. s.

Kontrola ve dnech 24. dubna 2009 – 6. května 2009 nezjistila porušení povinností uložených kontrolovanému zákonem o ochraně osobních údajů; na základě poznatků z této kontroly byla provedena kontrola u jiného subjektu.
– Druhý kontrolovaný subjekt: Úřad vlády České republiky

Kontrola ve dnech 4.–26. května 2009 zjistila porušení povinností uložených Úřadu vlády ustanoveními: §§ 9, 10 a § 13 odst. 1 zákona o ochraně osobních údajů. V roce 2009 nebylo správní řízení pravomocně ukončeno.

5. KONTROLA SPOLEČNOSTI MEDIASERVIS, s. r. o.,

v souvislosti s plněním povinností dodavatele pro předplatné a pro doručování předplaceného periodického tisku. Kontrola byla zaměřena na dodržování povinností správce týkající se zpracování osobních údajů předplatitele a odběratele periodického tisku.

Společnost pracuje jako zpracovatel osobních údajů předplatitelů a odběratelů periodického tisku pro správce těchto údajů, konkrétního vydavatele. Sama společnost nepoužívá osobní údaje předplatitelů a odběratelů k marketingovým účelům, i když by tak činit vzhledem k ustanovení § 5 odst. 5 zákona o ochraně osobních údajů mohla. Společnost byla pouze upozorněna na nepřesnosti v informování klientů v obchodních podmínkách. Porušení zákona nebylo kontrolou zjištěno.

6. KONTROLA SPOLEČNOSTI GOOGLE CZECH REPUBLIC,
jejímž cílem bylo prověřit dopady zákona č. 101/2000 Sb., o ochraně osobních údajů, na zpracování informací shromažďovaných a dále zpracovávaných v souvislosti s poskytováním služby Google Street View.

Pokynem předsedy ze dne 2. července 2009 byla zahájena kontrola služby Google Czech Republic, s. r. o., se zaměřením na službu Google Street View.

– Kontrolovaný subjekt: 3.–5. srpna 2009 Google Czech Republic, s. r. o.

Odpovědnost kontrolovaného subjektu při pořizování obrazových záznamů s osobními údaji nebyla zjištěna, proto byl prostřednictvím zahraničního odboru opakovaně kontaktován příslušný dozorový orgán v SRN, jemuž byly zjištěné poznatky postoupeny, a bylo mu navrženo prověřit zpracování, za něž byl odpovědný subjekt sídlící na území SRN a nezastoupený v ČR.

Na základě stížností občanů a žádosti **Google Inc.** o registraci se uskutečnila jednání o provozování služby Street View, která dosud nebyla ukončena.

V. KONTROLY ZAHÁJENÉ NA POKYN PŘEDSEDY V LETECH PŘEDCHÁZEJÍCÍCH A UKONČENÉ V ROCE 2009

Rovněž v případě kontrol zahájených na základě pokynů předsedy Úřadu se často nepodaří kontrolu ukončit za jednoroční období, a tak některé kontroly přecházejí do následujících let.

V roce 2008 šlo o kontrolu Fondu ohrožených dětí, která byla zahájena 27. září 2008 a ukončena dne 15. ledna 2009 se závěrem, že Fond ohrožených dětí ve své praxi porušoval zákon o ochraně osobních údajů. Byla uložena nápravná opatření.

POZNATKY INSPEKTORŮ Z KONTROLNÍ ČINNOSTI

VYUŽÍVÁNÍ EVIDENCE OBYVATEL V RESORTU MINISTERSTVA SPRAVEDLNOSTI

Informační systém evidence obyvatel (dále jen „evidence obyvatel“) je zejména v důsledku právní úpravy podmínek jeho využívání nejrůznějšími úředními instancemi jedním z nejživějších zpracování osobních údajů prováděných v působnosti a odpovědnosti veřejné správy a jiných orgánů státní moci v České republice. I proto Úřad prověřoval kontrolou v roce 2009 dvě stížnosti na zpracování osobních údajů v evidenci obyvatel. Stěžovatelka A. P. napadla přesnost zpracování. Podnět podala rovněž zástupkyně veřejného ochránce práv, a to v rámci šetření stížnosti manželů M. na používání údajů evidence obyvatel ve věci trestně stíhané biologické matky jejich osvojeného dítěte k opakovanému zaslání dopisu na adresu jimi osvojeného dítěte. Tento podnět směřoval kromě Ministerstva vnitra také do resortu Ministerstva spravedlnosti. Stěžovatelka shledala počet zaměstnanců Obvodního soudu I., kteří pracují s evidencí obyvatel, neúnosně vysokým a zakládajícím podezření z nedodržování pravidel ochrany osobních údajů.

Předseda Úřadu dospěl k závěru, že je nezbytné prověřit postupy Ministerstva vnitra a Ministerstva spravedlnosti pro aplikaci § 175a zákona č. 6/2002 Sb., o soudech a soudcích, upravující podmínky pro poskytování údajů z evidence obyvatel s ohledem na právní rámec povinností správce podle zákona o ochraně osobních údajů. Na tomto základě zahájil v roce 2009 jeden kontrolní tým celkem 8 kontrol zaměřených na evidenci obyvatel, z nichž šest rovněž ukončil. S výlučným zaměřením na zpracování osobních údajů získaných z evidence obyvatel a poskytování (zpřístupňování) osobních údajů z tohoto systému bylo kontrolováno šest soudů a Ministerstvo spravedlnosti.

Kontroly byly zahájeny u **Obvodního soudu I**. Tato kontrola se uskutečnila v přímé reakci na podnět zástupkyně veřejného ochránce práv. Podezření stěžovatelky se potvrdilo – bylo zjištěno porušení povinností uložených Obvodnímu soudu I. v ustanovení § 13 odst. 1, 2 a 4 zákona o ochraně osobních údajů. Obvodnímu soudu I. byla uložena čtyři opatření k nápravě.

V zájmu objektivity byly dále uskutečněny **kontroly jednoho z krajských soudů, dvou městských soudů a dvou okresních soudů**. Jedním okresním soudem byl ten, u něhož Ministerstvo spravedlnosti uvedlo absolutně nejvyšší počet aktivních uživatelských oprávnění pro evidenci obyvatel. Druhý nejvyšší počet oprávnění byl evidován u Městského soudu II. a třetí nejvyšší u nejdříve kontrolovaného Obvodního soudu I. Současně bylo dbáno na to, aby prověřovaný soubor soudů byl reprezentativní také zeměpisně. Při jedné kontrole byly získány relevantní poznatky o praxi u jednoho dalšího okresního soudu, která vykazovala shodné vady jako u kontrolovaného krajského soudu.

Ve všech kontrolách byly shodně prověřovány odpovídající povinnosti při zpracování osobních údajů stanovené zákonem o ochraně osobních údajů a zákonem č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „zákon o evidenci obyvatel“), za použití zákona č. 6/2002 Sb., o soudech, soudcích, přísedících a státní správě soudů a o změně některých dalších zákonů (zákon o soudech a soudcích), ve znění pozdějších předpisů, a několika dalších zákonů.

Při kontrolách byly používány auditní záznamy, které vede a poskytlo Ministerstvo vnitra podle § 3 odst. 8 zákona o evidenci obyvatel. Stejný postup byl použit i pro kontrolu na Ministerstvu spravedlnosti. Prověřeno bylo celkem 96 086 řádků záznamů o přístupech do evidence obyvatel, které obsahují údaj rozhodující pro vyhledávání příslušného obyvatele, identifikační údaje přístupu a důvod a konkrétní účel přístupu, tj. vyhledávání. S originální spisovou dokumentací nebo evidenčními pomůckami spisové služby byly prověřeny v několika případech vzorky auditních záznamů definované

za použití ČSN ISO 2859-1, v ostatních všechny záznamy. Výběr z vzorků byl volen tam, kde prověřovaný soubor obsahoval více než 10 000 řádků. Prověřeno bylo celkem 470 aktivních uživatelských oprávnění. Prověřování bylo úspěšné, pokud byla v auditních záznamech uvedena, nebo dodatečně z evidenčních pomůcek zjištěna, spisová značka. V ostatních případech bylo dohledání důvodu dotazu buď pracovně náročné, nebo nerealizovatelné.

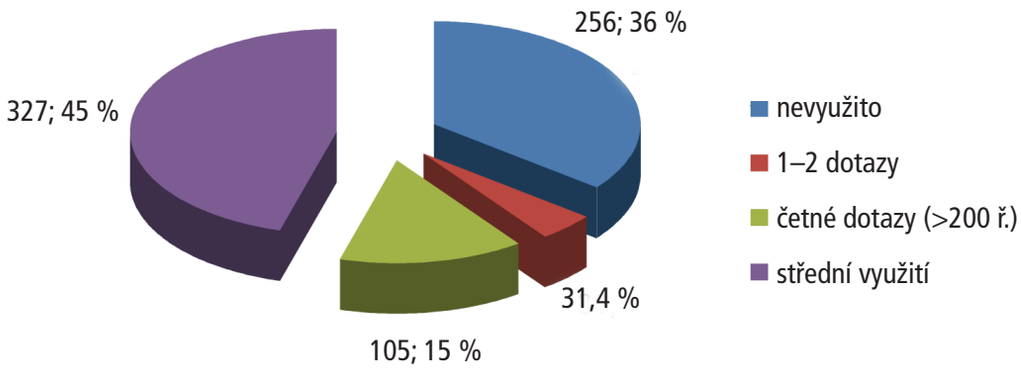
Ve všech kontrolách Úřad shledal, že struktura auditních záznamů, které byly pro účely kontroly poskytnuty, neumožňuje – až na výjimky – individuálně posuzovat splnění podmínky stanovené v ustanovení § 175a odst. 5 zákona o soudech a soudcích, použít z poskytovaných údajů v konkrétním případě vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu. Dále byl nucen konstatovat, že prostředky používané soudem ke zpracování osobních údajů evidence obyvatel a způsob zpracování neumožňují vyhodnotit v žádoucím rozsahu plnění povinnosti podle ustanovení § 5 odst. 3 zákona o ochraně osobních údajů dbát při zpracování osobních údajů na základě zvláštního zákona práva na ochranu soukromého a osobního života subjektu údajů. Pochybnost o dostání této povinnosti nastala ve všech případech, kdy soudci nebo úředníci zásadně a paušálně vyhledávají všechny dostupné údaje o zájmové osobě a s ní spojených blízkých (vazebních) osobách.

I za těchto omezení byl pouze postup Okresního soudu I. shledán v plném souladu jak se zákonem o ochraně osobních údajů, tak se zákonem o evidenci obyvatel. U všech ostatních kontrolovaných soudů bylo zjištěno, že nepřijaly ve své působnosti žádné specifické opatření účinně zabraňující neoprávněnému používání osobních údajů evidence obyvatel – nepromítly zásady zabezpečení osobních údajů evidence obyvatel do místních podmínek soudu a nezajistily dokumentaci vazby prováděného zpracování na spisovou dokumentaci, která je u nich vytvářena, ani jinak nevymáhaly podmínky stanovené v § 175a odst. 5 zákona o soudech a soudcích, použít z poskytovaných údajů v konkrétním případě vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu. Nebránily tak používání osobních údajů evidence obyvatel nad rámec aktuálně plněného služebního úkolu odpovídajícího pracovní pozici ve smyslu ustanovení § 13 odst. 4 písm. c) zákona o ochraně osobních údajů. Tím porušily povinnost podle § 13 odst. 1 zákona o ochraně osobních údajů a povinnost podle § 5 odst. 1 písm. f) téhož zákona.

Opakovaně byl zjištěn a konstatován také stav, že v rámci automatizovaného zpracování osobních údajů evidence obyvatel soud nezajistil, aby byly pořizovány elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly tyto osobní údaje vyhledávány. Nezajistil rovněž řádné dokumentování prověřovaného zpracování. V důsledku toho bylo zpětné prověřování jednak pracovně velmi náročné, jednak nebylo možné prověřit důvod vyhledávání ve všech případech. Někdy bylo možné dovodit důvod pouze na základě opětovného zadání identického dotazu do evidence obyvatel, někdy nevedl ani tento postup k doložení důvodu vyhledávání. Pouze v případě Okresního soudu I. bylo zjištěno, že s ohledem na zvolenou a důsledně používanou organizaci využívání evidence obyvatel, tj. zejména na to, že držitel oprávnění nedisponuje zpravidla osobními údaji zájmové osoby nad rámec údajů uvedených v Žádosti o šetření v ústřední evidenci obyvatel, jsou důsledky neodpovídající struktury auditních záznamů vytvářených Ministerstvem vnitra u tohoto soudu minimalizovány.

U Obvodního soudu I. bylo dále shledáno, že soud nedisponuje přiměřenou dokumentací přijatých a provedených technicko-organizačních opatření k zajištění ochrany osobních údajů získávaných z evidence obyvatel. U tohoto soudu nebyla stejně jako u Městského soudu I. uspokojivě zajištěna správa uživatelských oprávnění; jediným důvodem ke zrušení uživatelského oprávnění bylo ukončení pracovního poměru. Oprávnění bylo udržováno jako aktivní a platné i několik týdnů po dni ukončení pracovního poměru. Stejná situace byla konstatována u Okresního soudu II. Oprávněním disponovaly i osoby, které nepotřebují osobní údaje evidence obyvatel pravidelně využívat. Rovněž tento stav byl zjištěn u dalších čtyř soudů. Nevyužití přiděleného oprávnění bylo zjištěno u 256 z celkem 719 platných uživatelských oprávnění, přičemž s výjimkou jednoho soudu, kde vzorek tvořily záznamy za jediný měsíc, byly prověřovány záznamy vždy ze dvou kalendářních měsíců. Tři desítky uživatelů uskutečnily za sledovaná období pouze jeden nebo dva dotazy.

VYUŽÍVÁNÍ EVIDENCE OBYVATEL SOUDY



Žádný z těchto soudů nedoložil, že by se při volbě a provádění opatření k zabezpečení osobních údajů evidence obyvatel zabýval riziky ve smyslu ustanovení § 13 odst. 3 písm. c) zákona o ochraně osobních údajů. Soud dostatečně nevyužil k dosažení žádoucího účinku vedení auditních záznamů Ministerstvem vnitra pole „důvod dotazu" – neuložil oprávněným osobám povinnost jednoznačně a prokazatelně vázat vyhledávání na existující spisovou dokumentaci a vytvářet v případě potřeby části spisové dokumentace, které takovému účelu odpovídají (např. záznam ve spisu). Nezabýval se ani možností zaznamenávat využití evidence obyvatel v příslušné soudní aplikaci (ISAS a IRES). Žádný ze soudů, u nichž bylo konstatováno porušení zákona o ochraně osobních údajů, neprovedl do dne zahájení kontroly žádnou prověrku využívání osobních údajů evidence obyvatel a neměl stanovenu metodiku pro takové prověřování.

Na obecných závěrech nemohlo nic změnit ani zjištění, že kromě Okresního soudu I., kde byla zjištěna praxe vyhovující požadavkům na využívání osobních údajů evidence obyvatel jak podle zákona o evidenci obyvatel, tak podle zákona o ochraně osobních údajů, byli také u Okresního soudu II. a Městského soudu I. zjištěni uživatelé z řad soudců a zaměstnanců soudu, jejichž individuální postup splňuje veškeré zákonné podmínky uvalené na využívání evidence obyvatel – vyhledávají ve vazbě na spisovou dokumentaci a v rozsahu daném aktuální potřebou v rámci pracovního úkolu. Na straně druhé byli zjištěni uživatelé, u nichž nebylo možno zpětně úspěšně prověřit ani jeden dotaz.

Většina oprávněných uživatelů využívá možnosti zjišťování údajů i o vazebních osobách a všechny dotazy zadává zásadně v nejširším možném záběru. Úřad se pozastavil zejména nad vyhledáváním údajů o nezletilých dětech v souvislosti s nápadem návrhů na nařízení exekuce, aniž existovala jakákoliv indicie o potřebnosti takového úkonu. Úřad neshledal vhodnou praxi, kdy údaje o dětech předškolního věku jsou zakládány do spisové dokumentace k vymáhání pohledávky z městské hromadné dopravy nebo ze spotřebitelské půjčky ve výši nepřesahující hranici 1 500 Kč.

Vzhledem k rozsahu a formě dokumentování použití osobních údajů získávaných z evidence obyvatel nemohlo být kontrolou zjištěno, že by někdo u kteréhokoli z kontrolovaných soudů porušil svoji povinnost podle ustanovení § 15 odst. 1 zákona o ochraně osobních údajů, ani že by postupoval při zpracování osobních údajů evidence obyvatel jinak než za podmínek a rozsahu stanovenými mu kontrolovaným v návaznosti na věcně příslušné předpisy. Podmínky nebyly stanoveny zaměstnancům šesti soudů natolik těsně, aby bylo při absenci dokladu možno usuzovat na důvody vyhledávání a na formy a účely dalšího použití vyhledaných nebo ověřených osobních údajů.

Proto Úřad konstatoval, že v případě, že nebyly pořízeny tištěné výstupy z evidence obyvatel a vloženy do spisové dokumentace, není možné zjistit stav nad rámec toho, že nejsou vytvořeny místní podmínky pro řádné plnění povinnosti podle ustanovení § 5 odst. 1 písm. f) zákona o ochraně osobních údajů a § 8 odst. 2 písm. b) zákona o evidenci obyvatel.

Rovněž **kontrola na Ministerstvu spravedlnosti**, provedená ve stejném záběru jako kontrola u soudů, vyústila v konstatování, že povinnosti podle zákona o ochraně osobních údajů byly porušeny. Kromě problémů spojených s absencí vazby na spisovou nebo jinou přiměřenou dokumentaci bylo zjištěno zpracování osobních údajů, které nenaplňuje podmínku přípustnosti podle zákona o evidenci obyvatel a v jednom případě ani podmínku kauzální relevance – neexistuje zvláštní právní předpis umožňující zpracování s využitím dálkového přístupu k údajům evidence obyvatel, pro účely, pro které byly tyto údaje použity. Působnost ministerstva, v jejímž obecném rámci byly prokazatelně používány osobní údaje evidence obyvatel, zmocnění k využívání evidence obyvatel samoobslužným dialogovým vyhledáváním nezakládá. Tím, že se ministerstvo nezabývalo důsledky změny právních podmínek využívání osobních údajů evidence obyvatel s účinností od 1. 5. 2004, nenavrhlo změnu zvláštních právních předpisů ani nepřizpůsobilo rozsah jím prováděného zpracování osobních údajů platným zákonům, nastolilo stav, kdy opakovaně nedostává prováděné dialogové vyhledávání v evidenci obyvatel podmínkám stanoveným v § 5 odst. 1 písm. c) zákona o ochraně osobních údajů.

U ministerstva nebylo dbáno na přípustnost (legálnost) zpracování zakládaného zřízení individuálního přístupového práva. Uživatelé byli před zřízením oprávnění řádně poučeni; součástí poučení však nebyl závazný pokyn k vyplňování pole „důvod dotazu“ v dotazovacím formuláři. S úvodním poučením nebyla spojena ani instruktáž o způsobech dokladování důvodnosti využití evidence obyvatel. Činnost ministerstva ve vztahu k zaměstnancům zařazeným přímo na ministerstvu i ve vztahu k organizačním složkám resortu se omezila na zřizování uživatelských oprávnění, zajišťování ochrany infrastruktury a monitorování dostupnosti aplikace evidence obyvatel pro resortní uživatele.

Zjištěný stav je porušením povinnosti ministerstva jako subjektu odpovědného za zpracování přijmout bezpečnostní opatření podle § 13 odst. 1 a vést záznamy podle odst. 4 písm. c) zákona o ochraně osobních údajů. Dále bylo zjištěno, že ministerstvo nepostupuje při zpracování osobních údajů evidence obyvatel v souladu s podmínkami, jež stanoví zákon o evidenci obyvatel v ustanoveních § 8 odst. 2 písm. a) a b). Na druhé straně byl rozsah údajů zjišťovaných v evidenci obyvatel ve všech případech bez výjimky přizpůsoben pracovnímu úkolu: Nikdo z ministerstva nevyhledával údaje vazebních osob a v naprosté většině byla zjišťována adresa pobytu.

Z poznatků ze sedmi soudů různých stupňů a z Ministerstva spravedlnosti vyplývá, že ochraně osobních údajů evidence obyvatel není věnována odpovídající pozornost. Zda je Okresní soud I. bílou vránou, nebo reprezentantem menšiny, lze zjistit pouze individuálními kontrolami dalších soudů. Kontrolní zjištění z Městského soudu II., u něhož se očekávalo, že již zareaguje na výsledky prvních kontrol v resortu, nasvědčují možnosti první.

V návaznosti na výsledky pravomocně ukončených kontrol byla zahájena a ukončena první tři správní řízení.

ZDRAVOTNICTVÍ

Zásadní kontrolou, provedenou v roce 2009, byla **kontrola** prováděná ve **Státním ústavu pro kontrolu léčiv**, a to na základě podnětů, které Úřadu zaslalo Grémium majitelů lékáren a Svaz pacientů ČR. Předmětem této kontroly bylo dodržování povinností stanovených zákonem o ochraně osobních údajů v souvislosti se zahájením provozu centrálního úložiště elektronických receptů. Státní ústav pro kontrolu léčiv (Ústav) zřídil centrální úložiště elektronických receptů 31. prosince 2008 jako svou organizační složku. V prvním čtvrtletí roku 2009 probíhal zkušební provoz a na základě rozhodnutí Ústavu měly být k centrálnímu úložišti do 31. března 2009 připojeny všechny lékárny. Ke konci roku 2009 však tento předpoklad naplnilo jen něco přes polovinu lékáren.

Centrální úložiště bylo zřízeno dle zákona o léčivech, pro umožnění předepisování léčivých přípravků prostřednictvím elektronických receptů. Cílem zavedení elektronických receptů bylo především zamezit podvodům s listinnými recepty, snížení počtu návštěv pacientů u lékaře a zjednodušení práce lékaře i lékárníka. Zákon předpokládal, že elektronický recept bude využíván rovnocenně s lis-

tinným receptem. Rozhodující pro vystavení elektronického receptu měla být dohoda lékaře s pacientem o formě receptu, s níž bude pacient souhlasit. Vzhledem k tomu, že v průběhu roku 2009 žádný lékař neaktivoval připojení k centrálnímu úložišti, nebylo vystavování elektronických receptů realizováno, a proto nebyla shromažďována žádná data generovaná na základě elektronického předepisování léčivých přípravků. Nutno dodat, že v souladu se zákonem neměla být v centrálním úložišti žádná jiná data nežli data sloužící k vystavení elektronických receptů.

Na základě individuálního rozhodnutí Ústavu však došlo k rozšíření uplatnění nevyužitého centrálního úložiště. Do centrálního úložiště tak byla ukládána data o pacientech opisovaná z listinných receptů a dále data o pacientech, kterým byly prodány léčivé přípravky s omezením.

Kontrola se tedy zaměřila na zákonnost shromažďování osobních údajů pacientů, které byly Ústavu posílány lékárnami formou hlášení, a to o vydaných léčivých prostředcích na základě listinného receptu a o vydaných léčivých přípravcích s omezením.

Zákon o léčivech ukládá lékárnám a lékárníkům zajistit při výdeji léčivých přípravků evidenci jejich výdeje pomocí jejich kódů a tuto evidenci uchovávat po dobu 5 let. Dále jsou lékárny a lékárníci povinni poskytovat Ústavu údaje o vydaných léčivých přípravcích. Povinnost uchovávat informace o vydaných léčivých přípravcích na základě listinného receptu měly lékárny již podle předchozí právní úpravy. Ústav má dle zákona o péči o zdraví lidu právo na provádění dozorové kontrolní činnosti a v této souvislosti má právo se seznamovat i s osobními údaji pacientů. Novela zákona o léčivech tuto pravomoc Ústavu neomezila, ale ani nerozšířila. Ústavu tedy nebyla dána pravomoc shromažďovat osobní údaje, ale pouze informace o vydaných léčivých přípravcích. Ústav tak svým rozhodnutím překročil své kompetence dané mu zákonem. Kontrolující inspektor odmítl argumentaci Ústavu, že rozhodnutím o shromažďování informací o všech vydaných receptech, včetně osobních údajů pacienta, lékaře i lékárníka, plní požadavek sledovatelnosti a dohledatelnosti každého léčivého přípravku v celém řetězci od výroby až po konečného spotřebitele. Toto odmítá i příslušná směrnice EU č. 83/2001/ES, dle které cestu jednotlivých léčivých přípravků je nutno sledovat jen ve fázi distribuce, a ne ve fázi výdeje veřejnosti.

V rámci provedené kontroly bylo nutné se zabývat i dalšími požadavky na evidenci léčivých přípravků, jakou je mimo jiné i požadavek na plnění úkolu Ústavu zajistit předávání informací shromážděných v rámci systému farmakovigilance ostatním členským státům v Evropské lékové agentuře, a to v souladu s pokyny Komise a této agentury, nebo splnění povinnosti zajistit přehled o vydaných léčivých přípravcích ke splnění požadavku operativně a účinně a adekvátně v národním prostředí reagovat na opatření přijatá Evropskou komisí, Evropskou lékovou agenturou, dalšími orgány Evropské unie a WHO (World Health Organisation). Jedná se zejména o případy, kdy by Ústav stahoval léčivé přípravky z českého trhu v návaznosti na rozhodnutí jmenovaných orgánů a organizací. Kontrolou bylo konstatováno, že kompetence Ústavu v této oblasti nezahrnují zákonné zmocnění zpracovávat osobní údaje pacientů, lékařů a lékárníků. Kontrolující zcela odmítl argumentaci kontrolovaného, že shromažďování osobních údajů v souvislosti s evidencí léčivých přípravků vydaných na základě listinného receptu ukládá povinnost Ústavu při naplňování úkolů v oblasti cenové a úhradové agendy léčebných přípravků.

Kontrolující inspektor tedy v kontrolním protokolu konstatoval, že Ústavu není žádným zákonem uložena povinnost shromažďovat v centrálním úložišti ani nikde jinde osobní, resp. citlivé údaje pacientů formou hlášení o vydaných léčivých přípravcích na základě listinného receptu. Ústav tedy stanovil povinné poskytování osobních, resp. citlivých osobních údajů do centrálního úložiště lékárnám nad rámec zákona. Ústav stanovil tuto povinnost lékárnám a lékárníkům ve svém informačním prostředku – Věstníku, a to přes skutečnost, že dle § 9 písm. c) zákona o ochraně osobních údajů lze zpracovávat citlivé údaje pouze na základě zvláštního zákona. Rozhodnutí Ústavu však nemůže nahradit zákon a vůli zákonodárců v něm projevenou. Žádný zákon však Ústav nezmocnil ke shromažďování zdravotnických dat téměř všech občanů České republiky.

Ústav zpracování citlivých údajů stanovil svým opatřením, a to ve svém Věstníku. Takové stanovení zpracování citlivých údajů nebylo možné posoudit jako zpracování v souladu s § 9 písm. c) zákona

o ochraně osobních údajů, neboť zpracovávat citlivé údaje lze pouze na základě zvláštního zákona. Věstník Státního ústavu pro kontrolu léčiv zákonem není.

Kontrola se dále zaměřila na shromažďování a zpracovávání osobních údajů v souvislosti s výdejem léčivých přípravků bez lékařského předpisu s omezením. Jedná se o léčivé přípravky obsahující pseudoefedrin, které jsou zneužívány k výrobě drog. Kontrola se zaměřila na oprávněnost komunikace mezi lékárnou, resp. lékárníkem a centrálním úložištěm, v rámci které je v první fázi zjišťováno, zda ten který zákazník již v minulosti obdržel z některé lékárny léčivý přípravek s omezením a v jakém množství. Ve druhé fázi pak lékárna odesílá formou hlášení do centrálního úložiště údaje o právě provedeném výdeji s tím, že dále má možnost s těmito údaji provádět operace prohlížení, změny nebo zrušení záznamu. O zařazení léčivého přípravku do skupiny léčivých přípravků vydávaných bez lékařského předpisu s omezením rozhodl Ústav svým správním rozhodnutím, kterým ukládá lékárnám a lékárníkům při výdeji léčivého prostředku s omezením zjišťovat prostřednictvím dálkového elektronického přístupu v centrálním úložišti předchozí výdej, a to buď dle čísla pojištěnce (rodné číslo), nebo prostřednictvím identifikačních osobních údajů pacienta, včetně oprávnění požadovat ke kontrole průkaz pojištěnce či občanský průkaz.

Kompetence Ústavu k vydávání rozhodnutí v oblasti léčivých přípravků je odvozena ze zákona o léčivech. Na základě zákonného zmocnění upravilo Ministerstvo zdravotnictví vyhláškou č. 228/2008 Sb., o registraci léčivých přípravků, že v případě žádosti o zařazení přípravku mezi léčivé přípravky vydávané bez lékařského předpisu s omezením se předloží zdůvodnění navrhovaného způsobu výdeje a návrh omezujících opatření (např. kontrola věku, omezení počtu vydávaných balení, doporučení farmaceuta, evidence osob, evidence vydávaných balení). Povinnosti lékárnám a lékárníkům při výdeji léčivých přípravků bez lékařského předpisu s omezením upravuje a konkretizuje vyhláška Ministerstva zdravotnictví č. 378/2007 Sb. Ta ukládá lékárníkům, nikoliv Ústavu, povinnost při výdeji léčivého přípravku bez lékařského předpisu s omezením ověřit, zda jsou splněny podmínky omezení výdeje stanovené v rozhodnutí o registraci, ověřit totožnost osoby vyžadující výdej léčivého přípravku a poskytnout této osobě informace nezbytné pro bezpečné použití tohoto léčivého přípravku. Dále je lékárnám vyhláškou uložena povinnost vést evidenci výdeje těchto přípravků, a to v rozsahu jméno, příjmení, číslo pojištěnce nebo datum narození a krátký záznam o zdravotním stavu osoby, které byl přípravek vydán, včetně záznamu o provedení pohovoru, který by měl být v rozsahu nezbytně nutném pro posouzení indikace.

Z výše uvedeného vyplývá, že žádný právní předpis neumožňuje Ústavu, aby po lékárnách vyžadoval, a následně shromažďoval a dále zpracovával, osobní údaje osob, které lékárna vede v evidenci výdeje léčivého přípravku bez lékařského předpisu s omezením. Povinnost zpracovávat a uchovávat osobní údaje přísluší ze zákona výhradně lékárně, nikoliv Ústavu.

Ústav byl při shromažďování údajů z lékáren v pozici správce osobních údajů. Lékárny, v rámci zasílání dat do Ústavu, byly pro Ústav v roli zpracovatele.

Kontrolou bylo zjištěno, že Ústav nezabezpečil ochranu dat zasílaných z lékáren tak, aby k datům neměly přístup neoprávněné osoby, a to i z řad nelékárníků. Rovněž Ústav nezpracoval a nedokumentoval příslušná technicko-organizační opatření k ochraně těchto dat. Ústav se zcela distancoval od dohledu nad lékárnami jako svými zpracovateli a od jejich kontroly.

Na základě všech zjištění konstatoval kontrolující inspektor, že Ústav porušil povinnosti správce osobních údajů, a stanovil nápravná opatření k odstranění zjištěných nedostatků. Základem uložených opatření bylo opatření spočívající v povinnosti Ústavu neshromažďovat osobní a citlivé údaje osob v centrálním úložišti shromažďované prostřednictvím hlášení o výdeji léčivého přípravku na základě listinného receptu a dále prostřednictvím hlášení o výdeji léčivého přípravku bez lékařského předpisu s omezením. Dále stanovil Ústavu povinnost osobní a citlivé údaje již takto shromážděné zlikvidovat.

Ústav proti kontrolnímu zjištění podal řádný opravný prostředek. Ve svém podání zásadně nesouhlasil se závěry uvedenými v kontrolním protokolu. V druhoinstančním řízení předseda Úřadu námitkám kontrolovaného proti kontrolnímu protokolu nevyhověl a v plném rozsahu

závěry kontrolujícího inspektora potvrdil, včetně argumentace v nich obsažené. Konstatoval, že žádný právní předpis nezakládá oprávnění kontrolovaného zpracovávat v centrálním úložišti osobní údaje zjištěným způsobem. V téže věci bylo vydáno rovněž druhé rozhodnutí předsedy Úřadu, které řešilo námitku podanou proti uloženému opatření o likvidaci. Uložené opatření stanovilo Ústavu povinnost likvidovat ty osobní údaje uložené v centrálním úložišti, které jsou v něm uchovávány bez zákonného důvodu. Předseda této námitce nevyhověl a svým druhoinstančním rozhodnutím konstatoval, že dle kontrolních zjištění je uchovávání shromážděných osobních údajů nezákonné, a potvrdil tak v plném rozsahu kontrolní protokol.

Na základě pravomocného rozhodnutí předsedy Úřadu zaslal ředitel Ústavu kontrolujícímu inspektorovi zprávu o tom, že všechna uložená nápravná opatření akceptuje, a v termínu mu uloženém je splní.

Na základě pravomocného rozhodnutí zahájil Úřad se Státním ústavem pro kontrolu léčiv správní řízení pro podezření ze spáchání správního deliktu. Toto řízení nebylo do konce roku 2009 ukončeno.

Výsledky této mediálně sledované kontroly zcela zřetelně prokázaly, že Státní ústav pro kontrolu léčiv překročil své pravomoci a v rámci své činnosti, za tolerance Ministerstva zdravotnictví, opomenul práva pacientů na ochranu dat a jejich práva na soukromí. Potřeba chránit soukromí osob, ať už vývojové trendy budou jakékoli, zůstává základním úkolem nejenom pro ochránce dat, ale také pro ty, kterým leží na srdci základní práva a svobody. Nebudou-li brány v úvahu obavy o ochranu dat a soukromí, bude existovat skutečné nebezpečí, že budou podkopány nejzákladnější lidská práva a svobody. Nelze se přitom dovolávat např. nutnosti ochrany před osobami, které zneužívají léky k výrobě drog. Zcela jistě mělo být přijato jiné řešení, jak zabránit narkomanům ve zneužívání léků, nežli nezákonně zpracovávat osobní a citlivé údaje o většině občanů České republiky.

V oblasti ochrany osobních údajů a soukromí ve zdravotnictví se Úřad zabýval rovněž řadou podnětů, a to již v rámci **vyřizování dotazů, žádostí a poskytování konzultací**. Převážná část dotazů a konzultací v oblasti zdravotnictví se týká vedení zdravotnické dokumentace, tedy aplikace zákona č. 20/1966 Sb., o péči o zdraví lidu a prováděcích předpisů. Na Úřad se stále častěji obracejí pacienti, kterým nebylo umožněno nahlédnout do jejich zdravotní dokumentace, nebo mají podezření, že do jejich zdravotní dokumentace nahlížel někdo neoprávněný, či se domáhají toho, aby jejich zdravotní dokumentace byla předána novému ošetřujícímu lékaři. Svým způsobem Úřad supluje činnost příslušných dozorových orgánů.

Řada dotazů a žádostí o pomoc ale ve své podstatě směřuje k jednání zdravotnických zařízení a Úřad musí tazatele odkazovat na jiné instituce, zejména ČLK, příslušné zdravotnické odbory krajských úřadů apod. Mezi zvláštními žádostmi o poskytnutí konzultace byl například dotaz zaměstnance na postup nemocnice, která požaduje po svých zaměstnancích, kteří při své činnosti manipulují s opiáty, aby ke svým vzorovým podpisům založeným v tzv. opiátové knize připojili i svoji adresu bydliště. Tuto problematiku řeší zcela přesně zákon o návykových látkách a prováděcí vyhláška Ministerstva zdravotnictví o evidenci a dokumentaci návykových látek a přípravků. Je zarážející, že odborní pracovníci ve zdravotnictví, kteří mají oprávnění nakládat s opiáty, nemají znalosti o obsahu právního předpisu, dle kterého se mají ve své činnosti řídit.

Mezi žádosti o stanovisko Úřadu patřil i dotaz Generálního ředitelství Vězeňské služby, které požádalo Úřad o stanovisko k možnosti nahlížení veřejného ochránce práv do zdravotnické dokumentace vězněných osob a současně vyjádřilo svůj právní názor, že bez jejich souhlasu by docházelo k porušování zákona o ochraně osobních údajů. Vzhledem k tomu, že oprávnění veřejného ochránce práv vychází z příslušného ustanovení zákona o zdraví o péči lidu, není v tomto případě souhlas vězněných osob potřebný.

Úřad řešil v rámci registračního procesu a kompetence rozhodování o povolení k předávání osobních údajů do jiných států řadu žádostí, které se týkaly povolení k předávání osobních údajů pacientů

do třetích zemí v souvislosti s lékařským výzkumem. Jedná se o řešení problematiky související s výzkumy prováděnými ve zdravotnictví, kdy lékař podepíše smlouvu se společností, provádějící zdravotnický výzkum, se sídlem v zahraničí o provádění výzkumu léčebného procesu nebo léčivých přípravků. V rámci tohoto výzkumu jsou předávány informace o pacientovi. Většina požadavků se týká oprávněnosti předávání informací z výzkumu konkretizovaných na pacienta, tedy z hlediska zákona o ochraně osobních údajů se jedná o citlivé údaje. Úřad v této oblasti zastává zásadní postoj, že předávat osobní a citlivé údaje lze v tomto případě pouze s výslovným souhlasem pacienta.

Systém zdravotnictví je neoddělitelně propojen se zpracováním osobních a zejména citlivých údajů. Proto se Úřad v rámci své dozorové činnosti důsledně zabývá všemi podněty, dotýkajícími se tohoto odvětví. Na základě obdržených podnětů inspektoři Úřadu provedli v roce 2009 přes 15 šetření ve zdravotnických zařízeních a institucích, jejichž činnost se zdravotnictvím přímo souvisí.

Na základě stížnosti provedl inspektor Úřadu **šetření ve zdravotní pojišťovně**, která dle stěžovatele určila pouze bezhotovostní platební styk pro proplácení finančních prostředků při čerpání preventivních programů pojištěncem. Požadovala tedy od svých pojištěnců informace o jejich bankovním spojení, neboť hodlala hradit finanční prostředky pouze na bankovní účet pojištěnce. Současně určila, že tuto informaci požaduje ve formě fotokopie hlavičky bankovního výpisu, ne staršího než tři měsíce, se začerněnými informacemi o finančních operacích. Stěžovatel uvedl, že mu pojišťovna odmítla proplatit prokazatelné náklady vynaložené v souladu s podmínkami, a to v případě, že nemá zřízený bankovní účet. V průběhu šetření bylo zjištěno, že pojišťovna skutečně tuto podmínku určila. Podmínku zveřejnila na svých kontaktních místech a na svých internetových stránkách. Zdravotní pojišťovna tento postup přijala proto, aby byl příspěvek na preventivní léčbu poskytnut výhradně oprávněnému pojištěnci. Toto rozhodnutí bylo přijato na základě předchozích negativních zkušeností, kdy byl příspěvek zneužíván neoprávněnými osobami. V průběhu šetření ale bylo zjištěno, že v případě, kdy pojištěnec trvá na tom, že nepředloží informace o svém bankovním spojení, a žádá, aby úhrada byla provedena v hotovosti, je mu vyhověno. Problém spočíval v tom, že o této možnosti pojišťovna předem neinformovala a řádnou informaci v některých případech nepodávali ani zaměstnanci pojišťovny. Proto bylo inspektorem doporučeno, aby zdravotní pojišťovna změnila svoji informaci poskytovanou na kontaktních místech a na svých internetových stránkách i o možnost žádat o proplacení jinou formou. Současně bylo zjištěno, že v této souvislosti zdravotní pojišťovna shromažďuje od svých pacientů informace o jméně, příjmení, doručovací adrese, čísle účtu a datu vydání výpisu. Nad rámec svého oprávnění zpracovávat osobní údaje tedy zpracovávala osobní údaje v rozsahu číslo bankovního účtu a datum vystavení výpisu, ovšem se souhlasem pacienta. Dále bylo zjištěno, že zdravotní pojišťovna využívá informace o doručovací adrese k ověření bydliště pojištěnců ve své kmenové databázi. Důvodem byla zkušenost, že převážná většina pojištěnců neplní svoji zákonnou povinnost při změně bydliště nahlásit novou adresu své zdravotní pojišťovně. **Inspektor Úřadu neshledal v tomto postupu porušení zákona**.

Na základě podnětu provedl inspektor kontrolu ve fakultní nemocnici. Z této nemocnice odešli praktičtí lékaři, za něž nemocnice nezískala náhradu. Vzhledem k tomu, že nemocnice nebyla schopna zajistit zdravotní péči pro cca 5000 pacientů, rozhodla se, že tyto pacienty převede do péče jiného nestátního zdravotnického zařízení, které s tímto krokem souhlasilo. Nemocnice tedy zaslala pacientům dopis, který obsahoval informaci o tom, že není schopna zajistit zdravotní péči praktického lékaře, a proto **předává** jejich **zdravotnickou dokumentaci jinému** nestátnímu **zdravotnickému zařízení**. Dále v dopise vyzvala pacienty, aby v případě, že s tímto převedením k jinému registrujícímu lékaři nebudou souhlasit, tento nesouhlas písemně vyjádřili. Dopis byl nemocnicí vytištěn na hlavičkovém papíru nového nestátního zdravotnického zařízení. Společně s tímto dopisem byl v obálce přiložen i další inzertní leták, nabízející služby nestátního zdravotnického zařízení. Tím, že dopis byl psán na hlavičkovém papíru nového nestátního zdravotnického zařízení, oprávněně vznikl mezi pacienty dojem, že jejich registrace a předání jejich zdravotnické dokumentace se již uskutečnily.

V reakci na stížnosti mnoha pacientů a na základě zásahu inspektora Úřadu nemocnice celý proces převodu pacientů ihned ukončila. Nehledě na skutečnost, že podle obecného práva, upraveného v občanském zákoníku, samotné mlčení nebo nečinnost k předloženému návrhu samy o sobě neznamenají přijetí návrhu, by v případě realizace došlo nejen k významnému porušení práva pacientů na vlastní výběr ošetřujícího lékaře podle zákona o péči o zdraví lidu, ale z hlediska zákona o ochraně osobních údajů by došlo k neoprávněnému předání osobních údajů neoprávněnému správci.

Na základě stížnosti matky nezletilé pacientky provedl inspektor Úřadu kontrolu lékařky pediatričky. Matka nezletilé pacientky sdělila lékařce informaci, že si zvolila nového ošetřujícího lékaře, a požádala o zdravotnickou dokumentaci své dcery. Tento požadavek lékařka odmítla s tím, že zdravotnickou dokumentaci předá novému ošetřujícímu lékaři sama, a požádala o sdělení adresy nového zdravotnického zařízení. Postup lékařky byl v souladu se zákonem, dle kterého vede zdravotnickou dokumentaci ošetřující lékař, a v případě změny ošetřujícího lékaře je dosavadní lékař povinen předat nově zvolenému lékaři všechny informace potřebné pro zajištění návaznosti poskytování zdravotní péče. V praxi ovšem dochází převážně k předávání celé zdravotnické dokumentace.

V tomto případě však bylo zjištěno, že lékařka předala zdravotnickou dokumentaci kurýrní službě, a to na základě smlouvy o kurýrní službě, kterou má pediatrička uzavřenu s krajskou nemocnicí. Dle této smlouvy zabezpečuje kurýrní služba svoz a zpětný rozvoz biologických vzorků do laboratoří krajské nemocnice k provedení rozborů. Tato kurýrní služba krajské nemocnice tuto službu zajišťuje pro veškerá zdravotnická zařízení v krajském městě a okolí. Podle zvykového práva nad rámec smlouvy je kurýrní služba využívána k předávání písemností, včetně lékařských zpráv, nálezů a i zdravotnické dokumentace v podstatě mezi všemi lékaři v rámci města a okolí. Lékařka tedy pro **předání zdravotnické dokumentace novému ošetřujícímu lékaři** využila kurýrní službu. Dle ustálené praxe zdravotnickou dokumentaci vložila do zalepené obálky, označila adresou nového lékaře a tuto obálku položila ve zdravotnickém středisku na obvyklé místo. Tedy na místo, kam všichni lékaři ze střediska ukládají a kde si rovněž vyzvedávají zásilky, aniž by si od kurýra, který zásilky přebírá, nechali předání potvrdit. Ke škodě pacientky však v tomto případě došlo k situaci, kdy nebyla zásilka novému ošetřujícímu lékaři doručena. I přes snahu lékařky, která kontaktovala všechny lékaře ve městě a okolí, se zdravotnická dokumentace nezletilé pacientky nenašla. Tímto jednáním lékařka porušila zákonnou povinnost přijmout taková opatření, aby nemohlo dojít k neoprávněné ztrátě osobních údajů.

Součástí této kontroly bylo i zjištění, že příslušný dozorový orgán, kterým je v oblasti zdravotnictví odbor zdravotnictví příslušného krajského úřadu, neshledal ve skutku lékařky porušení zákona. K obdobnému závěru došla i místní revizní komise okresního sdružení České lékařské komory.

Stejný přístup k citlivým datům pacientů byl zjištěn u dvou lékařek specialistek v Praze. Obě lékařky, provozovatelky nestátního zdravotnického zařízení, využívaly ke své činnosti společné prostory, ve kterých se střídaly. Na základě podnětu bylo zjištěno, že zdravotnická dokumentace obou lékařek je uložena v neuzamčených registračních skříních, které byly umístěny v čekárně před ordinací. V rámci kontroly bylo zjištěno, že neuzamčené a v některých případech pootevřené registrační skříně, obsahující přes 600 zdravotních dokumentací pacientů obou lékařek, byly přístupné každému návštěvníkovi čekárny. Obě lékařky tak porušily ustanovení zákona o ochraně osobních údajů ukládajících povinnosti správci osobních údajů přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům. Na základě zjištění inspektora byla každé z lékařek uložena pokuta ve výši 50 000 Kč. Tato rozhodnutí však doposud nenabyla právní moci.

V průběhu roku 2009 přijal Úřad řadu stížností na **zabezpečení zdravotnické dokumentace**, kterou vedou větší zdravotnická zařízení, zejména nemocnice, v elektronické podobě. Podstatou stížností byla skutečnost, že v rámci zdravotnického zařízení je v neomezené míře umožněn přístup lékařů a zdravotnických pracovníků ke zdravotnické dokumentaci pacientů i v případě, že jim není poskytována zdravotní péče.

Inspektor Úřadu provedl v této věci kontrolu na velké poliklinice v Praze a rovněž v oblastní nemocnici. Důvodem pro obě kontroly bylo podezření z **neoprávněného nahlížení do zdravotnické**, elektronicky vedené **dokumentace** pacienta lékařem, který pacientovi neposkytoval žádnou zdravotní péči. Zdravotnická zařízení jsou povinna vést zdravotnickou dokumentaci svých pacientů, v listinné i v elektronické formě. Oprávnění přístupu do zdravotnické dokumentace upravuje zcela přesně příslušné ustanovení zákona o péči o zdraví lidu.

Obecně lze shrnout, že dle zákona mají právo nahlížet do zdravotnické dokumentace lékaři, zdravotní sestry a další odborní zdravotničtí pracovníci, kteří poskytují pacientovi zdravotní péči. Problematika nemocničních informačních systémů tedy spočívá v tom, jakým způsobem lze ošetřit přístup ke zdravotnické dokumentaci zdravotnickým pracovníkům tak, aby nebyla ohrožena péče o pacienta. V praxi to znamená, že nemocnice musí vyřešit problém, jak zajistit, aby každý lékař či jiný oprávněný zdravotnický pracovník měl v případě poskytování zdravotní péče kdykoliv přístup k informacím o zdravotním stavu pacienta a současně bylo zajištěno, že přístup nebude zneužit.

Dle zákona o ochraně osobních údajů je správce osobních údajů povinen přijmout taková technicko-organizační opatření, aby nemohlo dojít ani k nahodilému neoprávněnému přístupu k osobním údajům. Každý správce osobních údajů, který zpracovává osobní údaje automatizovaným způsobem, je povinen zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby, aby fyzické osoby oprávněné k používání systému měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění, zřízených výlučně pro tyto osoby, a dále je správce povinen pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo zpracovávány.

Zdravotnické zařízení tedy musí na straně jedné plnit svoji povinnost zabezpečit poskytování zdravotní péče, a to bez možného administrativního omezování přístupu k informacím o pacientovi, a současně musí plnit povinnosti dané zákonem o ochraně osobních údajů. Je akceptovatelné, jsou-li ve zdravotnickém zařízení přijata dostatečná technicko-organizační opatření, spočívající v omezení přístupu výhradně oprávněným zdravotnickým pracovníkům, ve správném přidělování administrátorských přístupů dle rozsahu oprávnění na základě přístupového jména a hesla, včetně logování všech přístupů a zpětné kontroly těchto přístupů, včetně stanovení pracovněprávní odpovědnosti konkrétních zaměstnanců.

V daných kontrolách bylo zjištěno, že na poliklinice v Praze nedošlo k neoprávněnému nahlížení. V kontrolovaných případech bylo zjištěno, že ani v případě polikliniky, ani nemocnice nebyly výše uvedené zásady porušeny. V oblastní nemocnici ale bylo na základě realizovaných technicko-organizačních opatření zjištěno a dokumentováno, že lékař nemocnice v několika případech neoprávněně nahlížel do zdravotnické dokumentace několika pacientů a tím porušil nejen pracovněprávní předpisy nemocnice, ale rovněž i ustanovení § 14 zákona o ochraně osobních údajů, neboť tím, že neoprávněně nahlížel do zdravotnické dokumentace pacientů, kterým neposkytoval zdravotnickou péči, zpracovával osobní údaje v rozporu s podmínkami a rozsahem stanoveným správcem, tedy nemocnicí. Nutno dodat, že tato činnost lékaře není skutkovou podstatou žádného přestupku ani správního deliktu, a lékař byl potrestán pouze v rámci pracovněprávního vztahu, tedy svým zaměstnavatelem.

Na základě provedených kontrol v oblasti zabezpečení osobních a citlivých údajů, které tvoří obsah zdravotnické dokumentace, lze shrnout, že přístup lékařů i kontrolních zdravotnických orgánů zůstává mnohdy stále v oblasti spíše zvykového práva a nereflektuje základní principy práva na ochranu dat pacientů.

ŠKOLSTVÍ

Kontrola znovu narazila na dávný problém rozsahu osobních údajů při přijímacím řízení. Vzhledem k tomu, že v současné době je přijímání do předškolních zařízení zcela v kompetenci dané mateřské školy nebo jeslí, je rozsah zpracovávaných osobních údajů dán pouze kritérii pro přijetí, které si dané zařízení s ohledem na konkrétní podmínky (málo míst a hodně uchazečů či naopak) vytváří: bydliště, zaměstnanost matky, věk, popř. počet sourozenců. Dále je nutné zpracovávat kontaktní údaje pro možnou komunikaci s rodiči. Všechny ostatní osobní údaje jsou nadbytečné. Tyto údaje v případě nepřijetí dítěte je možno uchovávat maximálně do šesti let dítěte, kdy nastupuje do základní školy, pokud by se mateřská škola domnívala, že se rodiče budou znovu ucházet o přijetí do dané mateřské školy. Jinak je třeba osobní údaje zlikvidovat neprodleně.

Kontrola také narazila na další starý problém: Existuje několik institucí, které mohou vyžadovat zpracovávané osobní údaje od všech státních i soukromých institucí, např. Policie ČR, NBÚ, BIS, popř. finanční úřady a také Odbor sociálně-právní ochrany dítěte. Pokud tedy osobní údaje škola zpracovává (i neoprávněně, po době nezbytně nutné pro jejich zpracování), musí je těmto institucím vydat, i když jsou mnohdy už zastaralé, a tudíž nepravdivé.

Pedagogicko-psychologické poradny (dále jen „poradna“) jsou určeny pro pomoc rodičům při problémech jejich dětí. Úkolem poraden je také spolupracovat se školami a školkami, protože pro žádost o odložení začátku školní docházky nebo pro žádost o speciální zacházení v případě nějakého postižení bývá vyžadováno posouzení poradnou.

Z hlediska zákona o rodině, kde je hlavní zodpovědnost za výchovu svěřena rodičům, je zcela vyloučené, aby škola komunikovala s poradnou bez vědomí a souhlasu rodičů.

Úřad obdržel stížnost, že učitelka z mateřské školy odmítla předat vyplněný dotazník poradny rodičům. Kontrola dospěla k tomuto právnímu názoru: Pokud rodiče požádají o pomoc poradnu, může ona požádat o spolupráci příslušnou základní nebo mateřskou školu a o vyplnění dotazníku o chování dítěte ve škole. Učitelé nejsou povinni tento dotazník vyplnit (není to součást jejich pracovních povinností), pokud tak z dobré vůle učiní, je správcem osobních údajů (často velmi citlivých) v něm obsažených poradna. Její pracovníci s těmito údaji pracují se zodpovědností a povinností mlčenlivosti danou jejich profesionálním postavením. Pokud rodiče chtějí znát obsah dotazníku, mohou požádat poradnu o informaci, které osobní údaje jejich dítěte zpracovávají, a mají také ostatní oprávnění dle ustanovení §§ 12 a 21 zákona o ochraně osobních údajů.

Učitel tedy posílá vyplněný dotazník do poradny se souhlasem rodičů (neboť pouze s jejich souhlasem bude dítě v poradně vyšetřeno), není ovšem povinen jeho obsah rodičům sdělit.

Kontroly také opět narazily na problém výročních zpráv škol. Škola zpracovává osobní údaje svých zaměstnanců včetně citlivých údajů o jejich nepřítomnosti, popř. ukončení pracovního poměru v důsledku zhoršeného zdravotního stavu i o jejich invalidních důchodech v rámci plnění povinností zaměstnavatele. Podle ustanovení § 13 zákona o ochraně osobních údajů musí ovšem zabránit, aby se k těmto údajům dostala neoprávněná osoba. Zpracování k jinému účelu je možné pouze na základě zákonného zmocnění, kterým je školský zákon a vyhláška č. 15/2005 Sb., kterou se stanoví pravidla pro zveřejňování zpráv o škole. Osobních údajů učitelů se týká § 7: *„Výroční zpráva o činnosti školy obsahuje vždy: […] c) rámcový popis personálního zabezpečení činnosti školy, […] g) údaje o dalším vzdělávání pedagogických pracovníků […].“* Povinnost stanovená vyhláškou je splněna uvedením jména a příjmení jednotlivých pracovníků školy, popř. jejich profesních atributů: jaké předměty učí, jaké kroužky vedou, ve které třídě jsou třídními učiteli, jakých školních zájezdů nebo výletů se účastnili, popř. informací o jejich dalším vzdělávání. Žádné jiné osobní údaje, jmenovitě např. údaje o jejich zdravotním stavu a důvodech dlouhodobé pracovní neschopnosti, nelze zveřejňovat. Je třeba si uvědomit, že zvláště tyto údaje mohou být klíčovou informací pro nového zaměstnavatele v případě, kdy se zaměstnanec uchází o jiné pracovní uplatnění. V žádném případě si nelze touto cestou vyřizovat účty mezi ředitelem a jeho kritiky z řad učitelů.

OSOBNÍ ÚDAJE A ANONYMNÍ ÚDAJE

Podle definice v zákoně o ochraně osobních údajů je osobním údajem *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“*

Kontrola se setkala s několika případy, kdy se jednalo o tzv. pseudoanonymní údaje, tj. údaje, které vystupovaly jako anonymní, ale v mnohých případech bylo možno identifikovat příslušný subjekt údajů. Často se jedná o citlivé údaje, které požívají vyšší stupeň ochrany a pro jejich zpracování je třeba buď výslovného souhlasu, nebo zákonného zmocnění pro dané citlivé údaje (zdravotnictví).

- Zpracování dotazníků dětmi, kdy jsou některé otázky položeny tak, že příslušná odpověď může jednoznačně identifikovat subjekt údajů: co dělají vaši rodiče?
- Zpracování údajů, kdy je rozsah získaných informací tak veliký, že může jednoznačně identifikovat subjekt údajů, kterého se týkají a který je pouze zdánlivě anonymní. Např. děti v dané škole: třída, rok narození, počet sourozenců, rodiče rozvedeni, počet aut v rodině, počet počítačů v rodině, záliby aj.
- Zpracování údajů, kdy jsou použity některé údaje, které mohou být velmi specifické a určovat konkrétní subjekt aspoň v některých případech: např. použití jména (Wilhelm, Van Doc, Scarlett) spolu s dalšími údaji (škola, třída, rok narození).
- Údaje, kdy je rodné číslo zakódováno do jiného čísla jednostranným algoritmem.

Ve všech výše jmenovaných případech jde o osobní údaje (minimálně za těch okolností, kdy je subjekt údajů jednoznačně určitelný), a je tudíž třeba s nimi jako s osobními údaji zacházet: Lze je zpracovávat pouze se souhlasem nebo na základě výjimek v § 5 odst. 2 písm. a)–g) zákona o ochraně osobních údajů, subjekty údajů musí být informovány o účelu zpracování, často je nutná registrace u Úřadu.

Zajímavým kritériem, zda se jedná o osobní údaje, či anonymní data, je myšlenkový experiment publikování údajů na internetu: Často se právě při takové úvaze ukáže, kolik lidí by se v takové databázi našlo...

ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ PŘI CASTINGU

Úřad se v roce 2009 v rámci své kontrolní činnosti zabýval plněním povinností správce, případně zpracovatele, při zpracování osobních údajů fyzických osob přihlášených v rámci castingu na některé reality show.

Účel zpracování osobních údajů fyzických osob přihlášených v rámci castingu na příslušnou reality show stanoví subjekt, který casting na konkrétní reality show vyhlásil, a ten je tedy v postavení správce osobních údajů. Tento subjekt však zpracování osobních údajů fyzických osob přihlášených v rámci castingu na konkrétní reality show někdy také neprovádí sám, ale předmětná zpracování provádí další subjekty, se kterými zmíněný subjekt uzavřel příslušné smlouvy k uskutečnění nejen castingu na příslušnou reality show, ale i k vytvoření, resp. k výrobě, televizního pořadu této reality show, k prezentaci příslušné reality show a také k následné informaci pro zájemce o vývoji a průběhu předmětné reality show na webových stránkách, které jsou v právním vztahu k tomuto správci (zpracovateli). Jelikož tyto další subjekty také určují účel a prostředky zpracování osobních údajů a odpovídají za tato zpracování, jedná se také o správce. Přihlášení se do castingu bylo v jednom případě reality show možno učinit zavoláním na telefonní záznamník, a později bylo uskutečňováno prostřednictvím formuláře k vyplnění, který zájemce o casting nalezl na webových stránkách příslušného subjektu. Tento formulář obsahoval nejen adresní a identifikační údaje, tedy jméno, příjmení, datum narození, adresu bydliště, číslo telefonu, číslo mobilního telefonu, e-mailovou adresu, nýbrž i informace, které bylo považováno za potřebné shromáždit vzhledem k obsahu, charakteru a zaměření příslušného televizního

pořadu, tedy reality show. Těmito informacemi byly kupř. zájmy, koníčky, dosažené vzdělání, odborná specializace, povolání, fotografie, různé rodinné informace, ale také přezdívka, váha a výška. Tyto informace jsou podle zákona osobními údaji. U některých z nich se jedná i o citlivé údaje.

Bylo zjištěno, že správce internetových stránek zasílal vyplněné formuláře v elektronické podobě elektronickou cestou subjektu, který na základě příslušné smlouvy kontaktoval fyzické osoby, které se přihlásily v rámci castingu na příslušnou reality show. Ten po přijetí vyplněného formuláře vždy zpětně zatelefonoval fyzické osobě, která tento formulář vyplnila a přihlásila se tím v rámci castingu na příslušnou reality show, aby se přesvědčil o jejím skutečném zájmu. Pokud se takto přesvědčil o tom, že došlý vyplněný formulář je od nerozhodnuté fyzické osoby, pak její vyplněný formulář vymazal z elektronické pošty a tak jej vyřadil z výběru. V případě, že telefonickým kontaktem zjistil zájem fyzické osoby, která se přihlásila v rámci castingu na příslušnou reality show, zkontroloval a ověřil zaslané osobní údaje, zda jsou přesné, a domluvil s touto fyzickou osobou, resp. zájemcem, termín návštěvy. Takto potvrzený formulář s osobními údaji převedl do svého seznamu zájemců uloženého ve wordovském dokumentu a okamžitě přidělil zájemci pořadové číslo. Pak v elektronické poště vymazal došlý vyplněný formulář. Před objížděním zájemců postupoval tak, že si udělal denní plán cest objíždění konkrétních zájemců, jichž mohlo být až pět denně. V praxi to proběhlo tak, že ze svého seznamu zájemců ve wordovském dokumentu vyjmul osobní údaje konkrétních zájemců, které měl naplánováno ten den navštívit, a takto upravený denní seznam vytiskl na tiskárně. Po skončení práce na přípravě castingů neobsahoval tento seznam uložený ve wordovském dokumentu žádné osobní údaje. Vytištěné seznamy skartoval. Pořízené fotografie v digitální podobě ve svém fotoaparátu vymazal. Při objíždění zájemců o účast na příslušnou reality show uzavíral jménem subjektu, který casting na konkrétní reality show vyhlásil, smlouvy o účasti na castingu a zájemci o casting sami a dobrovolně vyplňovali dotazník. Uzavřenou smlouvu, vyplněný dotazník a pořízené fotografie předával dramaturgovi příslušné reality show. S ohledem na uvedené lze konstatovat, že se jedná o zpracování osobních údajů se souhlasem těchto fyzických osob, které jsou subjekty údajů, a tedy jde ve smyslu zákona o ochraně osobních údajů o zpracování osobních údajů se souhlasem subjektu údajů. Jelikož se na toto zpracování nevztahuje žádný z liberačních důvodů z oznamovací povinnosti zakotvené v zákoně, je správce povinen plnit oznamovací povinnost vůči Úřadu.

Kontrolou byla zjištěna porušení ustanovení zákona o ochraně osobních údajů:
– povinnost informovat subjekt údajů při udělení jeho souhlasu o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období, a dále že souhlas subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování;
– informovat jej o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy, a že správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v ustanovení § 21 zákona.

V důsledku těchto zjištěných porušení zákona o ochraně osobních údajů byla kontrolovanému subjektu uložena v kontrolním protokolu i odpovídající opatření k nápravě a stanoveny lhůty k jejich splnění.

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

15 let, si mohou koupit zmrzlinu, ale nemohou dostat hypotéku, tzn. nemají způsobilost uzavřít smlouvu na casting a souhlasit se zpracováním svých osobních údajů a s případným fotografováním nebo natáčením ve spodním prádle či plavkách. K tomu je nutný souhlas jejich zákonných zástupců (nemluvě o pozdější případné smlouvě, ke které bude třeba povolení úřadu práce – viz § 121 nového zákona o zaměstnanosti).

Pro mladistvé, tj. mladíky a slečny ve věku 15–18 let, by bylo možno použít dikci § 9 občanského zákoníku a říci, že jsou už schopni rozpoznat povahu právního úkonu souhlasu se zpracováním svých osobních údajů. V konkrétním případě kontrolované castingové firmy byla ovšem formulace *„podnikatelská činnost agentury"* natolik neurčitá, že nebylo jasné, k čemu klient dává souhlas, a proto jsme požadovali souhlas zákonných zástupců pro všechny nedospělé.

Úřad se této problematice bude i nadále věnovat.

KAMEROVÉ SYSTÉMY

Tradičně velká pozornost byla Úřadem věnována oblasti zpracování osobních údajů prostřednictvím kamerových systémů se záznamem. Důslednost, s níž Úřad přistupuje k této problematice, se odrazila i na zvyšujícím se počtu dotazů jak v rámci přípravy registrace systémů, tak i obecně ze strany občanů i různých společností a institucí. Například odbor poskytující konzultace přijal v roce 2009 přes 250 písemných stížností a dotazů na kamerové systémy. Ke kontrole bylo postoupeno přes 30 stížností.

Vyšší kvalitu vykazovaly i **přihlášky správců kamerových systémů k registraci** do veřejného registru. Přesto ale zůstává řada správců, se kterými vedl Úřad jednání již v rámci registračního řízení. Níže uvedené příklady popisu registračních oznámení jsou vzorové.

V oznámení účastník řízení, kterým bylo středně malé město, Úřadu sdělil svůj záměr provádět **zpracování osobních údajů** svých **zákazníků** (strávníků) a třetích osob prostřednictvím 16 stacionárních kamer, které budou monitorovat konzumační prostory, prostor pro odkládání použitého nádobí, vestibul a přilehlý venkovní vchodový prostor v majetku účastníka řízení. Oznamovatel uvedl, že kamerový systém bude pomůckou při řešení škodních událostí na majetku správce i zákazníků (strávníků), záznam bude využíván k identifikaci vandalismu, výtržnictví a krádeží, které se opakovaně stávají jak na majetku účastníka řízení, tak na majetku strávníků (rozbití dveří, odcizení kol před budovou, odcizení odložené bundy na věšáku, rozříznutí ubrusů, krádeže příborů apod.). Osobní údaje nebudou zpracovávány se souhlasem subjektu údajů, záznam bude uchováván po dobu 3 měsíců. Vzhledem k důvodnému podezření na neoprávněné zpracování osobních údajů bylo zahájeno s účastníkem řízení z moci úřední. V následném řízení Úřad zpracování osobních údajů v tomto rozsahu nepovolil.

V oznámení účastník řízení sdělil svůj záměr provádět bez souhlasu subjektů údajů **zpracování osobních údajů zastupitelů, zaměstnanců** a třetích osob **v době zasedání zastupitelstva města**, prostřednictvím 1 stacionární kamery se zvukovým záznamem umístěné v zasedací místnosti městského úřadu, za účelem vyhotovení a následné kontroly zápisů ze zasedání zastupitelstva města, z níž by byl záznam uchováván po dobu 30 dnů.

Na základě uvedených skutečností vznikla důvodná obava, že by při zpracování osobních údajů mohlo dojít k porušení zákona o ochraně osobních údajů a z tohoto důvodu zahájil v souladu se zákonnou povinností Úřad řízení z moci úřední. Rovněž v tomto řízení nebyl povolen provoz kamerového systému v navrhovaném rozsahu.

V dalším typickém oznámení účastník řízení (provozovatel restaurace a baru) sdělil svůj záměr provádět bez souhlasu subjektů údajů **zpracování osobních údajů** svých **zákazníků a zaměstnanců** v jenom z největších pražských klubů, který sestává jednak z luxusní **restaurace**, jednak z vlastního klubu s tanečním parketem, prostory k sezení a bary, prostřednictvím 60 stacionárních a mobilních kamer monitorujících prostory tohoto klubu (vstupy, bary, restaurace, chodby), a to tak, že v prostoru luxusní restaurace mají být monitorovány prostory, kde dochází k manipulaci s hoto-

vostními prostředky zákazníků, konkrétně prostory barů, resp. pokladen, a to za účelem kontroly těchto hotovostních peněžních transakcí. V prostoru vlastního klubu s tanečním parketem, prostory k sezení a bary má být monitorován prakticky celý prostor, a to za účelem ochrany majetku a práv zákazníků, oznamovatele a pronajímatele před osobami, které mají v úmyslu zneužít nedostatečně osvětlených prostor k páchání trestné činnosti. I v tomto případě zahájil Úřad správní řízení z moci úřední. V rámci tohoto řízení došlo ze strany účastníka řízení k vlastnímu rozhodnutí o změně využívání kamerového systému.

V souvislosti s poskytováním konzultací souvisejících s provozováním kamerových systémů se Úřad nejčastěji setkává s dotazy zaměstnanců na **monitorování** jejich **pracovišť** zaměstnavateli. I přes skutečnost, že provozování kamerových systémů bez záznamů, v tzv. režimu on-line, nespadá pod jurisdikci Úřadu, vzhledem k tomu, že takovéto jednání může být v rozporu nejen s Listinou základních práv a svobod, ale rovněž s občanským zákoníkem, jsou stěžovatelům poskytovány rady, jak postupovat v těchto případech. Nejčastěji se stížnosti týkají zneužívání kamerového systému k uplatňování pracovněprávních následků. Kamery jsou v těchto případech nastaveny tak, že zpracování nenaplňuje deklarovaný účel – ochranu majetku. Jsou-li podání adresná, postupuje je Úřad dle místní příslušnosti oblastním inspektorátům práce. Ve větší části podání však adresa subjektu, proti kterému směřuje, není uvedena. Odesílatelům podnětů proto doporučujeme, aby se obraceli na příslušné inspektoráty práce.

Současně Úřad v rámci své dozorové činnosti spolupracuje se Státním úřadem inspekce práce a jednotlivými oblastními inspektoráty práce. Pokud inspektoráty práce dospějí svým postupem k závěru, že se jedná současně i o podezření z porušení zákona o ochraně osobních údajů, postoupí příslušnou část podání Úřadu.

V rámci vzájemné spolupráce se inspektor Úřadu zúčastnil i interního školení a semináře, který byl určen pro jednotlivé pracovníky oblastních inspektorátů práce.

Řada žádostí o informaci se týká **využívání městských kamerových systémů**. Důvody pro jejich zřízení spočívají především ve snaze místní správy zajistit veřejný pořádek. Častá otázka občanů se týká skutečnosti, že obec provozuje kamerový systém, který snímá jejich dům, pozemek, zahradu s bazénem. Nejčastěji však, že kamera je zaměřená do oken soukromého domu. V roce 2009 se na Úřad s žádostí o pomoc obrátili i politici z opozice s podezřením, že jsou soustavně sledováni kamerovým systémem.

V rámci své dozorové činnosti provedli inspektoři Úřadu na 30 incidenčních kontrol se zaměřením na zpracování osobních údajů prostřednictvím kamerového systému. Například bylo na základě podnětu předsedy Úřadu kontrolováno statutární město, jehož městská policie jako provozovatel kamerového systému předala soukromé celostátní televizi pořízený záznam. Záznam obsahoval osobní údaje osob zachycených v místě výplaty dávek v hmotné nouzi. Tento záznam byl několikrát zveřejněn ve zpravodajských pořadech v televizi. Město, které prostřednictvím městské policie umístilo kamery i do vnitřních prostor radnice, v rozporu se zákonem zpřístupnilo záznamy obsahující záběry konkrétních osob, a naplnilo tak skutkovou podstatu správního deliktu. Inspektorka Úřadu rozhodla o uložení pokuty. V této kontrole bylo dále prověřováno, zda statutární město dodržuje povinnosti správce osobních údajů v souvislosti se stanoveným účelem. Tímto účelem pro provoz kamerových systémů byla ochrana zdraví a života osob a majetku města, a ne předávání záznamů pro televizní vysílání. Městská policie je dle zákona o obecní a městské policii oprávněna, je-li to potřebné pro plnění jejích úkolů podle tohoto nebo jiného zákona, pořizovat zvukové, obrazové nebo jiné záznamy z míst veřejně přístupných, popřípadě též zvukové, obrazové nebo jiné záznamy o průběhu zákroku nebo úkonu. Pořízené záznamy mohou být dle zákona předány pouze policii, orgánům činným v trestním řízení, orgánům obce a dalším orgánům veřejné moci, je-li to nutné k plnění jejich úkolů. Předávání záznamů pro využití k jinému účelu a jinému subjektu je tedy v rozporu se zákonem.

Mezi další kontroly, které se týkaly provozování kamerového systému, patřila kontrola provedená v dalším statutárním městě. Město instalovalo kamerový systém v ubytovně, sloužící k trvalému bydlení i přechodnému ubytování svých občanů, kterým je město povinno poskytnout bytovou náhradu

ve formě náhradního ubytování nebo přístřeší. Provoz kamer zajišťovala městská policie. Bylo zjištěno a dokumentováno, že kamery sledují prostor v okolí ubytovny, vchod do ubytovny a všechny chodby v několikaposchoďové budově. V ubytovně byla zřízena stálá domovní služba. Důvodem bylo, že v objektu ubytovny se stále projevovaly problémy a město nemohlo v objektu trvale zajistit přítomnost strážníka. Kamerový systém byl tedy určen k nepřetržitému dohledu, jehož účelem bylo eliminovat rušení veřejného pořádku, porušování domovního řádu ubytovny, zabránit neoprávněnému odběru elektrické energie, nedodržování hygienických norem při nakládání s odpady a ničení společných prostor domu, ale rovněž i kontrola, zda ubytovaní nevpouštějí do objektu neoprávněné osoby. Město se v rámci přípravy sice zabývalo otázkou ochrany osobních údajů, ale rozhodlo, že z hlediska práva správce osobních údajů na ochranu svých práv a právem chráněných zájmů může občany sledovat. Město žádný souhlas ubytovaných nevyžadovalo a na jejich protesty nereagovalo. Kromě viditelně instalovaných kamer a tabulky, která informovala pouze o tom, že objekt je střežen kamerovým systémem, nebyla ubytovaným dána žádná informace, zejména ne ta, že kamery provozuje a záznamy pořizuje městská policie. **Ve svém zjištění inspektor konstatoval, že město porušilo zákon o ochraně osobních údajů. Právo na soukromí v ubytovně je zaručeno ustanovením čl. 7 odst. 1 a čl. 10 odst. 2 Listiny základních práv a svobod. Rovněž mají dotčené osoby právo na ochranu před neoprávněným shromažďováním údajů o své osobě a své rodině. K posouzení, zda pro deklarovaný účel, tedy jako prevence proti nežádoucím jevům, lze tolerovat takový zásah do soukromí, jako je shromažďování kamerových záznamů, lze nalézt i v rozhodovací praxi soudů. Např. Ústavní soud ČR v nálezu ÚS 191/05 konstatuje, že základní právo či svobodu lze omezit pouze v zájmu jiného základního práva či svobody. Při úvaze o prioritě jednoho ze dvou v kolizi se ocitajících práv je nutno zkoumat, zda byly využity všechny možnosti minimalizace zásahu do základních práv druhého. Město svým rozhodnutím nadřadilo svůj zájem spočívající v ochraně před drobnými krádežemi a zneužíváním prostor nad právo na ochranu soukromí a osobního života. I s ohledem na rozhodnutí Ústavního soudu je zřejmé, že město pochybilo.**

Další kontrola byla provedena na základě stížnosti, dle které měly být na internetových stránkách městské policie zveřejněny fotografie pořízené městským kamerovým systémem. Na fotografiích byly rozpoznatelné pouze postavy osob, které se ve sledovaném prostoru pohybovaly. V rámci kontroly prováděné inspektorem bylo zjištěno, že na webových stránkách městské policie obce byly skutečně zveřejněny a zpřístupněny snímky, které byly pořízeny z městských kamer. Záznamy zobrazovaly průjezd veteránů obcí. Městská policie zpřístupňovala na svých webových stránkách jednak vybrané a upravené obrazové snímky ze záběrů kamerového systému obce vybudovaného za účelem stanoveným zákonem o obecní policii, a dále vybrané obrazové snímky ze společenských akcí. Dříve, než byly fotografie zpřístupněny na internetu veřejnosti, bylo provedeno zaretušování obličejů fyzických osob. V důsledku toho nebyly fyzické osoby rozpoznatelné a přímo ani nepřímo identifikovatelné, a byly tedy anonymizovány. Jednalo se zejména o záběry pořízené při kontrole průjezdu křižovatkami. Nejednalo se tedy o osobní údaje ve smyslu zákona o ochraně osobních údajů.

Spojovacím článkem výše popsaných kontrol je využívání kamerových systémů se záznamem obcemi a městy, a to prostřednictvím jimi zřizované obecní nebo městské policie. Dle zákona plní obecní a městská policie úkoly svého zřizovatele. Obce a města jsou dle zákona o obcích povinny zajišťovat veřejný pořádek, a to na veřejných prostranstvích. Vnitřní prostory budov ve vlastnictví města či vnitřní prostory magistrátu nejsou veřejným prostorem. V rámci dozorové činnosti bylo například zjištěno, že na základě pověření starosty jednoho západočeského města sleduje městská policie na svých monitorech záznamy z kamer umístěných v bytových domech, které jsou v majetku města. Obecní a městská policie tedy využívá kamerové systémy, které jsou pořizovány z veřejných prostředků města nebo státu, ke sledování vlastních občanů, a to bohužel bez jakékoliv vnitřní i vnější kontroly. Účelem zpracování osobních údajů obecní a městskou policií je zabezpečování veřejného pořádku. Nelze tedy akceptovat jiné využití pořizovaných záznamů než jako dokumentace zjištěných trestných činů či přestupků.

Výrazně se zvýšil počet žádostí o konzultace ze strany majitelů **bytových domů**, a to bez ohledu na to, zda se jedná o majitele domu, či představitele samospráv nebo společenství vlastníků. Základem dotazů je vždy snaha zabránit drobným krádežím, vandalismu, sprejerství v bytovém domě. Projednávané otázky se týkají souhlasu obyvatel, možnosti využívání pořízených záznamů apod. Na druhé straně dostává Úřad téměř každý den stížnosti obyvatel bytových domů na skutečnost, že bez poskytnutí jakékoliv informace či vyžádání si souhlasu jsou podrobeni sledování kamerovým systémem.

Řadu kontrol provedli inspektoři Úřadu v bytových domech. Jednalo se o bytové domy ve vlastnictví soukromém či obecním, ve vlastnictví majitelů bytových domů či družstev. Společným článkem všech kontrol byla stížnost některého z nájemníků na provoz kamerového systému bez souhlasu ubytovaných osob, většinou doplněná i tím, že provozovatel kamerového systému nereagoval na vyjádření nesouhlasu s monitorováním uživatelů bytů. Problematikou kamerových systémů v bytových domech se Úřad dlouhodobě zabývá. Své stanovisko zveřejnil v květnu roku 2008.

Inspektoři se setkávají i s tím, že kamerové systémy jsou instalovány na základě doporučení místní policie, a to jak obecní, tak Policie ČR. Základním problémem kamerových systémů v bytových domech je skutečnost, že jsou primárně určeny a využívány ke sledování osob, a ne k deklarované ochraně majetku. Pouze ve zlomku případů jsou záznamy skutečně předávány příslušným orgánům k uplatnění jejich represivní činnosti. Samostatnou kapitolou zůstává využívání kamerových systémů v družstevních domech nebo společenstvích vlastníků. Zde dochází ke střetu práva společného rozhodování s právem jednotlivce na vyjádření svého souhlasu či nesouhlasu se zpracováním jeho osobních údajů. Převažuje rozhodnutí představenstva bytového domu o instalaci kamerového systému, které je předloženo ke schválení na schůzi. Přehlasování nesouhlasících osob je následně vydáváno za souhlas všech majitelů nebo uživatelů bytů. Tento omyl je však v rozporu s právem každé osoby vyjádřit svůj svobodný souhlas se zpracováním svých osobních údajů. **Ve všech kontrolovaných případech bylo konstatováno, že provozování kamerového systému je v rozporu se zákonem, neboť chráněný zájem nepřevažuje nad právem na ochranu soukromí. Hodnota ochrany soukromí spojené s bydlením je výrazně vyšší než zjištění osoby, která ukradla například rohožku. Dále lze shrnout, že kamerové systémy v bytových domech nejsou ve své většině schopny naplnit deklarovaný účel a že pořízený záznam není tím nejvhodnějším prostředkem k zajištění pořádku v domě**. Shodná téměř pro všechny kontrolované domy se rovněž stala skutečnost, že proti rozhodnutí inspektora jsou podávány někdy námitky, ze kterých vyplývá, že převážná většina provozovatelů vůbec nepochopila podstatu problematiky související s právem na soukromí. Přitom někdy stačí jen upravit úhel záběru, aby kamery plnily proklamované účely a vyhověly zákonu. **Na základě provedených kontrol byly v návazném správním řízení o spáchání správního deliktu ukládány pokuty v průměrné výši 50 000 Kč.**

V roce 2009 se na Úřad obrátilo několik stěžovatelů kvůli **provozování kamerových systémů v bazénech a aquaparcích**. Bylo zjištěno, že provozovatelé takovýchto zařízení instalují kamery v rámci celého areálu. Stanoveným účelem bývá nejčastěji deklarovaná ochrana před krádežemi. Ve dvou případech bylo zjištěno, že kamery jsou instalovány pouze v dámských šatnách a sprchách s odůvodněním, že jsou vykrádány pouze skříňky v šatnách žen. V jednom případě došlo k tomu, že provozovatel bazénu zveřejnil fotografii osoby podezřelé z krádeže v prostorách zařízení jak na svých internetových stránkách, tak i ve vstupním prostoru do svého areálu. Ale záznam zachycující údajnou krádež policii nepředal.

V rámci probíhající kontroly bylo zjištěno, že v celém areálu je nainstalováno přes 120 kamer. Návštěvník je zcela nedostatečně informován o tom, kdo všechno má možnost si záznamy prohlížet, komu mohou být předány apod. **Takové jednání je v rozporu se zákonem o ochraně osobních údajů**. Jednotlivé kontroly prováděné inspektory v oblasti kamerových systémů se záznamem se týkaly dále například umístění kamer v chodbě před převlékacími kabinkami **sportovního zařízení**.

Na základě stížností bylo provedeno několik kontrol **kamerového systému ve školách**. Často se jednalo o stížnosti učitelů, kteří měli pocit, že jsou neoprávněně kontrolováni ředitelem školy. Vzhledem k tomu, že záznamy z kamer mohou být uchovávány pouze tehdy, pokud jsou kamery používány k ochraně majetku školy nebo dětí (ostatní důvody, jako boj proti šikaně nebo ochrana zdraví dětí, se ukázaly jako liché a záznamy z kamer pro ně neužitečné), dospěly školy k názoru, že maximální rozsah kamer, ze kterých by bylo třeba uchovávat záznamy, jsou kamery v šatnách, popř. v chodbách, a to nejlépe po vyučování a o prázdninách. Překvapivě ale všechny školy, které byly kontrolovány, nakonec usoudily, že záznamy z kamer nepotřebují.

Byla také provedena kontrola v základní škole, kde na základě pořízeného záznamu byla udělena jednomu z žáků školy poznámka o jeho nevhodném chování.

V roce 2009 rozhodl Městský soud v Praze o žalobě základní umělecké školy proti Kontrolnímu protokolu a Rozhodnutí Úřadu o uložení pokuty ve výši 90 000 Kč, související s neoprávněným zpracováním osobních údajů prostřednictvím kamerového systému se záznamem. Městský soud žalobu školy zamítl a ztotožnil se se závěry Úřadu, dle kterého škola jako provozovatel kamerového systému se záznamem pořizovala a zpracovávala osobní údaje učitelů, žáků a dalších osob v rozporu se zákonem o ochraně osobních údajů a zasahovala do soukromí dotčených osob. Vedení této školy využívalo kamerový systém k tomu, aby sledovalo, jak pedagogové dodržují své pracovní povinnosti. Ve svém rozhodnutí o instalaci kamerového systému nevyužilo ostatní, méně invazivní prostředky, jak zabránit možným negativním jevům.

V několika případech provedli inspektoři kontrolu u subjektů, které z důvodu prevence nainstalovaly na své objekty pouze maketu kamery. V takovém případě nelze aplikovat povinnosti stanovené zákonem o ochraně osobních údajů, neboť nedochází ke shromažďování osobních údajů.

Kontroly byly provedeny v **psychiatrické léčebně, v sanatoriu pro seniory, v domově důchodců a jedné oblastní nemocnici**. V těchto zařízeních byly kamerové systémy využívány k tomu, aby odpovědný personál měl okamžitý přehled o svých klientech. Podstata spočívala tedy ve využívání on-line systému. Přesto se ve všech těchto zařízeních vše nahrávalo a zaznamenávalo. Dle názoru Úřadu ve všech případech zbytečně, neboť záznamy již nemohly sloužit k poskytnutí okamžité pomoci klientům.

Proběhla kontrola objektu, kde společně sídlí **ambasáda** cizí země **a společnost provozující hotel**, která celý objekt monitoruje prostřednictvím kamerového systému se záznamem. Po zásahu inspektora došlo ke změně tak, aby bylo zachováno soukromí nejen zaměstnanců ambasády, ale i osob, které ji navštěvují, při zachování zabezpečení ambasády.

Kontroly byly provedeny také ve velkých nákupních střediscích, ale i malých obchodech. Kontroly se uskutečnily v galerii, v budově centrálního dozorového úřadu, ve věznici, školách a školkách, restauracích.

Z uvedeného přehledu vyplývá, že zpracování osobních údajů prostřednictvím kamerových systémů je využíváno téměř ve všech možných životních situacích a v očích mnohých občanů se stávají zcela běžnou součástí našeho života a staly se velkým problémem naší společnosti. Pořízené záznamy jsou využívány pro dokazování sousedských sporů, k dokázání kázeňského prohřešku dětí ve škole. Jsou často zneužívány ve firmách ke sledování docházky, plnění pracovních úkolů, a to s pracovněprávními následky pro sledované osoby.

Proto Úřad vítá usnesení vlády ČR upravit v našem právním řádu využívání kamerových systémů.

ČIPOVÉ KARTY

V roce 2009 byla provedena kontrola využívání čipových karet, vybavených technologií RFID u autobusového dopravce, který provozuje jak městskou hromadnou dopravu, tak i dopravu v rámci celého kraje. Tato společnost současně v rámci krajské integrované dopravy umožňuje ostatním dopravcům využívat jejich technologii.

Společnost poskytuje cestujícím možnost získat předplatní nebo časový kupón pouze ve formě čipové karty. Tyto karty jsou vybaveny čipem s technologií RFID, bezkontaktně přenášející data. V rámci celého systému nabídky předplatních kupónů jsou společností vydávány osobní nepřenositelné karty pro dospělé, studenty, žáky a seniory. Společnost rovněž nabízí anonymní, tzv. rodinnou, přenositelnou kartu. Kromě rodinné karty jsou ostatní karty využívány jako běžná předplatní průkazka. Na kartě je otištěna fotografie držitele, jeho jméno a příjmení. Každá karta je označena jedinečným číslem a jednotlivé typy jsou od sebe vzájemně barevně a graficky odlišeny. Při podání žádosti o vydání karty vyžadovala společnost od žadatele kromě jména a příjmení ještě datum narození a adresu bydliště. Od cestujících, kteří mají dle přepravních podmínek nárok na některou ze slev, i příslušné potvrzení, např. o studiu. Rodinná karta označena není a je využívána de facto jako peněženka.

Držitel karty byl oprávněn využívat předplacené dopravní služby. V rámci jízd byly dopravní prostředky (přepravce a smluvních přepravců podílejících se na dopravní obslužnosti města a kraje) vybaveny čtečkami čipů RFID. Podle typu jízdného byly buď finanční prostředky odečítány z celkového finančního limitu, nebo byla zkontrolována platnost předplatního časového kupónu. V těchto čtecích zařízeních se zaznamenávaly informace vztahující se ke konkrétní kartě. Jednalo se o číslo karty, datum a čas nástupu, místo nástupu a místo výstupu. Dále byly u předplacených kupónů zaznamenávány informace o odečtení finančního limitu. Společnost tyto informace dále doplnila o informace z automatů určených pro dobíjení kupónů. Databáze obsahující identifikační údaje držitelů karet byla vedena samostatně, odděleně od databází o přepravních a dopravních transakcích. Veškeré transakce, spojené s využíváním čipových karet, byly prováděny na základě jedinečného čísla karty. Rovněž vzájemné vyúčtování nákladů spojených s poskytováním dopravních služeb, které zabezpečovali další přepravci, bylo prováděno prostřednictvím clearingového centra výhradně na základě jedinečného čísla karty. Všechny tyto informace o konkrétním držiteli karty a informace o transakcích uchovávala společnost po dobu pěti let. Kontrola v tomto případě konstatovala, že společnost, jako držitel databáze, ve které jsou uloženy identifikační osobní údaje držitelů čipových karet, současně disponuje informacemi o finančních transakcích, informacích o konkrétním místě a čase nástupu a výstupu z dopravního prostředku konkrétního cestujícího. Společnost pro své potřeby využívala pouze informace o využívání integrované dopravy ke svým obchodním a marketingovým účelům. Ke své činnosti informace o využití přepravy konkrétní osobou nevyužívala. V několika případech však tyto informace, týkající se konkrétní fyzické osoby, předala na základě své povinnosti příslušnému státnímu orgánu.

Kontrolou bylo prokázáno, že až na výjimku, týkající se žáků, tedy dětí, které nemají žádný osobní průkaz, není k vlastní činnosti nezbytné zpracovávat identifikační osobní údaje. Na každé nepřenosné kartě je otištěna fotografie držitele, jeho jméno, příjmení a datum narození. Dle zákonných oprávnění smí osoba pověřená přepravcem kontrolovat kromě jízdního dokladu i totožnost cestujícího dle jeho osobního průkazu (dle podmínek příslušných předpisů o osobní přepravě). Na základě tohoto závěru uložil kontrolující inspektor tomuto přepravci nápravné opatření likvidovat databázi držitelů čipových karet.

Společnost je oprávněna zpracovávat identifikační osobní údaje držitelů karet pouze v případě, že držitel karty žádá o vydání duplikátu z důvodu ztráty či odcizení čipové karty, a dá za tímto účelem svůj výslovný souhlas. Obdobně je tomu v případě dětí, které nemají svůj osobní průkaz, a tudíž se nepřenositelnost jejich čipové karty nedá jiným způsobem zkontrolovat.

Kontrolovaná společnost závěry kontrolního šetření akceptovala.

ÚSEKOVÉ MĚŘENÍ RYCHLOSTI

Kontrolovaným subjektem bylo hlavní město Praha, Městská policie.

Zařízení určené pro měření rychlosti vozidel stanovuje úsekovou rychlost vozidel jako podíl známé konstantní dráhy mezi dvěma měrnými profily k době, kterou vozidlo ujede za naměřenou dobu. Každé měřicí zařízení se skládá z řídicí jednotky (počítač) příslušné každé dvojici kamer (K1 a K2) a databázového serveru. Zařízení pracuje tak, že jednotlivá detekční zařízení (kamery) neustále sledují situaci v příslušných jízdních pruzích daných měrných profilů. Měrné profily jsou na vozovce v určité pevné vzdálenosti od sebe (cca 500 m) a definují tak měřený úsek. Řídicí jednotka detekuje vozidlo opatřené RZ/SPZ v zorném poli kamery a následně poznávací značku přečte. Zařízení jsou standardně vybavena kamerami s rozlišením HDTV, které zabezpečují výrazně vyšší kvalitu snímků oproti běžným kamerám s televizním rozlišením. Tím se dosahuje vysoké spolehlivosti detekce vozidel, dobře čitelné registrační značky a výrazného zkvalitnění zdokumentování tváře řidiče vozidla. Záznamy pořízené kamerou K1 při vjezdu vozidla do měřeného úseku a kamerou K2 při jeho výjezdu jsou ukládány do centrálního datového úložiště (technické zařízení – server). Pokud zařízení vyhodnotí překročení nastavené rychlosti, odešle pořízený záznam složený z fotografie vozidla včetně řidiče a spolujezdce a digitalizované RZ/SPZ (kamera K1), digitalizované RZ/SPZ (kamera K2) a údaje o rychlosti vozidla do úložiště Městské policie k dalšímu řešení přestupku. Vlastní měření probíhá tedy zcela bezobslužně a nelze je ovlivňovat. Přesnost měření je zaručena tím, že vzdálenost měřicích míst je velmi přesně zaměřena a oba snímky jsou opatřeny přesnými časovými razítky ze stabilní časové základny. Parametry měření lze dle potřeby dálkově spravovat a nastavovat pomocí vhodného rozhraní. Jedná se např. o nastavení maximálního rychlostního limitu, hodnoty rychlosti klasifikované jako přestupek (toleranční pole) apod.

Kamerové systémy sledující průjezdy na červenou jsou nastaveny tak, že pořizují fotografie řidičů vozidel, která vjíždí do křižovatky, ačkoliv je na semaforu signál „stůj“ (červená).

V Praze bylo v době kontroly nainstalováno 18 úsekových měřičů rychlosti a 9 systémů sledujících průjezdy na červenou.

Úsekové měřiče jsou instalovány na základě zprávy Policie ČR, která stanovila sdělením ze dne 31. prosince 2008 umístění technických prostředků určených k měření rychlosti. Tento způsob měření rychlosti však současně zpracovává i osobní údaje osob, které se nedopustily přestupku, a proto je toto nepřetržité sledování všech projíždějících vozidel silným zásahem do soukromí jednotlivce a jeho umístění musí být podloženo skutečnou nebezpečností daného úseku vyvolávající potřebu stálého dozoru. Úřad není kompetentní k posuzování oprávněnosti volby daných míst.

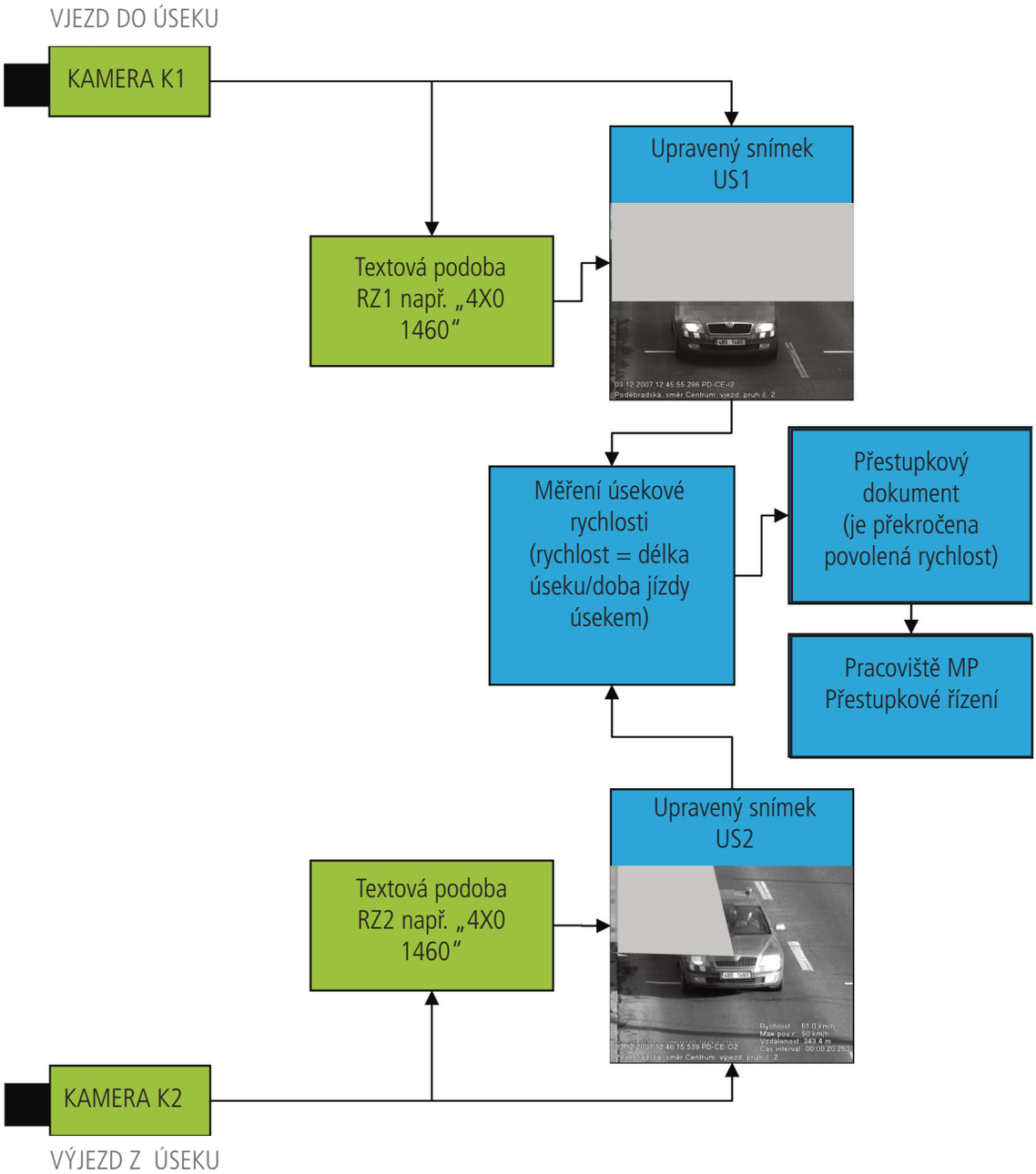
Kontrolovaný subjekt je správcem těchto údajů a uchovává je v přiměřené lhůtě, odpovídající přestupkovému zákonu.

Kontrola uložila zcela odstranit obrazovou informaci o spolujezdci, a tím nahradit sporné rozmazání jeho obličeje na fotografii.

Informace z uvedených kamerových systémů zpracovává Policie ČR v neupravené podobě v rámci centrálního datového úložiště. Policie ČR je ve smyslu zákona č. 101/2000 Sb. i správcem těchto údajů.

Blokové schéma: funkce systému

Z blokového schématu vyplývá, že v případě překročení rychlosti nad povolený limit jsou do přestupkového dokumentu vloženy: snímek z kamery K1, kde je vidět pouze registrační značka, a snímek, případně snímky, z kamery K2, kde není vidět spolujezdec.



Popis software UnicamPRIVACY

Úprava I – Zakrytí části snímku z kamery K1

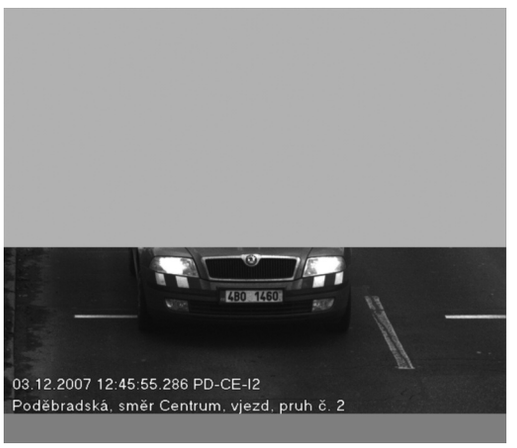
Snímek z kamery K1 na vjezdu do úseku je pro potřeby měření rychlosti upraven tak, že se rozmaže část snímku nad registrační značkou tak, jak je patrné z obrázku.

Příklad upravovaných snímků z kamery K1

Pouze pro potřeby PČR

Snímek S1 pořízený kamerou K1

Pouze pro potřeby MP



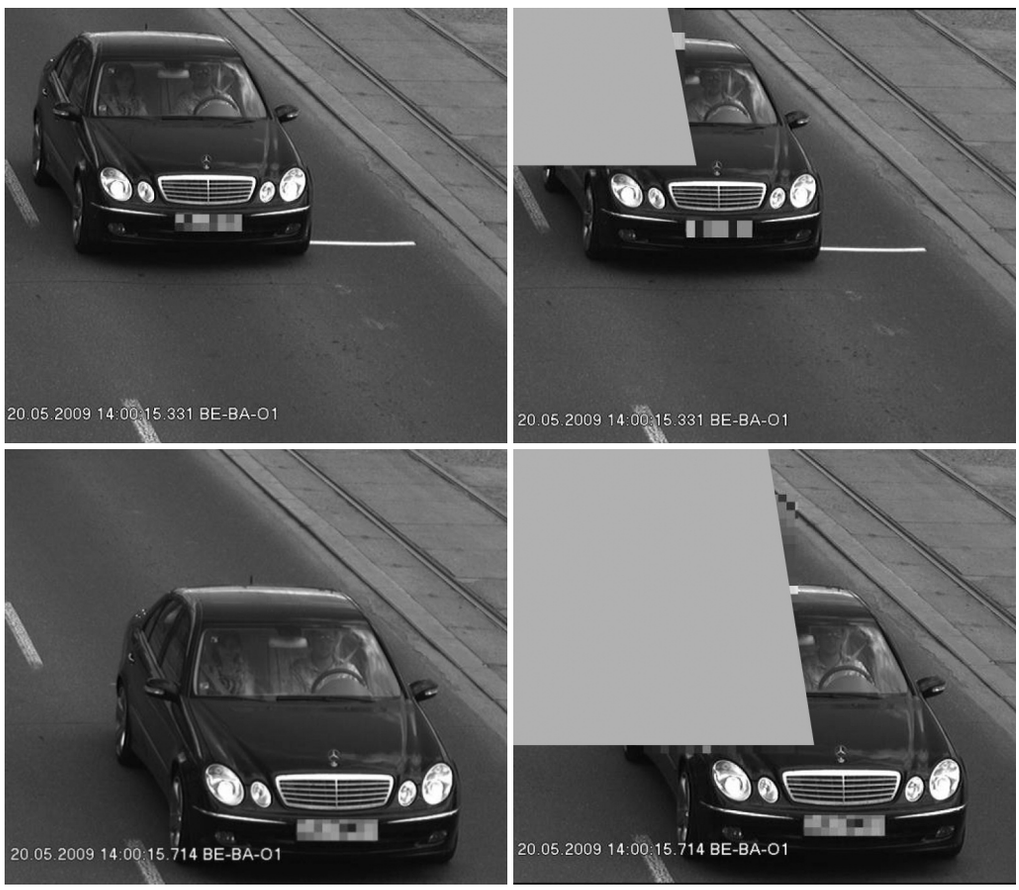
Upravený snímek US1 – automaticky upraven tak, aby byly zachovány pouze atributy nezbytné k prokázání případného přestupku – čitelná RZ1 a čára na vozovce, ale nebylo možno identifikovat řidiče ani spolujezdce

Technické řešení:
Pomocí lokalizace registrační značky se definuje oblast rozmazání nad registrační značkou.

Příklad upravovaných snímků z kamery K2

Pouze pro potřeby PČR

Pouze pro potřeby MP



Snímky S2 pořízené kamerou K2

Upravené snímky US2 – automaticky upraveny tak, aby byly zachovány pouze atributy nezbytné k prokázání případného přestupku – čitelná RZ2, čára na vozovce a tvář řidiče, ale nebylo možno identifikovat spolujezdce

Technické řešení:
Pomocí lokalizace masky vozidla s reflektory se definuje oblast zakrytí nad maskou vozidla v levé polovině odpovídající části vozidla se spolujezdcem.

INTERNET

Okolnosti a způsob vzniku internetu jsou všeobecně známé; jeho problém je, že jeho vývoj nikdo příliš nehlídal a nestanovil pravidla. Dnes je jak jejich absence, tak i snaha o jejich zavedení kritizována ze všech stran. Od roku 1980, kdy bylo na světě propojeno cca 1000 počítačů, přes rok 1990 s 1 milionem propojených počítačů až po dnešek s více než miliardou počítačů, rozprostřených po celém světě, došlo k tomu, že se na této síti odehrávají závažné věci nutné pro chod států i společnosti. Internetem se spravují účty v bankách, nakupuje se zboží, uzavírají se obchody. Státní správa přijímá podání a nově i zasílá svá rozhodnutí. Internet se stal součástí kritické infrastruktury, aniž by měl stát možnost jeho chod nějak ovlivnit, a to zejména v oblasti jeho bezpečnosti a spolehlivosti. V současné době tedy dochází v EU a zejména v USA ke změnám v legislativě, které mají vést k posílení bezpečnosti a spolehlivosti provozu internetu.

Na internetu se nachází nezměrné množství informací. Mnoho z nich se vztahuje k identifikovatelným osobám, a jde tedy o osobní údaje. Směrnice 95/46/ES se vztahuje na automatizovaná zpracování a na manuální pouze tehdy, mají-li se pořízená data stát součástí datových systémů. Úmluva č. 108, ze které uvedená směrnice vychází, stanovila, že se jedná o automatizované soubory dat, tj. takové, u kterých dochází k automatizovanému zpracování, tj. zpracování daným algoritmem, setřídění dat podle daného kritéria apod. Za automatizované zpracování osobních údajů, ve smyslu zákona o ochraně osobních údajů a podléhající registraci Úřadem, nelze považovat každé počítačové zpracování jednotlivých bytů v rámci základních počítačových funkcí, ale organizovanou činnost s komplexem informací splňujících kritéria osobního údaje. Jde tedy o to, že např. psaním nějakých údajů dochází k automatizovanému zpracování jednotlivých znaků, kdy tyto jednotlivé znaky samy o sobě nelze považovat za osobní údaje. Teprve vytvořením ucelené informace mohou nastat podmínky identifikovatelnosti. Nelze totiž tvrdit, že každé písmeno ve jméně či každá jednotlivá číslice v rodném čísle je osobním údajem a jako taková podléhá dozoru Úřadu.

Informace na internetu vztahující se k určitelným osobám totiž mohou mít soukromoprávní základ. Jak vyplývá z nálezu Ústavního soudu zn. I. ÚS 4/04 ze dne 23. března 2004, *„trestní právo a trestněprávní kvalifikace určitého jednání, které má soukromoprávní základ, jako trestného činu je třeba považovat za ultima ratio, tedy za krajní právní prostředek, který má význam především celospolečenský, tj. z hlediska ochrany základních společenských hodnot. V zásadě však nemůže sloužit jako prostředek nahrazující ochranu práv a právních zájmů jednotlivce v oblasti soukromoprávních vztahů, kde závisí především na individuální aktivitě jednotlivce, aby střežil svá práva, jimž má soudní moc poskytnout ochranu. Je však nepřijatelné, aby tuto ochranu aktivně přebíraly orgány činné v trestním řízení, jejichž úkolem je ochrana převážně celospolečenských hodnot, nikoliv přímo konkrétních subjektivních práv jednotlivce, jež svou povahou spočívají v soukromoprávní sféře.“*

V těchto případech je namístě aplikace občanskoprávní ochrany osobnosti dle zákona č. 40/1964 Sb., občanského zákoníku (dále o. z.), který upravuje v §§ 11 až 13 problematiku týkající se fyzické osoby. Pasivita jednotlivce při ochraně jeho práv či nedostatečná účinnost zákonných nástrojů sloužících k ochraně subjektivních práv osob nemůže vést k tomu, aby byla tato opatření nahrazována či doplňována prostředky práva trestního, resp. správního. Neboť podle § 13 o. z. má fyzická osoba právo se zejména domáhat, aby bylo upuštěno od neoprávněného zásahu do práva na ochranu její osobnosti, aby byly odstraněny následky těchto zásahů a aby jí bylo dáno přiměřené zadostiučinění (odst. 1 tohoto ustanovení). Obdobně postupoval i Nejvyšší soud ve svém rozhodnutí 30 Cdo 3070/2006 ze dne 21. prosince 2006 týkajícím se osobních údajů uvedených na internetových stránkách „kadran.cz“.

V oblasti zpracování osobních údajů na internetu je velmi důležitá kauza „Lindquist“.

Jde o případ, kdy paní Lindquist v rámci kurzu psaní internetových prezentací vytvořila v roce 1998 stránku, na které přehledně shromáždila informace o 18 žácích, kteří se připravovali na svaté přijímání. Paní Lindquist popsala mírně humorným způsobem informace o jejich práci

a jejich zálibách. Žáci byli uvedeni někdy celým jménem a někdy pouze křestním jménem, ve většině případů byly uvedeny rodinné poměry, telefonní čísla a další informace jako např. informace o úrazu nohy atp.

Paní Lindquist byla obžalována z porušení švédských právních předpisů na ochranu osobních údajů za to, že publikovala na internetu osobní údaje v souvislosti s přípravou několika žáků na svaté přijímání ve farnosti švédského protestantského kostela.

Vzhledem k pochybnostem o správnosti výkladu práva Společenství v této věci se odvolací soud obrátil na Soudní dvůr s žádostí o vydání předběžného rozhodnutí v několika otázkách.

Soudní dvůr jako odpověď na otázky předložené mu soudem Göta hovrätt žádostí ze dne 23. února 2001 vydal rozhodnutí, ve kterém je mimo jiné uvedeno:

„1. Úkon uvedení různých osob na internetové stránce a jejich identifikace jménem nebo jiným způsobem, například uvedením jejich telefonního čísla nebo informace o jejich pracovním poměru a zájmech, je zpracováním osobních údajů zcela nebo částečně automatizovaně ve smyslu čl. 3 odst. 1 směrnice 95/46/ES Evropského parlamentu a Rady ze dne 24. září 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů.

2. Na takové zpracování osobních údajů se nevztahuje žádná z výjimek uvedených v čl. 3 odst. 2 směrnice 95/46.

3. Informace, že jednotlivec utrpěl úraz nohy a je částečně invalidní, je osobní údaj týkající se zdraví ve smyslu čl. 8 odst. 1 směrnice 95/46.

4. Nejedná se o předávání osobních údajů do třetí země ve smyslu čl. 25 směrnice 95/46, když jednotlivec v členském státě vloží osobní údaje na internetovou stránku, která je uložena na internetu na místě, kde může být konzultována, a která hostuje u právnické osoby založené v tomto státě nebo v jiném členském státě, a tak jsou data přístupná každému, kdo se připojí k internetu, i osobám ve třetí zemi...“

Tento výrok je třeba v komplexu chápat tak, že byly shromážděny a následně zpracovány údaje o více (18) osobách a takto byly nahrány na server, včetně způsobu jejich interpretace (kód internetové stránky). Účelem tohoto zpracování bylo právě podání uvedených informací o těchto osobách. Tím, kdo stanovil účel a prostředky zpracování uvedených osobních údajů, byla nepochybně paní Lindquist.

Bylo by však asi nesmyslné a prakticky nemožné bránit uvedení jmen různých osob, odkazů na jejich práci či záliby na internetových stránkách bez jejich výslovného povolení. Znamenalo by to, že by nebylo možné se zmínit o ostatních lidech na blogu, novináři by nemohli o nikom psát v článcích, společnosti by se nemohly zmínit o svých členech, vydavatelé by se nemohli zmínit o autorech, fanoušci by se nemohli zmínit o zpěvácích nebo hercích... ledaže by měli jejich výslovný souhlas. Každé toto zpracování by se před jeho zahájením muselo zaregistrovat u Úřadu. Znamenalo by to, že by Úřadu každý musel dopředu hlásit to, že se chystá napsat článek, ve kterém se zmíní o někom konkrétním. Takový postup by jistě nebyl namístě a nebyl by ani prakticky proveditelný.

Odpovědnost za informace šířené internetem

Nalézt osobu odpovědnou za informace, které lze na internetu najít, je obtížné, a existuje mnoho nástrojů, které anonymitu posilují. Odpovědnost se tedy jak v EU, tak v USA přenáší na poskytovatele služeb informační společnosti, tj. na správce serverů. Zjistit potřebné připojovací údaje je totiž možné pouze v případě šetření trestného činu, a to podle § 97 zákona o elektronických komunikacích. Pokud se však jedná o přestupek či správní delikt, není poskytovatel služby informační společnosti (webhosting, provider...) oprávněn sdělit potřebné informace. Problém je tedy i v případě, že je autor správnímu orgánu „znám“, tj. např. když se autor ke svému dílu veřejně hlásí a vést správní řízení bez objektivního zjištění skutečnosti nemusí přinést kýžený výsledek. Je velmi obtížné určení osoby správce z pohledu zákona o ochraně osobních údajů, tj. toho, kdo určil způsob a prostředky tohoto zpracování.

Jisté možnosti opět dává zákon o některých službách informační společnosti, a to v § 5, který stanoví *„Odpovědnost poskytovatele služby za ukládání obsahu informací poskytovaných uživatelem:“*

„(1) Poskytovatel služby, jež spočívá v ukládání informací poskytnutých uživatelem, odpovídá za obsah informací uložených na žádost uživatele, jen

a) mohl-li vzhledem k předmětu své činnosti a okolnostem a povaze případu vědět, že obsah ukládaných informací nebo jednání uživatele jsou protiprávní, nebo

b) dozvěděl-li se prokazatelně o protiprávní povaze obsahu ukládaných informací nebo o protiprávním jednání uživatele a neprodleně neučinil veškeré kroky, které lze po něm požadovat, k odstranění nebo znepřístupnění takovýchto informací.

(2) Poskytovatel služby uvedený v odstavci 1 odpovídá vždy za obsah uložených informací v případě, že vykonává přímo nebo nepřímo rozhodující vliv na činnost uživatele.“

Sám poskytovatel uvedené služby, který je nepochybně zpracovatelem dle zákona o ochraně osobních údajů, tedy nemá přímou odpovědnost za obsah a je třeba ho o protiprávnosti obsahu uvedených stránek či jednání uživatelů účinně informovat. V tomto bodě je třeba definovat, co jsou to služby informační společnosti. Uvedený zákon to stanoví v § 2 tak, že službou informační společnosti je jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou elektronickými prostředky, poskytovaná zpravidla za úplatu; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat. Elektronickými prostředky se zde rozumí zejména síť elektronických komunikací, elektronická komunikační zařízení, koncová telekomunikační zařízení a elektronická pošta.

Poskytovatelem služby se rozumí každá fyzická nebo právnická osoba, která poskytuje některou ze služeb informační společnosti, a uživatelem každá fyzická nebo právnická osoba, která využívá službu informační společnosti, zejména za účelem vyhledávání či zpřístupňování informací. Z uvedeného vyplývá, že se jedná o služby, jako je „hosting“ čili poskytnutí diskové kapacity s možným dálkovým přístupem. Jde tedy nejen o webové stránky, ale i různá sdílená data jako fotografické galerie, různá videa apod. V této souvislosti je třeba chápat informace jako data, neboť se nejedná o informace zaručené ústavou, ale o data, která jsou mnohdy obchodním artiklem. Pokud například zakoupíte v internetovém obchodě nějaká data (program, hudbu aj.) a necháte si je zaslat, např. vypálená na CD, jde o klasický obchodní případ, pokud si je však necháte zaslat e-mailem či je sami stáhnete z webu, jde o službu informační společnosti.

Poskytovatel služby by měl mít smluvně podchycenu možnost ukončení poskytované služby při podezření na protiprávní obsah. Jde o to, aby se vyvaroval případných obchodních sporů v případě jeho odstranění či zablokování.

NEVYŽÁDANÁ OBCHODNÍ SDĚLENÍ

Statistika – NOS – za rok 2009:

Podněty (stížnosti) na šíření nevyžádaných obchodních sdělení	2 261
Vyřešené podněty (stížnosti) na šíření nevyžádaných obchodních sdělení	1 678
Neoprávněné podněty (stížnosti) – tzn. nejednalo se o obchodní sdělení nebo se jednalo o zahraniční obchodní sdělení či spam	266
Případy, ve kterých se nepodařilo dohledat odesílatele	91
Zahájených kontrol (počet kontrolovaných subjektů)	145
Ukončených kontrol	131
Počet subjektů, kterým bylo uloženo nápravné opatření	456
Počet správních řízení	112
Celková výše pokut za tato správní řízení	797 000 Kč

Oproti loňskému roku, kdy počet podaných stížností na šíření nevyžádaných obchodních sdělení dosáhl počtu zhruba 1 500 stížností, došlo v roce 2009 k velkému nárůstu, a to zhruba o 1/3. Příčin může být několik.

Jednou z nich je, že tento způsob komunikace (zasílání obchodních sdělení pomocí elektronických prostředků) je pro firmy stále efektivní a adresáti nevyžádaných obchodních sdělení si to již nenechávají líbit. Dalším důvodem, který jsme při naší kontrolní činnosti vysledovali, je skutečnost, že též podnikatelé přestali být lhostejní k obdrženým nevyžádaným obchodním sdělením, a to především poté, co byli Úřadem za nevyžádaná obchodní sdělení sami finančně postiženi.

Jinou příčinou nárůstu může být i nový fenomén internetové komunikace, který se v roce 2009 značně rozšířil, tzv. virální marketing. Ten funguje na principu „pošli to dál". Nabídka je tak přenášena pomocí lidí (lidského řetězce). Cílem je zvýšení prodeje, rozšíření obchodního potenciálu a budování povědomí o značce, a to s minimálními náklady. Takové nabídky, aby byly efektivní, mají podobu různých her, vtipných videí, audiosouborů, kdy často až na konci ukázky adresát zjistí, o jakou nabídku či propagaci jaké firmy se jedná. Podle zákona o některých službách informační společnosti se za obchodní sdělení považují „všechny formy sdělení určeného k přímé či nepřímé podpoře zboží či služeb nebo image podniku fyzické či právnické osoby, která vykonává regulovanou činnost nebo je podnikatelem vykonávajícím činnost, která není regulovanou činností; za obchodní sdělení se považuje také reklama podle zvláštního právního předpisu". V případě virálního marketingu se tedy o obchodní sdělení nepochybně jedná. Problém však nastává v případě odesílatele. Za rozesílání nevyžádaných obchodních sdělení totiž lze postihnout pouze odesílatele, a nikoliv toho, v čí prospěch je obchodní sdělení odesíláno. To se může stát například u tzv. přeposílání, kdy první adresát dá firmě souhlas se zasíláním obchodních sdělení; v takovém případě se o nevyžádané obchodní sdělení nejedná. On tuto zprávu (obchodní sdělení) přepošle dále, toto následné přeposílání se pak odehrává v rovině běžné korespondence mezi příbuznými, kolegy, kamarády..., a nelze tedy firmu, v jejíž prospěch je takto dále šířeno, postihnout.

Jiná situace však může nastat v případě jiného způsobu či techniky virálního marketingu, kterým jsou tzv. výzvy na webu, kdy webové stránky firem obsahují odkazy typu „pošli známému", „doporuč kamarádovi"... Po rozkliknutí takového odkazu se objeví připravená nabídka firmy, kterou lze okamžitě odeslat. Z hlediska zákona o některých službách informační společnosti jsou tyto případy poměrně jasné. Podle § 3 uvedeného zákona poskytovatel služby odpovídá za obsah přenášených informací, jen pokud:

a) přenos sám iniciuje,

b) zvolí uživatele přenášené informace, nebo

c) zvolí nebo změní obsah přenášené informace.

V případě takto provozovaného virálního marketingu jde tedy o třetí možnost, neboť zatímco přenos je iniciován a uživatele volí odesílající osoba, obsah je již předpřipraven samotnou firmou. Odpovědný je tedy jak odesílatel, tak též firma, v jejíž prospěch je nabídka tímto způsobem odeslána.

Zahraniční praxe

Úřad spolupracuje s ostatními členskými státy Evropské unie a je členem několika pracovních skupin. Ve vztahu k elektronickým komunikacím jsme členem pracovní skupiny CNSA (Contact Network of Spam Authorities). Díky této spolupráci a aktivitám máme možnost porovnat naše postupy a legislativu s tou zahraniční.

Jednou ze zemí, které jsou v boji se spamem nejdále, je například Holandsko. Výměna zkušeností s kolegy z Holandska je velkým přínosem, neboť již prošli fází, ve které se my nyní nacházíme; a máme tak možnost vyvarovat se chyb nebo urychlit vývoj směrem k účinnějšímu boji proti nevyžádaným sdělením a jiným nekalým praktikám provozovaným prostřednictvím sítě elektronických komunikací.

Jedním z aspektů této problematiky je potřeba rozlišovat mezi těmi, kdo úmyslně rozesílají spam v rozporu se zákonem, a těmi, kdo se snaží legálně podnikat a zasílají své obchodní nabídky prostřednictvím sítě elektronických komunikací a porušují zákon, aniž by si uvědomili, že se chovají

protiprávně. Dále je třeba přihlédnout k tomu, jaká vzniká škoda nebo újma způsobená rozesíláním obchodních sdělení. Tuto skutečnost můžeme odhadnout z počtu došlých stížností směřovaných proti jednomu ekonomickému subjektu, který je zodpovědný za rozesílání. Zkušenosti zahraničních kolegů jsou takové, že pokud se tvrdě trestá každé sebemenší porušení zákona na příklad v případě malého živnostníka, který rozeslal desítky e-mailů, v nichž nabízel své výrobky, které skutečně prodává, a nejedná se tedy o podvodnou nabídku, leč úřad mu uloží sankci už tehdy, kdy přijme jednu stížnost proti tomuto subjektu – má to pouze jediný výsledek: Tento subjekt, bude-li chtít rozesílat svá obchodní sdělení, nebude se snažit najít způsob, jak dodržet zákon, ale jak ho obejít. Tak se státní autorita *de facto* může podílet na vzrůstajícím počtu případů, kdy dochází k porušování zákona.

V Holandsku si to uvědomili a přijali určitá opatření a následně došlo i ke změnám legislativním, aby pozornost dozorových orgánů byla zaměřena na vážné problémy v oblasti elektronických komunikací, ať už se jedná o rozesílání škodlivých kódů nebo nabízení produktů mnohdy neexistujících firem. Je těžké určit, kdy se jedná o závažný problém, a kdy nikoliv. Proto v mnoha státech, kde už mají více zkušeností s řešením těchto problémů, přistoupili na jakýsi typ samoregulace: Závažnost případu se dovozuje na základě počtu stížností. Je totiž velmi nepravděpodobné, že se při obdržení jediné stížnosti jedná o závažný případ, který je třeba tvrdě trestat. Proto by bylo záhodno nastavit pro každou zemi specifický filtr, který by pomocí metody hromadnosti a závažnosti určoval, jak ke kterému případu přistupovat.

VYŘIZOVÁNÍ STÍŽNOSTÍ A POSKYTOVÁNÍ KONZULTACÍ

I v roce 2009 pokračoval trend nárůstu počtu dotazů, žádostí o právní názor či stanovisko, podnětů a stížností občanů k uplatnění dozorových činností Úřadu. Odbor pro styk s veřejností byl nucen optimalizovat své pracovní přístupy, tedy poskytovat prvotní právní posouzení obsahu podání z hlediska porušování povinností při zpracování osobních údajů a poskytování konzultací důsledně pouze v rozsahu působnosti Úřadu. Rozměr konzultací a odpovědí odboru dříve velmi často prvotně vycházel široce vstříc potřebám tazatelů. Zejména advokátní kanceláře požadovaly jménem svých klientů posouzení často složitých právních otázek souvisejících s obchodními vztahy právnických osob, které zákonu č. 101/2000 Sb. nepodléhají.

U telefonických dotazů byly zpravidla v souvislosti s medializovanými kauzami ochrany osobních údajů vyžadovány kvalifikovaně strukturované odpovědi, což kladlo, kromě značného časového vytížení jednotlivých referentů, enormní nároky i na jejich odbornou erudovanost. V závěru roku 2009 bylo proto nezbytné informovat veřejnost sdělením na webových stránkách Úřadu, že telefonicky budou poskytovány jen základní informace v obecné rovině a další postup tazatele se musí odvíjet především v písemné a elektronické komunikaci, případně formou osobní konzultace.

Z 62 osobních konzultací poskytnutých v roce 2009 orgánům státní správy, samosprávy, právnickým osobám, podnikajícím i nepodnikajícím fyzickým osobám, majících postavení správců a zpracovatelů osobních údajů, jejich zaměstnanců, ale i subjektů osobních údajů, pro ilustraci uvádíme nejdůležitější: ministerstva zahraničí, financí, životního prostředí, průmyslu a obchodu, Státní úřad pro jadernou bezpečnost, Český statistický úřad, Báňský úřad, LIDL Česká republika, v. o. s., Centrum pro zjišťování výsledků vzdělávání, Národní ústav odborného vzdělávání, Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

Přes pokračující nárůst počtu obdržených dotazů (odpovězeno na 1 934 oproti 1 778 v roce 2008) činila průměrná doba jejich vyřízení dva týdny. Nutno podotknout, že se nadále zvyšovala kvalifikovanost dotazů a požadavků na posouzení předložených projektů, z nichž k nejrozsáhlejším patřily: vedení evidence v souvislosti s připravovanou emisí státních dluhopisů, testování databáze cestovních

dokladů s biometrickými údaji, využití body scannerů fungujících na principu ionizujícího záření na letištích a různé typy interních předpisů vydávaných správci osobních údajů v souvislosti s povinnostmi uloženými § 13 zákona č. 101/2000 Sb.

Podnětů k zahájení řízení z moci úřední bylo vyřízeno celkem 879, což je, oproti roku 2008, nárůst o 26 %. Největší nárůst se promítl do počtu podání odložených jako nedůvodných, dvojnásobný počet stížností byl postoupen věcně příslušným orgánům veřejné správy a došlo k poměrně výraznému snížení počtu stížností předávaných k další analýze před zahájením kontroly (o 36 %). Společným důvodem tohoto stavu byly typově se opakující stížnosti nezakládající důvodné podezření z porušení zákona č. 101/2000 Sb. Anonymní podání byla zpravidla odkládána, s výjimkou stížností, z nichž vyplývala důvodná obava stěžovatele z postihu ze strany správce osobních údajů, což bylo patrné především v oblasti pracovněprávních vztahů, a to včetně reálného rizika ztráty zaměstnání. Dále byl brán v úvahu rozsah vedených databází osobních údajů a předpoklad opakování činnosti správci a zpracovateli zakládající závadný stav.

Statistika stížností vyřízených v roce 2009:

Celkem	879
z toho:	
předáno ke kontrole	129
předáno na zahájení řízení	43
postoupeno příslušným orgánům	24
odloženo s vyrozuměním	683

Častým předmětem zájmu občanů v postavení subjektů údajů byly i v roce 2009 kamerové systémy (více než čtvrtina celkového počtu stížností), zveřejňování osobních údajů na internetu a zpracovávání citlivých údajů ve zdravotnictví. Přestože jsou těmto problematikám věnovány samostatné pasáže výroční zprávy, považujeme za nutné uvést několik postřehů.

Úřad byl nucen zabývat se řadou stížností (36) na provozování kamerových systémů soukromými osobami, tedy v režimu § 3 odst. 3 zákona č. 101/2000 Sb. (dále jen „zákon“). Pokud nebylo prokázáno zneužití pořízených záběrů pro jiný než deklarovaný účel, tedy převážně ochranu vlastního majetku, a to včetně poskytnutí inkriminovaných záběrů orgánům činným v trestním řízení, byli stěžovatelé odkazováni s řešením svých sousedských sporů na občanský zákoník. V této souvislosti byly zaznamenány i zcela paradoxní dotazy potenciálních provozovatelů kamerových systémů, např. zda se nedostanou do rozporu se zákonem, pokud na pořízeném záběru kamery snímající neprůhledná vrata, která překonávají zloději stavebního materiálu, bude zaznamenána hlava osoby jedoucí na koni na veřejném prostranství za hranicí soukromého pozemku. Poměrně komplikovaným problémem je právo subjektu údajů na informaci podle § 12 zákona o zpracování svých osobních údajů, respektive na přímé prohlížení záznamů, aniž by byla dotčena práva dalších osob zaznamenaných kamerovým systémem. Pokud bude provozovatel kamerového systému postupovat v souladu s § 5 odst. 1 písm. e) zákona, bude předmětný záznam obvykle již vymazán. Z § 12 zákona tak nelze dovodit povinnost uchovávat záznam z důvodu vyřizování žádosti subjektu údajů déle, než je pro dosažení stanoveného účelu nezbytné (pohybuje se zpravidla v řádu několika dnů). Informační povinnost uloženou § 11 zákona může správce splnit i bez vlastního zpřístupnění pořízeného kamerového záznamu.

Primárním problémem zveřejňování osobních údajů na internetu je faktická nemožnost jejich zabezpečení na úrovni požadované § 13 zákona. Obdobně jako u kamerových systémů nebylo Úřadem zasahováno do vztahů, které lze řešit soukromoprávní cestou. Jednalo se o případy jednorázových, často nahodile získaných a následně zveřejněných osobních údajů. Naopak, pokud došlo k úniku informací z databáze systematicky zpracovávaných osobních údajů, je odpovědnost jejich správce za únik na internet již zcela zřejmá a takovéto případy byly řešeny v rámci dozorových činností Úřadu. Obecně lze uzavřít, že každý jednotlivý případ je nutno posuzovat důsledně individuálně.

Speciálním problémem je požadavek zabezpečené komunikace, k níž s účinností od 1. listopadu 2009 patří informační systém datových schránek. Na četné dotazy k této problematice Úřad odpovídal ve smyslu, že dosud nedisponuje poznatky o odůvodněnosti jejich nevyužívání s odkazem na principy ochrany osobních údajů, samozřejmě za předpokladu, že jsou provozovány v souladu se zvláštním zákonem č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.

Nejfrekventovanějším předmětem dotazů a stížností v roce 2009 bylo shromažďování osobních údajů pro daný účel nadbytečných především mobilními operátory, a to pořizováním kopií občanského průkazu, které je upraveno zákonem č. 328/1999 Sb., o občanských průkazech, ve znění pozdějších předpisů. Přestože porušení ustanovení § 2 odst. 6 tohoto zákona je přestupkem, k jehož vyřízení jsou příslušné obecní úřady obcí s rozšířenou působností, dochází tímto způsobem i k porušení povinnosti shromažďovat osobní údaje pouze v rozsahu nezbytném pro naplnění stanoveného účelu, kterému v tomto případě nebude odpovídat např. fotografie klienta nebo osobní údaje jeho příbuzných. Osobním dopisem předsedy Úřadu byl proto požádán předseda představenstva jednoho ze subjektů majících kontraktační povinnost při poskytování telekomunikačních služeb o zjednání systémové nápravy. Závadný stav bohužel přetrvává včetně vyžadování kopií dalších osobních dokladů, nejčastěji řidičského průkazu, které je při uzavírání smluvního vztahu již zcela irelevantní, neboť občan je povinen prokazovat svoji totožnost občanským průkazem. Úřad se této problematice bude věnovat i v příštím roce.

POZNATKY ZE SPRÁVNÍCH ŘÍZENÍ

ZPRACOVÁNÍ PROFILŮ DNA V NÁRODNÍ DATABÁZI DNA

S tím, jak se využívání genetických informací stává stále běžnějším, setkává se také Úřad s problematikou zpracování těchto citlivých údajů stále častěji. V roce 2009 se Úřad v této oblasti opět zabýval otázkou uchování profilu DNA Policií České republiky v tzv. Národní databázi DNA, konkrétně posuzováním případu stěžovatele, který byl odsouzen za zvlášť závažný trestný čin hospodářské povahy a jehož vzorek DNA byl získán při hromadném odběru, kdy Policie České republiky provedla bukální stěry všem osobám, které se v dané době nacházely ve výkonu trestu odnětí svobody pro úmyslný trestný čin.

Rozhodování v obdobných případech je s ohledem na absenci dostatečné právní úpravy využívání DNA při činnosti Policie České republiky poměrně obtížné, neboť je třeba vždy individuálně posoudit a aplikovat velmi obecné právní normy, na nichž se Národní databáze DNA v České republice zakládá. Úřad se nicméně může v těchto případech argumentačně opřít mimo jiné o rozsudek Evropského soudu pro lidská práva ve věci S. a Marper proti Spojenému království (rozhodnutí velkého senátu zn. 30562/04 a 30566/04 ze dne 4. prosince 2008; dále jen „ESLP“ a „rozhodnutí ESLP“). V tomto svém rozhodnutí ESLP konstatoval, že i pouhé uchovávání profilu DNA představuje zásah do práva podle čl. 8 Úmluvy o ochraně lidských práv a základních svobod, a to bez ohledu na to, zda je tato informace dále využita, nebo ne. Takový zásah je přitom v demokratickém a právním státě opodstatněný pouze při stanovení jasných, zákonem specifikovaných, dostatečně určitých a restriktivně pojatých pravidel. ESLP dále považuje za zcela zásadní, aby národní legislativa poskytovala dostatečné záruky k ochraně před zneužitím osobních údajů, přičemž nezbytnost těchto garancí roste v případě automatizovaného zpracování dat, a to zejména v rámci působnosti orgánů činných v trestním řízení. Právní řád musí tedy mimo jiné zaručit, aby zpracovávané údaje byly relevantní a nezbytné vzhledem k účelu, pro který byly zajištěny, a aby byly uchovávány ve formě umožňující identifikaci osob pouze po dobu nezbytnou k dosažení sledovaného účelu. Uvedené platí o to více v případě citlivých genetických údajů (tj. údajů získaných rozborem DNA).

Současně je třeba upozornit, že Úřad se v obdobných případech zabývá otázkou uchovávání profilu DNA v Národní databázi DNA, nikoli oprávněností či nezbytností odběru biologického vzorku v souvislosti s vyšetřováním konkrétního trestného činu. Tyto dvě situace je dle Úřadu nutno důsledně odlišovat, neboť další uchovávání získaného profilu DNA *pro futuro*, na rozdíl od odběru a využití vzorku v souvislosti s vyšetřováním konkrétního trestného činu, sleduje zcela odlišný účel.

V návaznosti na znění zákona č. 273/2008 Sb., o Policii České republiky (účinného od 1. ledna 2009, dále jen „zákon o policii"), a citovaný rozsudek ESLP vycházel Úřad v této věci ze skutečnosti, že zákon o policii neobsahuje výslovné zmocnění pro vytvoření a naplňování Národní databáze DNA a opravňuje policisty zpracovávat citlivé údaje osob (tedy i profil DNA) bez souhlasu, jen pokud je to nezbytné pro plnění úkolů Policie České republiky, současně však již nestanoví, co se rozumí pojmem „nezbytné".

Na základě těchto skutečností Úřad dospěl k závěru, že zákon o policii neobsahuje jasná a dostatečně určitá pravidla pro zpracování osobních a citlivých údajů v Národní databázi DNA. Chybějící jasná zákonná pravidla musí proto Úřad dovodit výkladem obecných pojmů zákona o policii s využitím Úmluvy o ochraně lidských práv a základních svobod, judikatury ESLP a také Doporučení č. R (92) 1 Výboru ministrů členským státům (Rady Evropy) o využívání analýzy deoxyribonukleové kyseliny (DNA) v rámci systému trestní justice. Dle čl. 8 tohoto doporučení mohou být výsledky analýzy DNA a informace z nich odvozené uchovány pouze tehdy, jestliže byl dotčený jednotlivec odsouzen pro závažné trestné činy ohrožující život, zdraví nebo bezpečnost osob. Jelikož se v posuzované věci jednalo o trestný čin hospodářský, nespadající pod toto vymezení, které Úřad považuje za zásadní vodítko (při absenci jiné právní úpravy) pro restriktivní výklad oprávnění Policie České republiky k uchování profilů DNA v Národní databázi DNA, dospěl k závěru, že zařazením předmětného profilu DNA do Národní databáze DNA byl porušen zákon o ochraně osobních údajů.

Úřad svým rozhodováním v obdobných věcech nezpochybňuje legitimitu existence Národní databáze DNA, nicméně důsledně požaduje, aby byl tento nástroj používán, pouze je-li zároveň splněna podmínka nezbytnosti zpracování citlivých údajů pro plnění úkolů Policie České republiky. Úřad přitom nemůže z hlediska své kompetence připustit, aby nezbytnost uchovávání profilů DNA v této databázi byla deklarována bez dalšího, např. u každého úmyslného trestného činu, nadto bez jednoznačného zákonného zmocnění.

ZVEŘEJŇOVÁNÍ OSOBNÍCH ÚDAJŮ OBCEMI

V souvislosti s výkonem svých dozorových kompetencí se Úřad opakovaně setkává s otázkou zveřejňování osobních údajů v rámci činností obcí, ať již v oblasti přenesené, nebo samostatné působnosti. Úřad si je vědom toho, že obce musí dostát požadavkům na transparentní výkon svých činností a současně respektovat práva na soukromí dotčených osob, což může být ve změti právních předpisů nesnadný úkol. V zájmu prevence porušování zákona o ochraně osobních údajů se Úřad k různým aspektům zpracování osobních údajů obcemi vyjadřuje ve svých stanoviscích a dalších textech publikovaných především na webových stránkách. Nicméně v situaci, kdy je zjištěno a prokázáno, že došlo k zásahu do práv chráněných zákonem o ochraně osobních údajů, je třeba ve správním řízení uložit dané obci sankci, byť i po téměř 10 letech existence Úřadu jsou pokuty v této oblasti stále spíše v symbolické výši.

Při zveřejňování informací je dle Úřadu zapotřebí důsledně zvážit rizika spojená s uvedením osobních údajů (tj. informací mnohdy způsobilých citelně zasáhnout do soukromí osob) v médiích a zejména na internetu, kde je možné informace dohledat i po dlouhé době od uveřejnění. Problematiku zveřejňování osobních údajů obcemi, se kterou se Úřad setkal v roce 2009, lze rozdělit do několika oblastí:

Návrh programu jednání zastupitelstva obce
Vyřizování podání občanů (žádostí, stížností či podnětů)
Usnesení z jednání zastupitelstva či rady obce
Úkony obce v rámci správního řízení
Informování v obecním zpravodaji

Návrh programu jednání zastupitelstva obce

Jedna z povinností směřujících ke zvýšení transparentnosti činnosti obcí je vyjádřena v § 93 odst. 1 zákona o obcích, dle kterého má obecní úřad alespoň 7 dní před zasedáním zastupitelstva obce informovat o místě, době a navrženém programu připravovaného zasedání. Tuto informaci je třeba vyvěsit na úřední desce obecního úřadu, případně lze informaci uveřejnit ještě jiným, v místě obvyklým způsobem. Je nepochybné, že velmi často budou na jednání zastupitelstva obce diskutovány otázky týkající se konkrétních fyzických osob, a nedílnou součástí takového jednání tedy budou osobní údaje.

Informování o návrhu programu jednání zastupitelstva je zákonem uloženou povinností, jejímž primárním smyslem je dle Úřadu informování o činnosti a záměrech obce, tj. o věci, která bude projednána, nikoli o osobách, kterých se věc týká. Ustanovení § 93 zákona o obcích výslovně povinnost zveřejňovat v rámci informace o navrženém programu osobní údaje těch, kterých se týkají projednávané věci, nestanoví. V takové situaci je třeba dospět k závěru, že zveřejnění osobních údajů pro splnění této povinnosti není nezbytné. V souladu se zákonem o ochraně osobních údajů je tak dle Úřadu postup, kdy je v návrhu programu (v případě, kdy se daný bod týká konkrétní fyzické osoby) uveden buď pouze popis věci, anebo iniciály jména a příjmení a obec bydliště (popř. část obce, nikoli ale přesná adresa).

Uvedené platí obdobně také pro případné zveřejňování dokumentů, které mají být projednány a které obsahují osobní údaje např. žadatelů či stěžovatelů. Z hlediska zákona o ochraně osobních údajů není rozhodné, zda dochází ke zveřejnění osobních údajů formou informace obce, anebo přímo zveřejněním předmětné (např. naskenované) listiny.

Veškeré informace (včetně osobních údajů) je samozřejmě možné, resp. nezbytné prezentovat při samotném jednání zastupitelstva. Tento odlišný postup je dán tím, že ve fázi zveřejnění návrhu programu jednání dochází ke zpřístupnění všech informací neomezenému okruhu osob (zejména prostřednictvím internetu), tedy i osobám ve věci naprosto nezainteresovaným.

Této problematice se Úřad blíže věnuje také na svých webových stránkách v rubrice Názory Úřadu – K problémům z praxe.

Vyřizování podání občanů (žádostí, stížností či podnětů)

Významnou součástí činností obcí je nepochybně také problematika vyřizování nejrůznějších podnětů, stížností, petic či žádostí občanů. Zřejmě ve snaze o co nejotevřenější postup při vyřizování podání zveřejňují obce některé kauzy (zejména sporné otázky jako např. nesouhlas se záměrem výstavby nebo stížnost na neplnění smluvních závazků ze strany obce) na svých webových stránkách, případně v místním tisku. Také v tomto případě dochází často ke zpracování osobních údajů, neboť občané obracející se na obec se ve svém podání identifikují obvykle jménem, příjmením, adresou bydliště, případně i datem narození nebo dokonce rodným číslem.

V souvislosti s vyřizováním podání občanů nelze v příslušných právních předpisech (především zákon o obcích, ale např. také správní řád) nalézt žádný právní titul, tedy oprávnění, ke zveřejnění osobních údajů v předmětném podání obsažených. Na základě požadavku vyjádřeného v návětí § 5 odst. 2 zákona o ochraně osobních údajů je tedy pro takové zpracování osobních údajů nutno disponovat souhlasem dotčených osob. Tento postup bude však možný pouze v některých případech, častější a pravděpodobně také vhodnější bude cesta anonymizace osobních údajů. Jinými slovy v situaci, kdy obec považuje za potřebné informovat o podání učiněném občany veřejnost, lze tak – s odkazem na smysl tohoto jednání, kterým je transparentnost co do projednávané věci, nikoli osob s ní spojených – učinit zveřejněním anonymizované informace, případně i samotného podání, v němž budou osobní údaje důsledně znečitelněny.

Usnesení z jednání zastupitelstva či rady obce

K otázce zveřejňování usnesení z jednání orgánů obce (zastupitelstva a rady), resp. výpisů z těchto usnesení, se Úřad vyjádřil již ve svém stanovisku č. 2/2004 – Zpřístupňování a zveřejňování osobních údajů z jednání zastupitelstev a rad obcí a krajů (viz www.uoou.cz/Názory Úřadu/Stanoviska).

Východiskem při aplikaci povinností stanovených zákonem o ochraně osobních údajů v této oblasti je důsledné rozlišování práva na účast na jednání orgánu obce, resp. práva na nahlížení do zápisů z těchto jednání, a práva na informace o činnosti obce.

Zákon o obcích výslovně definuje okruh osob oprávněných účastnit se jednání zastupitelstva obce (jednání rady nejsou veřejná) a okruh osob, které mají právo nahlížet do usnesení z jednání. Konkrétně se jedná o občany obce, fyzické osoby, které vlastní nemovitost ležící na území obce, a dále cizí státní občany, kteří jsou v obci hlášeni k trvalému pobytu, stanoví-li tak mezinárodní smlouva, jíž je Česká republika vázána a jež byla vyhlášena (viz § 16 a 17 zákona o obcích). Tento okruh osob je na základě zákona o obcích oprávněn seznamovat se, ať již přímo na jednání zastupitelstva, nebo nahlížením do zápisu z jednání rady či zastupitelstva, s celým obsahem jednání, tedy s obsahem všech dokumentů týkajících se projednávaných záležitostí, včetně osobních údajů osob, o nichž bylo jednáno. Tento postup je v souladu s § 5 odst. 2 písm. a) zákona o ochraně osobních údajů a není k němu zapotřebí souhlas dotčených osob.

Jiná situace však nastává v případě zveřejňování informací o činnosti obce široké veřejnosti, především na webových stránkách nebo v tisku. Povinnost obce postupovat transparentně a podávat informace o své činnosti vyplývá jak ze zákona o obcích, tak ze zákona o svobodném přístupu k informacím. V tomto případě však dochází ke zpřístupnění informací nejen uvedenému, zákonem úzce definovanému okruhu osob (tzv. občanů obce), ale *de facto* neomezenému počtu příjemců. Zásadní rozdíl proti výše uvedené situaci však spočívá v účelu zveřejňování informací obcí, kterým je v tomto případě transparentní výkon státní správy a samosprávy, nikoli informování o konkrétních osobách, jejichž záležitosti byly projednány. Ostatně zákon o svobodném přístupu k informacím tento princip výslovně odráží v § 8a, dle kterého právě osobní údaje do režimu tohoto zákona nespadají. Zveřejnění osobních údajů (např. v rámci zápisu usnesení z jednání zastupitelstva rady na webových stránkách) není v tomto případě dle zákona o ochraně osobních údajů možné jinak než se souhlasem osob, kterých se tyto údaje týkají. Praktičtějším postupem ale zřejmě bude anonymizace zveřejňovaných údajů. Obecně lze říci, že z hlediska požadavků na ochranu osobních údajů bude přípustné uvedení iniciál jmen a příjmení a obce, popř. části obce.

Úkony obce v rámci správního řízení

V rámci správních řízení, která obce vedou, dochází někdy k situaci, kdy je třeba doručit určitou písemnost zveřejněním na úřední desce, resp. elektronické úřední desce na webových stránkách obce. Takovým případem může být řízení s velkým počtem účastníků, kdy lze v souladu s § 144 odst. 5 a 6 správního řádu doručovat veřejnou vyhláškou. Takto doručované (zveřejněné) písemnosti musí mít veškeré požadované náležitosti, a budou tedy obsahovat také osobní údaje všech účastníků řízení. Zveřejnění osobních údajů tímto způsobem je tak zákonem předvídanou a dovolenou činností, a je tedy v souladu s § 5 odst. 2 písm. a) zákona o ochraně osobních údajů.

Současně je však třeba naplnit i další povinnosti stanovené zákonem o ochraně osobních údajů, tedy především zpracovávat osobní údaje pouze po dobu, která je nezbytná k naplnění sledovaného účelu, popř. zpracovávat údaje pouze v souladu s účelem, ke kterému byly shromážděny. Jestliže se tedy podle § 25 odst. 2 správního řádu písemnost považuje za doručenou patnáctým dnem po vyvěšení, je tím dána i doba nezbytná pro zveřejnění osobních údajů. Po uplynutí této doby je zveřejnění předmětným způsobem nutné považovat za zpracování osobních údajů po dobu delší než nezbytnou.

Informování v obecním zpravodaji

Obecní zpravodaj patří v mnoha obcích k hlavnímu zdroji informací o činnosti obce a jejích orgánů. Obecně lze říci, že pro zveřejňování osobních údajů touto formou platí totéž, co bylo uvedeno výše ve vztahu k internetu, neboť i přes svůj nepoměrně užší dosah je také obecní zpravodaj nutno považovat za médium dostupné neomezenému okruhu příjemců.

Obdobně jako v případě v minulosti velmi diskutované problematiky zveřejňování osobních údajů v souvislosti s gratulacemi k životnímu jubileu platí i v jiných případech (např. zveřejnění osob, které

nevrátily knihy vypůjčené z obecní knihovny) základní princip zákona o ochraně osobních údajů, tj. požadavek na právní titul pro jejich zpracování. Tímto právním titulem je buď souhlas dotčených osob, anebo postup v souladu s některou z výjimek dle § 5 odst. 2 písm. a) až g) zákona o ochraně osobních údajů, přičemž v naprosté většině situací bude třeba disponovat souhlasem osob.

Zpracování osobních údajů v rámci nejrůznějších evidencí je buď přímo zákonem stanovenou povinností, anebo nezbytností, bez níž nelze určitou službu (jako např. právě obecní knihovnu) provozovat. Je však třeba vždy důsledně dbát zásady vyjádřené v § 5 odst. 1 písm. f) zákona o ochraně osobních údajů, dle které je přípustné zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Osobní údaje nezbytné k zajištění služeb poskytovaných obcí proto není možné bez dalšího zveřejnit, neboť v takovém případě již dochází ke zpracování dat k jinému účelu.

V souvislosti se zveřejněním osobních údajů v důsledku nejrůznějších vztahů vyplývajících z neplnění smluvních povinností se Úřad často setkává s argumentací, že zveřejnění dlužníka je postupem v souladu s § 5 odst. 2 písm. e) zákona o ochraně osobních údajů, tedy formou ochrany práv dotyčného správce údajů. Citované ustanovení však obsahuje podmínku, dle které zpracování osobních údajů směřující k ochraně práv a právem chráněných zájmů správce nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života. Úřad dlouhodobě zastává názor, že zveřejňování osobních údajů osob, které neplní své smluvní závazky (dlužníků), bez jejich souhlasu je nepřípustným zasahováním do soukromí těchto osob, neboť zpřístupněním takového údaje, který byl získán na základě soukromoprávního vztahu, může dojít k poškození dobrého jména dotčené osoby v mnoha dalších vztazích, a to jak soukromoprávních, tak veřejnoprávních. Jedná se o nátlakové jednání, kterým je porušováno i ustanovení článku 10 odst. 1 až 3 Listiny základních práv a svobod, podle něhož má každý právo, aby byla zachována jeho lidská důstojnost, osobní čest, dobrá pověst a chráněno jeho jméno, každý má právo na ochranu před zasahováním do soukromého a rodinného života a každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním osobních údajů.

Závěrem lze uvést, že ve všech shora uvedených situacích, které Úřad v roce 2009 posuzoval ve správním řízení, bylo shledáno porušení zákona o ochraně osobních údajů a uložena sankce.

ZABEZPEČENÍ OSOBNÍCH ÚDAJŮ

Úřad se i v roce 2009, stejně tak jako v letech předchozích, zabýval řadou případů, kdy došlo ke zpřístupnění osobních údajů neoprávněným osobám, a to z důvodu nedostatečných bezpečnostních opatření na straně správce nebo zpracovatele. Povinnost správce (zpracovatele) osobních údajů přijmout bezpečnostní opatření směřující k tomu, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě nebo k jejich jinému neoprávněnému zpracování či zneužití, je v zákoně o ochraně osobních údajů vyjádřena v § 13.

Úřad tak v roce 2009 řešil např. ztrátu přihlášek sloužících k registraci pojištěnců u zdravotní pojišťovny v baru, odcizení dokumentů (hackerem) obsahujících osobní údaje plátců pojistného na zdravotní pojištění z domácího počítače zaměstnankyně zdravotní pojišťovny, nález kopií dokumentů pocházejících z činnosti Policie České republiky v kontejneru na odpad v blízkosti policejní služebny, „likvidaci“ dokumentů s osobními údaji v nepoužívaném komíně a následné roznesení částečně ohořelých dokumentů do okolí, nález dokumentů na ulici, poskytnutí kopie lékařské zprávy výrobci dětské výživy nebo zpřístupnění (neznámou osobou) nahrávky telefonického rozhovoru klienta s operátorem poskytovatele služby na internetu.

Úřad ve vztahu k těmto případům opakovaně rozhodl, že již samotná situace, kdy se osobní údaje dostanou mimo „sféru vlivu" správce, tedy se nacházejí volně na ulici či jiném veřejném místě, jsou odcizeny neznámým pachatelem atd., znamená, že správce nepřijal a neprovedl dostatečná bezpečnostní opatření a porušil tak povinnost uloženou mu § 13 zákona o ochraně osobních údajů; pro tento závěr není přitom rozhodující míra zavinění na straně správce, neboť ve všech případech se jednalo o správní delikty, kterých se dopustily právnické osoby nebo fyzické osoby v souvislosti se svojí podnikatelskou činností. V této situaci odpovídá poté správce za správní delikt na základě objektivní odpovědnosti.

Pro odstranění tvrdosti takovéto odpovědnosti stanoví zákon, že odpovědnost za správní delikt zaniká, pokud správce prokáže, že vynaložil veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránil; jedná se o tzv. liberaci z odpovědnosti za správní delikt (viz § 46 odst. 1 zákona o ochraně osobních údajů). K naplnění této podmínky poté Úřad ve shora uvedených případech konstatoval, že za vynaložení veškerého úsilí nelze považovat pouze přijetí vnitřních předpisů, směrnic, bezpečnostních opatření ve formě objektové (fyzické) bezpečnosti, opatření v oblasti zabezpečení IT systémů apod., ale že je třeba tato opatření také důsledně převést do praxe, jejich provedení a dodržování vyžadovat a kontrolovat. V této souvislosti bylo dále konstatováno, že pokud správce není schopen určit, resp. rekonstruovat, jakým způsobem došlo k neoprávněnému přístupu k osobním údajům (tedy nelze zjistit, který ze zaměstnanců je vynesl, kdo je zanechal na ulici, jak mohly být odcizeny z kanceláře atp.), nemůže se zprostit odpovědnosti za žádné situace.

Úřad se také ve své kontrolní a následně správní činnosti zabýval otázkou zabezpečení automatizovaného systému daňové správy ADIS. V této věci přitom bylo zjištěno, že správce tohoto systému, tedy Ministerstvo financí, nepořizuje elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovávány (tzv. logy zápisu a čtení), což je v rozporu s povinností dle § 13 odst. 4 písm. c) zákona o ochraně osobních údajů. S ohledem na rozsah osobních údajů zpracovávaných v rámci systému ADIS a rizika spojená s takto nedůsledným přístupem k jejich ochraně byla za tento správní delikt uložena nejvyšší pokuta v rámci sankcí za porušení bezpečnostních opatření dle § 13 zákona o ochraně osobních údajů (ve výši 350 000 Kč) v roce 2009. V této souvislosti je třeba upozornit, že právě z důvodu rizik spojených se zpracováním osobních údajů v informačních systémech ukládá zákon o ochraně osobních údajů v § 13 odst. 4 zvláštní povinnosti určené právě správcům těchto systémů, které je třeba beze zbytku naplnit.

ZVEŘEJŇOVÁNÍ OSOBNÍCH ÚDAJŮ V MÉDIÍCH

V roce 2009 se Úřad zabýval také otázkou zveřejňování osobních údajů v médiích. Jedná se nepochybně o jednu z problematických oblastí, kde se střetávají dva zcela odlišné zájmy – na straně jedné oprávněný požadavek dotčených osob na ochranu soukromí a na straně druhé neméně důležitá svoboda šíření informací. Vzhledem k tomu, že zákon o ochraně osobních údajů je (vedle jiných právních předpisů) určen především k ochraně jednotlivců před neoprávněnými zásahy do soukromí prostřednictvím zpracování osobních údajů, je dle Úřadu zcela důvodné aplikovat jeho požadavky také na tuto sféru, byť s jistými limity. Tato omezení spočívají v požadavku vyjádřeném ve Směrnici Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (dále jen „Směrnice"), která byla do českého právního řádu provedena právě zákonem o ochraně osobních údajů a dle které je třeba pro oblast žurnalistiky zavést odchylky a výjimky od obecné úpravy ochrany osobních údajů. Přestože tento požadavek nebyl v zákoně o ochraně osobních údajů ani v jiném relevantním právním předpise zcela proveden, je – i s ohledem na judikaturu Evropského soudního dvora – nutno zákon o ochraně osobních údajů aplikovat v duchu požadavků Směrnice. Dalším limitem pro aplikaci zákona o ochraně osobních údajů na novinářskou činnost jsou principy výkladu ústavních norem definované Ústavním soudem, podle kterého nelze žádnému ze základních práv přiznat vyšší důležitost. Ústavní soud konkrétně judikoval, že základní právo podle čl. 17 Listiny základních práv a svobod (právo na svobodu projevu

a na informace; dále jen „Listina“) je zásadně rovno základnímu právu upravenému v čl. 10 Listiny (právo na ochranu osobnosti, včetně osobních údajů).

S ohledem na uvedená východiska Úřad zastává názor, že je důvodné uplatňovat svěřené kompetence v oblasti žurnalistiky jen v krajních případech, které opodstatňují použití veřejnoprávních opatření (ve smyslu Ústavním soudem vyžadované zásady *ultima ratio* trestní represe). Podstatným pro vyhodnocení závažnosti případu a důvodnosti zásahu Úřadu je především postavení osoby, které se zveřejněné údaje týkají, charakter publikovaných informací a smysl a účel zveřejnění osobních údajů. Je zapotřebí odlišovat informace týkající se soukromí např. politiků či tzv. celebrit od informací o „obyčejných“ lidech, přísněji je dále třeba přistupovat ke zveřejnění osobních údajů týkajících se dětí či mladistvých anebo osob, které se z jiného důvodu nejsou schopny bránit dostatečně samy. Obdobně je nutno respektovat požadavek na zvýšenou ochranu citlivých údajů definovaných v § 4 písm. b) zákona o ochraně osobních údajů. A v neposlední řadě je dle názoru Úřadu významným kritériem to, zda má zveřejnění určitých informací sloužit čistě ke zvýšení „atraktivity“ zprávy, nebo zda je zpracováním (zveřejněním) osobních údajů v daném případě sledován skutečný veřejný zájem.

S ohledem na uvedená východiska a kritéria proto Úřad aplikoval požadavky zákona o ochraně osobních údajů např. v situaci, kdy došlo ke zveřejnění citlivého údaje vypovídajícího o zdravotním stavu v souvislosti s informováním o pátrání po pohřešované nezletilé osobě. V situaci, kdy Policie České republiky vyhodnotí situaci tak, že pro účely pátrání po pohřešované osobě není nezbytné uvádět detailní informaci o zdravotním stavu, není z hlediska zákona o ochraně osobních údajů přípustné, aby jiné subjekty (poskytující zpravodajství) detaily o zdravotním stavu dohledaly z jiných zdrojů a společně s dalšími citlivými informacemi o životě hledané osoby tyto údaje uveřejnily s odkazem, že tím plní veřejný zájem spočívající v právu veřejnosti na informace. V obdobné situaci je zřejmé, že poskytnutím informace doplněné o podrobnosti o zdravotním stavu (popř. další informace vypovídající např. o sexuálním chování) dochází k významnému zásahu do práv pohřešované osoby, přičemž nezveřejněním těchto doplněných údajů by žádné stejně významné hodnoty (zejména svoboda projevu) nebyly ani ohroženy, ani zasaženy. Uvedené okolnosti jsou tak dle Úřadu zcela dostačující pro vyvození odpovědnosti za správní delikt při zpracování osobních údajů v oblasti žurnalistiky.

Úřad se k této problematice blíže vyjadřuje ve svém stanovisku č. 5/2009 – Zveřejňování osobních údajů v médiích (viz webové stránky Úřadu).

REGISTRACE

Smyslem registrace je získat pro účely předběžné nebo standardní kontroly přehled o tom, kdo a jakým způsobem zpracovává osobní údaje.

Znamená to, že správce musí s jistým předstihem určit, zda se na jím připravované zpracování vztahuje oznamovací povinnost. Správci však v této věci často váhají, a tak se obracejí na Úřad s dotazem, jakým způsobem správně aplikovat výjimky uvedené v § 18 zákona o ochraně osobních údajů. Podobně i posouzení samotného záměru provádět určité zpracování tak, aby bylo v souladu se zákonem o ochraně osobních údajů, není mnohdy jednoduché, a tak se správci raději dříve, než svůj záměr oficiálně Úřadu oznámí postupem dle § 16 zákona o ochraně osobních údajů, obrátí na Úřad s žádostí o ústní konzultaci. Celkem bylo v roce 2009 vedeno 29 ústních konzultací se subjekty veřejného či soukromého sektoru a byl poskytnut nespočet konzultací telefonických. Poskytování tzv. „předregistračních“ konzultací se tak stalo nedílnou součástí činnosti oddělení v rámci vyřizování registračních oznámení či žádostí o předávání do jiných států.

Ze souhrnné registrační činnosti, kterou Úřadu ukládá zákon o ochraně osobních údajů, lze vybrat několik ilustračních případů, které do jisté míry charakterizují určitý trend zpracování osobních údajů v roce 2009.

V souvislosti s prudkým rozvojem informačních technologií byly vícekrát řešeny případy týkající se fungování nových technologií určených k zabezpečení vstupu do režimových pracovišť, které zároveň umožňují zpracovávat osobní údaje. Jednalo se např. o technologii „3D-biofotoportrét". Tato technologie pracuje na principu speciální kamery, která sejme řadu rozměrů obličeje. Tento scan ihned převede do jednostranně zašifrovaného binárního řetězce čísel, z něhož nelze zpětně reprodukovat podobu obličeje. Čtecí zařízení umístěné např. u vstupu do místnosti uchovává personální číslo zaměstnance a k němu přiřazený jednostranně zašifrovaný binární řetězec; při vstupu sejme obličej vstupujícího, převede jeho rozměry do binárního řetězce, který porovná s uloženým binárním řetězcem. Záznam o vstupu je uchováván v textové podobě jako jméno zaměstnance, datum a čas vstupu. Z poskytnutých informací bylo dovozeno, že binární řetězec, z něhož nelze reprodukovat podobu obličeje, není biometrický údaj, nicméně může být osobním údajem.

Jedna společnost projevila záměr provozovat internetový portál, kde návštěvníci stránek po zadání data narození získají pravděpodobný osobnostní profil na základě cyklu čínského horoskopu. Další zadané údaje (pohlaví, schopnosti, dovednosti, vlastnosti, pocity, zdravotní stav, výška a váha, názory a záliby) hodlá společnost databázově uchovávat pro rozšíření vzorku, na jehož základě zákonitosti závislosti osobnostního profilu na datu narození může dále zkoumat a zpřesňovat. V případě neregistrovaných uživatelů půjde o anonymní data pouze tehdy, pokud nebude shromažďován a zpracováván údaj o IP adrese, která je osobním údajem. V případě registrovaných uživatelů, kdy budou navíc shromažďovány další osobní údaje typu e-mailová adresa a jméno, půjde o zpracování citlivých údajů, na které se vztahují všechny povinnosti vyplývající ze zákona o ochraně osobních údajů.

Další novum související se zpracováním osobních údajů představuje projekt, při němž dochází ke zpracování dat, jehož cílem je vytvoření internetového vyhledávače, který registrovaným uživatelům (např. personálním agenturám) umožní vyhledat internetové stránky s relevantními informacemi o vzdělání a praxi odborníků v zadaném oboru. Princip fungování vyhledávače je naprosto stejný jako u běžných vyhledávačů (Google, Seznam): Počítačový program nepřetržitě prochází internetové stránky, zaznamenává každé relevantní slovo s kratičkým vzorkem dané stránky a indexuje do vlastní databáze. Uživatelem zadávaný dotaz je porovnán právě s touto databází relevantních slov a útržků internetových stránek, na kterých se slova vyskytují. Na rozdíl od běžných vyhledávačů, které indexují naprosto celý obsah webu, hodlá tento záměr indexovat pouze stránky, které jsou významné z hlediska odbornosti a praxe v zadaném oboru.

Velmi často se registrační oddělení v rámci své činnosti setkávalo s problémem monitorování (nahrávání) telefonického hovoru s klientem, obchodním partnerem apod., nejčastěji za účelem zlepšování kvality služeb zákaznické linky, řešení sporů o obsah hovoru, vyhodnocení kvality zaměstnanci poskytovaných informací, tréninku zaměstnanců. Jestliže jsou telefonické rozhovory s klienty, obchodními partnery atd. nahrávány, jedná se o zpracování osobních údajů dle zákona o ochraně osobních údajů za předpokladu, že je volající identifikován, např. identifikace jeho osoby dle databáze klientů s ověřením jeho totožnosti, např. dle hesla, PIN apod., a celý obsah hovoru je tedy osobním údajem.

Uvedené příklady dokumentují obecný trend, kdy je Úřad nucen posuzovat mnohem složitější a sofistikovanější druhy zpracování osobních údajů (projektů), které souvisí s rozvojem nových informačních a komunikačních technologií včetně zpracování na internetu. Dalším častým typem oznamovaných zpracování, podobně jako v minulém roce, byla zpracování prostřednictvím kamerového systému, dále zpracování v oblasti obchodu včetně internetového obchodu, marketingu, reklamy, spotřebitelských soutěží.

PŘEDÁVÁNÍ OSOBNÍCH ÚDAJŮ DO ZAHRANIČÍ

Pokračující globalizace světové ekonomiky ovlivňuje ve stále větší míře mezinárodní předávání osobních údajů. Předávání osobních údajů do třetích zemí, které nezajišťují adekvátní ochranu osobních údajů v takové míře, jak je upravena směrnicí 95/46/ES, resp. zákonem o ochraně osobních údajů, může představovat zvýšené riziko pro základní práva a svobody subjektu údajů.

Cílem právní úpravy obsažené v § 27 odst. 1 a 2 a odst. 3 písm. b) zákona o ochraně osobních údajů je zajistit, aby předané osobní údaje požívaly nadále i po předání do země určení příslušné ochrany.

V roce 2009 byla nejčastěji plněna podmínka, uvedená v § 27 odst. 3 písm. a), tedy předání údajů se souhlasem nebo na základě pokynu subjektu údajů. K souhlasu je třeba poznamenat, že se jím v souladu s § 4 písm. n) zákona o ochraně osobních údajů rozumí svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údajů se zpracováním jeho osobních údajů. Náležitosti tohoto souhlasu pak stanoví kromě § 4 písm. n) rovněž § 5 odst. 4 a § 9 písm. a) zákona o ochraně osobních údajů, spolu s § 34 an. zákona č. 40/1964 Sb., občanského zákoníku, v platném znění. Vedle plnění podmínky souhlasu byla nejčastěji plněna podmínka podle § 27 odst. 3 písm. e), podle které je předávání nezbytné pro jednání o uzavření nebo o změně smlouvy, uskutečněné z podnětu subjektu údajů, nebo pro plnění smlouvy, jejíž smluvní stranou byl subjekt údajů. Tato výjimka byla přijatelným právním východiskem zejména pro předávání osobních údajů cestovními kancelářemi, které se týkají jejich klientů, hotelům nebo jiným obchodním partnerům, kteří se podílejí na organizaci pobytu těchto klientů.

Velká většina žádostí dle ustanovení § 27 odst. 4 zákona o ochraně osobních údajů, které Úřad v rámci své kompetence posuzuje, se týká předání osobních údajů do Spojených států amerických. Jako příjemci těchto údajů jsou nejčastěji uváděny společnosti, se kterými jsou žadatelé kapitálově propojeni, a dále pak obchodní partneři žadatelů. Vzhledem k tomu proto mezi deklarovanými účely zpracování, resp. předání 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.). Jedná se tedy o předávání osobních údajů zaměstnanců, popř. uchazečů o zaměstnání mateřským společnostem v zahraničí, zejména pak ve Spojených státech amerických. V podobných případech doporučuje Úřad správcům, s ohledem na skutečnost, že lze taková zpracování kvalifikovat jako opakovaná, hromadná nebo strukturální, využít zvláštní právní rámec pro předávání, tj. smlouvu, jejíž součástí budou standardní smluvní doložky, závazná podniková pravidla („binding corporate rules“) nebo v případě předávání údajů do USA institut „Safe Harbor“.

Bohužel je často ze strany správců v těchto případech jako právní titul takového předání uváděn souhlas zaměstnanců. To je jistě možné, ovšem takové předávání má i určitá úskalí, která si správci ne vždy v dostatečné míře uvědomují. Problematika předávání zaměstnaneckých údajů do zahraničí není limitována jen podmínkami stanovenými v zákoně o ochraně osobních údajů. Na takové předání je nutné pohlížet nejen z hlediska aplikace tohoto zákona, ale také z hlediska dalších právních předpisů, zejména předpisů upravujících pracovněprávní vztahy. Relevantní souhlas subjektu údajů musí splňovat náležitosti ustanovení § 4 písm. n) zákona o ochraně osobních údajů, podle kterého musí být takový souhlas svobodným, výslovným a vědomým projevem vůle subjektu údajů. Např. svobodný souhlas v pracovněprávním poměru znamená, vzhledem k podřízenému vztahu zaměstnance vůči zaměstnavateli, že zaměstnanec musí mít skutečnou možnost odepřít jej, aniž by utrpěl jakoukoliv újmu, a také možnost jej dodatečně odvolat. Náležitost vědomého souhlasu vyžaduje, aby byl subjekt údajů předem řádně informován o konkrétních okolnostech předání (o jeho účelu, rozsahu předávaných osobních údajů, o příjemci či příjemcích atd.), přičemž tato informační povinnost je zakotvena

rovněž v ustanoveních § 5 odst. 4 a § 11 zákona o ochraně osobních údajů. Informace poskytnuté subjektům údajů musejí také zahrnovat informace o zvláštním riziku vyplývajícím ze skutečnosti, že jejich údaje budou předány do země, která nezajišťuje odpovídající ochranu osobních údajů. Souhlas s předáním osobních údajů do třetích zemí by měl být rovněž oddělen od souhlasu nebo potvrzení seznámení se s podmínkami vlastního zpracování osobních údajů.

V roce 2009 byl zaznamenán zvýšený počet předávání, která se uskutečňují na základě zásad „Safe Harbor". („Safe Harbor" představuje fakticky smlouvu mezi USA a Evropskou komisí, že společnosti, které budou na jejím seznamu, jsou svými politikami, respektive systémy ochrany soukromí konformní se zásadami vyjádřenými ve směrnici 95/46/ES.)

Americké firmy se mohou dobrovolně přihlásit k dodržování zásad „bezpečného přístavu" zasláním žádosti Ministerstvu obchodu USA. V takovém případě je Ministerstvo obchodu zařadí do on-line seznamu („Safe Harbor List"), který průběžně aktualizuje a zveřejňuje na svých webových stránkách. Kontrola nad tím, zda společnosti respektují dané principy, připadá Federální obchodní komisi (FTC), resp. americkému Ministerstvu dopravy v případě leteckých společností.

Dosavadní provádění zásad „bezpečného přístavu" však bylo podrobeno ostré kritice ze strany Evropské komise. Na základě vypracovaných studií od nezávislých expertů v roce 2008 bylo konstatováno mnoho nedostatků s tím, že se v případě „Safe Harbor" jedná více o fikci než o skutečně fungující nástroj zajišťující bezpečné předání dat. Základním nedostatkem bylo zejména nedostatečné plnění zásad ze strany jednotlivých společností hlásících se k dodržování zásad „bezpečného přístavu" a nedostatečný výkon dozoru nad dodržováním těchto zásad ze strany kompetentních orgánů (Ministerstvo obchodu USA a Federální obchodní komise) oprávněných vyšetřovat stížnosti a zjednat nápravu v případě nedodržování zásad prováděných v souladu s FAQ. Je nutné poznamenat, že v této oblasti se podařilo zástupcům Evropské komise a Working Party 29 (WP 29) v rámci jednání se zástupci amerických veřejných institucí prosadit určité změny, které by měly vést k nápravě současného stavu.

LEGISLATIVNÍ ČINNOST

V roce 2009 přinesl vývoj v legislativní oblasti Úřadu dvě nové kompetence:

Od 1. dubna, kdy zákon č. 52/2009 Sb. doplnil do zákona o ochraně osobních údajů **nové skutkové podstaty deliktů**, je Úřad povinen stíhat jednání spočívající v porušení zákazu zveřejnění osobních údajů stanovených jinými právními předpisy. Tato novela doprovodila tzv. „náhubkový" zákon, změnu trestního řádu aktuálně reagující na opakované případy „bulvárního" publikování velkého množství osobních údajů, a to i nezletilých osob, z trestního řízení. Úřad uvítal, že v rámci novely bylo upozorněno zejména na nebezpečnost bezmezného zveřejňování a hromadného zpřístupňování osobních údajů (vč. publikování v médiích a na internetu). Bohužel v rámci veřejné debaty doprovázející tuto změnu trestního procesu, či spíše kritické kampani v převážné části sdělovacích prostředků zaměřené na údajné potlačení svobody projevu, byl často opomíjen původní cíl novelizace: Ochránit soukromí poškozených (obětí) trestného činu.

Zákonem č. 111/2009 Sb., o základních registrech, je Úřadu v rámci nově vytvářeného sy-stému eGovernmentu uloženo vytvářet zdrojové a agendové identifikátory fyzických osob a zajišťovat převod agendových identifikátorů fyzických osob v rámci jednotlivých elektronických agend. Nové identifikátory by měly mj. snížit riziko neoprávněného nakládání s osobními údaji občanů uloženými ve státních evidencích. Úřad přijal uvedenou kompetenci s podmínkou, že vytváření a převod identifikátorů budou realizovány maximálně bezpečným způsobem a celý proces generování identifikátorů bude přísně oddělen od jakéhokoliv vlastního zpracování osobních údajů úřady. Přitom není nijak dotčen dosavadní dozor Úřadu nad zpracováním osobních údajů ve stávajících státních registrech i nově navrhovaných základních registrech.

Dosud neuzavřenou agendou, která se zásadně dotýká působnosti Úřadu, je **příprava nového zákona o kontrole**. Úřad na expertních jednáních s navrhovateli zákona i v připomínkovém řízení požadoval sladit zásady jednotného postupu v rámci dozoru (kontroly), prováděného veřejnou správou v České republice, se zvláštními, resp. komplexními požadavky na dozor v oblasti osobních údajů (dle unijního práva). V této souvislosti navrhnul zjednodušení některých úředních formalit v případě postupů před zahájením kontroly tak, jak je pro správní řízení podobným způsobem již stanoveno ve správním řádu. Z pohledu své působnosti Úřad spatřuje jako nejzávažnější, systémově stále nedořešený, problém nejednotné **právní úpravy mlčenlivosti**. Některé právní výklady kusých úprav mlčenlivosti v jednotlivých zákonech (neexistuje totiž obecná úprava podmínek mlčenlivosti a zejména procesu jejího zbavení) by vedly až ke znepřístupnění části informací a osobních údajů potřebných pro vykonávanou kontrolu. Jistě by bylo absurdní, aby v intencích takových výkladů fakticky stanovovala rozsah informací potřebných pro kontrolu sama kontrolovaná veřejná instituce; Úřad se v praxi již s touto „obstrukcí" při kontrole prováděné v oblasti daňové správy setkal.

V oblasti připomínkování právních předpisů se Úřad v roce 2009 nejčastěji setkával se zásadními **nedostatky v oblasti změn automatizovaného a centralizovaného zpracování dat**

v rámci databází vedených veřejnou správou. Předkladatelé nových právních úprav obvykle popisují a vyhodnocují zamýšlené zpracování osobních údajů formálně. Jako by v mnohých případech byla ochrana osobních údajů stále vnímána jako zbytečnost či přítěž, a nikoliv jako výhoda, ať již např. pro bezpečnost veřejné správy, její efektivnost nebo transparentnost. V mnoha částech především starších informačních systémů veřejné správy chybí komplexnější přístup k ochraně soukromí občanů. Nadcházející systém eGovernmentu by měl uvedené napravit a odstranit z hlediska ochrany dat rizikové postupy založené např. na chybných, zastaralých či zbytečně duplicitně uchovávaných údajích o občanech. Mezi příklady, kdy Úřad v rámci připomínkových řízení nad prováděcími předpisy ke školskému zákonu v roce 2009 sdělil opakovaně pochybnost nad rozsahem a potřebností shromažďování dat o občanech, vyžadovaných zákonem, patří centrální databáze údajů ze školních matrik vedená v resortu Ministerstva školství, mládeže a tělovýchovy.

V úvodu roku 2009 se Úřad obrátil dopisem na Ministerstvo zdravotnictví, aby jej upozornil na **nedostatečný postup legislativních prací v resortu zdravotnictví při přípravě databází obsahujících citlivé údaje občanů**. Po jednání o zdravotnických registrech, navrhovaných v balíku zákonů o zdravotnických službách v nezměněné zastaralé podobě, která nevyhovuje zásadám ochrany osobních údajů, se tento problém dále zřetelně ukázal u **centrálního úložiště elektronických receptů**. Tato obří databáze, zamýšlená jako centrální úložiště informací o všech lékařských předpisech (ovšem s důsledkem vedení informací o pacientech, jejich lékařích a lékárnících), nebyla vůbec v návrhu předložena a diskutována v řádném legislativním připomínkovém řízení, ale naopak schválena jako jeden z mnoha poslaneckých návrhů na doplnění zákona o léčivech.

Rozpory mezi kusou právní úpravou a rozsahem shromažďovaných dat ukázala kontrola inspektora Úřadu. Když následně Ministerstvo zdravotnictví v závěru roku 2009 navrhlo rychlou úpravu právního předpisu, Úřad požadoval, aby byl vyjasněn účel databáze a s tím spojené úkoly Státního ústavu pro kontrolu léčiv, který databázi spravuje, dále opodstatněnost povinného zřizování lékového záznamu každého pacienta, a také aby byla odůvodněna nezbytnost celého systému a důsledně zohledněny požadavky vyplývající z práva EU.

Rok 2009 byl nepochybně rokem se značným ohlasem veřejnosti na nové technologie, jejichž využívání může zasáhnout do soukromí občanů. U **elektronických dálničních známek** Úřad kladně přijal zákonnou podmínku anonymnosti a přenositelnosti známek – její splnění však bude možno posoudit až po předložení návrhů příslušných prováděcích předpisů k přijaté právní úpravě. Proklamovaný požadavek na anonymitu či přenositelnost známek totiž nemusí být zcela splnitelný, neboť každou věc označenou číslem či nějakým způsobem evidovanou, jíž využívá člověk, lze právě k identifikaci tohoto člověka využít. Kromě objasnění potřebného rozsahu údajů spojených s technologií bude třeba pečlivě promítnout pravidla pro sdílení a další zpracování dat v příslušných informačních systémech.

U **kamerových systémů**, vnímaných v poslední době částí veřejnosti jako sledovací systémy, které by měly podléhat zvláštní právní úpravě, se Úřad expertně podílel na formulaci požadavků na právní regulaci. Na první pololetí roku 2010 vláda uložila vypracovat novelu zákona o ochraně osobních údajů obsahující konkrétní pravidla pro shromažďování dat prostřednictvím kamerových systémů, jakož i další zpracování, včetně informační povinnosti o prováděném zpracování. Obdobný postup Úřad přepokládá v roce 2010 pro vznik zákona upravujícího agendu **zpracování dat o lidské DNA**.

S ohledem na aktuální vývoj evropského práva Úřad považoval v roce 2009 za potřebné upozornit v rámci legislativního připomínkového řízení na otázku komplexnějšího pohledu na spotřebitelské, resp. **úvěrové registry**. Úřad doporučil věnovat pozornost nejen již zákonem upraveným sdíleným registrům bank, ale také nebankovním registrům pro sdílení dat o některých, z úvěrového hlediska rizikových, klientech (dlužnících). Tyto databáze jsou v České republice provozovány nikoliv v rámci zákonného zmocnění, ale na základě souhlasu dotčených osob.

STYKY SE ZAHRANIČÍM A MEZINÁRODNÍ SPOLUPRÁCE

Mezinárodní smluvní základna, o kterou se opírá činnost Úřadu, se ve sledovaném roce prakticky nezměnila. I nadále ji tvoří dvě základní směrnice (95/46/ES a 2002/58/ES), Úmluva Rady Evropy č. 108/1981 převzatá Evropskou unií pro některé instrumenty 3. pilíře a řada právních aktů s úzce vymezenou aplikační oblastí, jako jsou četná rozhodnutí Komise, kterými se uznává adekvátnost ochrany osobních údajů v některých třetích zemích mimo EU a EHP nebo při použití specifických (např. standardizovaných smluvních) garancí.

Trvalé prioritní postavení spolupráce s orgány EU a partnerskými úřady ve členských státech EU v rámci zahraničních styků Úřadu bylo v první polovině roku mimořádně zdůrazněno aktivitou spojenou s předsednictvím ČR v Radě EU. Do **aktivit pod hlavičkou předsednictví** patří tři významné akce Úřadu:

(1) Převzetí předsednictví po Francii inspirovalo záměr pozvat francouzské kolegy z partnerského úřadu CNIL – Commission Nationale de l' Informatique et des Libertés, v čele s jeho předsedou Alexem Türkem, který je současně předsedou Pracovní skupiny pro ochranu dat podle článku 29 – tzv. WP 29 (viz níže). Delegace z Francie pobývala v Praze ve dnech 3. a 4. března 2009; kromě pracovního jednání s výměnou zkušeností s odborníky Úřadu také navštívila Senát Parlamentu ČR, kde diskutovala se členy Stálé komise Senátu pro ochranu soukromí a byla přijata předsedou Senátu MUDr. Sobotkou. Součástí programu byl rovněž kulatý diskusní stůl ve Francouzském institutu zaměřený na ochranu soukromí dětí před riziky internetu, což byl i námět společného tiskového prohlášení.

(2) Organizačně nejnáročnější akcí v rámci předsednictví s širokým mezinárodním ohlasem bylo uspořádání XIX. zasedání „Case Handling Workshop" v Praze ve dnech 12.–13. března 2009. Workshop je pravidelným pracovním setkáváním hlavních odborníků na kontrolní činnost nezávislých dozorových orgánů typu ÚOOÚ střídavě v různých hostitelských zemích EU. Přizváni byli i zástupci obdobných orgánů z několika evropských zemí mimo EU. Mezi hlavní témata patřila problematika vztahu veřejných sdělovacích prostředků a ochrany osobních údajů se snahou nalézt rovnovážný přístup k právu svobodně vyhledávat a šířit informace a právu na soukromí. Zasedání se dále věnovalo například všeobecnému rozšíření kamerových systémů, zpracování zaměstnaneckých dat a zacházení s osobními údaji pacientů ve zdravotnictví.

(3) Zcela bezprostřední vztah k českému předsednictví mělo svolání pracovní skupiny G.09 pro ochranu osobních údajů Rady/Coreperu (Brusel, 23. března 2009). Ne každé předsednictví se odhodlá tuto pracovní skupinu uspořádat. Úřad její svolání inicioval, spoluorganizoval a podílel se na jejím programu, i když není jejím členem, protože nemůže zastupovat ČR v pracovních orgánech Rady vzhledem ke své nezávislé pozici. Jako hlavní bod programu přednesl zástupce Úřadu s kritickými poznámkami informaci o nově přijaté právní normě EU – rámcovém rozhodnutí Rady o ochraně osobních údajů zpracovávaných v rámci policejní a justiční spolupráce v trestních věcech. Tento dlouhé

roky sjednávaný dokument je sice krokem správným směrem pro sjednocování hledisek ochrany osobních údajů ve 3. pilíři, zůstal však mnoho dlužen původnímu očekávání. Úřad rovněž připravil podklad pro prezentaci přednesenou zástupcem ČR v G.09 ze Stálého zastoupení ČR při EU k velmi kontroverznímu tématu přípravy návrhu rámcového rozhodnutí Rady o využití rezervačních a odbavovacích systémů pasažérů (PNR) pro účely prosazování práva.

Hlavní platformou pro výměnu zkušeností, tříbení praxe a sjednocování přístupů úřadů pro ochranu osobních údajů členských států EU je **Pracovní skupina pro ochranu dat podle článku 29 (dále jen „WP 29")**. Členy tohoto prestižního nezávislého poradního orgánu při Evropské komisi, zřízeného podle článku 29 směrnice 95/46/ES, jsou předsedové úřadů, obvykle na zasedáních doprovázení jedním nebo více experty. Příkladem projednávané problematiky je již zmíněné navrhované zpracování dat PNR z databází leteckých společností v rámci EU nebo již probíhající předávání těchto osobních údajů do třetích zemí, především do USA, Kanady, Austrálie a Korejské republiky a hodnocení nebo přípravy s tím souvisejících mezinárodních smluv. K tomu v poslední době přistupuje i autoritativně prosazovaný požadavek Velké Británie na poskytování obdobných údajů od leteckých dopravců z ostatních členských států EU do jejích elektronických systémů kontroly hranic, tzv. UK e-Border System. Na několika zasedáních WP 29 byla velká pozornost věnována porovnávání praxe vyhledávacích služeb (search engines) vybraných světových firem (Microsoft, Ixquick, Yahoo, Google), jejichž zástupci na zasedání vystoupili s prezentacemi a odpovídali na četné dotazy. Také službou Street View společnosti Google se WP 29 zabývá již delší dobu, aniž se zatím podařilo dojít k jednoznačnému hodnocení a závěrům. Vzhledem k tomu, že zpracování dat projíždějícími automobily z jiných zemí je mnohde na národní úrovni obtížně kontrolovatelné a těžko právně postižitelné, zástupce Úřadu vyzval ke společnému postupu na základě zaujetí společného stanoviska.

WP 29 dále na sklonku roku doporučila Izrael a Andorru k přijetí do zatím velmi omezené skupiny „třetích zemí", jejichž legislativa ochrany osobních údajů byla Evropskou komisí oficiálně shledána jako adekvátní požadavkům práva EU.

Pracovní skupina se schází pětkrát ročně na dvoudenních zasedáních, kromě toho však si ještě zřídila celou řadu pracovních podskupin. Odborníci Úřadu se účastní na práci pěti podskupin, a to Děti a soukromí, Budoucnost soukromí, Zdravotnické údaje, Technologická podskupina a Víza a biometrie. Mimořádnou aktivitu v roce 2009 vyvinula ad hoc zřízená podskupina o budoucnosti soukromí a dlouhodobě působící podskupina k technologickým otázkám.

Zapojení Úřadu do evropských dozorových orgánů (SIS, CIS, Eurodac, Europol)

V rámci svých zahraničních aktivit se zástupci Úřadu účastní také jednání společných dozorových orgánů ustanovených za účelem dohledu nad sdílenými evropskými informačními systémy, jedná se konkrétně o tyto orgány:

- společný dozorový orgán pro Schengenský informační systém (Joint Supervisory Authority – JSA Schengen),
- společný dozorový orgán pro Celní informační systém (Joint Supervisory Authority – JSA Customs),
- koordinační skupina pro dohled nad systémem Eurodac,
- společný dozorový orgán pro Europol (Joint Supervisory Body – JSB Europol).

Participace na činnosti těchto orgánů představuje z pohledu Úřadu příležitost prohloubit zkušenosti v oblasti kontroly rozsáhlých informačních systémů, ale především možnost ovlivnit připravované společné postoje či metodiky a v neposlední řadě evropskou legislativu, kterou jsou sdílené databáze postupně nově upravovány (a to za soustavného tlaku na rozšíření rozsahu zpracovávaných dat i okruhu subjektů, kterým jsou zpřístupněny).

Kromě kontroly zpracování údajů v Schengenském informačním systému a účasti v dozorovém orgánu JSA Schengen se zástupci Úřadu podílí také na pravidelném hodnocení úrovně ochrany osobních údajů v ostatních schengenských zemích. Při těchto hodnotících misích se posuzuje naplnění požadavků tzv. schengenské acquis (tedy Schengenské úmluvy a souvisejících právních dokumentů) v oblasti ochrany osobních údajů. Na rok 2009 připadlo hodnocení hned pěti stávajících (Belgie, Nizozemí, Lucembursko, Německo a Francie) a dvou kandidujících (Bulharsko a Rumunsko) zemí, přičemž

s ohledem na české předsednictví v Radě EU v první polovině roku 2009 byli zástupci Úřadu pověřeni náročnou rolí vedoucích expertů v rámci těchto hodnotících misí. Na základě nekonfliktního průběhu schvalování závěrečných hodnotících zpráv a z reakcí zástupců ostatních členských zemí lze soudit, že se této role zhostili odpovědně.

Úřad byl řádně zastoupen na všech čtyřech plenárních schůzích JSB Europol a dvou schůzích jeho odvolacího výboru. Zástupkyně Úřadu, která je zapojena i do tří pracovních podskupin, byla navíc koordinátorkou kontrolního týmu, který provedl v březnu r. 2009 pravidelnou kontrolu v sídle Europolu.

Úřad se podílel také na práci Pracovní skupiny pro policii a justici (WP on Police and Justice). Skupina je orgánem Konference evropských orgánů ochrany osobních údajů (tzv. Jarní konference) a jejím úkolem je sledovat vývoj ve zpracování osobních údajů orgány činnými v trestním řízení. Stanoviska zpracovává samostatně nebo ve spolupráci s WP 29. Po schválení katalogu spolupráce Jarní konferencí se skupina zaměřila na koordinaci kontrolní činnosti. Pro Jarní konferenci evropských komisařů soukromí a ochrany dat připravila návrh rezoluce o dvoustranných a mnohostranných dohodách mezi evropskými státy a třetími zeměmi v oblasti policejní a justiční spolupráce v trestních věcech. Začala rovněž mimo jiné diskutovat o důsledcích vstupu Lisabonské smlouvy v účinnost v oblasti aktivit skupiny.

Již delší dobu se na mezinárodních setkáních ochránců osobních údajů upozorňovalo na výzvu, kterou přináší globalizační trendy i do této oblasti. Velké rozdíly v přístupech k základním lidským právům včetně práva na soukromí v různých částech světa jsou bariérou rostoucích nároků na výměnu informací a v důsledku i mezinárodní spolupráci ve všech oblastech včetně hospodářské. **30. mezinárodní konference komisařů pro ochranu osobních údajů a soukromí ve Štrasburku** v r. 2008 schválila mandát pro pracovní skupinu, která by se pokusila formulovat „globální standardy" ochrany osobních údajů. Hlavní práce koordinované Španělskou agenturou ochrany dat proběhly právě v r. 2009 a výsledky úsilí, na kterém se podíleli i zástupci Úřadu formou písemných připomínek i účastí na dvou pracovních zasedáních (Barcelona v lednu a Bilbao v červnu 2009), mohly být předloženy na 31. mezinárodní konferenci v Madridu v listopadu 2009. Otazníky nad uplatněním výsledného dokumentu „International Standards on the Protection of Personal Data and Privacy" z hlediska nezbytného institucionálního zastřešení a mechanismu hodnocení shody s praxí jednotlivých zemí, které se ke Standardům přihlásí, budou námětem diskusí a jednání v příštím roce.

Kromě EU a jejích orgánů představují významné platformy pro mnohostrannou spolupráci také **Rada Evropy a Organizace pro hospodářskou spolupráci a rozvoj (OECD)**.

V **Radě Evropy** pokračovalo aktivní zapojení z předchozích let zastoupením v sedmičlenném byru Výboru pro ochranu dat zřízeného podle Úmluvy 108 (T-PD). Intenzivně zde bylo v průběhu roku připravováno Doporučení o profilování. Složitá problematika zahrnující jak aspekty technické a technologické, tak právní byla zahrnuta do dokumentu, který má zajistit ochranu osobních údajů v oblasti stále šíře využívané technologie umožňující velmi citelný zásah do soukromí občanů. Na základě intervence představitelů soukromé sféry bude dokument s ohledem na vznesené připomínky ještě dopracován a předložen plenárnímu zasedání T-PD v dubnu 2010, aby mohl být předložen radě ministrů. Pozornost věnoval Výbor mimo jiné rovněž otázce vytvoření celosvětového dne/týdne ochrany osobních údajů, návrhu celosvětových standardů ochrany osobních údajů, přípravě na 28. ledna 2010, kdy bude počtvrté připomínán Den ochrany osobních údajů spojený s Úmluvou 108, přípravě aktivit k jejímu 30. výročí v roce 2011.

Již celou řadu let se Úřad v součinnosti s bývalým Ministerstvem informatiky a následně s příslušným útvarem Ministerstva vnitra účastní činností **WPISP – pracovní skupiny pro informační bezpečnost a soukromí ve výboru ICCP v rámci sekretariátu OECD**. Pracovní skupina se v poslední době zabývala např. sítěmi založenými na senzorech, problematikou malware, modelovými praktikami pro poskytovatele internetových služeb, národní strategií pro kybernetickou bezpečnost, autentizací a správou digitálních identit, zabezpečením ochrany dat v globální ekonomice, spoluprací v přeshraničním vymáhání práva v oblasti ochrany soukromí a dat aj.

V rámci bilaterální spolupráce s nově vznikajícími evropskými i mimoevropskými orgány ve sféře činnosti obdobné působnosti Úřadu v poslední době prudce narostl zájem o semináře a pracovní setkání organizované většinou v Praze, na kterých Úřad předává své zkušenosti v oblasti legislativy a praxe. Zájem je zejména o organizaci Úřadu, jeho silné kompetence a mechanismy dozorových činností, včetně praktických poznatků z kontrol a souvisejících správních řízení, tradičně úspěšných public relations a mezinárodní spolupráce. Úřad tak v roce 2009 uspořádal dvakrát seminář pro Agenturu ochrany dat Bosny a Hercegoviny (v Sarajevu a v Praze), dvakrát v Praze přivítal skupinu kolegů z aktuálně se formující Komise pro ochranu dat z Albánie, své poznatky předal čtyřčlenné delegaci Ministerstva průmyslu a informačních technologií z Číny při její studijní cestě po EU a dále se rovněž v Praze setkal se studenty práv z Gruzie.

Kromě aktivity na setkáních spojených se zastoupením v různých výše zmíněných pracovních orgánech patří k účinným formám mezinárodní spolupráce i účast zástupců Úřadu v celé řadě mezinárodních konferencí, seminářů, workshopů apod. Za všechny zmiňme dvě nejprestižnější akce, kterými jsou následující každoroční konference:

Jarní konferenci evropských komisařů ochrany soukromí a osobních údajů (Edinburgh, 23.–24. 4. 2009) zorganizoval britský ICO – Úřad informačního komisaře – s mottem „Zdokonalení ochrany dat". Hlavním cílem bylo zvažovat, do jaké míry současné právní normy EU/ES v oblasti ochrany osobních údajů odpovídají potřebám vývoje, zejména vzhledem ke globalizačním tendencím a prudkému rozvoji informačních technologií a sítí.

Příští konferenci uspořádá Úřad v Praze ve dnech 29.–30. dubna 2010.

31. mezinárodní konference komisařů pro ochranu osobních údajů a soukromí (Madrid, 4.–6. 11. 2009): Pro tradiční celosvětové setkání komisařů ochrany dat, konané v Madridu za rekordní účasti více než 1000 delegátů, byla jednotící myšlenkou bohatého programu snaha o prohloubení a rozšíření mezinárodní spolupráce. Delegáti konference schválili a vydali usnesení o mezinárodních standardech ochrany osobních údajů a soukromí. Dalším zajímavým a do budoucnosti zaměřeným tématem bylo tzv. privacy by design, tedy princip včasného zohlednění požadavků ochrany dat již při vývoji informačních systémů.

ÚŘAD, SDĚLOVACÍ PROSTŘEDKY A KOMUNIKAČNÍ NÁSTROJE

V roce 2009 Úřad zachoval tradici svých bilančních tiskových konferencí, avšak komunikace s médii se soustředila na denní servis a aktuální informování prostřednictvím webových stránek.

Jarní a podzimní tiskové konference široce bilancovaly práci Úřadu za značného zájmu médií tištěných a zejména elektronických (přítomno 20–25 novinářů). Předseda věnoval štědře také prostor individuálním dotazům přítomných novinářů a osvětloval podrobně postoj Úřadu ke stěžejní problematice rekapitulovaného období (např. postoje Úřadu k ochraně osobních údajů dětí a mladistvých, využívání kamerových sledovacích systémů, nejrozsáhlejší databáze citlivých údajů, s níž se Úřad dosud setkal – kontrolovaná databáze elektronických receptů SÚKL). Rozsah zveřejněných zpráv týkajících se ochrany osobních údajů vycházejících z tiskových konferencí odpovídal množství v roce předcházejícím (30–60 výstupů v následujících třech dnech po tiskové konferenci). V přílohách k tiskovým zprávám poskytuje Úřad soustavně informace o kontrolách ukončených správním řízením. Důležitá je zde nejen otevřenost, s níž hovoří o výsledcích své práce, ale především zpráva o důvodech uložených pokut, čímž zároveň prohlubuje právní povědomí ve vztahu k zákonu o ochraně osobních údajů i způsobu jeho aplikace.

Kontakty s médii

Obecně se dá říci, že znalost zákona o ochraně osobních údajů se prohlubuje. Lze tak soudit zejména z denního servisu poskytovaného novinářům, kteří kladou podstatně fundovanější a přesněji formulované dotazy, než tomu bylo v letech předcházejících, a upozorňují na kauzy, které většinou z hlediska porušení zákona jsou skutečně relevantní. Tato praxe odpovídá i zkušenostem se stížnostmi, které na Úřad přicházejí.

Obdobně lze také soudit ze zaměření přímých vystoupení v médiích, které jsou požadovány po předsedovi Úřadu, po odborných pracovnících či tiskové mluvčí: Ubylo obecně formulovaného tématu „ochrana osobních údajů“, naopak přibylo specializovaných témat (např. opakovaně problematika využívání kamerových systémů se soustřeďuje na detaily konkrétních situací, zájem o právní kvalifikaci kauz – centrální databáze lékařských receptů, názor Úřadu na připravovaný loterijní zákon, otázku exekucí atd.).

Mediální výstupy Úřad obvykle publikuje na svých webových stránkách (po dohodě, a jedině na jejím základě, s konkrétním médiem). Je tak posílena i možnost, aby veřejnost sledovala názorovou kontinuitu Úřadu a novináři měli okamžitou odpověď na kladené dotazy – není zajisté žádným tajemstvím, že jistá témata, jakmile jsou otevřena, spustí velký mediální zájem.

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

Faktem ovšem zůstává, že je třeba opakovaně vysvětlovat, že Úřad není nadán legislativní iniciativou a že je povinen respektovat ve výsledných legislativních krocích vůli zákonodárců, přestože uplatňuje erudovaně své připomínky z hlediska právních norem ochrany osobních údajů a respektování soukromí s ohledem na domácí i evropskou legislativu i judikaturu. Faktem také je, že „netrpělivost srdce" médií i jednotlivců danou skutečnost ne vždy s pochopením a smyslem pro realitu přijímá.

Šíření znalostí o ochraně osobních údajů

V souvislosti se Dnem ochrany osobních údajů 2009 a se skutečností, že ČR předsedala v prvním pololetí roku Evropské unii, pozval předseda Úřadu k setkání svého francouzského partnera do Prahy. V návaznosti na setkání byla za účasti předsedy francouzské Commission Nationale de l' Informatique et des Libertés (CNIL) senátora Alexe Türka a jeho doprovodu uspořádána s Francouzským institutem veřejná diskuse o současné problematice ochrany osobních údajů. Úřad uspořádal také ve spolupráci s Francouzským institutem filmovou projekci. Na večeru nazvaném „Informatika a svoboda" byl promítnut francouzský dokument „Total contrôle" režiséra Étiena Labroue a legendární český film Vlastimila Venclíka „Nezvaný host".

Zvýšenou účast i značný kvalitativní posun zaznamenal Úřad v soutěži pro děti a mládež „Moje soukromí! Nekoukat, nešťourat!". Předání cen vítězům, tradičně v rámci zlínského Mezinárodního festivalu pro děti a mládež, se zúčastnila předsedkyně Stálé komise Senátu pro ochranu soukromí senátorka Ing. Jana Juřenčáková a senátor PaedDr. Václav Homolka. Soutěžní práce dětí byly vystaveny pod záštitou senátorky Juřenčákové u příležitosti zahájení nového školního roku v předsálí jednacího sálu Senátu ČR.

Výstava dětských prací byla také vítaným doplňkem odborné konference pořádané společností International Data Group, a. s. (IDG). Práce dětí zaujaly i zahraniční kolegy: Výstavka se konala na Kypru, jedním z vítězných obrázků doprovodil informaci o soutěži časopis vydávaný úřadem pro ochranu osobních údajů ve státě Victoria v Austrálii.

Rok 2009 byl třetím rokem, kdy Úřad realizoval v rámci tříleté akreditace Ministerstva školství, mládeže a tělovýchovy program dalšího vzdělávání pedagogických pracovníků zaměřený na ochranu osobních údajů ve vzdělávání. Přestože poslední ze seminářů tříletého projektu bylo třeba vzhledem k chřipkové epidemii přesunout až na počátek roku 2010, lze říci, že semináři, které zajišťoval po odborné stránce Úřad, prošlo na 200 pedagogů; na základě testů, zajišťujících pro Úřad také zpětnou vazbu a informaci o pochopení přednášené látky, získali účastníci seminářů certifikáty. Seminář se těšil opravdovému zájmu, který potvrzovala nejen vyjádření v testech a následně zasílaná poděkování, ale také zájem některých pedagogů zúčastnit se semináře opakovaně (kupříkladu vzhledem k novým dotazům, které by chtěli zodpovědět).

Úřad považuje za důležité pokračovat ve spolupráci se školstvím a má připraven další projekt, jehož realizace se bude v roce 2011 odvíjet z obsahu soutěže „Moje soukromí! Nekoukat, nešťourat!", která proběhne v roce 2010.

Za důležité považoval Úřad i setkání s generací seniorů (za spolupráce 3. lékařské fakulty UK), jíž je třeba stále objasňovat nejen smysl ochrany osobních údajů, ale zejména mezi ní šířit vědomí, že ochrana soukromí je jejich právem.

Nepochybně přínosné jsou i přednášky pracovníků Úřadu (právníci Úřadu odpřednášeli v loňském roce 258 hodin) a setkání předsedy, inspektorů a vedení Úřadu se Stálou komisí Senátu pro ochranu soukromí. Za úspěšný je třeba jednoznačně označit seminář k problematice profilů DNA, který byl iniciován na základě kontrolních poznatků Úřadu a který pod záštitou místopředsedy Senátu ČR MVDr. Lišky uspořádala senátorka Ing. Jana Juřenčáková a předseda Úřadu na podzim roku 2009. Byla jím otevřena řada problémů, které potřebují precizaci legislativního ukotvení.

Knihovna a publikace Úřadu

Knihovna nadále slouží jako odborné zázemí pro pracovníky Úřadu, ale je otevřena na individuální vyžádání též odborné veřejnosti. Využívají ji studenti pro své seminární a diplomové práce dotýkající

se ochrany osobních údajů. V roce 2009 poskytla svůj fond sedmi studentům a získala dvě diplomové a jednu seminární práci. Fond knihovny se rozrostl o 98 svazků (67 jich bylo zakoupeno, 31 obdržel Úřad jako dar).

Věstník Úřadu publikoval ve svých 4 částkách zásadní stanoviska Úřadu i důležité dokumenty o ochraně osobních údajů zahraniční provenience.

V roce 2009 tradičně vyšla čtyři čísla Informačního bulletinu, která vzhledem k úsporným opatřením vystřídají v roce 2010 pouze čísla dvě, tematicky zaměřená na konkrétní a pro Úřad aktuálně řešené problematiky.

Vzhledem k úsporným opatřením na konci roku 2009 Úřad rovněž ukončil soustavné elektronické zveřejňování informací o dění v oblasti ochrany osobních údajů v zahraničí.

NOVÁ KOMPETENCE ÚŘADU NA ZÁKLADĚ ZÁKONA O ZÁKLADNÍCH REGISTRECH – INFORMAČNÍ SYSTÉM ORG V SYSTÉMU ZÁKLADNÍCH REGISTRŮ

Zákon č. 111/2009 Sb., o základních registrech, stanovuje vznik základních registrů včetně vytvoření informačního systému pro tvorbu agendových identifikátorů fyzických osob (informační systém ORG v systému základních registrů veřejné správy, zkráceně ORG), s účinností od 1. 7. 2010. To s sebou přináší novou kompetenci Úřadu pro ochranu osobních údajů.

Celou koncepcí systému základních registrů (ZR) prolíná několik principů, jejichž hlavním účelem je ochrana dat před zneužitím, což je řešeno právě projektem ORG. Prvním z nich je použití systému bezvýznamových identifikátorů fyzických osob. Každá fyzická osoba bude mít přidělen tzv. zdrojový identifikátor, z něhož budou odvozeny další, tzv. agendové identifikátory fyzických osob pro každou agendu, ve které daná osoba figuruje. Díky tomu, že v každé agendě bude osoba označena jiným identifikátorem, bude možné zabránit neoprávněnému sdílení údajů mezi agendami. Dalším bezpečnostním opatřením je striktní rozdělení rolí mezi různé úřady. V praxi tak bude jeden úřad správcem vlastního registru, jiný úřad bude zajišťovat provoz informačního systému základních registrů a v neposlední řadě zde sehraje speciální úlohu Úřad pro ochranu osobních údajů, který bude generovat identifikátory fyzických osob pro jednotlivé agendy a na základě oprávněných požadavků je mezi nimi převádět. Součástí koncepce je i centrální systém správy rolí pro přístup k datům, který zajistí, že ke každému referenčnímu údaji v jednotlivých základních registrech bude moci přistupovat pouze úředník, který je k tomu ze zákona oprávněn. Veškeré přístupy k referenčním údajům budou samozřejmě evidovány a budou tak moci být kdykoliv zpětně kontrolovány.

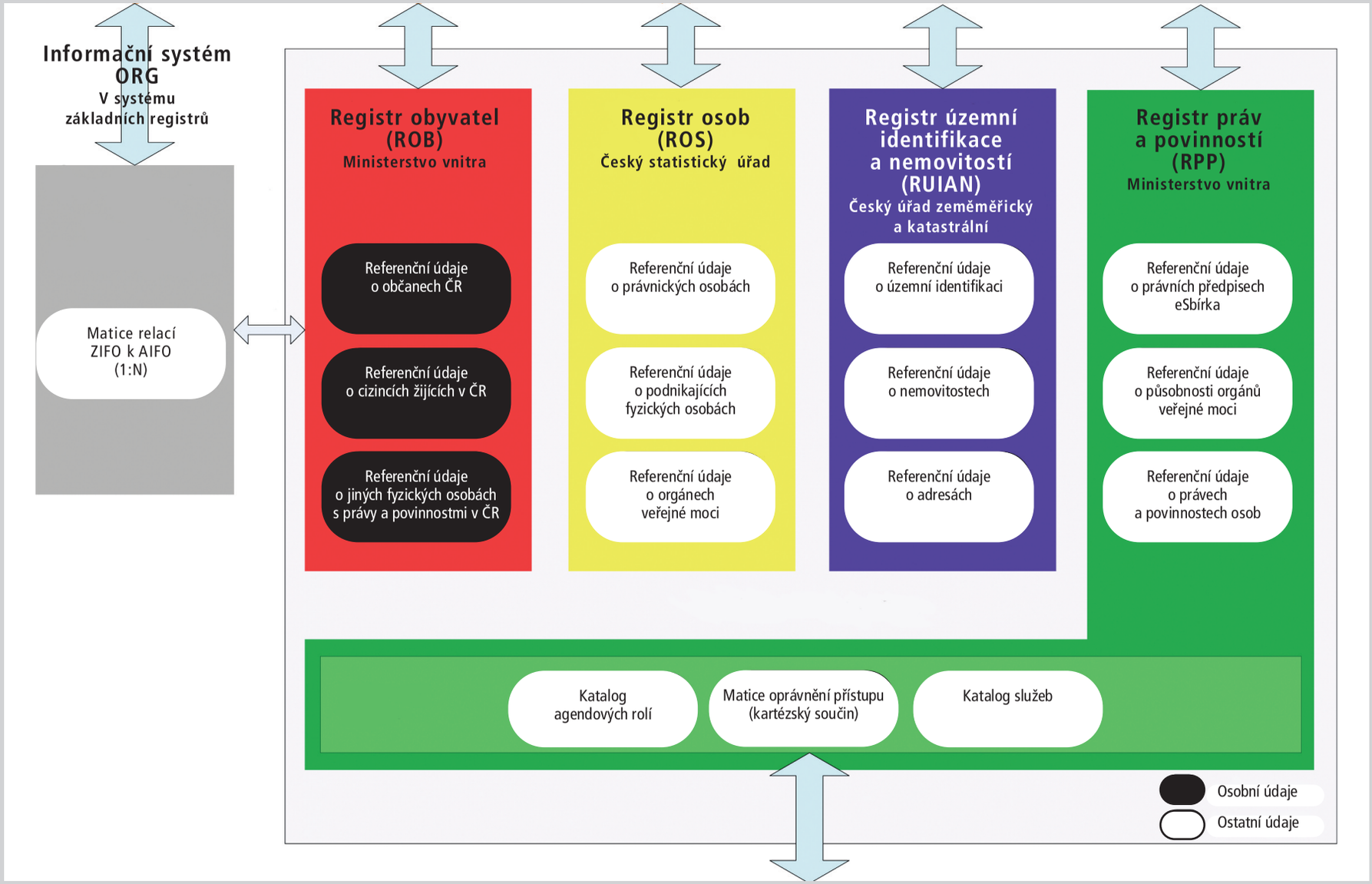
Zákon č. 111/2009 Sb., o základních registrech, zavádí následující funkční bloky systému základních registrů:

- základní registr obyvatel (dále ROB),
- základní registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci (dále ROS),
- základní registr územní identifikace, adres a nemovitostí (dále RUIAN),
- základní registr agend orgánů veřejné moci a některých práv a povinností (dále RPP),
- informační systém základních registrů (dále ISZR),
- informační systém ORG (dále jen ORG).

INFORMAČNÍ SYSTÉM ZÁKLADNÍCH REGISTRŮ (ISZR)

Kompetenční centrum (Ministerstvo vnitra)

Obsahuje auditní logy!!!



Informační systém ORG v systému základních registrů

Informační systém ORG je samostatným funkčním blokem systému základních registrů, který bude zajišťovat procesy týkající se identifikátorů fyzických osob. Jedná se zejména o tyto procesy:

- Vytváří zdrojové identifikátory fyzických osob a agendové identifikátory fyzických osob a vede jejich seznam.
- Zajišťuje převod agendového identifikátoru fyzické osoby v jedné agendě na agendový identifikátor této fyzické osoby v jiné agendě, a to na základě zákonného požadavku.

Identifikátory fyzických osob jsou:

- Agendový identifikátor fyzické osoby (dále též AIFO) – neveřejný identifikátor, který je jednoznačně přiřazen záznamu o fyzické osobě; je odvozen ze zdrojového identifikátoru fyzické osoby a kódu agendy a je užíván výlučně k jednoznačnému určení fyzické osoby pro účely výkonu agendy, pro kterou byl přidělen. Nelze z něj odvodit zdrojový identifikátor fyzické osoby ani osobní nebo jiné údaje o fyzické osobě, jíž byl přiřazen.
- Zdrojový identifikátor fyzické osoby (dále též ZIFO) – neveřejný identifikátor, který je veden a používán výhradně v informačním systému ORG k vytváření agendových identifikátorů fyzických osob pro jednotlivé agendy. Nelze z něj dovodit osobní ani jiné údaje o fyzické osobě, jíž byl přiřazen.

Fyzická osoba může být identifikována v jednotlivé agendě pouze jedním agendovým identifikátorem fyzické osoby.

Rozdělení projektu do dílčích etap umožní postupnou implementaci ORGu v návaznosti na budování ostatních částí Informačního systému základních registrů (ISZR). Vzhledem k tomu, že generování ZIFO a AIFO je klíčová funkčnost, která musí být k dispozici již na začátku implementace ZR, je harmonogram navržen tak, aby základní funkcionalita s omezeným výkonem byla dostupná v průběhu roku 2010.

Financování projektu ORG

V současné době na základě usnesení vlády ze dne 17. 8. 2009 č. 1019 bylo zajištěno i financování projektu, a to jak v roce 2009, tak i v dalších letech, včetně zajištění části finančních prostředků na provoz a údržbu informačního systému v letech 2011 a 2012. U projektu bude podíl státního rozpočtu (SR) České republiky ve výši 15 % a podíl prostředků z rozpočtu Evropské unie ve výši 85 %. Předpokládaná finanční náročnost projektu je uvedena v následující tabulce:

(Údaje v tisících Kč)

Název položky	2009		2010			
	ze SR	z EU	**Celkem**	ze SR	z EU	**Celkem**
Programové vybavení	5 444	30 851	**36 295**	7 695	43 600	**51 295**
Ostatní nákupy dlouhodobého majetku	360	**2 040**	2 400	2 385	13 505	**15 890**
Výpočetní technika	1 696	9 609	**11 305**	2 410	13 655	**16 065**
Celkem	7 500	42 500	**50 000**	12 490	70 760	**83 250**

(pokračování tabulky)

Název položky	2011		Celkem ORG	
	ze SR	z EU	Celkem	
Programové vybavení	6 529	36 995	43 524	131 114
Ostatní nákupy dlouhodobého majetku	2 313	13 083	15 396	33 686
Výpočetní technika	4 998	28 322	33 320	60 690
Celkem	13 840	78 400	92 240	225 490

PERSONÁLNÍ OBSAZENÍ ÚŘADU

Pro rok 2009 měl Úřad dáno státním rozpočtem 96 funkčních míst, z toho jedno funkční místo bylo určeno na zabezpečení úkolů vyplývajících z výkonu předsednictví ČR v Radě Evropské unie v roce 2009. Toto funkční místo zaniklo dne 30. 9. 2009.

K 1. 1. 2009 byl fyzický počet zaměstnanců v Úřadu 93, z toho 90 funkčních míst bylo obsazeno a 3 zaměstnanci byli v mimoevidenčním stavu.

K 31. 12. 2009 byl počet zaměstnanců 95 (z toho 3 zaměstnanci v mimoevidenčním stavu).

V průběhu roku nastoupilo do Úřadu 11 nových zaměstnanců a 9 zaměstnanců pracovní poměr ukončilo.

Průměrný přepočtený evidenční počet zaměstnanců za rok 2009 byl 90,807.

V Úřadu jsou 2/3 zaměstnanců s vysokoškolským vzděláním a zhruba 1/3 zaměstnanců s úplným středním nebo úplným středním odborným vzděláním. Úřad svým zaměstnancům umožňuje a zajišťuje prohlubování kvalifikace, její zvyšování a zajišťuje jazykovou výuku, a to v jazyce anglickém, francouzském i německém.

Členění zaměstnanců Úřadu podle věku a pohlaví – stav k 31. 12. 2009

Věk	muži	ženy	celkem	%
18–20 let	0	0	0	0,0 %
21–30 let	7	11	18	18,9 %
31–40 let	3	9	12	12,6 %
41–50 let	7	10	17	17,9 %
51–60 let	17	15	32	33,7 %
61 let a více	12	4	16	16,8 %
Celkem	46	49	95	100,0 %
%	48,4 %	51,6 %	100,0 %	

Členění zaměstnanců Úřadu podle vzdělání a pohlaví – stav k 31. 12. 2009

Vzdělání	muži	ženy	celkem	%
základní	0	0	0	0,0 %
vyučen	1	1	2	2,1 %
střední odborné	0	1	1	1,1 %
úplné střední všeobecné	3	6	9	9,5 %
úplné střední odborné	4	16	20	21,1 %
vyšší odborné	0	1	1	1,1 %
bakalářské	0	0	0	0,0 %
vysokoškolské	34	26	60	63,2 %
VŠ + vyšší kvalifikace	1	1	2	2,1 %
Celkem	43	52	95	100,0 %

Celkový údaj o vzniku a skončení pracovních poměrů zaměstnanců v roce 2009

	Počet
nástupy	11
odchody	9

HOSPODAŘENÍ ÚŘADU

Rozpočet Úřadu byl schválen zákonem č. 475/2008 Sb., o státním rozpočtu České republiky na rok 2009.
Čerpání státního rozpočtu kapitoly 343 – Úřad pro ochranu osobních údajů

Souhrnné ukazatele	v tisících Kč
Příjmy celkem	3 104,41
Výdaje celkem	91 816,19
Specifické ukazatele – příjmy	
Nedaňové příjmy, kapitálové příjmy a přijaté transfery celkem	3 104,41
Specifické ukazatele – výdaje	
Výdaje na zabezpečení plnění úkolů ÚOOÚ	91 816,19
v tom: výdaje spojené s výkonem předsednictví ČR v Radě EU	1 162,25
ostatní výdaje na zabezpečení plnění úkolů ÚOOÚ	90 653,94
Průřezové ukazatele výdajů	
Platy zaměstnanců a ostatní platby za provedenou práci	41 705,00
Povinné pojistné placené zaměstnavatelem*)	14 181,00
Převod fondu kulturních a sociálních potřeb (FKSP)	789,44
Platy zaměstnanců v pracovním poměru	30 493,00
Platy zaměstnanců v prac. poměru odvozované od platů ústav. činitelů	8 972,00
Výdaje na programy vedené v ISPROFIN celkem	8 327,57

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

Příjmy

Příjmy pro rok 2009 nebyly schváleným rozpočtem stanoveny. Rozpočet příjmů kapitoly 343 – Úřad pro ochranu osobních údajů byl naplněn částkou 3 104,41 tisíc Kč.

Jednalo se zejména o refundace zahraničních cest zaměstnanců Úřadu Radou Evropy, Europolem a Evropskou komisí, o sankce uložené podle zákona č. 480/2004 Sb., o některých službách informační společnosti, o sankce uložené podle zákona č. 101/2000 Sb., o ochraně osobních údajů, o náhrady nákladů řízení, o úroky za finanční prostředky uložené na účtech u ČNB, o pojistné náhrady, o příjmy vztahující se k roku 2008 (odvod zůstatku depozitního účtu po vyplacení platů a přídělu do FKSP za prosinec 2008).

Úroky z finančních prostředků uložené na účtech u ČNB činily 2,11 tisíc Kč.

Přijaté sankční platby byly ve výši 1 720,20 tisíc Kč, pojistné náhrady ve výši 13,30 tisíc Kč, náklady řízení ve výši 124,06 tisíc Kč, neinvestiční dotace z EU ve výši 51,23 tisíc Kč a refundace týkající se minulých let ve výši 84,45 tisíc Kč. Veškeré příjmy Úřadu byly odvedeny do státního rozpočtu.

Ostatní běžné výdaje

Čerpání běžných výdajů ve výši 26 813,18 tisíc Kč odpovídá běžným provozním výdajům, které vyplývají z hlavní činnosti Úřadu; jde zejména o položky spojené s nákupem drobného hmotného majetku, materiálu, služeb, cestovného, vzdělávání, údržby a o výdaje související s neinvestičními nákupy.

Výdaje za vodu, plyn a elektrickou energii činily v roce 2009: 1 529,33 tisíc Kč.

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

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. 2009 byl 95 zaměstnanců.

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

V souladu se schválenou dokumentací programu 143 010 „Rozvoj a obnova materiálně-technické základny Úřadu pro ochranu osobních údajů“ bylo celkem vyčerpáno 8 327,57 tisíc Kč.

V programu 143 010 „Rozvoj a obnova materiálně technické základny“ šlo zejména o:

Podprogram 143 011 „Pořízení, obnova a provozování ICT ÚOOÚ“, kde byly v roce 2009 čerpány **investiční** *systémově určené výdaje SR* na:

	v tis. Kč
akci 143 011 0008 „Prodloužení smlouvy Enterprise na používání produktů Microsoft“	1 681,90
akci 143 011 0009 „Datové schránky“	460,53
akci 143 011 0010 „IS ÚOOÚ – Informační modul“	1 752,25
akci 143 011 0011 „Rozšíření sítě LAN“	102,74
akci 143 011 0012 „Rozšíření sítě SAN“	209,19
akci 143 011 0013 „Lehký výkonný notebook“	54,88
akci 143 011 0014 „Rozšíření modulu EKLEP“	171,90
akci 143 011 0015 „Úprava modulů v GIS WORKS“	440,30
akci 143 011 0016 „Elektronická tabule“	49,88
akci 143 011 0020 „Rozšíření datové sítě“	138,04
akci 143 011 0021 „Upgrade modulu klíčové hospodářství“	62,48
akci 143 011 0022 „Adobe LifeCycle ES“	518,27
akci 143 011 0023 „Změna počtu licencí MS“	100,52
akci 143 011 0024 „Upgrade modulů Organizace“	145,00

Podprogram 143 012 „Reprodukce majetku ÚOOÚ“ – kde byly čerpány **investiční** *systémově určené výdaje SR* na:

akci 143 012 0010 „Drobné úpravy budovy“	337,30
akci 143 012 0011 „Klimatizace kanceláří“	1 502,11
akci 143 012 0012 „Zabezpečení objektu“	555,42
akci 143 012 0013 „Klimatizace (chlazení) jednací místnosti“	44,86

Investiční systémově určené výdaje byly čerpány celkem ve výši 8 327,57 tisíc Kč , z toho čerpání na investiční akce v podprogramu 143 011 „Pořízení, obnova a provozování ICT ÚOOÚ“ 5 887,88 tisíc Kč, v podprogramu 143 012 „Reprodukce majetku ÚOOÚ“ 2 439,69 tisíc Kč.

Interní audit a vnitřní kontrola

Funkce vnitřního auditu je personálně zajištěna od roku 2006.

V červnu roku 2009 byl proveden v souladu s plánem audit ověření správnosti evidence a proplácení příspěvku na stravování (stravenky) zaměstnancům Úřadu.

PŘEHLED ČERPÁNÍ ROZPOČTU V ROCE 2009

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2009 v tis. Kč	Upravený rozpočet 2009 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2009 v tis. Kč	Skut./uprav. rozpočet v %
	PŘÍJMY CELKEM	0	42 500	3 104,41	7,30
501	Platy	39 465	39 465	39 465	100,00
5011	Platy zaměstnanců	30 493	30 493	30 493	100,00
5014	Platy zaměstnanců odvozované od platů úst. činitelů	8 972	8 972	8972	100,00
502	Ostatní platby za provedenou práci	2 240	2 240	2 240	100,00
5021	Ostatní osobní výdaje	1 940	1 940	1 940	100,00
5024	Odstupné	300	300	300	100,00
503	Povin. pojist. placené zaměstnavatelem	14 181	14 181	14 181	100,00
5031	Povin. pojist. na sociální zabezpečení	10 427	10 427	10 427	100,00
5032	Povin. pojist. na veřejné zdrav. pojištění	3 754	3 754	3 754	100,00
513	Nákup materiálu	3 160	2 665	1 547,09	58,05
514	Úroky a ostatní fin. výdaje	27	27	10,40	38,52
515	Nákup vody, paliv a energie	2 380	2 125	1 812,36	85,29
516	Nákup služeb	19 642	18 833	15 141,83	80,40
5167	Školení a vzdělávání	1 700	1 767	1 343,26	76,02

Druh rozpočtové skladby	Název ukazatele	Schválený rozpočet 2009 v tis. Kč	Upravený rozpočet 2009 v tis. Kč	Skutečnost dle účetních výkazů k 31. 12. 2009 v tis. Kč	Skut./uprav. rozpočet v %
517	Ostatní nákupy	7 426	6 876	5 832,83	84,83
5171	Opravy a udržování	2 998	2 598	2 233,73	85,98
5173	Cestovné	2 626	2 626	2 452,22	93,38
518	Poskytnuté zálohy	0	0	0	0
519	Výdaje souvis. s neinv. nákupy	2 910	2 615	2 123,56	81,21
5342	Převody FKSP	790	790	789,44	99,93
5346	Neinv. převody do RF		0	0	0
536	Ostatní neinv. transf. jiných veřej. rozpočtů	15	28	13,10	46,78
542	Náhrady plac. obyvatelstvu	560	560	120	21,43
5424	Náhrady v době nemoci	500	500	120	24
590	Ostatní neinv. výdaje jinde nezařazené	0	212	212	100
	Běžné výdaje celkem	92 796	90 617	83 488,61	92,13
611	Pořízení dlouh. nehmot. majetku	2 500	44 035	5 333,15	12,11
612	Pořízení dlouh. hmot. majetku	6 000	14 465	2 994,42	20,70
6361	Inv. převody do RF				
	Kapitálové výdaje celkem	8 500	58 500	8 327,57	14,24
	VÝDAJE CELKEM	**101 296**	**149 117**	**91 816,19**	**61,57**

Číselné údaje jsou použity z výkazů zpracovaných ke dni 31. 12. 2009.

PŘEHLED VÝDAJŮ SPOJENÝCH S VÝKONEM PŘEDSEDNICTVÍ ČR V RADĚ EU V ROCE 2009

Položka – název	Schválený rozpočet (v tis. Kč)	Upravený rozpočet (v tis. Kč)	Čerpání (v tis. Kč)
5011/15 Platy	428	428	428,00
5031/15 Povinné pojistné na SZ	108	108	108,00
5032/15 Povinné pojistné na ZP	39	39	39,00
5139/15 Nákup materiálu	5	5	0,00
5342/15 FKSP	9	9	8,40
5142/15 Realizované kurzové ztráty	2	2	0,06
5163/15 Služby peněžních ústavů	0	1	0,59
5164/15 Nájemné	550	382	174,00
5169/15 Nákup ostatních služeb	0	167	157,00
5173/2/15 Cestovné zahraniční	26	26	15,30
5175/15 Občerstvení	432	432	231,90
5194/15 Dary	30	30	0
Celkem	1 629	1 629	1 162,25

POSKYTOVÁNÍ INFORMACÍ PODLE ZÁKONA O SVOBODNÉM PŘÍSTUPU K INFORMACÍM

Úřad v roce 2009 obdržel celkem jedenáct žádostí o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. Oproti předchozímu roku, kdy Úřad obdržel žádostí šest, je to nárůst takřka na dvojnásobek.

Ve dvou případech byla žádost o informace odmítnuta (v obou případech bylo toto rozhodnutí žadateli napadeno rozkladem k předsedovi Úřadu), ve zbylých případech bylo žadatelům vyhověno. Obsah poskytnuté informace byl dále v souladu s povinností uloženou Úřadu § 5 odst. 2 zákona o svobodném přístupu k informacím zveřejněn na webových stránkách Úřadu.

V sedmi případech se žádost o poskytnutí informace týkala konkrétního řízení, kdy se žadatel dotazoval na vyřízení svého podnětu nebo na výsledek jiného řízení či na to, zda v předmětné věci Úřad kontrolu či řízení vedl. V jednom případě se žádost týkala personálního složení Úřadu, jeden žadatel požadoval zaslání publikovaných stanovisek Úřadu, jedna žádost se týkala toho, jaké osobní údaje a za jakým účelem Úřad v obecné rovině zpracovává, a jedna žádost se týkala postupu Úřadu při poskytování informací.

Počet žádostí o konzultace, které je Úřad povinen poskytovat podle § 29 písm. h) zákona o ochraně osobních údajů a které byly žadatelem mylně označeny jako žádosti o informace, se mírně snížil, nicméně i přesto se takové nesprávně označené žádosti vyskytly. Úřad je povinen obdržené podněty a podání posuzovat podle jejich obsahu bez ohledu na to, jak jsou označeny. Označovat žádost o vyjádření nebo dotaz adresovaný Úřadu za žádost o poskytnutí informace dle zákona o svobodném přístupu k informacím je proto nepřesné a nadbytečné. I v takovém případě totiž Úřad dotaz vyřizuje podle výše uvedeného ustanovení zákona o ochraně osobních údajů.

Výroční zpráva Úřadu pro ochranu osobních údajů za rok 2009
Úřad pro ochranu osobních údajů
Pplk. Sochora 27, 170 00 Praha 7
E-mail: posta@uoou.cz
Internetová adresa: www.uoou.cz
Na základě povinnosti, kterou mu ukládá zákon č. 101/2000 Sb.,
o ochraně osobních údajů, ve znění pozdějších předpisů, § 29, písm. d), a § 36,
zveřejnil Úřad pro ochranu osobních údajů tuto výroční zprávu
v únoru 2010 na svých webových stránkách.

Editor: PhDr. Hana Štěpánková, telefon 234 665 286
Redakční zpracování: Mgr. Nina Táborská
Grafické řešení: Eva Lufferová
Jazyková korektura: Tiskové odd. ÚOOÚ a Mgr. Eva Strnadová
Tisk: Tiskárna Helbich, a. s., Valchařská 36, 614 00 Brno
Pro Úřad pro ochranu osobních údajů vydalo Nakladatelství MU Brno, 2010

ISBN 978-80-210-5130-0