úřad
pro ochranu
osobních
údajů

informační bulletin
1 / 2005

1. TADY A TEĎ

Výroční zpráva za rok 2004

Úřad zveřejnil svou výroční zprávu za rok 2004 v únoru 2005 (26. 2.), jak mu ukládá zákon o ochraně osobních údajů /§ 29 d) a § 36/. Zpráva je dostupná na webových stránkách, na adrese Úřadu www.uoou.cz/vz_2004.pdf. Tištěnou podobu výroční zprávy dostane veřejnost k dispozici do konce prvního pololetí roku 2005. Úřad se rozhodl tiskem vydat výroční zprávu za rok 2004 v plném znění dvojjazyčně – česky a anglicky a v souvislosti s tím, že se Česká republika stala roku 2004 členem Evropské unie, učinit zprávu plně dostupnou nejen občanům České republiky (dříve Úřad publikoval anglicky pouze resumé). Níže přetištěná přehledová tabulka je součástí výroční zprávy a přináší v číselných údajích přehled o činnosti Úřadu.

V roce 2004 dosáhla celková výše Úřadem uložených pokut 1 534 400 Kč. Je ovšem třeba zdůraznit, že trestání a ukládání pokut, kterému Úřad v souladu se zákonem samozřejmě musí dostát, není meritorním smyslem jeho působnosti: Úřad usiluje a důrazně i nadále bude usilovat především o nastolení praxe zákonného a korektního jednání správců osobních údajů, které je v souladu s dobrým fungováním demokratické společnosti i s principem dobrých mravů. Toto Úřad považuje za podstatné pro kvalitu života občanů České republiky.

V souvislosti se zjištěními, k nimž dospěla kontrolní činnost Úřadu, výroční zpráva za rok 2004 upozorňuje na praktiky, s nimiž by se měla společnost dokázat vypořádat.

(srv. www.uoou.cz/vz_2004.pdf, s. 10 – 24)

Činnost Úřadu v číslech – rok 2004

Dotazy	e-mailové dotazy	975
	Dotazy došlé poštou – právnické osoby	261
	Dotazy došlé poštou – fyzické osoby	96
	Telefonické dotazy	5 207*
Stížnosti**		335 + 306***
Kontrolní činnost	Celkem kontrol	79
	ukončeno	71
	dle plánu	19
	incidenčních kontrol	60
Správní trestání	Přijato podnětů celkem	45
	Rozhodnutí o uložení pokuty	35
Registrace	Celkový počet správců	21 709
	Zaregistrováno zpracování celkem	24 588
	V roce 2004 oznámení celkem	1 972

	Počet žádostí týkajících se předávání osobních údajů do zahraničí (§ 27 zákona č. 101/2000 sb.)	52
	Povolených předání	35
Připomínkované legislativní návrhy	Zákony	72
	Vyhlášky	107
	Nařízení vlády	36
	Ostatní	80
Instituce, jejichž materiály (nejen legislativní povahy) byly připomínkovány	Česká národní banka	1
	Český báňský úřad	1
	Český úřad zeměměřický a katastrální	4
	Český statistický úřad	1
	Úřad pro ochranu hospodářské soutěže	1
	Správa státních hmotných rezerv	1
	Státní úřad pro jadernou bezpečnost	1
	Úřad průmyslového vlastnictví	1
	Úřad vlády	11
	Ministerstvo informatiky	14
	Ministerstvo životního prostředí	34
	Ministerstvo práce a sociálních věcí	20
	Ministerstvo dopravy a spojů	15
	Ministerstvo vnitra	29
	Ministerstvo obrany	4
	Ministerstvo zahraničních věcí	10
	Ministerstvo školství, mládeže a tělovýchovy	26
	Ministerstvo spravedlnosti	25
	Ministerstvo zdravotnictví	56
	Ministerstvo financí	15
	Ministerstvo pro místní rozvoj	15
	Ministerstvo kultury	2
	Ministerstvo průmyslu a obchodu	9
	Veřejný ochránce práv	1
Osobní konzultace	Konzultace poskytované občanům a institucím	89
Přednášky, semináře	(aktivní vystoupení)	33
Publikované materiály	Věstník Úřadu (počet částek)	6
	Bulletin Úřadu (počet čísel)	4

	Stanoviska / „K problémům z praxe“	7
	Překlady zahraničních dokumentů	10
	Tiskové zprávy a sdělení pro tisk	26
	Další podkladové materiály pro potřeby médií	66
Tiskové konference	Pravidelné TK Úřadu	4
	Mimořádné	1
Kontakty s médii	Agenturní servis, tisk, rozhlas a televize	354

** Zahrnuje s přesností v řádu desítek pouze výstupy z pracovišť poskytujících speciálně telefonické odpovědi.*

*** Zahrnuje podněty zaslané Úřadu přímo jako stížnost.*

**** Počet přijatých stížností na nevyžádaná obchodní sdělení od dne nabytí účinnosti zákona č. 480/2004 Sb., o některých službách informační společnosti (tj. za období 7. 9. – 31. 12. 2004)*

(Tabulka zobrazuje stav k 31. 12. 2004.)

Z činnosti Úřadu v 1. čtvrtletí roku 2005

Úřad se zabýval intenzivně problémem záměru zřízení registru nebankovních informací o klientech, a především sdílení informací s registrem bankovních informací. Šlo o hledání vyvážené pozice mezi zájmy poskytovatelů nebankovních úvěrů a klienty a rovněž o nalezení pravidel pro sdílení údajů mezi bankovním a nebankovním registrem. V rámci svých pravomocí Úřad požaduje respektování určitých principů jednání, jimiž lze zajistit jak ochranu soukromí občanů, tak zájmy finančních institucí:

Registr nebankovních informací o klientech – LLCB (Leasing & Loan Credit Bureau, „Nebankovní registr klientských informací sdružující leasingové společnosti a společnosti splátkového prodeje“) – byl zaregistrován na Úřadu pro ochranu osobních údajů 25. února 2005.

Konzultační jednání, která proběhla mezi jeho představiteli a Úřadem, vyústila ve stanovení podmínek, za nichž je možné získávat jednotlivé informace o klientech z bankovního registru (a naopak). Základní principy pro získání uvedených informací jsou:

1. souhlas subjektu údajů – klienta (pojem souhlas je přesně definován zákonem), který se týká
   a) uvedení osobních údajů do registru (LLCB), a to údajů v rozsahu a výběru, o němž rozhoduje každý subjekt údajů (tj. zjednodušeně řečeno každá dotčená fyzická osoba)
   b) následně souhlas poskytovaný vždy každému jednotlivému zájemci, který o klientovi chce z registrů informace získat (ze zákona tento souhlas musí být prokazatelný)
2. pro požadování souhlasu je předpokladem úplná a vyčerpávající informace o tom, k čemu je daný souhlas poskytován (účel, k jehož naplnění ho může provozovatel registru využít) a v jakém rozsahu. Tedy klientovi musí být poskytnuto předem svého druhu „informační memorandum“, na jehož základě souhlas s využitím svých osobních údajů poskytuje.

Úřad pro ochranu osobních údajů tedy stanovil podmínky pro možné využívání údajů z registrů v jednotlivých a konkrétně definovaných případech, ale jednoznačně odmítá možnost formálního a neomezeného propojení registru bankovních a nebankovních informací.

Média žádala v prvním čtvrtletí Úřad o vyjádření v souvislosti se záměrem Ministerstva spravedlnosti a Vězeňské správy vytvořit spisovnu, v níž by vězňové přepisovali záznamy ze soudních jednání. Úřad opakovaně v průběhu roku 2004 vyjádřil k danému záměru svůj skeptický postoj. Žádost o zfor-

mulování svého postoje vůči precizovanému návrhu na fungování uvedené spisovny Úřad obdržel 10. 3. 2005 od předsedy Městského soudu v Praze JUDr. Jana Sváčka. K záměru zaujal odmítavé stanovisko, protože neshledal, že existují dostatečné záruky toho, že osobní údaje by nemohly být zneužity a že není možné nastavit taková pravidla, aby nebyla vysoká pravděpodobnost toho, že zneužity být mohou.

Pravomocně rozhodnuté případy ve správním trestání 26. 11. 2004 – 9. 3. 2005

Deliktní jednání	Sankční opatření	Nápravná opatření
zpracování osobních údajů leasingových nájemců a dalších osob v rozsahu nikoli nezbytném pro naplnění stanoveného účelu § 5 odst. 1 písm. d)	pokuta 90.000 Kč	ano
zpracování osobních údajů, včetně citlivých údajů, osob podezřelých z krádeže zboží bez jejich souhlasu, v rozsahu nikoli nezbytném pro naplnění stanoveného účelu a nesplnění informační povinnosti vůči těmto osobám § 5 odst. 2, § 9 písm. a), § 5 odst. 1 písm. d), § 11 odst. 1 a 2	pokuta 50.000 Kč	ano
absence smlouvy o zpracování osobních údajů se zpracovatelem těchto osobních údajů § 6	pokuta 30.000 Kč	ano
zveřejnění osobních údajů dlužníků nájemného § 5 odst. 1 písm. f)	pokuta 9.000 Kč	ne
nakládání se zdravotnickou dokumentací 4 pacientů bez přijetí opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, k jejich zničení či ztrátě, k jejich neoprávněnému zpracování nebo jinému zneužití § 13 odst. 1	pokuta 5.000 Kč	ne

2. NEMĚLO BY VÁM UNIKNOUT

Nevyžádaná obchodní sdělení

Úřad předkládá aktuální přehledovou tabulku o své agendě plynoucí z povinností ukládaných mu **zákonem o některých službách informační společnosti**, která je zpracována k 31. 3. 2005. K dané kompetenci Úřadu – postihu šíření nevyžádaných obchodních sdělení – se objevila řada rozhovorů a informací v médiích. Vždy a stále je ale třeba zdůrazňovat, že Úřadu je uložena **povinnost postihu šíření nevyžádaných obchodních sdělení**, nikoli spamu jakožto takového. Se zavádějícími informacemi, které ne dosti jednoznačně informují veřejnost o kompetenci Úřadu a mohou tak vzbuzovat její zcela mylná očekávání, se bohužel v médiích můžeme setkávat ještě stále. Speciálně zavedená rubrika na webových stránkách Úřadu poskytuje eventuálním stěžovatelům nejen formulář, který jim usnadní podání stížnosti, ale také soubor Úřadu nejčastěji kladených dotazů v souvislosti s postihem nevyžádaných obchodních sdělení.

O výsledcích kontrol prováděných na základě Úřadu zaslaných podnětů, které jsou uzavřeny a předány do správního řízení, veřejnost může být informována prostřednictvím čtvrtletní tiskové konference Úřadu v červnu.

Statistika podnětů podaných na nevyžádaná obchodní sdělení zaslaných na Úřad v období od 7. 9. 2004 do 31. 3. 2005

Podnět – stížnost	Rok 2004	Rok 2005
zaslaná e-mailem	117	12
běžnou poštou	9	1
z webu ÚOOÚ	180	211
Celkem podaných	**306**	**224**
z toho: uznaný jako neoprávněný	29	29
NOS ze zahraničí	7	9

Poznámka: hodnoceno k 31. 3. 2005

Evropské země zahájily společnou akci v rámci boje proti „spamu"

Úřady pověřené bojem proti spamu ve 13 evropských zemích se dohodly na sdílení informací a vyřizování stížností přes hranice států v rámci celoevropského boje proti spamu. Budou spolupracovat při šetření stížností týkajících se přeshraničního spamu z jakéhokoli místa v EU, takže bude snadnější identifikace a stíhání spammerů kdekoli v Evropě.

Viviane Reding, komisařka pro informační společnost a média, dohodu uvítala a vyzvala úřady ve všech evropských státech, aby se připojily k dohodě. Dále uvedla, že „Výkonné orgány v členských státech musejí být schopné účinným způsobem řešit případy spamu pocházejícího z jiných zemí EU, i když v současné době většina spamu pochází ze zemí mimo EU. Zároveň probíhají práce na spolupráci s třetími zeměmi jak na bilaterálních, tak na mezinárodních fórech – například v rámci OECD a Mezinárodní telekomunikační unie".

Dobrovolným přistoupením, které ustanovuje společný postup pro vyřizování přeshraničních stížností na spam, se vytváří kontaktní síť úřadů pověřených bojem proti spamu (CNSA – Contact Network of Spam Enforcement Authorities), zřízená na základě iniciativy Komise v návaznosti na její Sdělení z ledna 2004. CNSA umožňuje sdílení informací a osvědčených postupů při provádění antispamových právních předpisů národními orgány členských států EU.

Národní agentury, které již přistoupily k používání tohoto postupu, jsou tyto: rakouské Federální ministerstvo pro dopravu, inovace a technologie, belgická Komise pro ochranu soukromí a Federální hospodářská správa, generální ředitelství pro výkon práva a zprostředkování smíru, kyperský Úřad komisaře pro ochranu osobních údajů, český Úřad pro ochranu osobních údajů, dánský ombudsman pro spotřebitele, francouzská Komise pro ochranu dat (CNIL), řecký Úřad pro ochranu dat, irské Ministerstvo pro komunikaci, mořské a přírodní zdroje a Úřad komisaře pro ochranu dat, italský Úřad pro ochranu dat, litevský Státní inspektorát pro ochranu dat, maltský Úřad komisaře pro ochranu dat, nizozemský regulátor elektronických komunikací (OPTA) a Úřad pro ochranu dat (CBP) a španělský Úřad pro ochranu dat.

Smluvní strany se zavázaly, že vyvinou "maximální snahu" při vyřizování stížností obdržených od ostatních stran, aby širší spoluprací zajistily odstranění mezer v právních předpisech, které by mohly být zneužity spammery a zloději dat.

Informovaný občan dokáže chránit své soukromí

Na přelomu roku 2004 a 2005 Úřad zahájil informační kampaň o ochraně osobních údajů. Jejím účelem je poskytnout občanům České republiky informace, které jim poslouží v tom, aby se dokázali orientovat ve svých právech na ochranu soukromí. Důležitou součástí poskytovaných informací je také upozornění na rizika, která ohrožují soukromí lidí v souvislosti s využíváním nejmodernějších informačních technologií. Leták byl distribuován ve více než 200 000 výtiscích na více než 6000 samosprávných úřadů (ve škále od magistrátů po obecní úřady); na těchto místech by leták Úřadu

měl být k dispozici občanům – přinejmenším o tuto spolupráci požádal uvedené orgány předseda Úřadu. Dle požadavků obcí a zastupitelů občanů byl dotištěn leták a jimi požadovaný náklad dodatečně distribuován v dubnu 2005. Informační kampaň podpořila řada médií (např. ČRo, TV NOVA, měsíčník Moderní obec).

V následující etapě Úřad jedná s MŠMT o možnosti poskytnout informační leták studentům středních škol.

Na základě spolupráce s ČT a vstřícného postoje společnosti Benny TV bude využívána k informování občanů také část seriálu „Neznalost zákona neomlouvá", který odvysílala ČT – konkrétně díl věnovaný ve vtipném zpracování ochraně osobních údajů.

V příštím období se chce Úřad zaměřit na edukační kampaň směřující k žákům základních škol.

Úřad vítá spolupráci všech institucí a organizací, které s pochopením pomáhají poskytnout občanům potřebnou informaci o dosud stále ještě ne dost známé problematice ochrany osobních údajů a každé spolupráce si váží a vítá ji. Ochotně také vyjde vstříc všem zájemcům o uvedené informační materiály.

Přílohou tohoto čísla bulletinu Úřadu je výše uvedený informační leták.

3. TÉMA: Zdravotnictví – Zdravotní knížky

Naše zdraví je naším kreditem. Průzkumy ukazují, že si svého zdraví velice ceníme, vážíme a že většina z nás je klade na jedno z prvních míst žebříčku hodnot. V posledních letech dochází také ke změně našich postojů k otázkám zdraví, jeho utužování a prevence. Více či méně úspěšně se snažíme vlastními silami své zdraví vylepšovat, nebo alespoň udržovat na dobré úrovni. Existuje ovšem hranice, od které je všechno naše úsilí marné a kdy se musíme obrátit o radu a pomoc k lékaři. Resort zdravotnictví se oprávněně řadí mezi oblasti, které jsou pod přísným pohledem veřejnosti. Jakoby viditelněji a výrazněji se zde projevují bezkoncepčnost, odkládání rozhodnutí či osobní selhání.

Občané aktivně a kriticky sledují vývoj a dění v resortu zdravotnictví. Se zájmem, ale i se znepokojením nahlížejí na jeho současný stav a hodnotí nejen odbornou úroveň léčby a zdravotnických úkonů, ale i strukturu, řízení a koncepci zdravotnictví.

Při návštěvě u lékaře, na vyšetření či při pobytu v nemocnici očekáváme nejen vysokou odbornou úroveň, lidské a ohleduplné zacházení, ale také diskrétnost a citlivý přístup k naší osobě a k našemu soukromí. Stále větší počet obyvatel považuje za samozřejmé, že naše osobní údaje, včetně citlivých osobních údajů – kategorie osobních údajů, do které zdravotní informace patří – jsou řádně zabezpečeny a že se s nimi nakládá podle daných pravidel, tj. v souladu se zákonem o ochraně osobních údajů.

Občané mají oprávněně obavy z možného úniku zdravotních informací či necitlivého a nesprávného nakládání s nimi. Někdy i sami, pod tíhou obav o zdraví své či svých blízkých, zapomínají na jistou opatrnost při ochraně svého soukromí, nebo na ni ve chvíli ohrožení zdraví či dokonce života vůbec nemyslí. V dobře fungující demokratické společnosti, by se ovšem měli bez obav spolehnout na pravidla, nástroje a mechanismy, které efektivně, citlivě a přitom bezpečně konají v zájmu a pro dobro občana.

V loňském roce v resortu zdravotnictví upoutala, kromě jiného, pozornost veřejnosti otázka plošného zavádění zdravotních knížek obyvatel.

Analýza by měla nabízet konkrétní odpověď na základní otázky – tj. k čemu vlastně má zdravotní knížka sloužit a co se od tohoto kroku očekává. Oslovení občanů, potenciálních pacientů, kterými jsme my všichni, a srozumitelné vysvětlení, jak by v praxi vše probíhalo a co by to pro občany znamenalo, by mělo být samozřejmostí. Občany zajímá, kdo by knížku vystavoval, kdo by byl za knížku odpovědný, jakým způsobem by knížka byla vedena, kdo všechno by k údajům měl přístup a za jakých podmínek a jak by údaje do ní vkládané byly chráněny.

Rozhodně není přínosem názorová neshoda a roztříštěnost v postojích k tak důležitému úkolu, jako je plošné zavedení komplexní zdravotní dokumentace, který je bezesporu záležitostí nákladnou po stránce finanční, organizační i etické.

Vedení ministerstva zdravotnictví v rámci koncepce péče o zdraví plánuje od podzimu roku 2005 zavedení papírových zdravotních knížek, které budou každého pacienta provázet léčením. Papírovou zdravotní knížku s kompletní zdravotní dokumentací mají mít pacienti u sebe a předkládat ji u lékaře. V knížce mají být záznamy o zdravotním stavu pacienta, data léčení i operací, informace o předepsaných lécích, krevní skupině i údaje o očkování. Záznam do knížky by měl vést k úspoře nákladů na léčiva přibližně o jednu třetinu stávajícího stavu, mělo by se předcházet duplicitě v předepisování léků, navodit racionálnější nakládání s nimi a celkově omezit plýtvání peněz ve zdravotnictví. Úspora peněz je jedním z argumentů, proč ministerstvo zdravotnictví prosazuje zavedení papírové knížky, která má být levnější než její elektronická podoba. „Správcem" zdravotní knížky bude praktický lékař, který by tak mohl lépe zabezpečovat diagnostické i léčebné postupy a koordinovat péči o pacienta. Výhradním majitelem bude pouze pacient. Zastánci řešení uvádějí, že tato varianta je ihned použitelná a v podstatě aplikovatelná pro jakoukoliv koncepci zdravotnictví. Může být jakýmsi mezičlánkem v procesu zdokonalování funkčního zdravotnického systému a péče o zdraví občanů. Smyslem zavedení papírové formy zdravotní knížky je vytvoření skutečného kontaktu a spolupráce praktického lékaře s pacientem. Při aplikaci této formy pacient nepotřebuje žádné technické vybavení jako je internet nebo čtecí zařízení. Zavedení klasické papírové zdravotní knížky podporuje i předseda lékařské komory.

Odpůrci této varianty naopak namítají, že zavedení papírových knížek je nákladné, zastaralé, provoz neefektivní, pomalý a navyšující hladinu již tak vysoké byrokracie a administrativy v českém zdravotnictví. Namítají také, že papírová forma je nevhodná i z důvodu rychlé opotřebovatelnosti při častém používání. Podle jejich názoru je tento návrh polovičatým řešením hodným dob dávno minulých. Navíc vláda se zavázala ve Státní informační a komunikační politice, v souladu s cíli EU, k zavádění informačních a komunikačních technologií do zdravotnictví, které jsou nezbytné pro efektivní spolupráci jednotlivých zdravotnických zařízení. Česká republika si uložila postupovat v souladu s aktivitami a cíly v EU v oblasti e-zdravotnictví a například postupně nahrazovat současné průkazy pojištěnců zdravotních pojišťoven čipovými kartami, které budou kompatibilní s mezinárodními pojištěneckými kartami užívanými v zemích EU.

A co na věc „vox populi"? Mnozí lidé, spíše střední a starší generace, možná ministerstvem navrhovanou variantu uvítají. Papírová knížka, kterou si mohou vzít do ruky, přečíst si ji v klidu bez použití jakékoliv techniky – ne všichni mají doma počítač, či přistup na internet – budí pocit důvěry a jistoty. Důležitým aspektem hodnocení je také otázka zabezpečení ochrany osobních údajů. Občané mají přirozeně na první pohled dojem, že právě papírová zdravotní knížka, kterou mají neustále u sebe, kdy údaje s jejich zdravotními informace nekolují „záludnými a nepřehlednými" cestami internetu, splňuje nezbytná kritéria ochrany jejich osobních údajů. Je tomu ale opravdu tak? Komplikace pro občana mohou nastat také například v případě, že zdravotní knížku zapomene. V případě ztráty nebo krádeže knížky vzniká riziko zneužití osobních údajů.

Jiným řešením je elektronická zdravotní karta, neboli tzv. e-karta. Co to vlastně je? Elektronické karty nejsou v České republice ničím novým či neznámým. Můžeme hovořit o dvou formách realizace zdravotních knížek v elektronické podobě.

Při první z nich by pacient sám nenosil s sebou nic „hmatatelného". Všechna data, veškeré osobní i zdravotnické údaje by byly zaneseny, a tedy i dostupné, on-line prostřednictvím internetu. V současné době je příkladem takového řešení například systém IZIP, zatím dostupný pouze pro pojištěnce VZP. Výhodou je obrovský rozsah informací, které mohou být v systému obsaženy. Lze hovořit o nabídce komplexní zdravotnické dokumentace, včetně například výstupů diagnostických počítačových systémů, či rentgenových snímků. Neopominutelnou výhodou je také dostupnost odkudkoli v dosahu internetu. Přístup je zabezpečen přes PIN, takže číst v ní může buď sám pacient, nebo lékař, kterému to pacient umožní. Vkládat údaje, tj. zdravotní záznamy, mohou jen zdravotničtí pracovníci registrovaní v sytému IZIP. Do určitých částí může zapisovat i pacient. Dalším, neméně vý-

znamným pozitivním aspektem, je nemožnost takovou knížku ztratit, či zapomenout doma. V současné době je už přibližně tři sta padesát tisíc lidí účastníkem systému IZIP, tj. má na internetu svou zdravotní knížku.

Druhou formou e-karty je jakási „hmatatelná" elektronická knížka. V současné době má například podobu čipové karty. Tento typ e-karty by měl pacient u sebe a musel by si ji vždy k lékaři nosit sám. Na čipovou kartu se jistě vejdou veškeré základní údaje o pacientovi, přehled diagnóz, ordinovaných léků, alergií, očkování atd., nicméně objem paměti, obsažený v tomto typu nosičů, je omezený. Nevýhodou je možnost zapomenutí doma, ztráty nebo i krádeže. Na tomto místě bychom chtěli připomenout projekt Mácha. Koncem roku 1995 byl Evropskou komisí schválen projekt „národní zdravotnický informační systém a statistika", financovaný z programu EK Phare. Samostatnou částí tohoto pilotního projektu byl experiment zavedení čipové karty ve zdravotnictví a ve zdravotním pojištění. Zkušebním městem se staly Litoměřice. Občané měli k projektu velice pozitivní přístup. Postupně bylo vydáno 27 tisíc čipových karet. Obdrželi je ti občané Litoměřic, kteří jsou pojištěni u VZP ČR. Všichni, kdo byli zapojeni v tomto projektu, lékaři i majitelé karet, byli s technologií karet seznámeni a neměli s jejím užíváním žádné problémy. Bezpečnost obsažených údajů je zajištěna, pouze oprávněné osoby mohou číst nebo vkládat určité údaje. K výzkumnému projektu se připojila i místní nemocnice. V prostorách nemocnice byla zabudována informační centra, kde si pacienti mohli číst a kontrolovat údaje zapsané ve svých čipových kartách. Čtečky by byly v ostrém provozu instalovány i ve vozech záchranné služby. Pacienti byli projektem zaujati, byli aktivní, měli oprávněný pocit, že se mohou sami aktivně podílet na probíhajícím procesu. Velice dobře spolupracovali s lékaři a dožadovali se aktualizace zápisů do svých karet. Zájem o čipové karty měly i lékárny a hygienická stanice. Výsledky a zkušenosti tohoto pilotního projektu potvrzují, že využívání technologie čipových karet je funkční a efektivní a že plošné zavedení je reálné.

Je důležité, že lidé věděli, že oni jsou těmi hlavními aktéry, chápali pravidla tohoto projektu a byli náležitě motivováni e-karty využívat. Důležité bylo lidem vysvětlit, že není čeho se obávat, že malá čipová karta je jistým a spolehlivým garantem předávání zdravotních informací o každém jednotlivci, v případě prevence, léčení, ale i záchrany jejich života a že na péči o sebe samé mají účast a zároveň drží ve svých rukou i ochranu svého soukromí.

Argument, že v případě zavedení čipových karet bude pacient opět lokálně omezen pouze na místo, kde bude čtecí zařízení, je zavádějící: Jestliže by byl plošně zaveden systém rozmístění čteček čipových karet – například v čekárnách zdravotnických zařízení, v knihovnách, v blízkosti umístění bankomatů, tento problém odpadá. Stačí si připomenout například čtecí zařízení cen nabízených výrobků v obchodních domech. Lidé se je běžně naučili užívat, zrovna tak jako bankomaty. Při aplikaci čipové e-karty naopak mohou být občané velmi snadno zainteresováni.

E-karty mohou zaručit účinnou spolupráci zdravotnických zařízení, zvýšit dostupnost a kvalitu lékařské péče. Jejich aplikací lze zabránit zbytečným a opakovaným vyšetřením a tím nadměrnému zatěžování organismu pacientů. Obrovskou výhodou je sdílení informací o provedených vyšetřeních, což oceňují i praktičtí lékaři, kterým je průběh a výsledky vyšetření u specialistů pacienty často ne správně interpretován. Lékařům i lékárníkům bude urychlen přístup ke zdravotnickým informacím pacientů. Nezanedbatelná je také skutečnost, že díky rychlé a přesné informovanosti mohou být zachráněny životy mnoha pacientů při zásazích pracovníků první pomoci.

Výhodou e-karty je tedy schopnost dostat informace ve správnou dobu na správném místě. Každý z nás si jistě umí představit, že každá doplňující a rychle předaná informace může zachránit život. Elektronické nástroje mají i tu výhodu, že maximálně snižují nebezpečí zneužití osobních údajů. E-karty, v jakékoliv podobě, je možné chránit řadou bezpečnostních prvků.

Odpůrci e-karet zmiňují především starší generaci našich občanů. Vzpomeňme však užívání videokamer, situace zavádění prvních mobilů, nutnost zvládnout manipulace s různými typy bankovních či jiných čipových karet. Za zmínku stojí i účast seniorů na různých školeních práce na PC a užívání internetu. Svou pílí, snahou vyrovnat se „těm mladším" a především svým zájmem tuto problematiku mnozí velice dobře zvládají.

Svět kolem nás se mění, ale přesto existují hodnoty, které – i přes neustále se zrychlující tempo našeho života - zůstávají pro nás neměnné a určují kvalitu našeho života. Naše zdraví k těmto základním hodnotám patří. Dobré zdraví není ale pouze produkt péče dobře fungujícího a prosperujícího zdravotnického systému. Mnohé závisí na našich postojích a na našem způsobu života. Aktivní účast občanů v kvalitě jak vlastního života, tak zdraví bude znamenat mnohé – projeví se v zájmu preventivně pro své zdraví něco dělat – a stejně tak k aktivnímu postoji stimuluje i používání e-karty.

Situace dnes navozuje otázku: Bude v českém zdravotnictví zavedena nová zdravotní dokumentace? V jaké formě – papírové či elektronické? Obě varianty mají své zastánce i odpůrce...

K věci

Zdravotní pojištěnecká karta v zemích EU

Jak řeší otázku komplexní zdravotní dokumentace Evropská unie? EU apeluje na členské státy, aby postupně, podle možností, zaváděly elektronické čipové zdravotní karty. V současné době je v EU zaveden jednotný evropský pojištěnecký průkaz. Stávající plastová karta bude nahrazena elektronickou.

Projekt EU předpokládá, že v roce 2008 bude všech 350 milionů občanů EU používat elektronické čipové karty. Součástí projektu bude instalace asi 2 milionů čteček v nemocnicích, lékárnách a v prostorách lékařských ordinací na celém území EU. Zavedení projektu lze nazvat revolucí v systémech zdravotnictví v každé členské zemi, protože dojde k propojení jednotlivých součástí v národních zdravotnických zařízeních v každém z členských států. Technologii čipových karet lze využít tak, že jedna strana karty je nosičem identifikačních i zdravotních informací o občanovi a zadní strana je současně evropskou pojišťovací kartou. Přední strana může být ještě doplněna o jiné údaje – například číslo sociálního pojištění či možnost autentifikace prostřednictvím elektronického podpisu pro komunikaci se státní správou. Cílem projektu zdravotní péče s označením Netc@rds je výměna papírových formulářů a ověření možnosti poskytování zdravotní péče občanům na základě elektronicky čitelných karet. Například Rakousko nyní prochází obdobím testů pro zavádění tohoto typu zdravotnické karty. Plný provoz by měl být zahájen od roku 2006. V rámci zdravotní reformy také v některých spolkových zemích Německa probíhají zkušební testy aplikace e-karet s představou, že od příštího roku dojde k plošnému zavedení. Do projektu jsou zapojeny i další členské státy EU například Francie a Řecko. Za zmínku stojí, že právě hostitelská města Olympijských her pořádaných v Řecku v roce 2004, Atény a Soluň, sloužila jako testovací místa nového systému zdravotních karet, který by občanům EU umožnil využívat služby zdravotní péče kdekoliv na území Evropské unie.

Důležitou předností čipové e-karty a její nezbytnou součástí z pohledu ochrany osobních údajů je zabezpečení uložených dat prostřednictvím elektronického klíče. Nakládání s daty, která jsou na kartě uvedena (základní povinné údaje – jméno a příjmení, datum narození, zdravotní pojišťovna, životně důležitá data – krevní skupina, alergie, diabetes apod., vyšetření, předepsané léky, očkování, fotografie pojištěnce i doplňující nepovinné údaje jako jsou například rentgenové snímky, záznamy o prodělaných operacích a užívaných léčivech) je výhradně pod kontrolou pojištěnce a souhlas k přístupu k nim dává pouze on. Držitel karty díky komplexnosti zdravotních údajů zanesených v kartě získává kvalitativně větší přehled o svém zdravotním stavu i o nákladech, které na svou léčbu vynakládá. Elektronický klíč zabezpečuje přístup ke všem datům uloženým na kartě.

4. CO NOVÉHO V ZAHRANIČÍ

Prostředek k potírání automobilové kriminality, nebo oko „Velkého bratra"?

Ve městě New Haven, v americkém státě Connecticut, žije asi 125 tisíc obyvatel. Jeho populace, z níž většina jsou studenti, se neustále mění. Město se potýká s narůstající automobilovou kriminalitou. Ročně činí ztráta na automobilové dani asi 1 milion USD a jenom v loňském roce bylo ukradeno tisíc automobilů.

Správní rada města New Haven se rozhodla, že jako jedni z prvních v zemi, a to od konce podzimu roku 2004, začnou využívat infračervené snímací pistole schopné přečíst poznávací značky jedoucích či parkujících vozidel. Technologie, kterou snímače používají, umožňuje okamžitý přístup nejen k daňovým registrům a záznamům pojišťoven, ale i k policejním záznamům o vozidlech.

Zařízení stojí asi 25 tisíc USD, skládá se z „pistole" využívající infračervené záření, notebooku, doplňujících zařízení a ovládají je dva lidé, z nichž jeden řídí automobil a druhý snímačem zaměřuje vybrané objekty.

Prostřednictvím těchto zařízení budou moci městští úředníci okamžitě zjistit, zda je zaplacena automobilová daň a pojištění, zda není odcizena poznávací značka, nebo jestli auto není kradené. Policie i výběrčí daní prohlásili, že vozidlo, které tímto způsobem bude odhaleno, bude odtaženo a zadržováno do té doby, než si majitel vůz řádně zaregistruje a pojistí. Vedoucí představitel policie je přesvědčen, že tímto způsobem je možné postupně vypěstovat u občanů větší zodpovědnost za svá vozidla.

Systém je mnohem efektivnější než jiné doposud používané metody, jako jsou například rozesílání upomínek, návštěvy výběrčích daní v místě bydliště neplatičů, či kontroly automobilů a nasazování „botiček". Starosta prohlásil, že občanům, jejichž auto bylo infračerveným snímačem označeno a následně odtaženo, bude nabídnuta finanční pomoc na zaplacení poplatků za odtažení vozidla i daní.

Ochránci občanských práv a svobod protestují proti zavádění technologií připomínajících taktiky z románu G. Orwella „1984", kde vláda prostřednictvím „Velkého bratra" pod záminkou ochrany pořádku, bezpečí a jistot svých občanů je neustále sleduje. Cílem takového počínání bylo naprosté ovládnutí a zmanipulování společnosti.

Starosta města New Haven odmítá přijmout argument „orwellovského syndromu". Předkládá výsledky zkušebního testu tohoto snímacího zařízení z jara roku 2004. Během čtyř hodin bylo zjištěno 25 majitelů automobilů, kteří celkem dlužili 10 000 USD na daních a v průběhu dvou hodin zajistila policie 11 automobilů z odcizenými poznávacími značkami a dvě auta byla kradená. Pachatelé krádeží byli nalezeni a zadrženi.

Zavádění systému monitorování automobilů prostřednictvím výše uvedené technologie je prezentováno jako pomoc a výhoda pro občany. Bude to opravdu tak? Výkonná ředitelka Connecticut Civil Liberties Union prohlásila, že je silně znepokojena, a že její organizace bude situaci kontrolovat a pečlivě sledovat využívání tohoto systému v praxi.

Volně zpracováno podle článku v Associated Press

Rádiové bankovky

V internetovém vydání německého týdeníku Die Welt se nedávno objevila zpráva, že Evropská centrální banka údajně pracuje na tajném projektu „rádiových bankovek". Myšlenka je jednoduchá: Opatřit bankovky rádiovým čipem, který umožní sledovat jejich pohyb.

Oficiálním cílem projektu je vytvoření bankovek s vysokou ochranou proti padělání. Je ovšem zřejmé, že nový typ bankovek umožní především sledování jejich oběhu v platebním styku.

Již v roce 2003 představil japonský koncern Hitachi miniaturní rádiový čip, který lze snadno zapracovat do bankovky. Čip pracuje na principu radiofrekvenční identifikace (RFID). Dostane-li se do blízkosti čtecího zařízení, vyšle k němu signál vyjadřující určitou kombinaci čísel. Potřebnou energii dokáže čip načerpat z rádiových vln vysílaných čtečkou. Nepotřebuje tedy žádnou baterii. Zařízení dokáže fungovat zatím jen na vzdálenost asi jednoho metru.

Projekt rádiových bankovek nemohl nechat v klidu ochránce dat. Slyšet se už nechal například Peter Schaar, německý spolkový komisař pro ochranu dat, když vyjádřil určité obavy v souvislosti s „datovou stopou", kterou by takové peníze zanechávaly.

Celý projekt čeká ovšem ještě dlouhá cesta a také zavedení bankovek s čipem do praxe narazí především na ekonomické potíže. Prvním aspektem je výrobní cena takových platidel, dále je potřeba vzít v úvahu náklady na pořízení čtecích zařízení v bankách a prodejnách. Navíc by bylo potřeba upravit infrastrukturu pro přenos dat. Jsou tu však i problémy technického rázu: Mnohé, běžně rozšířené materiály odstiňují rádiové vlny (hliníkové fólie na obalech, ocelová kostra auta) a také dosah systému je krátký (max. 1 m, jak již bylo uvedeno).

Ať už osud tohoto projektu bude jakýkoli, zřetelně ukazuje možnosti rádiofrekvenční identifikace a přináší námět k úvahám a také obavám z hlediska ochrany soukromí

volně zpracováno podle týdeníku Die Welt, www.welt.de

Výměna řidičských průkazu v Austrálii

Ve státě Queensland v Austrálii zvažují výměnu stávajících plastových kartičkových řidičských průkazů za nové řidičské čipové karty. Nové řidičské průkazy bude obtížné napodobit, což sníží počet řidičů jezdících bez řidičského průkazu i počet krádeží identity.

Nový řidičský průkaz by také mohl obsahovat digitální oprávnění umožňující občanům přístup k vládním službám prostřednictvím internetu. Současně by uchovával životně důležité zdravotní údaje a spojení na důležitá kontaktní místa první pomoci. Podle vyjádření pana Gary Mahona, ředitele strategie řízení dopravy ve státě Queensland, bude vláda koncem tohoto roku o projektu jednat. V případě jeho schválení by se v roce 2006 nebo 2007 odstartovala výměna 2,5 milionů řidičských průkazů.

Volně zpracováno podle článkuv CTWeekly

Indická legislativa zřejmě zareaguje na obavy ochránců dat v EU

Ve snaze zmírnit obavy západních zaměstnavatelů, kteří využívají služeb nebo dodávek firem ze zahraničí („outsourcing services"), hodlá Indie ještě během tohoto roku zavést přísnější právní úpravu ochrany dat a soukromí. Podle slov prezidenta Národní asociace softwarových a servisních společností (NASSCOM) v Dillí, která úzce spolupracuje s vládou na nových nařízeních, by měla být nová opatření uzákoněna.

Indická vláda je nyní vystavena stále rostoucímu tlaku z „call center" po celé zemi, která disponují velkým objemem dat z USA a Evropy, kvůli správnému fungování „zadávání práce zahraničním externistům" („Business Process Outsourcing" /BPO/), aby přijala zákon o ochraně dat. Dillijský konzultant pro legislativu v otázkách informatiky říká, že pro Indii je nesmírně důležité zajistit zvláštní právní úpravu ochrany dat. Je nezbytné získat patřičnou důvěru investorů a zahraničních společností, aby si mohli být jisti, že data, která posílají do svých poboček v Indii, jsou adekvátně zabezpečena a fungují tam náležité zákonné mechanismy zabraňující úniku dat.

Spíše než samostatný zákon zabývající se bezpečností dat a ochranou soukromí zvažuje vláda dodatek k zákonu o informačních technologiích z roku 2000, jehož současné znění řeší pouze otázky neoprávněného přístupu a krádeže dat z počítače nebo sítě při výši pokuty max. 220 000 USD, ovšem neobsahuje žádná zvláštní ustanovení vztahující se k ochraně soukromí. Vláda hodlá zavést pokuty za porušení budoucích ustanovení až do výše 5,5 mil. – 11 mil. USD. Podle NASSCOMu by měl nový dodatek indickému zákonu o informačních technologiích zajistit splnění podmínek stanovených směrnicí na ochranu dat EU, jakož i zásadami ochrany soukromí daných americkou smlouvou o tzv. bezpečném přístavu (Safe Harbour) a umožnil by tak bezpečné předávání dat do Indie. Poté by chtěla Indie s EU vyjednat své uznání za zemi s odpovídající úrovní ochrany osobních údajů. Do té doby se však musejí zahraniční zákazníci spoléhat jen na řádné plnění povinností stanovených smlouvou – chránit a dále nešířit osobní údaje, což je ovšem záruka nedostačující.

Volně zpracováno podle Network World Fusion: www.nwfusion.com/news/2004/0421indialawm.html

Spam vážně ohrožuje obchodování po síti

Ne právě příznivé výsledky přinesl průzkum, který na objednávku mezinárodní organizace Business Software Alliance (BSA) uskutečnila firma Forrester Data. Studie pod názvem „Postoj spotřebitelů vůči spamu" byla prezentována začátkem prosince 2004 v Mnichově a ukazuje, že spam (nevyžádaná elektronická pošta) se může svým rozesílatelům vyplácet.

Řeč je o reprezentativním průzkumu šesti tisíc uživatelů internetu v šesti zemích světa (Brazílie, Německo, Francie, Velká Británie, USA a Kanada). Výsledky byly vyhodnoceny podle jednotlivých států. Ve všech zkoumaných zemích dostává podle této studie téměř 90 procent všech uživatelů internetu spamovou elektronickou poštu s nabídkami na různé zboží a služby. Asi 20 – 40 procent spamových nabídek (v závislosti na zemi) příjemci otevřou a prostudují. Nejvíce v tom vynikají Brazilci, u kterých tento ukazatel uvedené hodnoty překračuje. Alespoň jednou už tímto způsobem nakupovalo 32 – 48 procent uživatelů, rekord ve výši 66 procent drží opět Brazilci. Mezi nejčastěji prostřednictvím spamu nabízené komodity patří softwarové vybavení, oblečení, bižuterie a zájezdy. Nejvíce se nakupuje software.

Organizace BSA, která se věnuje podpoře bezpečného a legálního digitálního prostředí, vystupuje jménem předních světových výrobců softwaru. V souvislosti se zmíněnou studií prohlásilo její vedení, že spam ohrožuje normální obchodování on-line a přes rostoucí objem prodejů v předvánočním období roku 2004 hrozí internetu jako prodejnímu místu krize důvěry. Stále více spotřebitelů se obává o bezpečnost svých osobních údajů. Každý druhý z dotázaných během průzkumu vyjádřil domněnku, že jeho data jsou předávána dalším subjektům.

To ovšem může vést ke ztrátě dynamizujícího účinku, který internet na hospodářství má. BSA proto uživatele internetu varuje před nabídkami rozesílanými prostřednictvím spamu a na svých webových stránkách (www.bsa.org) poskytuje rady pro bezpečné nakupování on-line.

Volně zpracováno podle internetové verze časopisu Manager-magazin

Australské ceny „Velký bratr"

25. listopadu 2004 vyhlásila Australská agentura pro ochranu soukromí (APF) vítěze 2. ročníku australských cen „Velký bratr", které jsou důvěrně známé jako „Orwellové" (podle G. Orwella a jeho románu „1984", v němž se Velký bratr objevil vůbec poprvé). Soutěž probíhá nejen v Austrálii, ale i v mnoha jiných zemích světa, kde je stejně tak pořádána národními organizacemi spolupracujícími s mezinárodní Privacy International. Od roku 1998 se takto uskutečnilo v 16 zemích již více než 50 soutěží (např. ve Velké Británii, Spojených státech, Rakousku, Německu, Švýcarsku, Nizozemí, Maďarsku, Dánsku, Španělsku, Finsku, Belgii nebo Francii), které ale rozhodně nemají nic společného s televizní show stejného jména vysílanou nedávno v některých zemích.

Vítězi této soutěže se mohou stát veřejní činitelé, společnosti nebo vládní orgány, kteří/které jsou považováni/y za největší vetřelce do soukromí, projevili/y nebývalou neúctu k soukromí druhých, nebo kteří/které se zasloužili/y nejvíce o ohrožení soukromí svých spoluobčanů. „Velký bratr" ale zahrnuje také 2 kategorie – pro jednotlivce a organizace, kteří/které naopak zásadně přispěli/y k ochraně soukromí ve své zemi a svou příkladnou prací posílili/y toto nezpochybnitelné lidské právo. Ceny pro tyto „kladné" kategorie byly pojmenovány také podle Orwellova hrdiny Winstona Smithe „Smithové". Stejně tak jejich název připomíná Ewarta Smithe, který v Austrálii zrušil systém identifikačních průkazů a evokuje také určitou anonymitu poskytovanou jménem Smith, což je jedno z nejběžnějších anglických příjmení.

Nominace na „Orwelly" i „Smithe" jsou získávány od veřejnosti buďto prostřednictvím webových stránek APF nebo e-mailu. Poté nominace posoudí porota (složená např. z komisařů pro ochranu soukromí, akademiků, právníků, novinářů, atd.), která vybere vítěze pro každou kategorii a sečtením hlasů pro nejčastěji nominovaného určí i vítěze v kategorii „Volba veřejnosti".

V roce 2004 získal australskou cenu v nelichotivé kategorii „Celoživotní hrozba" ministr pro silniční komunikace Nového Jižního Walesu Carl Scully; za „Největšího vetřelce mezi korporacemi" by-

ly označeny vedoucí politické strany; „Nejhorším veřejným činitelem nebo institucí" porota vyhlásila generálního prokurátora v Novém Jižním Walesu Boba Debuse; za „Nejinvazivnější technologii" pro rok 2004 jsou považovány biometrické pasy a v kategorii „Volba veřejnosti" občané svými hlasy zvolili společnost vydávající řidičské průkazy ve formě čipových karet Queensland Smartcard. Naopak v kategorii „Nejlepší strážce soukromí" byl oceněn za svou činnost v roce 2004 Hlavní pověřenec pro ochranu dat při australské poště John Pane.

Plnou informaci o „Australian Big Brother Awards" v angličtině lze najít na adrese www.privacy.org.au/bba/index.html.

5. KDYŽ SE ŘEKNE SKO Europolu

Rozhovor s PhDr. Miroslavou Matoušovou – členkou Společného kontrolního orgánu EUROPOLU

„Europol je organizace, která je založena proto, aby členským státům EU pomáhala předcházet závažné mezinárodní trestné činnosti a potírat ji, ovšem pouze tehdy, pokud jsou do této trestné činnosti zapojeny organizované zločinecké struktury a pokud se dotýká alespoň dvou členských států. Na praktické úrovni je hlavním úkolem Europolu usnadnit výměnu informací mezi členskými státy a zajistit odbornou analytickou práci.

Vzhledem k tomu, že Europol pracuje s velkým množstvím citlivých informací týkajících se jednotlivců, obsahuje Úmluva o Europolu řadu ustanovení požadujících od Europolu, aby při používání těchto informací bral ohled na práva jednotlivců.

Úmluva rovněž stanoví vznik společného kontrolního orgánu – nezávislého útvaru, který je pověřen zaručit to, že Europol dodržuje zásady týkající se ochrany údajů."

Takto je definován Europol v úvodu k právě vydané druhé Zprávě o činnosti Společného kontrolního orgánu Europolu. Členkou uvedeného orgánu, zastupující v něm od roku 2004 Českou republiku, je inspektorka Úřadu pro ochranu osobních údajů PhDr. Miroslava Matoušová. V prosinci 2004 byla fórem Společného kontrolního orgánu Europolu (SKO) zvolena jeho místopředsedkyní. V březnu letošního roku se dr. Matoušová účastnila kontroly v sídle Europolu v Haagu. Při této příležitosti jsme se ptali na práci, působnost a organizační uspořádání SKO.

Paní doktorko, zřejmě není náhodné, že jste se členkou společného kontrolního orgánu Europolu za Českou republiku stala právě vy? Od prosince jste místopředsedkyní SKO. Jak probíhá volba jeho řídících funkcionářů?

Mne jmenoval do kontrolního orgánu Europolu předseda Úřadu pro ochranu osobních údajů především proto, že jsem inspektorkou Úřadu, která v České republice provádí kontrolu nakládání s osobními údaji v policii. Řídící funkcionáři jsou voleni fórem SKO na základě návrhů, které se shromáždí. Existuje tu však také jistý princip – je jakousi zásadou, že místopředseda se po uplynutí tříletého předsednického mandátu stává předsedou SKO.

Mohla byste konkretizovat základní úkoly Společného kontrolního orgánu Europolu?

Tento orgán existuje od roku 1996, kdy nabyla účinnosti Úmluva o Europolu a není bez zajímavosti, že to byl vůbec první dozorový orgán v Evropské unii. Členství v něm je závislé na přistoupení jednotlivých členských států Evropské unie k Úmluvě o Europolu. Svého člena a jednoho jeho alternáta – náhradníka vysílá každý národní dozorový orgán pro ochranu osobních údajů.

V činnosti SKO Europolu je možné vymezit tři hlavní oblasti:

– Především je to posuzování Europolem vydávaných dokumentů, posuzování nově zřizovaných nebo využívaných databází osobních údajů apod. Tedy v podstatě expertní a konzultační činnost.

– Za druhé je to dohled nad způsobem vyřizování stížností jednotlivých občanů na nakládání s jejich osobními údaji Europolem, případně nad korektností vyřízení jejich žádostí o informace, zda Europol o nich zpracovává osobní údaje. Občan tedy dostává od SKO vyjádření, zda nedošlo k porušení zákonných norem upravujících ochranu osobních údajů.

– Za třetí pak je to konkrétní kontrolní činnost, kterou SKO provádí v centrále sídla Europolu, v Haagu a zpracování veřejně přístupné – i tiskem vydávané zprávy, z níž citujete v úvodu k našemu rozhovoru

Zpráva Společného kontrolního orgánu, kterou český Úřad vaším prostřednictvím obdržel, je právě shrnujícím výsledkem kontrol prováděných v Europolu?

Vlastně ano, je výstupem z činnosti SKO. Problémem ovšem je, že ne vše, co se na SKO projednává, může být zveřejňováno. Tendence je, aby již zápisy z jednání a z kontrol byly zpracovávány tak, aby mohly být zpřístupněny i veřejnosti. V jednání SKO, v jeho dozorové složce práce kupříkladu existuje odvolací výbor, který projednává stížnosti a žádosti občanů. Zde se řeší důvěrné otázky. Výstupy z jednání tohoto výboru nejsou veřejné. Závěry se předávají základnímu dozorovému orgánu, který vezme na vědomí, zda na stížnost bylo, či nebylo odpovězeno a jakým způsobem. Tento postup se poté promítá i do zprávy SKO.

Je zpráva SKO pro Europol závazná?

Svým způsobem. Záleží na tom, jaký postoj zaujmou řídící orgány Europolu. Je to tak, že některé skutečnosti jsou pevně zakotveny v Úmluvě o Europolu a tak je vymezena i kompetence SKO, kterou právě Úmluva ukládá Europolu zřídit, a dokonce financovat jeho činnost. SKO se vyjadřuje k problémům, které shledá, a o jejich řešení se někdy musejí vést opravdu diplomatická jednání, aby mohlo být dosaženo konsensuálních rozhodnutí – a slovo konsensuálních bych ráda zdůraznila. Je třeba si uvědomit, že na rozdíl od rozhodovacích oprávnění, která pro nás plynou z kontrolní činnosti, jak nám ukládá zákon o ochraně osobních údajů, SKO dává doporučení. A vždy je snaha jednat tak, aby bylo konsensu dosaženo.

Mohla byste přiblížit, jak probíhá taková kontrola Europolu, které jste se v březnu zúčastnila?

Kontrolní komisi tvořilo šest členů. Polovina z nich se zabývala prvořadě právními aspekty, v této sestavě jsem byla i já, a druhá část se více zaměřila na kontrolu informačních technologií a posuzování informačních systémů. Náš šestičlenný tým ještě doplnil generální tajemník SKO, zaměstnanec placený Radou EU, a jeho zástupce. Celkově tedy na kontrole pracovalo osm expertů a byli jsme rozděleni do čtyř „minitýmů." Dvojice pracovaly intenzivně po tři dny a čtvrtý den se zpracovávala zpráva. Chtěla bych zdůraznit, že závěr kontroly musel každý člen komise předložit sám za sebe, tj. na místě v anglickém jazyce vypracovat zprávu. Bez toho nelze kontrolované prostory opustit. Je stanovena jistá struktura sestavování zprávy (svým způsobem má dotazníkovou formu), kterou představuje zjištění, posouzení souladu s ustanoveními Úmluvy o Europolu a nakonec doporučení. Zpráva se poté projednává na plénu SKO. V případě vyslovení souhlasu je zpráva předána Europolu, který se ke zprávě vyjadřuje a připomínkuje ji.

Občany jistě zajímá, jakým způsobem mohou podávat stížnosti a jak vyřizování stížnosti probíhá?

V podstatě to není složité. V Úmluvě o Europolu, v článcích 19 a 24 je zakotveno, že každý občan má právo se obrátit na Europol a žádat, aby mu podal informaci, zda o něm Europol zpracovává osobní údaje. Znamená to, že každý občan má právo přístupu k informacím. Europol provede šetření a žadateli odpoví. V případě, že žadatel není spokojen s tím, jak mu Europol odpověděl, může se obrátit se stížností na SKO. Ten zahájí proceduru, která spočívá v přešetření. Zpravodajem k tomu úkolu je vždy zástupce toho členského státu, odkud stížnost pochází. Europol nikdy nic nezjišťuje bez účasti jakéhokoliv členského státu. Například jestliže si stěžuje občan Španělska na počínání francouzské policie, pak zahajuje – je zpravodajem o konání zástupce francouzského dozorového orgánu. A jednou možná přijde chvíle, kdy i český občan si bude stěžovat. V tom okamžiku ten, kdo bude členem SKO za ČR, se stane zpravodajem k této stížnosti.

Děkujeme za rozhovor.

Poznámka: Více informací o Europolu lze nalézt v Bulletinu Úřadu, číslo 1/2004, v rubrice Když se řekne...

6. OSOBNÍ ÚDAJE V ŠIRŠÍCH SOUVISLOSTECH

Národní den informační bezpečnosti ve Finsku

„Národní den informační bezpečnosti" je základním projektem finského vládního Výboru pro informační bezpečnost. Mezi další významné projekty Výboru patří také **„Program informační bezpečnosti"**, **„Zločinnost v informačních sítích jako problém zabezpečení informací"** a **„Povědomí o stavu vnitrostátních rizik v oblasti informační bezpečnosti"**.

První **Národní den informační bezpečnosti** se konal ve Finsku 11. února 2004 s cílem zajistit, aby byly na všech počítačích připojených k internetu nastaveny aktualizované operační systémy, antivirové softwary a firewally.

Titulní stránky největších deníků přinesly reklamu, která čtenáře přiměla k zamyšlení nad závažností ohrožení bezpečnosti informací. Na stejném obrazovém materiálu byla založena také reklama, kterou týden vysílala největší finská komerční televize a dá se říci, že **Národním dnem informační bezpečnosti** se poměrně rozsáhle zabývala veškerá média ve Finsku. V tento den také přes milion finských domácností obdrželo poštou leták nazvaný „Domácí průvodce informační bezpečností", který jasně popisoval bezpečné používání počítače a internetu.

Výsledky této kampaně byly potěšující, protože po tomto dni výrazně vzrostl počet domácích počítačů, na kterých měli jejich majitelé nainstalovaný jak antivirový program, tak zároveň firewall.

V pořadí druhý **Národní den informační bezpečnosti** se konal 8. února 2005 a byl zaměřen především na školní mládež, učitele a rodiče. Účelem bylo zajistit bezpečné používání internetu ve školách a také to, aby se poznatky o bezpečnosti informací dostaly i rodičům školou povinných dětí.

V rámci příprav na **Národní den informační bezpečnosti** byl v listopadu zahájen provoz internetové služby, která má pomoci učitelům ve výuce informační bezpečnosti. Tato služba ovšem nepodává informace pouze vyučujícím, ale obsahuje i sekci pro studenty různých věkových kategorií.

V **Národní den informační bezpečnosti** by ve školách měla být zdůrazňována především tato témata:

■ **Chraň svůj počítač** – každý počítač připojený na internet musí mít dostatečně aktualizovaný operační systém, antivirový program i firewall. Uživatelé by měli věnovat pozornost tomu, jaké materiály si ze sítě stahují do svého počítače a neměli by zapomínat na pravidelné zálohování pro ně důležitých dokumentů.

■ **Zabezpeč sám sebe** – ochranu osobních údajů v internetovém prostředí nelze považovat za samozřejmost; je dobré uvažovat o tom, komu poskytujeme naše osobní údaje nebo s kým komunikujeme, protože ne každý udává na internetu pravdivé informace.

■ **Dodržuj pravidla** – na internetu platí tytéž zákony jako v každodenním životě a stejně tak i pravidla slušného chování; zločin zůstává zločinem i v informační síti.

volně zpracováno podle informace na www.ficom.fi/en/issue_a.html?Id=1076333093.html

7. Dobrá rada na závěr

Není nad dobré heslo

Pro skutečně účinnou bezpečnost vašeho počítače je, kromě jiného, nezbytné vymyslet to správné heslo. Ale jaké? Každý uživatel osobního počítače dnes ví, že takové heslo je věcí velmi osobní. A že rozhodně není dobrý nápad poznamenávat si je na štítek, který si pak nalepíme na monitor počítače.

Jenomže potíž je v tom, že v dnešní době jsme často nuceni pamatovat si desítky všelijakých uživatelských jmen a přístupových hesel. A to zase vede k tomu, že většina z nás podlehne pokušení vytvořit si takové heslo, které je nejsnadnější k zapamatování. Právě takové počínání však bohužel mívá velmi neblahé důsledky. Protože nejrůznější „prolamovací" programy, které dnes mají hackeři běžně k dispozici, jsou schopny taková hesla hravě identifikovat během několika vteřin.

úřad
pro ochranu
osobních
údajů

Aby nějaké heslo splňovalo alespoň minimum nároků na bezpečnost systému, nemělo by se například vyskytovat v žádném ze slovníků vašeho mateřského jazyka. Takové heslo by totiž hackerský software objevil velmi rychle.

Takže dobré heslo by mělo mít minimální délku osmi znaků, kromě malých písmen by mělo obsahovat i několik velkých, a vůbec nebude na škodu, zahrneme-li do něj kromě písmen i některé speciální znaky.

Pravda, to vše klade poněkud větší nároky na naši paměť i na náš čas. Můžeme si to však alespoň trochu zjednodušit: Odborníci doporučují využívat například různých mnemotechnických vět, v nichž vždy první písmeno každého slova bude (v odpovídajícím pořadí) jedním z písmen, která tvoří naše heslo. Sami jistě přijdete na řadu dalších podobných pomůcek.

Chcete-li některým příliš zvědavým jedincům z vašeho okolí zabránit průniku do vašeho systému, je dobré mít na paměti i několik dalších zásad:

Nepoužívejte jako hesla jména svých blízkých nebo domácích mazlíčků (ani jejich zdrobněliny). Vyvarujte se též jejich dat narození či svátků (ani ve zpřeházeném pořadí). Velmi mnoho matek a otců je v pokušení použít jako přístupové heslo například datum narození dcerky apod. Vězte, že každý hacker, který chce neoprávněně vniknout do vašeho systému, zkusí prověřit podobné triky jako první v pořadí. Když se totiž hacker snaží dostat pod kůži vašemu PC, často už je vybaven nemalou řádkou dat z vašeho osobního života.

Lk

VYDÁVÁ ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
EDITOR: PHDR. HANA ŠTĚPÁNKOVÁ
REDAKTOR: MILENA NEJEDLÁ, BOHUMÍR LUKAJ
GRAFICKÁ ÚPRAVA: MILOSLAV ŽÁČEK
ADRESA REDAKCE: ÚOOÚ, PPLK. SOCHORA 27, PRAHA 7, 170 00
TELEFON: 234 665 286, FAX: 234 665 505
E – MAIL: INFO@UOOU.CZ
INTERNETOVÁ ADRESA: WWW.UOOU.CZ

PERIODIKUM JE ZAPSÁNO V EVIDENCI PERIODICKÉHO TISKU POD ČÍSLEM MK ČR E 10548

DÁNO DO TISKU 11. 5. 2005