úřad
pro ochranu
osobních
údajů

informační bulletin
3–4/ 2005

## Přeji si dialog s veřejností

*Za dobu svého působení ve funkci předsedy Úřadu jsem získal jasnou představu o tom, že prosazování principů ochrany osobních údajů do povědomí veřejnosti potřebuje soustavné působení a je někdy bolestné: Při porušení zákona se totiž nelze vyhnout ani uplatňování finančních sankcí a nápravných opatření. Bolestné ovšem může být i pro občany – subjekty údajů, pokud si z neznalosti či ignorance vůči svým právům sami své soukromí nestřeží a svá osobní data či souhlas s jejich využíváním poskytují bez uvážení. Domnívám se, že je to především proto, že si občané možné dopady zneužití svých osobních údajů neumějí představit.*

*Zásah Úřadu, pokud je v takovém případě vůbec možný, nemusí být vždy dostatečnou „náplastí" na způsobené morální či materiální škody.*

*Potvrzuje se tak mé přesvědčení, že je vysoce aktuální, aby se k problematice ochrany osobních údajů široce otevřela veřejná a rovněž odborná debata.*

*Hned po svém zvolení předsedou Úřadu jsem prohlásil, že budu usilovat o nastavení pravidel ochrany soukromí rovněž v diskusi s veřejností odbornou i laickou i s organizacemi, které se ochraně soukromí věnují. Potvrdil jsem to i na své první tiskové konferenci v Úřadu.*

*Uvítal jsem tedy možnost poskytnout požadované poznatky Úřadu společnosti Iuridicum remedium, pořadateli udílení Ceny Velkého bratra pro ty, kdo narušují soukromí občanů.*

*Potěšilo mne, že zásady pro používání kamerových systémů, které Úřad na přelomu roku předložil k veřejnému připomínkovému řízení, našly odezvu. Výsledkem je nepochybné zkvalitnění poznatků Úřadu o rozsahu používání kamerových systémů, prohloubení aplikace zákona o ochraně osobních údajů, byť se tak děje za cenu značného rozšíření agendy Úřadu v oblasti registrační i konzultační. Vidím v tom ale také prohloubení služby, kterou Úřad pro ochranu osobních údajů občanům poskytuje.*

*V počátku roku se proto také musíme zhostit povinnosti prokázat, že Úřad je schopen efektivně chránit osobní údaje i po přistoupení České republiky do schengenského prostoru v roce 2007. O výsledcích hodnotící mise EU, která tuto připravenost u nás v březnu prověřovala, přineseme informace prostřednictvím našich komunikačních prostředků.*

*Patří k nim i tento Informační bulletin, čtvrtletník určený široké veřejnosti, vydávaný se záměrem šíření poznatků o práci Úřadu i o ochraně soukromí a jejích úskalích v našem domácím prostředí i ve světě. Uvítal bych odezvu Vás, čtenářů bulletinu i návštěvníků webových stránek Úřadu nebo odběratelů jeho Věstníku. Dostatek podnětů můžete najít i ve výroční zprávě za rok 2005, zveřejněné na našich webových stránkách (www.uoou.cz).*

*Pokud nám napíšete o svých zkušenostech, případně trápeních s ochranou osobních údajů, váš dopis určitě neskončí v koši: Odpovíme Vám ať už individuálně, nebo v případě podnětu k zaujetí obecněji platného postoje v dalším čísle bulletinu či na našich webových stránkách.*

*Igor Němec*
*předseda Úřadu pro ochranu osobních údajů*

## 1. TADY A TEĎ

Vzhledem k tomu, že se již 1. ledna 2007 Česká republika spolu se Slovenskem, Polskem a Maďarskem, Litvou, Lotyšskem, Estonskem, Slovinskem, Maltou a Kyprem připojí k Schengenské dohodě, musí dojít také k zesílení spolupráce policejních sil a dalších orgánů odpovědných za bezpečnost v dalších schengenských státech (jsou jimi: Německo, Francie, Itálie, Belgie, Rakousko, Dánsko, Finsko, Řecko, Lucembursko, Nizozemí, Portugalsko, Španělsko, Švédsko, Island a Norsko). Vstup státu do schengenského prostoru znamená svobodu pohybu jeho občanů po teritoriu ostatních států, které uvedenou dohodu přijaly. Znamená to ovšem, mimo jiné, že osobní údaje obyvatel každého z těchto států mohou být dostupné podstatně širšímu okruhu orgánů než dosud. Zabezpečit, aby tak nemohlo docházet k porušení práva občanů na ochranu soukromí, znamená přijetí mnoha opatření a procedurálních postupů i pro instituce, kterým je uložena povinnost chránit osobní údaje, jež jsou velmi snadnou cestou k soukromí jednotlivého občana.

V posledních měsících roku 2005 se tedy pozornost Úřadu soustředila na přípravu k jarní evaluační misi, která vyhodnotí úroveň schengenské praxe jak policie, tak ochránců dat v ČR.

Schengenský informační systém (tzv. SIS II) je největší mezinárodní databází s osobními údaji v Evropě. Na centrální databázi jsou navázány národní informační systémy se sítí úřadoven a s národními databázemi s osobními údaji. Pro Úřad to znamená náročnou přípravu v oblasti legislativní, informatické i z hlediska praktického provádění inspekcí v tuzemsku i v zahraničí. Již delší dobu se zástupci Úřadu v roli pozorovatelů zúčastňují zasedání společného kontrolního orgánu v Bruselu. Inspektor Úřadu Ing. Zapletal se jako zástupce českého Úřadu účastnil také práce týmu prověřujícího situaci „v terénu" Islandu a Dánska, kde své zkušenosti prezentovali zástupci ostatních severských členů Schengenské úmluvy.

Zahraniční experti, kteří budou hodnotit připravenost ČR chránit osobní údaje svých občanů po 1. 1. 2007, pracovali na Úřadu od 7. do 9. března 2006. O výsledcích hodnocení přineseme informaci v příštím čísle informačního bulletinu.

Přelom roku v práci Úřadu přinesl i jistou novinku: Vzhledem k tomu, že v České republice neexistuje zvláštní právní úprava, která by regulovala využívání kamerových sledovacích systémů, Úřad se v rámci svých kompetencí ujal úkolu nastavit pravidla zaručující ochranu soukromí osob, která by vyvažovala účinné využívání technických prostředků k zajištění bezpečnosti občanů a ochrany majetku. Tato pravidla předložil k připomínkám veřejnosti na svých webových stránkách 17.12. 2005 – 15. 1. 2006. Vypořádal připomínky a poté publikoval zásady pro využívání kamerových sledovacích systémů z hlediska ochrany osobních údajů.

Důraz, který je položen na potřebu registrace správců osobních údajů vyvolal velké množství dotazů provozovatelů kamerových systémů. Proto Úřad vypracoval vysvětlující materiály a návod pro vyplnění registračních formulářů pro uživatele kamerových systémů. Uvedené materiály jsou dostupné na webových stránkách Úřadu http://www.uoou.cz/ .

Z mediálně velmi sledovaných kauz Úřad řešil na přelomu roku kauzu stížnosti účastníka Czech-Teku na zpracování osobních údajů Policií ČR v rámci jejího zásahu na technoparty. Rozhodnutí Úřadu o udělení pokuty nabylo právní moci 10. ledna 2006 a uložená pokuta 15 000 Kč byla Ministerstvem vnitra řádně uhrazena.

## Pravomocně rozhodnuté případy ve správním trestání v době od 11. června 2005 do 31. prosince 2005

| Deliktní jednání | Sankční opatření | Nápravná opatření |
|---|---|---|
| zveřejnění osobních údajů tzv. „sociálních nájemníků", tj. konkrétních nájemníků bytů, kteří dle názoru účastníka řízení nepotřebují ochranu tzv. regulovaného nájemného z bytů, prostřednictvím internetové domény (...), za účelem upozornit na problematiku tzv. regulovaného nájemného z bytů. Tyto osobní údaje neodpovídaly stanovenému účelu ani nebyly v rozsahu nezbytném pro naplnění stanoveného účelu. Uvedené osobní údaje, které byly zpracovávány k rozdílným účelům, účastník řízení sdružil a ukládal a prostřednictvím volně přístupné internetové domény je zveřejnil, aniž by informoval subjekty údajů 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 či komu jsou určeny, a aniž by před započetím zpracování osobních údajů oznámil tuto skutečnost Úřadu pro ochranu osobních údajů,<br>§ 5 odst. 1 písm. d) a h), § 11 odst. 1 a § 16 odst. 1 | pokuta 550.000 Kč | ano |
| instalace a provozování monitorovacího systému v objektu bytového domu, v souvislosti s výkonem práv a povinností při správě bytového družstva, spočívající v instalaci kamerového systému propojeného s elektronickými zámky, jehož prostřednictvím byly zpracovávány osobní údaje nájemníků bytů v tomto domě, a to bez jejich souhlasu,<br>§ 5 odst. 2 | pokuta 180.000 Kč | ano |
| shromažďování a následné uchovávání kopií občanských průkazů, oddacích listů a jiných dokumentů obsahujících osobní údaje majitelů chovatelských stanic a jejich rodinných příslušníků, tj. zpracování osobních údajů v rozsahu, který není nezbytný pro výkon činnosti v oblasti kynologie, a dále zpracovávání rodných čísel těchto osob,<br>§ 5 odst. 1 písm. d), § 13c odst. 1 zákona č. 133/2000 Sb. | pokuta 30.000 Kč | ano |
| zpřístupnění osobních údajů člena bytového družstva jiným osobám prostřednictvím umístění listiny o vyloučení z družstva, obsahující osobní údaje vylučovaného člena v rozsahu jméno, příjmení, rodné číslo, adresa trvalého bydliště a informace vztahující se k vyloučení z družstva, v informační skříňce domu,<br>§ 5 odst. 1 písm. f), § 13c odst. 1 zákona č. 133/2000 Sb. | pokuta 12.000 Kč | ne |
| zasílání obchodních sdělení obsahujících nabídku na zařazení adresáta do databáze podnikatelských subjektů a institucí umístěné na internetové adrese (...), a to bez prokazatelného předchozího souhlasu adresátů se zasíláním obchodního sdělení,<br>§ 7 odst. 2 zákona č. 480/2004 Sb. | pokuta 160.000 Kč | ne |
| nepřijetí takových opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům obsažených v lékařských protokolech z let 1963 až 1966 umístěných v areálu bývalé léčebny – sanatoria, v důsledku čehož došlo k jejich zpřístupnění neoprávněné osobě,<br>§ 13 odst. 1 | pokuta 10.000 Kč | ne |

úřad pro ochranu osobních údajů

| Deliktní jednání | Sankční opatření | Nápravná opatření |
|---|---|---|
| zpracování osobních údajů neodpovídajících stanovenému účelu a v rozsahu nikoliv nezbytném pro naplnění stanoveného účelu u osob, které nesplňovaly požadavky na přípustnost daktyloskopování, uchovávání osobních údajů o otiscích prstů osob neomezeně dlouhou dobu, nikoliv nezbytnou k účelu jejich zpracování, a zpracování osobních údajů o otiscích prstů osob v rozporu s účelem, k němuž byly shromážděny, v souvislosti se snímáním (pořizováním) biometrických šablon nebo obrazů otisků prstů, § 5 odst. 1 písm. d), e) a f) | pokuta 100.000 Kč | ano |
| rutinní používání systému organizačních a technických bezpečnostních opatření, který neodpovídal používaným způsobům a prostředkům zpracování osobních údajů a účinně nebránil zpracování osobních údajů evidence obyvatel spočívajícím v jejich vyhledání pro jiné účely, než připouští některý ze zvláštních právních předpisů, a přijetí a provedení technicko-organizačních opatření k zajištění ochrany osobních údajů evidence obyvatel, která nebyla v úplnosti dokumentována, v souvislosti se zpracováním osobních údajů v informačním systému evidence obyvatel podle zákona č. 133/2000 Sb., o evidenci obyvatel a rodných číslech a o změně některých zákonů (zákon o evidenci obyvatel), § 13 odst. 1 a 2 | pokuta 30.000 Kč | ano |
| zpracování rodných čísel cestujících za účelem vystavení čipové karty a prodeje jízdních dokladů jejím prostřednictvím, které nebylo pro stanovený účel vzhledem k současnému zpracování data narození nezbytné, a uchovávání osobních údajů cestujících shromážděných při vystavení a užívání čipových karet, jejichž platnost již vypršela, § 5 odst. 1 písm. d) a e) | pokuta 15.000 Kč | ano |
| využití elektronických prostředků k šíření nevyžádaného obchodního sdělení, jehož obsahem byla nabídka leteckých zájezdů na Sardínii, a to bez prokazatelného souhlasu adresáta, § 7 odst. 2 zákona č. 480/2004 Sb. | pokuta 5.000 Kč | ne |
| využití elektronických prostředků k šíření nevyžádaného obchodního sdělení, jehož obsahem byla nabídka dodávky organického hnojiva, a to bez prokazatelného souhlasu adresáta, § 7 odst. 2 zákona č. 480/2004 Sb. | pokuta 10.000 Kč | ne |
| shromažďování osobních údajů zákazníků, aniž by zákazníci byli řádně informováni o možných příjemcích osobních údajů, o jejich právech podle § 21 zákona č. 101/2000 Sb. a o tom, zda je poskytnutí osobních údajů povinné či dobrovolné, § 11 odst. 1 a 2 | pokuta 40.000 Kč | ano |
| zveřejnění dopisu, vyvěšením na nástěnce sborovny základní školy, adresovaného a určeného nestátnímu zdravotnickému zařízení obsahujícího osobní údaje 24 zaměstnanců, kteří měli absolvovat preventivní periodické lékařské prohlídky v uvedeném zdravotnickém zařízení, včetně jejich rodného čísla § 5 odst. 1 písm. f) | pokuta 20.000 Kč | ne |
| zpracování osobních údajů klientů, kteří vyjádřili nesouhlas se zpracováním svých osobních údajů za účelem nabízení obchodu nebo služeb ve smyslu § 5 odst. 5 zákona č. 101/2000 Sb., v rozsahu nadbytečném z hlediska účelu stanoveného v § 5 odst. 9 zákona č. 101/2000 Sb. § 5 odst. 1 písm. d) | pokuta 20.000 Kč | ano |

úřad pro ochranu osobních údajů

| Deliktní jednání | Sankční opatření | Nápravná opatření |
|---|---|---|
| zpracování osobních údajů uchazečů o studium na vysoké škole prostřednictvím tiskopisu formuláře Přihláška ke studiu na vysoké škole pro akademický rok 2004/2005 a elektronické podoby přihlášky, včetně osobních údajů v rozsahu z hlediska daného účelu nadbytečném, § 5 odst. 1 písm. d) | pokuta 40.000 Kč | ano |
| využití elektronických prostředků k šíření nevyžádaných obchodních sdělení, jejichž obsahem byla nabídka zájezdu do Benátek a nabídka zájezdu na vystoupení Holiday on Ice do Ostravy, a to bez prokazatelného souhlasu adresátů, § 7 odst. 2 zákona č. 480/2004 Sb. | pokuta 20.000 Kč | ne |
| zaslání listiny obsahující seznam postoupených pohledávek úpadce, která obsahovala také osobní údaje dlužníků, fyzických osob, v rozsahu jméno, příjmení, rodné číslo a adresa bydliště, jednotlivým dlužníkům, tedy neoprávněné zpřístupnění předmětných osobních údajů, § 13 odst. 1 | pokuta 28.000 Kč | ne |
| zpracování osobních údajů uchazečů o studium na vysokých školách a studentů vysokých škol v souvislosti s prováděním statistických zjištění, aniž by (...) byl tímto zpracováním pověřen zvláštním zákonem a aniž by disponoval souhlasem dotčených studentů se zpracováním jejich osobních údajů, § 5 odst. 2 | pokuta 20.000 Kč | ano |
| zaslání dopisu, který obsahoval také osobní údaje bývalého zaměstnance v rozsahu jméno, příjmení, adresa trvalého pobytu a rodné číslo, a to bez jeho souhlasu, § 13c odst. 1 zákona č. 133/2000 Sb. | pokuta 2.000 Kč | ne |
| neinformování klientů v souvislosti se zpracováním jejich osobních údajů za účelem zasílání propagačních materiálů prostřednictvím dalších společností o možných příjemcích osobních údajů a o jejich právech podle § 21 zákona č. 101/2000 Sb. a o tom, zda je poskytnutí rodného čísla povinné či dobrovolné, a dále zasílání osobních údajů klientů elektronickou poštou bez jakéhokoliv zabezpečení a jejich předávání další společnosti, aniž měl s touto společností uzavřenu smlouvu o zpracování osobních údajů dle § 6 zákona č. 101/2000 Sb., § 11 odst. 1 a 2, § 13 odst. 1 | pokuta 20.000 Kč | ano |
| zveřejnění protokolu o konání veřejné dobrovolné dražby, v souvislosti s prováděním veřejné dražby podle zákona č. 26/2000 Sb., o veřejných dražbách, obsahujícího také osobní údaje navrhovatele v rozsahu jméno, příjmení a adresa trvalého pobytu, vydražitele v rozsahu jméno, příjmení, adresa trvalého pobytu a rodné číslo a rodné číslo licitátora, prostřednictvím internetové domény (...), v rozporu s § 27 odst. 7 zákona č. 26/2000 Sb., § 5 odst. 1 písm. f) | pokuta 20.000 Kč | ano |
| zpracování osobních údajů syna ručitelky, v rozsahu jméno a rok narození, v rozporu se stanoveným účelem v souvislosti s vyřizováním žádosti o poskytnutí spotřebního úvěru zajištěného ručitelem a dále neinformování ručitelky o tom, že poskytnutí rodného čísla je pro daný účel zpracování osobních údajů dobrovolné, a tedy zpracování jejího rodného čísla bez potřebného souhlasu, § 5 odst. 1 písm. d), § 11 odst. 2 zákona č. 101/2000 Sb., § 13c odst. 1 písm. c) zákona č. 133/2000 Sb. | pokuta 25.000 Kč | ano |

| Deliktní jednání | Sankční opatření | Nápravná opatření |
|---|---|---|
| zaslání výpisu aktuálního stavu účtu penzijního připojištění s osobními údaji jiné osoby shodného jména a příjmení a dále zaslání potvrzení o zrušení účtu rovněž s osobními údaji jiné účastnice penzijního připojištění, § 5 odst. 1 písm. c), § 13 odst. 1 | pokuta 10.000 Kč | ano |
| zaslání zálohových faktur 105 zaměstnancům Úřadu městské části (...) dopisy s uvedením jejich rodných čísel v adresní části dopisních obálek, a to bez jejich souhlasu, § 13c odst. 1 zákona č. 133/2000 Sb. | pokuta 20.000 Kč | ne |
| zpřístupnění mezinárodního zatýkacího rozkazu (...) reportérům České televize, aniž by bylo přijato opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům obviněného a jeho rodičů, v něm uvedených, a k jejich zveřejnění v pořadu České televize Reportéři ČT, § 13 odst. 1 | pokuta 20.000 Kč | ne |
| zpřístupnění usnesení, kterým bylo zahájeno trestní stíhání, obsahující osobní údaje v rozsahu jméno, příjmení, datum narození, místo narození a adresa trvalého pobytu, (...) České televizi, aniž by přijala opatření, aby nemohlo dojít k neoprávněnému přístupu k osobním údajům, v něm uvedených, a k jejich zveřejnění ve zpravodajských pořadech České televize, § 13 odst. 1 | pokuta 15.000 Kč | ne |
| pořizování fotokopií průkazů totožnosti 202 návštěvníků hostů ubytovaných v hotelu (...) od roku 2000 do 1. června 2005, tj. zpracování osobních údajů návštěvníků hostů bez jejich souhlasu, a to v rozsahu nikoliv nezbytném pro naplnění stanoveného účelu a jejich následné uchovávání po dobu delší než nezbytnou k účelu jejich zpracování, § 5 odst. 1 písm. d) a e), § 5 odst. 2 | pokuta 100.000 Kč | ano |
| zveřejnění, mimo osobní údaje autora článku, v rozsahu akademické tituly, jméno, příjmení a název zaměstnavatele, také adresy jeho trvalého pobytu, a to bez jeho souhlasu, v časopise (...) a prostřednictvím internetových domén (...), § 5 odst. 1 písm. f) | pokuta 3.000 Kč | ne |
| zveřejnění osobních údajů 28 osob v rozsahu jméno, příjmení, datum narození, ulice a č.p. trvalého pobytu v regionálním periodiku (...) v rubrice „Věková výročí", a to aniž by zveřejnění adresy subjektů údajů bylo pro dosažení stanoveného účelu nezbytné, § 5 odst. 1 písm. d) | pokuta 7.000 Kč | ne |
| zpřístupnění protokolu o výsledku kontroly v (...) v deníku (...), a to včetně všech osobních údajů zaměstnanců (...), které byly v předmětném protokole uvedeny, § 5 odst. 1 písm. f) | pokuta 20.000 Kč | ne |
| zasílání nevyžádaných obchodních sdělení bez prokazatelného souhlasu adresáta § 7 odst. 2 zákona č. 480/2004 Sb. | pokuta 10.000 Kč | ne |
| zasílání nevyžádaných obchodních sdělení bez prokazatelného souhlasu adresáta § 7 odst. 2 zákona č. 480/2004 Sb. | pokuta 10.000 Kč | ne |

úřad pro ochranu osobních údajů

# Zahraniční aktivity Úřadu

## Twinningový projekt s cílem pomoci Bosně a Hercegovině harmonizovat zákon o ochraně osobních údajů s evropským právem startuje

V minulém čísle Bulletinu jsme vás informovali o výběrovém řízení na udělení twinningového projektu nazvaném „Podpora Komisi ochrany dat Bosny a Hercegoviny", kterého se český Úřad pro ochranu osobních údajů ve spolupráci s partnerským španělským úřadem Agencia Española de Protección de Datos, zúčastnil.

Úřad byl úspěšný a 15. listopadu 2005 předseda Úřadu podepsal smlouvu, která byla 3. listopadu 2005 signována v Sarajevu Michaelem Humphreysem, vedoucím delegace Evropské komise v Sarajevu, a Petarem Kovačevičem, předsedou Komise pro ochranu informací Bosny a Hercegoviny (dále jen BaH). Oficiálně tak byl zahájen projekt BA 04-IB-OT-01 financovaný z prostředků EU vypsaný v rámci programu CARDS. Tento program je obdobou programu PHARE a je zaměřen na podporu států západního Balkánu. Jeho obsahem jsou určité dílčí kroky směřující k dosažení úrovně ochrany osobních údajů v BaH odpovídající podmínkám EU a tedy směřované ve svém důsledku na budoucí členství BaH v Evropské unii.

Vlastní aktivity byly zahájeny dnem 1. 2. 2006, kdy vyslaný pracovník ÚOOÚ odjel na dlouhodobou misi do Sarajeva, aby zahájil realizaci projektu, jehož ukončení se předpokládá k 31.3.2007. V průběhu této doby se jednotlivých akcí v rámci projektu zúčastní řada expertů jak z ÚOOÚ, tak ze španělského úřadu.

Projekt bude realizován v samém úvodu druhé dekády po uzavření Daytonské dohody, jíž byla ***de facto*** učiněna tečka za válkou v BaH. Věříme, že právě zahajovaný projekt bude dobrou podporou úspěšné ouvertuře nové a lepší éry BaH. Všem zúčastněným přejeme tvůrčí a přátelskou atmosféru a úspěšné splnění mise.

## Mezinárodní konference v Montreux

Ve dnech 14. – 16. září 2005 se v Montreux, ve Švýcarsku, konala v pořadí již „27. Mezinárodní konference pro ochranu dat a soukromí". Jednání se zúčastnilo 40 předsedů akreditovaných orgánů ochrany osobních údajů („komisařů") v doprovodu dalších řídících pracovníků. Celkem 300 delegátů z celého světa přijelo na letošní setkání, jehož nosným tématem byla „Ochrana osobních údajů a soukromí v globalizovaném světě: Univerzální právo respektující odlišnosti." Hlavní téma konference, tj. hledání odpovědi na otázku, jak zajistit v globálním měřítku aplikaci společných principů ochrany osobních údajů a soukromí při současném respektování právních, společenských, kulturních, atd. odlišností bylo nejen zajímavé, ale i velice aktuální.

Setkání v Montreux mělo navíc i mimořádně přínosný odborný doprovodný program – přednášejícími byli přední odborníci na danou problematiku, včetně universitních profesorů, zástupců mezinárodních organizací i ochránců dat ze soukromého sektoru.

Z hlediska ČR měla letošní akce zvláštní význam i vzhledem k tomu, že byla první příležitostí nového předsedy Úřadu RNDr. Igora Němce osobně se setkat s vedoucími představiteli zahraničních partnerských dozorových orgánů.

Postupující globalizace a prudký rozvoj informačních technologií způsobují, že ochrana osobních údajů a soukromí se celosvětově stává ohniskem zájmu. Současná geopolitická situace, zejména válka s terorismem, problémy spojené s využíváním internetu, rozvoj invazivních technologií, vznik biobank, to vše a mnohé další „výdobytky naší civilizace a pokroku", přinášejí s sebou vzrůstající potřebu soustředit pozornost na otázku základních práv a svobod – především na právo na soukromí.

Na konferenci byly přijaty dvě rezoluce:

1. Rezoluce o používání osobních údajů pro politickou komunikaci
2. Rezoluce o použití biometrických prvků v pasech, průkazech totožnosti a cestovních dokladech.

Komisaři pro ochranu dat a soukromí se dohodli, že budou prosazovat uznání všeobecného charakteru zásad ochrany dat a přijali závěrečnou deklaraci, ve které vytyčili hlavní cíle svého úsilí.

V preambuli uvádí deklarace např. přehled hlavních zásad, kterými by se ochrana osobních údajů měla řídit. V hlavním textu mj. vyzývá OSN, aby vypracovala právně závazný a vymahatelný nástroj stanovící jasně a podrobně práva na ochranu údajů a soukromí a adresuje i celou řadu dalších výzev a doporučení vládám světa, Radě Evropy, Světovému summitu o informační společnosti (WSIS) v Tunisu, mezinárodním, nadnárodním a nevládním organizacím a výrobcům technologií na podporu ochrany soukromí.

Plnění stanovených úkolů a cílů zhodnotí ochránci soukromí opět za rok na následující 28. Mezinárodní konferenci, kdy místem setkání budou Atény.

*Poznámka:*
*Plné znění textů deklarace i obou rezolucí je k dispozici ve Věstníku Úřadu v částce 39*
*nebo na webové stránce Úřadu www.uoou.cz/index.php?l=cz&m=left&mid=08&u1=&u2=&t=.*
*Materiály z konferenčních přednášek jsou k dispozici na webové stránce www.privacyconference2005.org.*

### Účast delegátů Úřadu na mezinárodním pracovním setkání v Paříži

Ve dnech 17.– 18. listopadu 2005 proběhl v Paříži „XII. Case handling workshop" jako další z pravidelných setkání zástupců institucí, které mají v jednotlivých evropských zemích na starosti ochranu osobních údajů. Jednání se zúčastnili zástupci většiny evropských zemí a také EDPS (Evropský inspektor ochrany osobních údajů).

Konferenci zahájil president francouzského úřadu CNIL Alex Türk, který je současně také senátorem francouzského Parlamentu. Po dopoledním plenárním zasedání, kde byl detailně představen hostitelský úřad CNIL a také práce EDPS, v rámci Evropské unie, bylo odpolední jednání rozděleno do dvou paralelních sekcí, ve kterých probíhala odborná část konference. V první sekci se vyměňovaly zkušenosti z trestání jednotlivých kauz a druhý den se projednávaly informace o praxi ochrany osobních údajů v bankovním sektoru. Druhá sekce se věnovala především výměně zkušeností o ochraně zdravotních údajů. Jednalo se například o stavu příprav elektronické zdravotní dokumentace v jednotlivých státech, probírala se rizika takového systému a jednotlivé státy představovaly svá řešení z hlediska ochrany osobních údajů. Druhý den se tato sekce zaměřila především na informace o řešení problémů s internetovým přenosem dat a diskriminaci v zaměstnání.

Závěrečná část workshopu proběhla opět společně a nosným tématem byl způsob komunikace jednotlivých úřadů s médii a veřejností obecně.

Příští setkání se koná v březnu 2006 v Madridu.

## 2. NEMĚLO BY VÁM UNIKNOUT

### Infolinky v bankách – dotaz na RPSN

Každý z nás, v různé míře a objemu, využívá bankovní služby. České banky se stále ještě většinou nechovají k těm, kterým prokazují své služby, jako k zákazníkům – tj. vstřícně, informativně, zodpovědně a citlivě. Jako příklad uveďme informace o poskytování půjček. V případě, že máme zájem půjčit si od banky peníze, nás samozřejmě zajímá, kolik nás půjčka bude celkem stát. Hodnotu těchto peněz nejlépe vyjadřuje RPSN – roční procentuální sazba nákladů – údaj, který přesně vystihuje, kolik peněz za půjčku každý rok zaplatíme, a to včetně všech poplatků. Vypočítat RPSN nepředstavuje nijak složitý matematický úkon a v zahraničí jej banky poskytují běžně. Jak se vypočítá? K výpočtu je potřeba znát výši splátky, délku splácení a poplatky banky. V poslední době však přichází na Úřad

stále větší počet písemných i telefonických stížnosti a dotazů na postup některých bank při poskytování telefonických informací o RPSN.

Na co si občané stěžují: Postup bank při poskytování informací není jednotný, informace od různých pracovníků jedné banky se značně rozcházejí a banky často žádají před poskytnutím telefonických informací nadbytečné údaje. Někdy jsou otázky kladené operátorem na infolince banky až zarážející! Proč banka potřebuje pro telefonickou odpověď na dotaz o možnostech půjčky, jejich výhodách či nevýhodách od volajícího znát druh bydlení, rodné číslo, adresu, počet dětí, dobu v současném a předchozím zaměstnání a podobně? Mnohé z těchto dotazovaných údajů jsou nadbytečné, zejména rodné číslo. Podle § 5 odst. 1 písm. d) zákona o ochraně osobních údajů je správce povinen shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu. Rodné číslo v tomto případě banka požadovat nemůže. Mohla by vyžadovat datum narození, neboť věk může ovlivnit výši úvěru. Nadbytečné jsou i místo narození, ulice, PSČ, obec, okres, pevná linka a telefon do zaměstnání.

Zájmem Úřadu je, aby banky v rámci svých služeb nakládaly s našimi osobními údaji v souladu se zákonem o ochraně osobních údajů. Přístup bank k zákazníkům by tedy měl být nejen profesní, ale i férový. Telefonicky by se občan měl dozvědět vše, co potřebuje znát ve věci možného čerpání půjčky, aniž by musel udávat zbytečně mnoho osobních údajů. Také je dobře vědět, že osobní údaje volajícího na infolinku banky, který ještě nechce uzavřít smlouvu o půjčce, ale jen se informuje o možnostech půjčky a o RPSN, nesmějí být dále zpracovávány ani ukládány. Musejí být okamžitě zlikvidovány. Jen správně informovaný občan se může účinně chránit.

*Poznámka:*
*Více informací je k dispozici ve Věstníku Úřadu pro ochranu osobních údajů v částce 39 a na webových stránkách Úřadu http://www.uoou.cz v rubrice Názory Úřadu.*

## Využívání kamerových sledovacích systémů

Úřad zpracoval zásady využívání kamerových sledovacích systémů s ohledem na požadavky ukládané zákonem o ochraně osobních údajů. Vzhledem k tomu, že v České republice neexistuje zvláštní právní úprava, která by regulovala využívání kamerových sledovacích systémů, Úřad se v rámci svých kompetencí ujal úkolu nastavit pravidla zaručující ochranu soukromí osob, která by vyvažovala účinné využívání technických prostředků k zajištění bezpečnosti občanů a ochrany majetku. Pravidla předložil k připomínkám veřejnosti na svých webových stránkách. Tímto postupem Úřad splnil příslib předsedy Úřadu, který vyslovil po svém zvolení i na první tiskové konferenci po uvedení do funkce: Úřad bude usilovat o nastavení pravidel ochrany soukromí rovněž v diskusi s veřejností.

## Zásady provozování kamerového systému z hlediska zákona o ochraně osobních údajů

1. **Provozování kamerového systému je považováno za zpracování osobních údajů, pokud je** vedle kamerového sledování **prováděn záznam pořizovaných záběrů**, nebo jsou v záznamovém zařízení uchovávány informace a zároveň účelem pořizovaných záznamů, případně vybraných informací, je jejich využití k identifikaci fyzických osob v souvislosti s určitým jednáním. Samotné kamerové sledování fyzických osob není zpracováním osobních údajů podle zákona č. 101/2000 Sb., protože postrádá úroveň podmínek pro zpracování údajů ve smyslu § 4 písm. e) zákona č. 101/2000 Sb. To však nevylučuje aplikaci jiných právních předpisů, zejména ustanovení občanského zákoníku upravujícího podmínky ochrany osobnosti.

2. **Údaje uchovávané v záznamovém zařízení, ať obrazové či zvukové, jsou osobními údaji za předpokladu, že na základě těchto záznamů lze přímo či nepřímo identifikovat kon-**

**krétní fyzickou osobu (tedy: Informace z obrazových či zvukových nahrávek umožňují, byť nepřímo, identifikaci osoby).** Fyzická osoba je identifikovatelná, pokud ze snímku, na němž je zachycena, jsou patrné její charakteristické rozpoznávací znaky (zejména obličej) a na základě propojení rozpoznávacích znaků s dalšími disponibilními údaji je možná plná identifikace osoby. Osobní údaj pak ve svém souhrnu tvoří ty identifikátory, které umožňují příslušnou osobu spojit s určitým na snímku zachyceným jednáním.

**3.** Zpracování osobních údajů provozováním kamerového systému je přípustné:

a. V rámci **plnění úkolů uložených zákonem** (např. Policii České republiky); v těchto případech je třeba dbát ustanovení příslušného zákona,

b. dále je toto možné na základě řádného **souhlasu subjektu údajů**; to však je prakticky realizovatelné ve velmi omezených případech, kdy je možné jednoznačně vymezit okruh osob nacházejících se v dosahu kamery,

c. užití kamerového systému však je možné i bez souhlasu subjektu údajů s **využitím ustanovení § 5 odst. 2 písm. e) zákona č. 101/2000 Sb.**; přitom je však nutno respektovat podmínky uvedené sub 4.

**4.** Povinnosti správce při provozování kamerového systému vybaveného záznamovým zařízením:

a. **Kamerové sledování nesmí nadměrně zasahovat do soukromí.** Kamerový systém je možno použít zásadně v případě, kdy sledovaného účelu nelze účinně dosáhnout jinou cestou (např. majetek je možno chránit před odcizením uzamčením místnosti). Dále je vyloučeno užití kamerového systému v prostorách určených k ryze soukromým úkonům (toalety, sprchy). Je ovšem možné řešení, kdy subjekt údajů má na výběr z alternativ (např. lze monitorovat prostory šatny plaveckého stadionu za předpokladu, že je vymezen prostor pro převlékání, který není kamerami sledován).

b. **Specifikace sledovaného účelu.** Je třeba předem jednoznačně stanovit účel pořizování záznamů, který musí korespondovat s důležitými, právem chráněnými, zájmy správce (např. ochranou majetku před krádeží). Záznamy tak mohou být využity pouze v souvislosti se zjištěním události, která poškozuje tyto důležité, právem chráněné zájmy správce. Přípustnost využití záznamů pro jiný účel musí být omezena na významný veřejný zájem, např. boj proti pouliční kriminalitě.

c. Je třeba stanovit **lhůtu pro uchovávání** záznamů. Doba uchovávání dat by neměla přesáhnout časový limit maximálně přípustný pro naplnění účelu provozování kamerového systému. Uchovávaná data by měla být uchovávána v rámci časové smyčky např. 24 hodin, pokud jde o trvale střežený objekt, nebo případně i dobu delší, v zásadě ne však přesahující několik dnů, nejde-li o pořizování záznamů policejním orgánem podle zvláštního zákona, a po uplynutí této doby vymazána. Pouze v případě existujícího bezpečnostního incidentu by měla být data zpřístupněna orgánům činným v trestním řízení, soudu nebo jinému oprávněnému subjektu.

d. Je třeba řádně zajistit **ochranu** snímacích zařízení, přenosových cest a datových nosičů, na nichž jsou uloženy **záznamy**, před neoprávněným nebo nahodilým přístupem, změnou, zničením či ztrátou nebo jiným neoprávněným zpracováním, viz § 13 zákona č. 101/2000 Sb.

e. **Subjekt údajů** musí být o užití kamerového systému vhodným způsobem **informován** (např. nápisem umístěným v monitorované místnosti), viz § 11 odst. 5 zákona č. 101/2000 Sb., nejde-li o uplatnění zvláštních práv a povinností vyplývajících ze zvláštního zákona.

f. Je třeba garantovat další práva subjektu údajů, zejména právo na přístup k zpracovávaným datům a právo na námitku proti jejich zpracování, viz § 1 zákona č. 101/2000 Sb.

g. **Zpracování osobních údajů je třeba registrovat** u Úřadu pro ochranu osobních údajů, nejde-li o uplatnění zvláštního práva či povinností vyplývajících ze zvláštního zákona, viz § 18 odst. 1 písm. b) zákona č. 101/2000 Sb.

*Poznámka:*
*Zásady využívání kamerových sledovacích systémů zpracoval Úřad s ohledem na požadavky uložené zákonem o ochraně osobních údajů ve Stanovisku č. 1/2006. Toto stanovisko i doplňující materiály k problematice provozu kamerových systémů jsou publikovány ve Věstníku Úřadu v částce 40 a jsou také k dispozici na webových stránkách Úřadu http://www.uoou.cz/ v rubrikách Názory Úřadu a Registr.*

# 3. TÉMA: Ohlédnutí za ročním působením zákona č. 480/2004

## Slovo úvodem

Dnem 7. září 2004 nabyl účinnosti zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů. Od tohoto data Úřad pro ochranu osobních údajů vyřizuje v rámci České republiky stížnosti uživatelů sítě internet na nevyžádanou obchodní poštu. Kompetence Úřadu v této problematice spočívá ve výkonu dozoru nad šířením obchodních sdělení prováděných v rámci podnikatelské činnosti. Součástí výkonu dozoru je i prověřování podání neboli podnětů, týkajících se této činnosti, které na Úřad pro ochranu osobních údajů přicházejí.

Úřadu byla svěřena pravomoc udělit pokutu do výše až deset milionů korun těm právnickým osobám, které šířením nevyžádaných obchodních sdělení s využitím elektronických prostředků výše uvedený zákon porušují.

Jestliže Vás obtěžují neustálé nevyžádané e-maily, nebojte se a braňte se – můžete se obrátit na Úřad pro ochranu osobních údajů a podat stížnost.

*Poznámka:*
*Plné znění zákona č. 480/2004, obecnou informaci k zákonu a formulář k podání stížnosti na neoprávněně zaslané obchodní sdělení je k dispozici na internetové adrese Úřadu www.uoou.cz v rubrice Kontrolní činnost Úřadu. V klasické tištěné podobě jsou informace publikovány ve Věstníku Úřadu v částce 35. Úřad pro ochranu osobních údajů zveřejnil rozhovor představitelů úřadu pro časopis Sdělovací technika na téma "Ochrana soukromí v elektronických komunikacích". Rozhovor je k dispozici na webových stránkách Úřadu www.uoou.cz v rubrice Média ve formátu PDF nebo na stránkách serveru Sdělovací technika ve formátu HTML.*

## Dnes vám představujeme:

### Rozhovor s inspektorem Úřadu pro ochranu osobních údajů panem Ing. Milošem Šnytrem

*V čem spočívá poslání Úřadu pro ochranu osobních údajů v problematice nevyžádaných obchodních sdělení a co je klíčovým úkolem vyplývajícím z daných kompetencí?*

Hlavním posláním Úřadu pro ochranu osobních údajů je ochrana soukromí v prostředí elektronických komunikací. Lze říci, že zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, v tomto směru zachází ještě o něco dále než zákon č. 101/2000 o ochraně osobních údajů, neboť zajišťuje jistou míru soukromí nejen fyzickým, nýbrž dokonce i právnickým osobám. Pokud jde o problematiku nevyžádané elektronické pošty, zabývá se Úřad tou její částí, která obsahuje obchodní sdělení. Kompetenčně je zájem Úřadu z pochopitelných důvodů soustředěn na subjekty, působící v České republice.

*Co je vlastně předmětem vaší kontroly?*

Zjednodušeně řečeno je předmětem kontroly zjišťování, zda odesílatel obchodního sdělení, nebo chcete-li komerční nabídky, adresuje své zprávy těm příjemcům, kteří o ně skutečně stojí. To znamená těm, kteří k jejich zasílání dali předem nějakým způsobem souhlas. My pak zjišťujeme nejen existenci takového souhlasu, ale i další náležitosti, které má takové správné obchodní sdělení podle zákona mít.

*V čem vidíte největší problémy ve své práci?*

Proces šetření je velmi zdlouhavý a ačkoliv v mnoha případech stojí za rozeslanými nevyžádanými zprávami jediný viník, je velice obtížné jej vypátrat. Skutečnost, že Úřad nemůže šetřit „ve věci" ale musí jít takříkajíc „po krku" nějaké konkrétní osobě, znesnadňuje a mnohdy skoro až maří naši práci. To, že nemáme právo zjišťovat, kdo byl v danou chvíli (v momentu odeslání zprávy) připojen na internet, kdo je majitelem účtu, ze kterého jsou hrazeny poplatky a podobně, je velký problém a výsledkem je, že úspěch kontroly bývá velmi často nejistý. V našem případě, kdy máme dohledat a najít někoho, kdo utajuje svou identitu, kdo se skrývá, vydává za někoho jiného, je problematické aplikovat stejné zásady a postupy jako při běžné kontrole organizace nebo „slušného" živnostníka. Zjednodušeně řečeno nám chybí více operativních kompetencí, jaké při své práci používá např. policie. Tím nechci říct, že bychom měli mít např. právo odposlouchávat telefony nebo provádět sledování osob, spíše jde o některá oprávnění nahlížet do určitých neveřejných databází nebo požádat telekomunikačního operátora o zpřístupnění provozních a zprostředkovacích dat. Při své práci narážíme na jisté nesrovnalosti a neprůhlednosti živnostenského zákona v této oblasti zejména na neaktuálnost rejstříků, obtížnou prokazatelnost neoprávněného podnikání atp.

Objektivizace závažnosti a množství se uskutečňuje až v průběhu správního řízení, tedy až ve fázi udělení sankce, které následuje – v případě zjištění závady – po kontrole.

*Je Česká republika zapojena do mezinárodní spolupráce?*

Spam je celosvětový problém. V tomto globálním prostoru jsou pro potírání nevyžádaných obchodních sdělení vytvořeny mezinárodní dohody a rozvíjí se koordinace legislativních postupů.

Zákonem č. 480/2004 se do právního řádu České republiky implementují zásady „Směrnice Evropské unie o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací" a „Směrnice o některých právních aspektech služeb informační společnosti, zejména elektronického obchodování". Elektronické komunikace, to je dnes zejména internet a mobilní sítě. Internet je medium, které je organizováno dle jednotlivých navzájem propojených sítí, které nejsou organizovány jako vnitrostátní útvary. Tyto sítě propojují celý svět. Je proto nemyslitelné, aby si jednotlivé státy vystačily pouze s národními zákony. Účelem citovaných Evropských směrnic je především vytvoření právního rámce v prostředí společného trhu EU.

*Probíhají v současné době i nějaké mezinárodní iniciativy?*

V současné době probíhají společné iniciativy, které se paralelně snaží potlačit spam jako takový. První bylo třeba identifikovat, co vlastně spam je, jak jej lze kvantifikovat a měřit. Probíhá rozsáhlá spolupráce státních organizací s provozovateli jednotlivých sítí. Ti mají obrovský zájem na spolupráci, protože spam je velice zatěžuje, musejí zvyšovat přenosové i diskové kapacity svých sítí a v podstatě musejí vynakládat obrovské finanční prostředky na technické zajištění přenosu množství dat, o které nikdo nestojí neboli na zajištění služby, kterou si nikdo neobjednal a přesto musí být provedena.

*Jaký je přínos této spolupráce?*

Každý poskytovatel služeb elektronických komunikací má ve svých obchodních podmínkách klauzuli, že pokud uživatel hrubým způsobem poruší daná pravidla, přestane mu operátor tyto služby poskytovat. Obdobně to funguje i v České republice. Problém ale je, že nová registrace je otázkou několika minut. Dotyčný se může zaregistrovat u jiného provozovatele, přemístit se na jiné místo v republice nebo odejít provozovat svou nekalou činnost do zahraničí. Tak jako v jiných oblastech i zde platí, že ti, kteří zneužívají vymožeností nově vyvinutých technologií, jsou zatím vždy o krůček vepředu před legislativou, kontrolou a následným postihem.

*Co by občan v rámci ochrany svého soukromí měl vědět o NOSu a jak se může proti němu bránit?*

V zásadě je možné doporučit, pokud to jde, nezveřejňovat příliš svou e-mailovou adresu a předávat ji pouze těm partnerům, o kterých jsme si jistí, že ji nezneužijí. Obecně je známo, že po internetu neustále slídí stovky speciálních programů, které takzvaně sklízejí e-mailové adresy z růz-

ných diskusních fór nebo webových stránek. Dále je dobré vědět, že zvláště na zprávy přicházející ze zahraničních serverů je lépe neodpovídat, neboť reakce na e-mail pro odesílatele zpravidla znamená pouze jistotu, že e-mailová adresa je funkční.

***Čtenáři se v tisku v souvislosti se spamem často setkávají s pojmy opt– in a opt– out. Co tyto termíny znamenají?***

V České republice platí „pravidlo „opt– in", což znamená „k čemu se nepřihlásím, to nedostávám". Například v Americe platí opačné pravidlo „opt– out", od čeho se neodhlásím, to dostávám. Pro pružný obchodní styk při zachování ochrany soukromí je možno si představit kombinovaný systém založený na principu opt– in pro soukromé osoby a opt– out ve firemním styku.

***Mohl byste uvést příklady opakujících se zkušeností z kontrol, které mohou uživatelům napomoci vyvarovat se chyb a lépe si poradit s nežádoucími e-maily?***

V praxi existují dvě možnosti jak se vypořádat s nevyžádaným obchodním sdělením. Někdo vám pošle e-mail s dotazem, zda souhlasíte s tím, že od něj budete obchodní nabídky dostávat. Vy buď svým souhlasem potvrdíte že ano, nebo neodpovíte, či odpovíte, že nesouhlasíte a že nemáte zájem. Situace je jasná a v případě, že od tohoto rozesílatele obdržíte v budoucnu obchodní nabídku, lze na tuto zprávu nahlížet jako na nevyžádané obchodní sdělení.

***A druhá možnost?***

Zvláště nově vznikající firmy potřebují nové zákazníky a činí tak někdy na hraně zákona. Nejedná se sice o agresivní chování „lovců adres", nicméně i tito rozesílatelé zpráv obcházejí zákony ve snaze co nejrychleji vytvořit databázi zákazníků a vytvořit pro sebe výhodný konkurenční prostor. Často jsou například uživatelé e-mailové pošty při otevření nabídky oslovováni způsobem, který na první pohled vypadá jako reakce na již probíhající komunikaci. Cílem je vytvořit dojem, že právě došlá zpráva je pokračováním předešlé komunikace, při které již došlo k dohodě atd.

***Ve společnostech a firmách, kde je více zaměstnanců, dochází mnohdy k tomu, že jeden dá souhlas se zasláním nabídky a jiný takto obdrženou zprávu označí jako nevyžádanou a stěžuje si u nás.***

Problém může také vzniknout v situaci, kdy uživatel internetu má několik e-mailových účtů, které užívá pro příjem a odesílá pouze z jedné z nich. Rozesílatel obchodního sdělení si nemůže v takovém případě „odškrtnout" ve své databázi, zda zákazník souhlasí se zasíláním obchodních sdělení či nesouhlasí, protože odpověď dostal z úplně jiné adresy.

Jiný příklad může posloužit jako ukázka, jak z naprosto jednoduché a obyčejné situace může vzniknout i závažnější problém a následně i kontrola na základě podnětu na nevyžádané obchodní sdělení: Na služebních cestách, návštěvách konferencí, kongresů či při jiných obchodních a společenských akcích si účastníci domluví zasílání obchodních nabídek, katalogů atd. Po návratu do zaměstnání velice často zapomenou o této skutečnosti informovat svého zaměstnavatele, nebo si ani nejsou vědomi, že by tak měli učinit. Při pozdějším obdržení takových zpráv, zaslání katalogů nebo nabídek může dojít k situaci, že se s nimi nakládá jako s nevyžádaným obchodním sdělením.

***Jak Úřad nahlíží na tak zvané „patičky"?***

Patička je obchodní sdělení, které se však od ostatních liší především tím, že nemá všechny náležitosti tohoto druhu komunikace. Hlavně však postrádá tzv. vlastní nosič, čili není zasílána jako samostatná zpráva. Jde spíše o jakýsi druh reklamy. Nicméně v otázce patiček Úřad doporučuje pečlivě se seznámit s obchodními podmínkami, na které uživatel služby přistupuje. Jedná se vlastně o jakousi daň za využívání bezplatné služby. Operátor si poskytování této služby kompenzuje tím, že svých technických prostředků využívá jako nosiče reklamních sdělení. Pravidlo tedy je – než podepíšu smlouvu, tak si ji pečlivě přečtu. V případě, že nejsem spokojen, vypovím smlouvu, najdu si jiného provozovatele, kde za všechny služby zaplatím a tím také platím garanci, že nebudu tento typ reklamy dostávat.

***Setkal jste se v poslední době při své práci s nějakou zajímavostí?***

Možná zajímavostí, možná námětem jak prakticky a pružně navazovat na „živá" obchodní jednání. Při otázce týkající se mezinárodní spolupráce jsem zmínil dobrou, přátelskou spolupráci se špa-

nělskými kolegy. Při posledním pracovním setkání jsme, mimo jiné, hovořili o vizitkách. Shodli jsme se na faktu, že předání vizitky neznamená souhlas se zasíláním obchodních sdělení. Španělé situaci vyřešili velmi dobře. Doporučují umístit na zadní stranu vizitek razítko, z jehož stručného textu jednoznačně vyplývá, že ten, kdo tuto zadní část vizitky podepíše, vyslovuje souhlas se zasíláním obchodních nabídek. Tento způsob vyžádání si souhlasu je jednoduchý, jednoznačný a přitom elegantní.

*Děkujeme za rozhovor.*

## Udělení prvních pokut za spam

Postih rozesílání nevyžádaných obchodních sdělení prostřednictvím elektronické pošty je poměrně mladá oblast působení „zákona". Jedná se o novou problematiku, kterou se ze zákona již rok zabývá Úřad pro ochranu osobních údajů. Za období od září 2004 do konce října 2005 evidoval Úřad celkem 1 165 stížností. Z tohoto počtu bylo 52 stížností odeslaných ze zahraničí, 104 stížností uznal Úřad jako neoprávněné a 1 009 řešil jako oprávněné stížnosti. Smyslem „antispamového zákona", jak je nesprávně zákon č. 480/2004 označován, je nastolení jasných pravidel a mantinelů v oblasti elektronického marketingu.

Cílem práce inspektorů Úřadu je odhalit ty, kteří zákon porušují. Uložení prvních trestů za spam si vyžádalo určitou dobu. Úřad tím, že využil své pravomoci udělit pokuty, dal jasně najevo, že otázku porušování ustanovení zákona pro využívání elektronické pošty pro marketingové účely bere vážně a že podceňování dozorové úlohy Úřadu se nevyplácí. Období od 7. září 2004, kdy zákon nabyl účinnosti, až do konce roku 2004 Úřad ponechal podnikatelům jako časový prostor k zažití a uvědomění si litery zákona. První udělené finanční sankce mají být výrazným signálem pro všechny, kteří využívají internet k rozesílání obchodních sdělení zákazníkům, aby si uvědomili své povinnosti vyplývající pro ně ze zákona č. 480/2004.

Nejvyšší pokuta ve výši 160 000 korun byla uložena za zasílání obchodních sdělení, která obsahovala nabídku na zařazení adresáta do databáze podnikatelů, a to bez prokazatelného souhlasu příjemců se zasíláním. Další firmy obdržely pokuty od pěti do dvaceti tisíc korun.

Výčet nemá být chválou sankcí. Úřad v žádném případě nechápe udělování sankcí jako prioritu své kompetence v postihu nevyžádaných obchodních sdělení. Důraz se snaží klást na vymáhání respektu k zákonu a na korektní jednání správců osobních údajů.

## Dodržování zásad internetové etiky – podmínka při elektronické komunikaci

Podmínky zasílání informací marketingového charakteru elektronickými prostředky jsou zákonem nově upraveny. Pod pojmem šíření nevyžádaných obchodních sdělení si lze představit rozesílání všech možných forem sdělení určených k přímé či nepřímé podpoře zboží nebo služeb konkrétního podniku. Nevyžádaným obchodním sdělením však není například elektronická korespondence na podporu nadační nebo charitativní činnosti, přímá neobchodní nebo neprofesní komunikace mezi uživateli e-mailů. Za obchodní sdělení nelze také považovat uvedení pouhé e-mailové či webové adresy jako kontaktního údaje.

Je možné odeslat elektronickou cestou obchodní nabídku a neporušit ustanovení zákona? Odpověď zní ano, pokud se dodržují pravidla. Základní pravidlo zní – nejdříve odeslat žádost o souhlas se zasíláním obchodních nabídek v budoucnu, a to bez udání konkrétní služby, nabídky a ceny. Jsou však i jiné možnosti, jak se zviditelnit v nepřehledné a přehuštěné podnikatelské sféře a vybojovat si své místo na konkurenčním kolbišti. V každém případě je však třeba respektovat zásady internetové etiky a slušnosti. Dobrým řešením může být například prezentace vlastní webové stránky na internetu. Tento způsob prezentace bude pravděpodobně pří-

jemnější i pro uživatele internetu, kterým chce Úřad pomoci a jejichž zájmy v tomto smyslu má na zřeteli.

Cílem Úřadu je, kromě jiného, vytvořit v síti internet čisté a bezpečné prostředí pro elektronické obchodování a ochránit občany před záplavou spamů při každodenním spuštění počítače.

### K věci: Jak vyzrát na nechtěné e-maily?

Ze spolupráce holandského ministerstva pro ekonomiku a Organizace pro ekonomickou spolupráci a rozvoj (OECD) vznikla přínosná edukativní pomůcka v boji proti spamu. Jde o leták, který přehledně, názorně a jednoduše vysvětluje obsah tohoto pojmu, zařazuje do spektra „internetového úskalí" a vysvětluje podstatu jeho fungování. Většina z nás dennodenně tráví u svého počítače kratší či delší dobu při velice neproduktivní, fádní a zbytečné činnosti – tj. čistí počítač od nechtěných e-mailů.

Všem uživatelům internetu spam vadí – bere si náš čas, peníze a odčerpává naši energii. Úřad využívá nabídku OECD publikovat leták jako pomůcku všem, kteří vědí, že s vyšší informovaností problém spamu lépe zvládnou. K dispozici je na webové stránce Úřadu www.uoou.cz/index.php?l=cz&m=left&mid=08&u1=&u2=&t= v rubrice zahraničí / OECD.

*Poznámka:*
*Více informací o spamu lze získat například na internetových adresách: http://www.oecd.org/sti/spam, http://www.itu.int/osg/spu/spam/background.html.*

## 4. CO NOVÉHO V ZAHRANIČÍ

### 1. Velká Británie – požadavek zákazu označovat a sledovat zaměstnance na pracovištích

Odbory ve Velké Británii důrazně požadují zákaz využívání technologií RFID a GPS k označování a sledování zaměstnanců na pracovištích. Vedení britských odborů předalo Evropské komisi zprávu, ve které upozorňuje na skutečnost, že tímto jednáním dochází k zásadnímu narušení soukromí zaměstnanců. Odbory současně požadují legislativní úpravu, která by takové jednání zakazovala.

*Poznámka: RFID – Radio Frequency Identification, bezdrátová radiofrekvenční identifikace – je technologie bezdotykové identifikace a přenosu dat. Začíná se prosazovat především v logistice, kde časem zřejmě zcela nahradí čárové kódy. Mezi její slabé stránky patří mimo jiné bezpečnost a ochrana dat. Globální satelitní navigační systém, zkráceně GPS (Global Positioning System), je soustava orbitálních družic, za účelem přesného zjištění zeměpisné polohy kdekoliv na Zemi. Určení polohy pomocí GPS je využíváno řadou technických odvětví, např. v geodézii a logistice.*

### 2. Holandsko – soudní rozhodnutí ve prospěch provozovatelů sítě internet

Soud v holandském Utrechtu rozhodl 12. července 2005, že provozovatelé služeb sítě internet (ISP) nemusejí sestavovat a předávat seznamy se jmény či adresami svých uživatelů, kteří si ze sítě internet ilegálně kopírují filmy, hudební nahrávky nebo jiné autorskými právy chráněné soubory. Holandská organizace Brein reprezentující 52 mediálních a zábavních společností, požadovala od největších provozovatelů sítě internet, aby pořizovali a předávali specifická identifikační čísla, tzv. IP adresy, těch uživatelů počítačů, kteří načerno kopírují soubory ze sítě internet. Provozovatelé služeb sítě internet, kteří byli o tuto službu požádáni – UPC, Essent, Tiscali, Wanadoo a KPN – odmítli záznamy o svých zákaznících předávat s tím, že pouze soud má právo obrátit se na ně s takovým požadavkem. Právní zástupce ISP prohlásil, že rozhodnutí soudu představuje významný krok v ochraně soukromí uživatelů sítě internet a dodal: „Nesmí dojít k situaci, kdy by si soukromé organizace mohly dovolit „slídit" kolem počítačů občanů a shromažďovat jakákoliv jejich data".

*Poznámka:*
*IP adresa (Internet Protocol Address) je číslo, které jednoznačně určuje váš počítač v síti internet.*

### 3. Holandsko – internetová společnost musí odhalit identitu svého klienta

Holandský Nejvyšší soud nařídil internetové společnosti Lycos odhalit identitu svého klienta. Tímto rozhodnutím je umožněno ochráncům autorských práv pronásledovat ilegální „stahovatele" on-line hudby a filmů ze sítě internet. Jde o první rozhodnutí svého druhu v Holandsku.

### 4. Japonsko – první výsledky zavedení zákona o ochraně osobních údajů

Poté, co zákon o ochraně osobních údajů vstoupil v dubnu letošního roku v Japonsku v platnost, mnohé organizace začaly preventivně věnovat více pozornosti možnému úniku důvěrných informací. Například firma Toyota Motor Corp. povoluje svým zaměstnancům používat při práci pouze firemní počítače. Zakázala jim používat jejich vlastní počítače k možnému napojení na místní síť. Jiné společnosti například zakazují svým zaměstnancům vynášet mimo pracoviště jakékoliv údaje týkající se jejich zaměstnání. V případě nezbytnosti jsou povinni požádat o povolení vedoucího oddělení, který zabezpečuje ochranu osobních dat zákazníků. Samozřejmě že dochází k případům, kdy zaměstnanci pod tlakem dodržení stanovených termínů tato nařízení porušují. Z těchto důvodů je možná lepší způsob, který zvolila firma Hitachi Ltd., která povoluje svým zaměstnancům užívat vlastní počítače v případě, že mají nainstalován antivirový a ochranný software, který provozuje a zabezpečuje firma a také software, který umožňuje pouze vstup do sítě LAN (Local Area Network), kterou společnost užívá.

### 5. USA – uživatelé sítě internet podceňují možnost zneužití osobních údajů

Centrum pro veřejnou politiku na Universitě v Pennsylvanii uskutečnilo letos v březnu průzkum 1 500 uživatelů sítě internet v USA. Cílem bylo zjistit, co občané vědí o nakupování prostřednictvím sítě internet a zda mají povědomí o možném zneužití osobních údajů zákazníků při tomto způsobu nákupů. Výsledek průzkumu, který byl podkladem studie nazvané „Open to Exploitation: American Shoppers Online and Offline," byl alarmující. Ukázal na velice neuspokojivý až nebezpečný jev – uživatelé internetu se téměř nezajímají o to, které z jejich osobních údajů majitelé webových stránek shromažďují a jak s nimi dále nakládají a nemají představu o možném zneužití svých osobních údajů. Například 75 % z dotazovaných se mylně domnívá, že jestliže nabízená webová stránka má své vlastní prohlášení o ochraně osobních údajů a soukromí, tak se osobní údaje zákazníků využívajících nabídku webové stránky nemohou dostat do rukou třetí straně. Jiný příklad – 49 % dotazovaných nevědělo, co znamená výraz „phishing", a ani nemělo představu o jiných možných podvodných e-mailech kolujících v prostředí internetu. Zpracovatelé studie vytvořené na základě tohoto průzkumu navrhují především rozšířit edukativní osvětovou činnost vůči zákazníkům, kteří využívají možnosti internetového nakupování s cílem rozšířit jejich znalosti v oblasti ochrany soukromí. Současně ale také navrhují, aby majitelé obchodních řetězců zveřejňovali, které osobní údaje zákazníků shromažďují, za jakým účelem a jak dlouho je uchovávají.

*Poznámka:*
*Phishingem lze nazvat podvodné e-maily, kdy na velké množství e-mailových adres jsou rozesílány podvodné dopisy, které ovšem na první pohled vypadají velice věrohodně. Uživatelům je rozeslán například e-mail, že vyhráli vysokou cenu v mezinárodní loterii, nebo prosba o pomoc při převodu obrovské částky peněz s nabídkou provize. Naivním příjemcům těchto zpráv, kteří se nechají nachytat, jsou pak předkládány falešné doklady i podvodné odkazy na finanční instituce. Více informací je k dispozici v Bulletinu Úřadu 2/2005.*

### 6. USA – nová aktivita s cílem snížit počet případů krádeží identity

ITAC – The Identity Theft Assistance Center – Centrum pomoci v případě krádeže a Federal Trade Commission (americký vládní úřad na dodržovní tržních pravidel) se domluvily na spolupráci při předávání informací týkajících se pachatelů krádeží identit. Cílem je snížit počet případů krádeží identity. ITAC je centrum fungující pod záštitou bank a nabízí pomoc všem obětem krádeže identity.

Pracovníci centra napomáhají takto postiženým spoluobčanům nejen překonat psychické problémy spojené se ztrátou soukromí, ale jsou jim také nápomocni v procesu obnovy a znovuzřízení jejich nové identity. Informace získávané z centra jsou v FTC ukládány do Consumer Sentinel Database, která slouží jako zdroj informací při vyšetřováních krádeží identit. Do této databáze má přístup více než 1300 státních, federálních i místních institucí zabývajících se ze zákona vyšetřováním krádeží identit, včetně soudních orgánů.

## 7. Geolokalizace zaměstnanců: Hledání hranic

*Tzv. geolokalizační technologie jsou v dnešní době čím dál výkonnější, přičemž jejich pořizovací ceny klesají a jsou stále přístupnější. Při využití těchto technologií v oblasti dopravy a provozu dopravních prostředků různých firem a společností lze vlastně v libovolném okamžiku stanovit geografickou polohu těchto prostředků a určit tak i místo, kde se nachází příslušný řidič.*

Tyto technologie mohou pro řadu organizací představovat naplnění jejich specifických potřeb plynoucích z jejich pracovních aktivit. Může jít například o lepší správu různých, právě potřebných, zásahů do procesu přepravy zboží, ale také o zajištění vyšší bezpečnosti majetku a osob. Geolokalizační zařízení se mohou uplatnit se zřetelem na dohled nad zaměstnanci a na rozbor jejich pracovní činnosti, neboť jsou schopna monitorovat použité cestovní trasy, příslušné časové rozvrhy, a do své paměti dokáží např. ukládat také údaje o cestovní rychlosti.

Instalace geolokalizačních prostředků, které samozřejmě vždy směřují k větší "transparentnosti" sledovaných osob, však vyvolává dvě základní otázky: První otázka zní, kde se nacházejí hranice mezi prací a soukromým životem. Druhou otázkou, kterou je zapotřebí si položit, je problém nastavení úrovně permanentní kontroly, která je ještě v souvislosti s určitým psychickým tlakem, jež je přitom na zaměstnance vyvíjen, přípustná.

Aby bylo možné tyto otázky zodpovědět, rozhodl se francouzský CNIL (Národní výbor pro informace a svobody) zahájit v této věci konzultace a rozhovory s představiteli odborů, úřadů a s představiteli profesní sféry. Cílem těchto konzultací je pak vypracovat kompetentní doporučení, které by stanovilo metodiku a správné postupy, které by měly být v souvislosti s nasazením geolokalizačních technologií ve firmách a v dalších organizacích uplatněny a respektovány.

## 8. Velká Británie – rozhodnutí firem sdílet zákaznické údaje

Některé britské společnosti zabývající se kreditními kartami oznámily, že hodlají sdílet údaje o tom, jak jejich zákazníci, uživatelé kreditních karet, zvládají své dluhy a jak s nimi nakládají. Společnosti Barclaycard, Co-operative Bank, Egg a firma Abbey se domluvily, že se budou vzájemně informovat o výši úvěrového limitu svých zákazníků a také o tom, kolik peněz utrácejí a jak svůj dluh splácejí. Společnosti tímto krokem naplňují doporučení parlamentu, který sdílení dat navrhl v souvislosti s počtem lidí, kteří problém neschopnosti splácet dluhy na svých četných kreditních kartách, vyřešili sebevraždou. Zástupci kreditních společností ujišťují o tom, že shromažďování zákaznických údajů a nakládání s nimi se bude řídit přísnými bezpečnostními zásadami. I přes tato ujištění vyjádřil představitel organizace Liberty, která se zabývá ochranou lidských práv a svobod, své obavy. Upozornil, že existuje mnoho přiměřených způsobů jak nakládat s dluhy zákazníků, ale ochrana soukromí může být „smetena" pouze jednou.

*Příspěvky 1 – 8 jsou volně zpracovány ze zahraničního tisku*
*(Zdroj je k dispozici v knihovně Úřadu.)*

# 5. OSOBNÍ ÚDAJE V ŠIRŠÍCH SOUVISLOSTECH

## Udělení Cen pro Velkého bratra

V České republice byly 28. října v pražském divadle Na zábradlí poprvé uděleny Ceny pro Velkého bratra ***(viz článek „Velký bratr dorazil do České republiky" – Bulletin 2/2005, s. 16).*** Tyto ceny (nebo spíš anticeny) se udělují těm, kteří se nejvíce provinili zneužíváním základních principů ochrany osobních údajů a soukromí. (Zde je ovšem třeba připomenout, že jedna cena je vyhrazena pro ty, kteří se naopak o podporu ochrany osobních údajů a soukromí nějakým způsobem zasloužili.) Hlavním pořadatelem soutěže v ČR je česká nevládní nezisková organizace na ochranu lidských práv Iuridicum remedium, jejím spolupořadatelem je německá partnerská organizace FoeBuD. V současné době se národní soutěže o Ceny pro Velkého bratra každoročně pořádají v 16 zemích světa – v západní i východní Evropě, v USA, Austrálii a v Asii.

Většina uvedených cen se týká kauz, kterým se již Úřad pro ochranu osobních údajů věnoval, a s výběrem „oceněných" subjektů se v podstatě shoduje. Smyslem těchto cen je upozornit veřejnost na chování některých úřadů a dalších organizací, ale také některých jednotlivců. I tato cesta může být určitým základem pro obranu před nejrůznějšími typy slídilů. Dobrou zprávou je i to, že soutěž vyvolala poměrně velký zájem médií.

Ceny se udělovaly v osmi kategoriích. Nominovaní byli představeni v červnu 2005. Vítěze vybírala odborná porota ze 70 nominací navržených občany.

V kategorii ***Největší slídil roku*** zvítězil Magistrát hl. m. Prahy.
Cenu ***Největší komerční slídil*** obdržela společnost Tesco, a.s.

***Předseda Úřadu pro ochranu osobních údajů RNDr. I. Němec u příležitosti udělení této ceny uvedl, že společnost Tesco byla potrestána Úřadem pokutou ve výši 230000 Kč už v roce 2004. Dále informoval, že na základě poznatků z inspektory Úřadu provedených jednotlivých kontrol i na základě zjištění společnosti Iuridicum remedium dospěl k rozhodnutí pojmout obchodní řetězce do plánovaných komplexních kontrol Úřadu. V příštím roce pak výsledky kontroly Úřad předloží veřejnosti jako svou speciální zprávu.***

V kategorii ***Slídil mezi národy*** zvítězila Evropská komise.
Jako ***Nebezpečná nová technologie*** bylo oceněno zavádění biometrických údajů do cestovních pasů, s nímž počítá vládní návrh zákona, kterým se mění některé zákony na úseku cestovních dokladů.
Nejvyššího ocenění v kategorii ***Právní norma Velkého bratra*** se dočkal Národní akční plán boje proti terorismu, který předložil ministr vnitra F. Bublan.
Další kategorií bylo ***Dlouhodobé porušování lidského soukromí***, ve které byla oceněna společnost Czech Credit Bureau (CCB).
Vítězem v kategorii ***Výrok Velkého bratra*** je následující sdělení:
***„Já vedu rozhovory a ať si je každý odposlouchává, jak chce. Když si je člověk jistý, že nic nespáchal, může mu to být jedno."***

Tato slova bývalého policejního prezidenta Jiřího Koláře, byla pronesena v pořadu ČT Události a komentáře dne 23. 10. 2004.

Žádný z „oceněných" v této soutěži si svou cenu osobně nepřevzal.

A nakonec ocenění pro změnu příznivé: V kategorii Pozitivní cena za ochranu soukromí cenu obdržel Phil Ziemmermann, americký autor programu PGP pro šifrování e-mailů. Ovládání programu je natolik jednoduché, že by ho měl zvládnout snad každý uživatel osobního počítače. Autor poskytl navíc tento program veřejnosti zdarma. Blahopřejeme.

## 6. Vy vy vy

*Jdeme cestu života, která je pro mnohé přímkou, pro jiného spirálou, či kruhem. Možná právě druh naší základní životní „komunikace" již sám o sobě určuje jak a s kým jdeme, koho potkáváme, s kým se zastavíme, koho oslovíme, komu se snažíme vyhnout a koho naopak přizveme putovat s námi. Je to naše volba – naše svoboda. V jednom se ale jistě shodneme – všichni toužíme naplňovat své životní cíle bez újmy nejen na těle, ale i na duši.*

*Media jsou oprávněně součástí našeho denního života – rádi čteme noviny, posloucháme rádio a díváme se na televizi. V našich rukou je volba odložit noviny, vypnout knoflík rádia a zhasnout zářící obrazovku televize. V poslední době však media pracují nejméně na dvě stě procent. Ve snaze plnit všechny své úkoly a poslání se předhánějí v úsilí naplnit náš čas a prostor potoky zpráv, řekami soutěží a především – mořem zábavy. Jakoby se jejich hlavním posláním stalo nás buď uděsit nebo ubavit k smrti. Zahlcují nás a vcházejí do našich životů. A mnozí je stále ochotněji vpouštějí do svého soukromí, jakoby tíhu svého soukromí – svého já, své identity – nebyli v současném světě svobod schopni sami unést. Potřebují ze skutečnosti uniknout. Snad i proto nový typ zábavy, který je v televizích nabízen, reality show, nebo výměny manželek, či jiné obdobné kratochvíle mají „zelenou". Touha po zviditelnění, penězích, zábavě, touha uniknout do snadného života plného jídla a pití a nicnedělání. Alespoň na chviličku být hvězdou. Padají zábrany, obecně platné mravní a etické normy přestávají existovat – všechno se může. Vyvolení jedinci ve vilách postupně odhalují o sobě vše. Lehce svlékají nejen své tělo, ale za vyvolenost jsou ochotni předhodit divákům svou osobnost i soukromí své rodiny, svých dětí. Mají na to právo? Kam až sahá moje svoboda? Až tam, kde neohrožuje druhého.*

*Soukromí v reality show přestává existovat, skryté kamery sledují vše. Vulgarita, hrubost a neskutečná hloupost v přímém přenosu. Co bude příště k vidění – porod, boj o život nebo poprava? Je skupina lidí, křečků v kleci, kteří se předvádějí a všem napospas odhalují své já. Proč ne – teď jsem někdo, všichni mě vidí, fandí mi, třeba já budu ten vyvolený i já mohu být celebritou. Jiná skupina lidí je sleduje. Někdo náhodou či proto, aby vůbec věděl o čem se vlastně tolik mluví. Někdo pravidelně a se zájmem. Proč ne – teď jsem důležitý, mám trochu moci, mohu volit toho, kdo mi vyhovuje a v příští „hře" můj hlas třeba bude ještě důležitější.*

*Některá média reality show připravují a realizují, jiná o nich píší, v dalších se o nich diskutuje. Z mediálního prostoru se debaty přesunují do rodin, do zaměstnání i do škol. Z televizních reality show se stal společenský fenomén, který již vlastně nelze zvládnout vypnutím televizní obrazovky. Normální „dospělák" „šou masáž" přežije. Ale co naše děti, které jako houby nasávají vše dobré i špatné. Bezesporu je hodně zodpovědných rodičů, kteří o takových pořadech s dětmi mluví, zaujímají k nim jasný postoj, vysvětlují a hlavně – nabízejí a společně s dětmi prožívají daleko zajímavější a kvalitnější programy. Ale přece jenom. Jaké stopy asi na dětech zanechá povolená a obdivovaná smršť průlomů do lidského soukromí a pošlapávání morálních principů? Jak se bude formovat jejich žebříček hodnot? Nejde o moralizování. Společnost bez závazných a obecně uznávaných morálních pravidel nemůže dobře prospívat. A co křečci? Nebudou chtít doživotně hrát roli křečků, kterých bude přibývat a přibývat.... Jistě podpisem potvrdili svůj souhlas s pravidly a způsoby hry. Ale budou se na všechno dívat stejně i po odchodu z vily do reality každodenního života? Nedolehne na ně časem tíha jistého narušení osobnosti?*

*Přestože mají reality show velkou diváckou sledovanost, představy a očekávání tvůrců pořadu se naštěstí nesplnily. Chvála zdravému rozumu. Važme si svého soukromí a respektujme soukromí druhých, protože*

jednou ztracené soukromí je obtížné získávat zpět.

*mn*

*Poznámka k 20. 1. 2006: Sebevražda v přímém přenosu. Mladý Američan ve věku 21 let, fanoušek on-line her, spáchal v polovině týdne sebevraždu v přímém přenosu. Videozáznam přenášel prostřednictvím webkamery na stránky bulharského diskusního fóra, kde jeho skon sledovalo dalších několik lidí (přepis zprávy z on-line magazínu deníku Právo a portálu Seznam.cz ze dne 19.1. 2006).*

úřad
pro ochranu
osobních
údajů

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
© ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ

DÁNO DO TISKU 6. 4. 2006